Project Proposal for

sovergence

sovergence

Estimate

 # EST-000004

Tony DeGonia
107 Main Street
Richardson, TX 75280

Bill To
Jimbob's Towing and Wrecker Services
404 Mockingbird Lane
Dallas
75201 Texas
United States

Estimate Date :	06.29.17
Expiry Date :	07.31.17
Reference# :	TSC-0123323445-A

#	Item & Description	Qty	Rate	Discount	Amount
1	HPE FlexNetwork 5510 48G PoE+ 4SFP+ HI 1-slot Switch SKU : JH148A	130.00 1	6,359.99	15.00%	702,778.89
2	SFP+ 10GB Fiber Optic Module for JH148A	260.00	599.00	15.00%	132,379.00
3	Second Power Supply for JH148A Switch	130.00	299.00	15.00%	33,039.50
4	HPE ProLiant DL360 Gen9 E5-2650v4 2P 32GB-R P440ar 8SFF 800W RPS Perf SAS Server	6.00	5,369.99	15.00%	27,386.95
5	HPE 3TB SAS 12G Midline 7.2K LFF (3.5in) SC 1yr Wty HDD	24.00	537.99	15.00%	10,975.00
6	Microsoft Server 2016 Datacenter Edition - 5 user CALs	8.00	3,099.00	10.00%	22,312.80
7	Microsoft Server 2016 User CALs	2,500.00	99.99	20.00%	199,980.00
8	10G Fiber Jumpers	100.00	24.99	0.00	2,499.00
9	Fiber Optic Patch Panel 24 Port 10G compatible	6.00	499.00	0.00	2,994.00
10	19inch 42U Computing Racks for Datacenter	14.00	999.00	10.00%	12,587.40
11	Category 6 cabling for all 6 locations	6,000.00	129.99	15.00%	662,949.00
12	WatchGuard Firebox M5600 with 3-yr Total Security Suite - WG561643	1.00	97,625.00	20.00%	78,100.00
13	High Availability - WatchGuard Firebox M5600 and 3-yr Standard Support - WG561003	1.00	21,565.00	20.00%	17,252.00
14	WatchGuard Firebox M4600 with 3-yr Total Security Suite - WG460643	6.00	38,530.00	20.00%	184,944.00
15	High Availability - WatchGuard Firebox M4600 and 3-yr Standard Support - WG460003	6.00	8,510.00	20.00%	40,848.00
16		12.00	3,950.00	20.00%	37,920.00

#	Item & Description	Qty	Rate	Discount	Amount
	WatchGuard Firebox M 4 Port 10Gb SFP+ Fiber Module - WG8023				
17	Transceiver 10Gb Short-Range SFP+ for WatchGuard Firebox M - WG8583	24.00	350.00	20.00%	6,720.00
18	WatchGuard Firebox M4600 Rack Rails Kit	12.00	125.00	20.00%	1,200.00
19	WatchGuard Management Server - Licensing	2.00	299.00	20.00%	478.40
20	WatchGuard AP320 and 3-yr Wi-Fi Cloud Subscription and Standard Support	350.00	990.00	20.00%	277,200.00
21	WatchGuard AP420 and 3-yr Wi-Fi Cloud Subscription and Standard Support - Outdoor	100.00	1,099.00	20.00%	87,920.00
22	Installation, Deployment, Testing and Turnup	0.00	0.00	0.00	0.00
23	Project Management	100.00	150.00	0.00	15,000.00
24	Engineering and Architecting	200.00	250.00	0.00	50,000.00
25	Technician Level 1 - 3 (5 technicians workng on the project to completion)	4,500.00	150.00	0.00	675,000.00
				Sub Total	3,282,463.94
				Total	**$3,282,463.94**

Notes

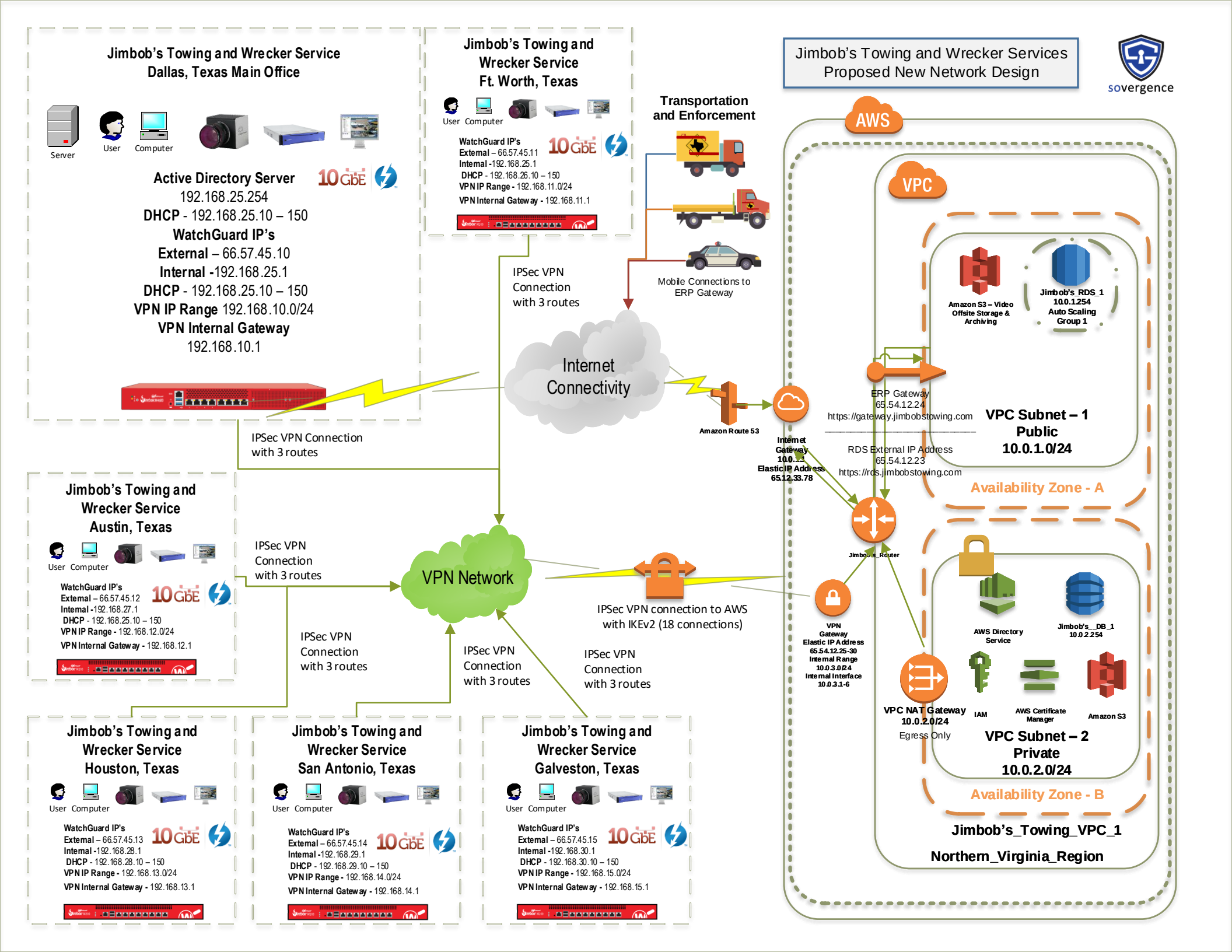
Looking forward for your business.

Terms & Conditions

To get started simply

1. Agree to estimate or sign and email back to tonydegonia@sovergence.com
2. Enclose payment for 50% of estimated costs.
3. Plan time for a project meeting to finalize details so that I can ensure you get exactly what you want and have a great experience.

Note - 50% of project fees + applicable hosting fees due at start of project. Remaining 50% of fees due before site goes live. No exceptions unless discussed and agreed upon by both parties in writing.


Jimbob's Towing and Wrecker Service
Dallas, Texas Main Office
Server
User
Computer
Active Directory Server
192.168.25.254
DHCP - 192.168.25.10 – 150
WatchGuard IP's
External – 66.57.45.10
Internal -192.168.25.1
DHCP - 192.168.25.10 – 150
VPN IP Range 192.168.10.0/24
VPN Internal Gateway
192.168.10.1
10GbE
Jimbob's Towing and Wrecker Service
Ft. Worth, Texas
User
Computer
WatchGuard IP's
External – 66.57.45.11
Internal -192.168.25.1
DHCP - 192.168.26.10 – 150
VPN IP Range - 192.168.11.0/24
VPN Internal Gateway - 192.168.11.1
10GbE
Transportation and Enforcement
Mobile Connections to ERP Gateway
IPSec VPN Connection with 3 routes
Internet Connectivity
IPSec VPN Connection with 3 routes
Amazon Route 53
Jimbob's Towing and Wrecker Service
Austin, Texas
User
Computer
WatchGuard IP's
External – 66.57.45.12
Internal -192.168.27.1
DHCP - 192.168.25.10 – 150
VPN IP Range - 192.168.12.0/24
VPN Internal Gateway - 192.168.12.1
10GbE
IPSec VPN Connection with 3 routes
VPN Network
IPSec VPN Connection with 3 routes
IPSec VPN Connection with 3 routes
IPSec VPN Connection with 3 routes
IPSec VPN connection to AWS with IKEv2 (18 connections)
Jimbob's Towing and Wrecker Service
Houston, Texas
User
Computer
WatchGuard IP's
External – 66.57.45.13
Internal -192.168.28.1
DHCP - 192.168.28.10 – 150
VPN IP Range - 192.168.13.0/24
VPN Internal Gateway - 192.168.13.1
10GbE
Jimbob's Towing and Wrecker Service
San Antonio, Texas
User
Computer
WatchGuard IP's
External – 66.57.45.14
Internal -192.168.29.1
DHCP - 192.168.29.10 – 150
VPN IP Range - 192.168.14.0/24
VPN Internal Gateway - 192.168.14.1
10GbE
Jimbob's Towing and Wrecker Service
Galveston, Texas
User
Computer
WatchGuard IP's
External – 66.57.45.15
Internal -192.168.30.1
DHCP - 192.168.30.10 – 150
VPN IP Range - 192.168.15.0/24
VPN Internal Gateway - 192.168.15.1
10GbE
Jimbob's Towing and Wrecker Services
Proposed New Network Design
sovergence
AWS
VPC
Amazon S3 – Video Offsite Storage & Archiving
Jimbob's_RDS_1
10.0.1.254
Auto Scaling Group 1
ERP Gateway
65.54.12.24
https://gateway.jimbobstowing.com
RDS External IP Address
65.54.12.23
https://rds.jimbobstowing.com
VPC Subnet – 1
Public
10.0.1.0/24
Availability Zone - A
Internet Gateway
10.0.1.1
Elastic IP Address
65.12.33.78
Jimbob's_Router
VPN Gateway
Elastic IP Address
65.54.12.25-30
Internal Range
10.0.3.0/24
Internal Interface
10.0.3.1-6
AWS Directory Service
Jimbob's_DB_1
10.0.2.254
VPC NAT Gateway
10.0.2.0/24
Egress Only
IAM
AWS Certificate Manager
Amazon S3
VPC Subnet – 2
Private
10.0.2.0/24
Availability Zone - B
Jimbob's_Towing_VPC_1
Northern_Virginia_Region

Hewlett Packard Enterprise

HPE FlexNetwork 5510 HI Switch Series

Key features

- Scalable with 10 Gigabit uplinks and 9-chassis IRF with up to 160 Gbps stacking bandwidth
- 40G QSFP+ ports for uplink or stacking
- Four convenient built-in SFP+ 10GbE uplinks provide performance for bandwidth hungry applications
- PoE+ for up to 30 W of PoE power per port on all ports simultaneously
- MACsec support

Product overview

The HPE FlexNetwork 5510 HI Switch Series comprises Gigabit Ethernet switches that deliver outstanding resiliency, security, and multiservice support capabilities at the edge layer of data center, large campus, and metro Ethernet networks. The switches can also be used in the core layer of SMB networks.

With Intelligent Resilient Fabric (IRF) support and available dual power supplies, the HPE FlexNetwork 5510 HI Series Switch can deliver the highest levels of resiliency and manageability. In addition, the PoE+ models provide up to 1440 W of PoE+ power with the dual power supply configuration.

Designed with four fixed 10GbE ports and supports additional modular uplinks, these switches can provide up to six 10GbE uplink ports. With complete IPv4/IPv6, OpenFlow, and MPLS/VPLS features, the series provides investment protection with an easy transition from IPv4 to IPv6 networks.

Features and benefits

Software-defined networking

- OpenFlow

  Supports OpenFlow 1.3 specification to enable SDN by allowing separation of the data (packet forwarding) and control (routing decision) paths

Quality of Service (QoS)

- Advanced classifier-based QoS

  Classifies traffic using multiple match criteria based on Layer 2, 3, and 4 information; applies QoS policies such as setting priority level and rate limit to selected traffic on a per-port or per-VLAN basis

- Traffic policing

  Supports Committed Access Rate (CAR) and line rate

- Powerful QoS feature

  Creates traffic classes based on access control lists (ACLs), IEEE 802.1p precedence, IP, and DSCP or Type of Service (ToS) precedence; supports filter, redirect, mirror, or remark; supports the following congestion actions: strict priority (SP) queuing, weighted round robin (WRR), weighted fair queuing (WFQ), weighted random early discard (WRED), weighted deficit round robin (WDRR), SP+WDRR, and SP+WFQ

- Storm restraint

  Allows limitation of broadcast, multicast, and unknown unicast traffic rate to reduce unwanted broadcast traffic on the network

- Broadcast control

  Allows limitations of broadcast traffic rate to cut down on unwanted network broadcast traffic

Management

- Friendly port names

  Allows assignment of descriptive names to ports

- sFlow® (RFC 3176)

  Provides scalable ASIC-based wire-speed network monitoring and accounting with no impact on network performance; this allows network operators to gather a variety of sophisticated network statistics and information for capacity planning and real-time network monitoring purposes

- Complete session logging

  Provides detailed information for problem identification and resolution

- Remote configuration and management

  Enables configuration and management through a CLI located on a remote device

- Manager and operator privilege levels

  Provides read-only (operator) and read/write (manager) access on CLI management interface

- Management VLAN

  Segments traffic to and from management interfaces, including CLI/Telnet, and SNMP

- Command authorization

  Leverages RADIUS/HWTACACS to link a custom list of CLI commands to an individual network administrator's login; also provides an audit trail

- Remote monitoring (RMON)

  Uses standard SNMP to monitor essential network functions; supports events, alarm, history, and statistics group plus a private alarm extension group

- Multiple configuration

  Files store easily to the flash image

- Remote intelligent mirroring

  Mirrors ingress/egress ACL-selected traffic from a switch port or VLAN to a local or remote switch port anywhere on the network

- In-service software upgrade (ISSU)

  Enables operators to perform upgrades in the shortest possible amount of time with reduced risk to network operations or traffic disruptions

- Network Management

  SNMPv1/v2c/v3, MIB-II with Traps, and RADIUS Authentication Client MIB (RFC 2618); embedded HTML management tool with secure access

- IPv6 management

  Provides future-proof networking because the switch is capable of being managed whether the attached network is running IPv4 or IPv6; supports pingv6, tracertv6, Telnetv6, TFTPv6, DNSv6, syslogv6, FTPv6, SNMPv6, DHCPv6, and RADIUS for IPv6

- Troubleshooting

  Ingress and egress port monitoring enables network problem solving; virtual cable tests provide visibility into cable problems

- HPE Intelligent Management Center (IMC)

  Integrates fault management, element configuration, and network monitoring from a central vantage point; built-in support for third-party devices enables network administrators to centrally manage all network elements with a variety of automated tasks, including discovery, categorization, baseline configurations, and software images; the software also provides configuration comparison tools, version tracking, change alerts, and more

Connectivity

- Auto-MDIX

  Automatically adjusts for straight-through or crossover cables on all 10/100/1000 port

- Packet storm protection

  Protects against broadcast, multicast, or unicast storms with user-defined thresholds

- Ethernet operations, administration, and maintenance (OAM)

  Detects data link layer problems that occurred in the "last mile" using the IEEE 802.3ah OAM standard; monitors the status of the link between two devices

- Flow Control

  Provides back pressure using standard IEEE 802.3x, reducing congestion in heavy traffic situations

- Fixed 10GbE ports

  Provides four fixed SFP+ ports for a 20GbE connection to the network without the need for additional extension interface modules

- Optional 10GbE or 40GbE ports

  Deliver, through the use of optional modules, additional 10GbE or 40GbE connections, which are available for uplinks or high-bandwidth server connections; flexibly support copper, SFP+, or 40GbE QSFP+ connections

- Jumbo packet support

  Supports up to 10000-byte frame size to improve the performance of large data transfers

- IEEE 802.3at Power over Ethernet (PoE+)

  Provides up to 30 W per port that allows support of the latest PoE+-capable devices such as IP phones, wireless access points, and security cameras, as well as any IEEE 802.3af-compliant end device; eliminates the cost of additional electrical cabling and circuits that would otherwise be necessary in IP phone and WLAN deployments

Performance

- Hardware-based wire-speed access control lists (ACLs)

  Help provide high levels of security and ease of administration without impacting network performance with a feature-rich TCAM-based ACL implementation

- Non-blocking architecture

  Delivers up to 336 Gbps of wire-speed switching with a non-blocking switching fabric and up to 250 million pps throughput

Resiliency and high availability

- Separate data and control paths

  Separates control from services and keeps service processing isolated; increases security and performance

- Device Link Detection Protocol (DLDP)

  Monitors link connectivity and shuts down ports at both ends if unidirectional traffic is detected, preventing loops in STP-based networks

- Intelligent Resilient Fabric (IRF)

  Creates virtual resilient switching fabrics, where two to nine switches perform as a single L2 switch and L3 router; switches do not have to be co-located and can be part of a disaster-recovery system; servers or switches can be attached using standard LACP for automatic load balancing and high availability; can eliminate need for complex protocols like Spanning Tree Protocol, Equal-Cost Multipath (ECMP), or VRRP, thereby simplifying network operations

- Rapid Ring Protection Protocol (RRPP)

  Connects multiple switches in a high-performance ring using standard Ethernet technology; traffic can be rerouted around the ring in less than 50 ms, reducing the impact on traffic and applications

- Smart Link

  Allows under 100 ms failover between links

- Virtual Router Redundancy Protocol (VRRP)

  Allows groups of two routers to dynamically back each other up to create highly available routed environments

- IRF capability

  Provides single IP address management for a resilient virtual switching fabric of up to nine switches using up to 160 Gbps bidirectional using QSFP+ links

- Spanning Tree/PVST+, MSTP, RSTP

  Provides redundant links while preventing network loops

- Internal Dual-Redundant Power Supply

  Provides high reliability by keeping network up while delivering up to 1440 W of PoE+

Manageability

- Dual-flash images

  Provides independent primary and secondary operating system files for backup while upgrading

- Multiple configuration files

  Allow multiple configuration files to be stored to a flash image

- Troubleshooting

  Allows ingress and egress port monitoring, enabling network problem solving; virtual cable tests provide visibility into cable problems

- IPv6 management

  Future-proofs networking, as the switch is capable of being managed whether the attached network is running IPv4 or IPv6; supports pingv6, tracertv6, Telnetv6, TFTPv6, DNSv6, and ARPv6

Layer 2 switching

- GARP VLAN Registration Protocol

  Allows automatic learning and dynamic assignment of VLANs

- IP multicast snooping and data-driven IGMP

  Automatically prevents flooding of IP multicast traffic

- Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) protocol snooping

  Controls and manages the flooding of multicast packets in a Layer 2 network

- 32K MAC addresses

  Provide access to many Layer 2 devices

- IEEE 802.1ad QinQ and selective QinQ

  Increase the scalability of an Ethernet network by providing a hierarchical structure; connect multiple LANs on a high-speed campus or metro network

- 10GbE port aggregation

  Allows grouping of ports to increase overall data throughput to a remote device

- Spanning Tree/MSTP, RSTP, and STP root guard

  Prevent network loops

- 64 MSTP instances

  Allow multiple configurations of STP per VLAN group

- Isolation at data link layer with private VLANs

  Provides, through a two-tier VLAN structure, an additional layer of protection, simplifying network configuration while saving VLAN resources

- VLAN support and tagging

  Supports the IEEE 802.1Q (4094 VLAN IDs)

Layer 3 services

- Address Resolution Protocol (ARP)

  Determines the MAC address of another IP host in the same subnet; supports static ARPs; gratuitous ARP allows detection of duplicate IP addresses; proxy ARP allows normal ARP operation between subnets or when subnets are separated by a Layer 2 network

- Dynamic Host Configuration Protocol (DHCP)

  Simplifies the management of large IP networks; supports client; DHCP Relay enables DHCP operation across subnets

- Loopback interface address

  Defines an address that can always be reachable, improving diagnostic capability

- User Datagram Protocol (UDP) helper function

  Allows UDP broadcasts to be directed across router interfaces to specific IP unicast or subnet broadcast addresses and prevents server spoofing for UDP services such as DHCP

- Route maps

  Provide more control during route redistribution; allow filtering and altering of route metrics

- DHCP server

  Centralizes and reduces the cost of the IPv4 address management

Layer 3 routing

- IPv4 routing protocols

  Support static routes, RIP, OSPF, ISIS, and BGP

- IPv6 routing protocols

  Provide routing of IPv6 at wire speed; support static routes, RIPng, OSPFv3, IS-ISv6, and BGP4+ for IPv6

- PIM-SSM, PIM-DM, and PIM-SM (for IPv4 and IPv6)

  Support IP Multicast address management and inhibition of DoS attacks

- MPLS support

  Provides extended support of MPLS, including MPLS VPNs and MPLS Traffic Engineering (MPLS TE)

- Virtual Private LAN Service (VPLS)

  Establishes point-to-multipoint Layer 2 VPNs across a provider network

- Bidirectional Forwarding Detection (BFD)

  Enables link connectivity monitoring and reduces network convergence time for RIP, OSPF, BGP, IS-IS, VRRP, MPLS, and IRF

- Policy-based routing

  Makes routing decisions based on policies set by the network administrator

- Equal-Cost Multipath (ECMP)

  Enables multiple equal-cost links in a routing environment to increase link redundancy and scale bandwidth

- IPv6 tunneling

  Allows a smooth transition from IPv4 to IPv6 by encapsulating IPv6 traffic over an existing IPv4 infrastructure

Security

- Access control lists (ACLs)

  Provide IP Layer 2 to Layer 4 traffic filtering; support global ACL, VLAN ACL, port ACL, and IPv6 ACL; up to 3K ingress ACLs and 1K egress ACLs are supported

- IEEE 802.1X

  Defines an industry-standard method of user authentication using an IEEE 802.1X supplicant on the client in conjunction with a RADIUS server

- MAC-based authentication

  Client is authenticated with the RADIUS server based on the client's MAC address

- Identity-driven security and access control

  – Per-user ACLs

    Permits or denies user access to specific network resources based on user identity and time of day, allowing multiple types of users on the same network to access specific network services without risking network security or providing unauthorized access to sensitive data

  – Automatic VLAN assignment

    Automatically assigns users to the appropriate VLAN based on their identities

- Port security

  Allows access only to specified MAC addresses, which can be learned or specified by the administrator

- Secure FTP/SCP

  Allows secure file transfer to and from the switch; protects against unwanted file downloads or unauthorized copying of a switch configuration file

- STP BPDU port protection

  Blocks Bridge Protocol Data Units (BPDUs) on ports that do not require BPDUs, preventing forged BPDU attacks

- DHCP protection

  Blocks DHCP packets from unauthorized DHCP servers, preventing denial-of-service attacks

- DHCP snooping

  Helps ensure that DHCP clients receive IP addresses from authorized DHCP servers and maintain a list of DHCP entries for trusted ports; prevents reception of fake IP addresses and reduces ARP attacks, improving security

- DHCPv6 snooping

  Ensures that DHCPv6 clients obtain IPv6 addresses from authorized DHCPv6 servers and record IP-to-MAC mappings of DHCPv6 clients

- Dynamic ARP

  Protection blocks ARP broadcasts from unauthorized hosts, preventing eavesdropping or theft of network data

- STP root guard

  Protects the root bridge from malicious attacks or configuration mistakes

- Guest VLAN

  Provides a browser-based environment to authenticated clients that is similar to IEEE 802.1X

- Port isolation

  Secures and adds privacy, and prevents malicious attackers from obtaining user information

- Endpoint Admission Defense (EAD)

  Provides security policies to users accessing a network

- RADIUS/HWTACACS

  Eases switch management security administration by using a password authentication server

- Secure management access

  Delivers secure encryption of all access methods (CLI, GUI, or MIB) through SSHv2, SSL, HTTPS, and/or SNMPv3

- Unicast Reverse Path Forwarding (URPF)

  Allows normal packets to be forwarded correctly, but discards the attaching packet due to lack of reverse path route or incorrect inbound interface; prevents source spoofing and distributed attacks; supports distributed URPF

- IP source guard

  Helps prevent IP spoofing attacks

- IPv6 source guard

  Helps prevent IPv6 spoofing attacks using ND Snooping as well as DHCPv6 Snooping

- ND Snooping

  Allows only packets with a legally obtained IPv6 address to pass

Virtual private network (VPN)

- Generic Routing Encapsulation (GRE)

  Transports Layer-2 connectivity over a Layer-3 path in a secured way; enables the segregation of traffic from site to site

Convergence

- LLDP-MED (Media Endpoint Discovery)

  Defines a standard extension of LLDP that stores values for parameters such as QoS and VLAN to automatically configure network devices such as IP phones

- Internet Group Management Protocol (IGMP)

  Utilizes Any-Source Multicast (ASM) or Source-Specific Multicast (SSM) to manage IPv4 multicast networks; supports IGMPv1, v2, and v3

- IEEE 802.1AB Link Layer Discovery Protocol (LLDP)

  Facilitates easy mapping using network management applications with LLDP automated device discovery protocol

- Multicast Source Discovery Protocol (MSDP)

  Allows multiple PIM-SM domains to interoperate; is used for inter-domain multicast applications

- Multicast VLAN

  Allows multiple VLANs to receive the same IPv4 or IPv6 multicast traffic, lessening network bandwidth demand by reducing or eliminating multiple streams to each VLAN

- LLDP-CDP compatibility

  Receives and recognizes CDP packets from Cisco's IP phones for seamless interoperation

- IEEE 802.3at Power over Ethernet (PoE+)

  Provides up to 30 W per port that allows support of the latest PoE+-capable devices such as IP phones, wireless access points, and security cameras, as well as any IEEE 802.3af-compliant end device; eliminates the cost of additional electrical cabling and circuits that would otherwise be necessary in IP phone and WLAN deployments

- PoE allocations

  Supports multiple methods (automatic, IEEE 802.3af-class, LLDP-MED, or user-specified) to allocate PoE power for more efficient energy savings

- Voice VLAN

  Automatically assigns VLAN and priority for IP phones, simplifying network configuration and maintenance

- IP multicast snooping (data-driven IGMP)

  Prevents flooding of IP multicast traffic

Additional information

Green initiative support

Provides support for RoHS and WEEE regulations

- Green IT and power

  Improves energy efficiency through the use of the latest advances in silicon development; shuts off unused ports and utilizes variable-speed fans, reducing energy costs

- Unified HPE Comware operating system with modular architecture

  Provides an easy-to-enhance-and-extend feature set, which doesn't require whole-scale changes; all switching, routing, and security platforms leverage the Comware OS, a common unified modular operating system

- Energy Efficient Ethernet (EEE) support

  Reduces power consumption in accordance with IEEE 802.3az

Warranty and support

- Limited Lifetime Warranty

  See **hpe.com/networking/warrantysummary** for warranty and support information included with your product purchase.

- Software releases

  To find software for your product, refer to **hpe.com/networking/support**; for details on the software releases available with your product purchase, refer to **hpe.com/networking/warrantysummary**

HPE FlexNetwork 5510 HI Switch Series

Specifications



	HPE 5510 24G 4SFP+ HI 1-SLOT SWITCH (JH145A)	HPE 5510 48G 4SFP+ HI 1-SLOT SWITCH (JH146A)	HPE 5510 24G POE+ 4SFP+ HI 1-SLOT SWITCH (JH147A)
I/O ports and slots	24 RJ-45 autosensing 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T); Media Type: Auto-MDIX; Duplex: 10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only; Ports 1—8 support MACsec 4 SFP+ 10GbE ports 1 port expansion module slot Supports a maximum of 6 SFP+ ports or 2 1/10GBASE-T ports or 2 40GbE ports, with optional module	48 RJ-45 autosensing 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T); Media Type: Auto-MDIX; Duplex: 10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only; Ports 1—8 support MACsec 4 SFP+ 10GbE ports 1 port expansion module slot Supports a maximum of 6 SFP+ ports or 2 1/10GBASE-T ports or 2 40GbE ports, with optional module	24 RJ-45 autosensing 10/100/1000 PoE+ ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T, IEEE 802.3at PoE+); Media Type: Auto-MDIX; Duplex: 10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only; Ports 1—8 support MACsec 4 SFP+ 10GbE ports 1 port expansion module slot Supports a maximum of 6 SFP+ ports or 2 1/10GBASE-T ports or 2 40GbE ports, with optional module
Additional ports and slots	1 dual-personality (RJ-45 or mini USB) serial console port 1 RJ-45 out-of-band management port 1 USB 2.0	1 dual-personality (RJ-45 or mini USB) serial console port 1 RJ-45 out-of-band management port 1 USB 2.0	1 dual-personality (RJ-45 or mini USB) serial console port 1 RJ-45 out-of-band management port 1 USB 2.0
Power supplies	2 power supply slots 1 minimum power supply required (ordered separately)	2 power supply slots 1 minimum power supply required (ordered separately)	2 power supply slots 1 minimum power supply required (ordered separately)
Fan tray	Airflow direction is Front (port side) to Back (power cord side)	Airflow direction is Front (port side) to Back (power cord side)	Airflow direction is Front (port side) to Back (power cord side)
Physical characteristics			
Dimensions	17.32(w) x 14.17(d) x 1.72(h) (44.00 x 36.00 x 4.37 cm) (1U height)	17.32(w) x 14.17(d) x 1.72(h) (44.0 x 36.0 x 4.37 cm) (1U height)	17.32(w) x 18.11(d) x 1.72(h) (43.99 x 46 x 4.37 cm) (1U height)
Weight	16.53 lb (7.5 kg) shipping weight	16.53 lb (7.5 kg)	27.56 lb (12.5 kg) shipping weight
Memory and processor	2 GB SDRAM; Packet buffer size: 4 MB, 512 MB flash	2 GB SDRAM; Packet buffer size: 4 MB, 512 MB flash	2 GB SDRAM; Packet buffer size: 4 MB, 512 MB flash
Mounting and enclosure	Mounts in an EIA standard 19-inch telco rack or equipment cabinet (hardware included)	Mounts in an EIA standard 19-inch telco rack or equipment cabinet (hardware included)	Mounts in an EIA standard 19-inch telco rack or equipment cabinet (hardware included)
Performance			
	IPv6 Ready Certified	IPv6 Ready Certified	IPv6 Ready Certified
1000 Mb Latency	< 5 µs	< 5 µs	< 5 µs
10 Gbps Latency	< 3 µs	< 3 µs	< 3 µs
Throughput	Up to 214 Mpps	Up to 250 Mpps	Up to 214 Mpps
Routing/Switching capacity	288 Gbps	336 Gbps	288 Gbps
Routing table size	32768 entries (IPv4), 16384 entries (IPv6)	32768 entries (IPv4), 16384 entries (IPv6)	32768 entries (IPv4), 16384 entries (IPv6)
MAC address table size	32768 entries	32768 entries	32768 entries
Environment			
Operating temperature	32°F to 113°F (0°C to 45°C)	32°F to 113°F (0°C to 45°C)	32°F to 113°F (0°C to 45°C)
Operating relative humidity	10% to 90%, noncondensing	10% to 90%, noncondensing	10% to 90%, noncondensing
Nonoperating/Storage temperature	-40°F to 158°F (-40°C to 70°C)	-40°F to 158°F (-40°C to 70°C)	-40°F to 158°F (-40°C to 70°C)
Nonoperating/Storage relative humidity	5% to 95%, noncondensing	5% to 95%, noncondensing	5% to 95%, noncondensing
Acoustic	Low-speed fan: 52.8 dB, High-speed fan: 66.7 dB; ISO 7779	Low-speed fan: 49.9 dB, High-speed fan: 64.8 dB; ISO 7779	Low-speed fan: 57.6 dB, High-speed fan: 66.9 dB; ISO 7779

HPE FlexNetwork 5510 HI Switch Series

Specifications (continued)

	HPE 5510 24G 4SFP+ HI 1-SLOT SWITCH (JH145A)	HPE 5510 48G 4SFP+ HI 1-SLOT SWITCH (JH146A)	HPE 5510 24G POE+ 4SFP+ HI 1-SLOT SWITCH (JH147A)
Electrical characteristics			
Frequency	50/60 Hz	50/60 Hz	50/60 Hz
Maximum heat dissipation	365 BTU/hr (385.08 kJ/hr), Ranges from 167 BTU/hr to 392 BTU/hr, depending on power supply configuration	238 BTU/hr (686.81 kJ/hr), Ranges from 201 BTU/hr to 443 BTU/hr, depending on power supply configuration	2217 BTU/hr (3599.66 kJ/hr), Ranges from 228 BTU/hr to 3412 BTU/hr, depending on power supply configuration
Voltage	100–240 VAC, rated (90–264 VAC, max) -48 to -60 VDC, rated (-36 to -72 VDC, max) (depending on power supply chosen)	100–240 VAC, rated (90–264 VAC, max) -48 to -60 VDC, rated (-36 to -72 VDC, max) (depending on power supply chosen)	100–240 VAC, rated (90–264 VAC, max) (depending on power supply chosen)
Maximum power rating	107 W	150 W	650 W
Idle power	55 W	70 W	67 W
PoE power			740 W PoE+
Notes	Idle power is the actual power consumption of the device with no ports connected. Maximum power rating and maximum heat dissipation are the worst-case theoretical maximum numbers provided for planning the infrastructure with fully loaded PoE (if equipped), 100% traffic, all ports plugged in, and all modules populated.	Idle power is the actual power consumption of the device with no ports connected. Maximum power rating and maximum heat dissipation are the worst-case theoretical maximum numbers provided for planning the infrastructure with fully loaded PoE (if equipped), 100% traffic, all ports plugged in, and all modules populated.	Idle power is the actual power consumption of the device with no ports connected. Maximum power rating and maximum heat dissipation are the worst-case theoretical maximum numbers provided for planning the infrastructure with fully loaded PoE (if equipped), 100% traffic, all ports plugged in, and all modules populated. PoE+ power range is from to PoE+ power is the power supplied by the internal power supply(ies). It is dependent on the type and quantity of power supplies. Device supports 1 or 2 internal modular power supplies.
Safety	UL 60950-1; EN 60825-1 Safety of Laser Products-Part 1; EN 60825-2 Safety of Laser Products-Part 2; IEC 60950-1; EN 60950-1; CAN/CSA-C22.2 No. 60950-1; FDA 21 CFR Subchapter J; ROHS Compliance; AS/NZS 60950-1; GB 4943; EAC (EurAsian Conformity Certification)	UL 60950-1; EN 60825-1 Safety of Laser Products-Part 1; EN 60825-2 Safety of Laser Products-Part 2; IEC 60950-1; EN 60950-1; CAN/CSA-C22.2 No. 60950-1; FDA 21 CFR Subchapter J; ROHS Compliance; AS/NZS 60950-1; GB 4943; EAC (EurAsian Conformity Certification)	UL 60950-1; EN 60825-1 Safety of Laser Products-Part 1; EN 60825-2 Safety of Laser Products-Part 2; IEC 60950-1; EN 60950-1; CAN/CSA-C22.2 No. 60950-1; FDA 21 CFR Subchapter J; ROHS Compliance; AS/NZS 60950-1; GB 4943; EAC (EurAsian Conformity Certification)
Emissions	EMC Directive 2004/108/EC; FCC (CFR 47, Part 15) Class A; EN 61000-4-11:2004; ANSI C63.4-2009; EN 61000-3-3:2008; VCCI V-3/2012.04; EN 61000-3-2:2006+A1:2009+A2:2009; EN 61000-4-3:2006; EN 61000-4-4:2012; EN 61000-4-5:2006; EN 61000-4-6:2009; CISPR 22:2008 Class A; EN 55022:2010 Class A; EN 61000-4-29: 2000; CISPR 24:2010; EN 300 386 V1.6.1; VCCI V-3/2013.04 Class A	EMC Directive 2004/108/EC; FCC (CFR 47, Part 15) Class A; EN 61000-4-11:2004; ANSI C63.4-2009; EN 61000-3-3:2008; VCCI V-3/2012.04; EN 61000-3-2:2006+A1:2009+A2:2009; EN 61000-4-3:2006; EN 61000-4-4:2012; EN 61000-4-5:2006; EN 61000-4-6:2009; CISPR 22:2008 Class A; EN 55022:2010 Class A; EN 61000-4-29: 2000; CISPR 24:2010; EN 300 386 V1.6.1; VCCI V-3/2013.04 Class A	EMC Directive 2004/108/EC; FCC (CFR 47, Part 15) Class A; EN 61000-4-11:2004; ANSI C63.4-2009; EN 61000-3-3:2008; VCCI V-3/2012.04; EN 61000-3-2:2006+A1:2009+A2:2009; EN 61000-4-3:2006; EN 61000-4-4:2012; EN 61000-4-5:2006; EN 61000-4-6:2009; CISPR 22:2008 Class A; EN 55022:2010 Class A; EN 61000-4-29: 2000; CISPR 24:2010; EN 300 386 V1.6.1; VCCI V-3/2013.04 Class A
Immunity			
Generic	EN 55024	EN 55024	EN 55024
ESD	EN 300 386	EN 300 386	EN 300 386
Management	IMC—Intelligent Management Center; Command-line interface; SNMP manager	IMC—Intelligent Management Center; Command-line interface; SNMP manager	IMC—Intelligent Management Center; Command-line interface; SNMP manager
Services	Refer to the HPE website at **hpe.com/networking/services** for details on the service-level descriptions and product numbers. For details about services and response times in your area, please contact your local HPE sales office.	Refer to the HPE website at **hpe.com/networking/services** for details on the service-level descriptions and product numbers. For details about services and response times in your area, please contact your local HPE sales office.	Refer to the HPE website at **hpe.com/networking/services** for details on the service-level descriptions and product numbers. For details about services and response times in your area, please contact your local HPE sales office.

HPE FlexNetwork 5510 HI Switch Series

Specifications (continued)

	HPE 5510 48G PoE+ 4SFP+ HI 1-slot Switch (JH148A)	HPE 5510 24G SFP 4SFP+ HI 1-slot Switch (JH149A)
I/O ports and slots	48 RJ-45 autosensing 10/100/1000 PoE+ ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T, IEEE 802.3at PoE+); Duplex: 10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only; Ports 1—8 support MACsec 4 SFP+ 10GbE ports 1 port expansion module slot Supports a maximum of 6 SFP+ ports or 2 1/10GBASE-T ports or 2 40GbE ports, with optional module	16 fixed Gigabit Ethernet SFP ports; Ports 1—8 support MACsec 8 Combo GbE (SFP and RJ-45) dual-personality 1000 Mbps port, IEEE 802.3ab Type 1000BASE-T); Duplex: 10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only 4 SFP+ 10GbE ports 1 port expansion module slot Supports a maximum of 6 SFP+ ports or 2 1/10GBASE-T ports or 2 40GbE ports, with optional module
Additional ports and slots	1 dual-personality (RJ-45 or mini USB) serial console port 1 RJ-45 out-of-band management port 1 USB 2.0	1 dual-personality (RJ-45 or mini USB) serial console port 1 RJ-45 out-of-band management port 1 USB 2.0
Power supplies	2 power supply slots 1 minimum power supply required (ordered separately)	2 power supply slots 1 minimum power supply required (ordered separately)
Fan tray	Airflow direction is Front (port side) to Back (power cord side)	Airflow direction is Front (port side) to Back (power cord side)
Physical characteristics		
Dimensions	17.32(w) x 18.11(d) x 1.72(h) (43.99 x 46 x 4.37 cm) (1U height)	17.32(w) x 14.17(d) x 1.72(h) (43.99 x 35.99 x 4.37 cm) (1U height)
Weight	27.56 lb (12.5 kg) shipping weight	16.53 lb (7.5 kg) shipping weight
Memory and processor	2 GB SDRAM; Packet buffer size: 4 MB, 512 MB flash	2 GB SDRAM; Packet buffer size: 4 MB, 512 MB flash
Mounting and enclosure	Mounts in an EIA standard 19-inch telco rack or equipment cabinet (hardware included)	Mounts in an EIA standard 19-inch telco rack or equipment cabinet (hardware included)
Performance		
	IPv6 Ready Certified	IPv6 Ready Certified
1000 Mb Latency	< 5 µs	< 5 µs
10 Gbps Latency	< 3 µs	< 3 µs
Throughput	Up to 250 Mpps	Up to 214 Mpps
Routing/Switching capacity	336 Gbps	288 Gbps
Routing table size	32768 entries (IPv4), 16384 entries (IPv6)	32768 entries (IPv4), 16384 entries (IPv6)
MAC address table size	32768 entries	32768 entries
Environment		
Operating temperature	32°F to 113°F (0°C to 45°C)	32°F to 113°F (0°C to 45°C)
Operating relative humidity	10% to 90%, noncondensing	10% to 90%, noncondensing
Nonoperating/Storage temperature	-40°F to 158°F (-40°C to 70°C)	-40°F to 158°F (-40°C to 70°C)
Nonoperating/Storage relative humidity	5% to 95%, noncondensing	5% to 95%, noncondensing
Acoustic	Low-speed fan: 57.6 dB, High-speed fan: 66.9 dB; ISO 7779	Low-speed fan: 50.5 dB, High-speed fan: 66.9 dB; ISO 7779

HPE FlexNetwork 5510 HI Switch Series

Specifications (continued)

	HPE 5510 48G PoE+ 4SFP+ HI 1-slot Switch (JH148A)	HPE 5510 24G SFP 4SFP+ HI 1-slot Switch (JH149A)
Electrical characteristics		
Frequency	50/60 Hz	50/60 Hz
Maximum heat dissipation	2286 BTU/hr (2411.73 kJ/hr), Heat dissipation ranges from 256 BTU/hr to 6142 BTU/hr, depending on power supply configuration	409 BTU/hr (431.49 kJ/hr), Heat dissipation ranges from 163 BTU/hr to 498 BTU/hr, depending on power supply configuration
Voltage	100–240 VAC, rated (90–264 VAC, max) (depending on power supply chosen)	100–240 VAC, rated (90–264 VAC, max) -48 to -60 VDC, rated (-36 to -72 VDC, max) (depending on power supply chosen)
Maximum power rating	670 W	120 W
Idle power	75 W	48 W
PoE power	1440 W PoE+	
Notes	Idle power is the actual power consumption of the device with no ports connected. Maximum power rating and maximum heat dissipation are the worst-case theoretical maximum numbers provided for planning the infrastructure with fully loaded PoE (if equipped), 100% traffic, all ports plugged in, and all modules populated. PoE+ power range is from to PoE+ power is the power supplied by the internal power supply(ies). It is dependent on the type and quantity of power supplies. Device supports 1 or 2 internal modular power supplies.	Idle power is the actual power consumption of the device with no ports connected. Maximum power rating and maximum heat dissipation are the worst-case theoretical maximum numbers provided for planning the infrastructure with fully loaded PoE (if equipped), 100% traffic, all ports plugged in, and all modules populated.
Safety	UL 60950-1; EN 60825-1 Safety of Laser Products-Part 1; EN 60825-2 Safety of Laser Products-Part 2; IEC 60950-1; EN 60950-1; CAN/CSA-C22.2 No. 60950-1; FDA 21 CFR Subchapter J; ROHS Compliance; AS/NZS 60950-1; GB 4943; EAC (EurAsian Conformity Certification)	UL 60950-1; EN 60825-1 Safety of Laser Products-Part 1; EN 60825-2 Safety of Laser Products-Part 2; IEC 60950-1; EN 60950-1; CAN/CSA-C22.2 No. 60950-1; FDA 21 CFR Subchapter J; ROHS Compliance; AS/NZS 60950-1; GB 4943; EAC (EurAsian Conformity Certification)
Emissions	EMC Directive 2004/108/EC; FCC (CFR 47, Part 15) Class A; EN 61000-4-11:2004; ANSI C63.4-2009; EN 61000-3-3:2008; VCCI V-3/2012.04; EN 61000-3-2:2006+A1:2009+A2:2009; EN 61000-4-3:2006; EN 61000-4-4:2012; EN 61000-4-5:2006; EN 61000-4-6:2009; CISPR 22:2008 Class A; EN 55022:2010 Class A; EN 61000-4-29: 2000; CISPR 24:2010; EN 300 386 V1.6.1; VCCI V-3/2013.04 Class A	EMC Directive 2004/108/EC; FCC (CFR 47, Part 15) Class A; EN 61000-4-11:2004; ANSI C63.4-2009; EN 61000-3-3:2008; VCCI V-3/2012.04; EN 61000-3-2:2006+A1:2009+A2:2009; EN 61000-4-3:2006; EN 61000-4-4:2012; EN 61000-4-5:2006; EN 61000-4-6:2009; CISPR 22:2008 Class A; EN 55022:2010 Class A; EN 61000-4-29: 2000; CISPR 24:2010; EN 300 386 V1.6.1; VCCI V-3/2013.04 Class A
Immunity		
Generic	EN 55024	EN 55024
ESD	EN 300 386	EN 300 386
Management	IMC—Intelligent Management Center; Command-line interface; SNMP manager	IMC—Intelligent Management Center; Command-line interface; SNMP manager
Services	Refer to the HPE website at **hpe.com/networking/services** for details on the service-level descriptions and product numbers. For details about services and response times in your area, please contact your local HPE sales office.	Refer to the HPE website at **hpe.com/networking/services** for details on the service-level descriptions and product numbers. For details about services and response times in your area, please contact your local HPE sales office.

Standards and Protocols
(applies to all products in series)

BGP	RFC 1657 Definitions of Managed Objects for BGPv4	RFC 1771 BGPv4	RFC 2385 BGP Session Protection via TCP MD5 RFC 2858 BGP-4 Multi-Protocol Extensions
Device management	RFC 1155 Structure and Mgmt. Information (SMIv1) RFC 1157 SNMPv1/v2c RFC 1305 NTPv3 RFC 2573 (SNMPv3 Applications) RFC 2578-2580 SMIv2	RFC 2819 (RMON groups Alarm, Event, History and Statistics only) RFC 3416 (SNMP Protocol Operations v2) RFC 3417 (SNMP Transport Mappings) HTML and telnet management	Multiple Configuration Files SNMP v3 and RMON RFC support SSHv1/SSHv2 Secure Shell TACACS/TACACS+
General protocols	IEEE 802.1ad Q-in-Q IEEE 802.1ak Multiple Registration Protocol (MRP) and Multiple VLAN Registration Protocol (MVRP) IEEE 802.1AX—2008 Link Aggregation IEEE 802.1D MAC Bridges IEEE 802.1p Priority IEEE 802.1Q (GVRP) IEEE 802.1Q VLANs IEEE 802.1s Multiple Spanning Trees IEEE 802.1v VLAN classification by Protocol and Port IEEE 802.1w Rapid Reconfiguration of Spanning Tree IEEE 802.1X PAE IEEE 802.3 Type 10BASE-T IEEE 802.3ab 1000BASE-T IEEE 802.3ac (VLAN Tagging Extension) IEEE 802.3ad Link Aggregation (LAG) IEEE 802.3ad Link Aggregation Control Protocol (LACP) IEEE 802.3ae 10-Gigabit Ethernet IEEE 802.3af Power over Ethernet IEEE 802.3at Power over Ethernet Plus IEEE 802.3az Energy Efficient Ethernet IEEE 802.3i 10BASE-T IEEE 802.3u 100BASE-X IEEE 802.3x Flow Control IEEE 802.3z 1000BASE-X RFC 768 UDP RFC 783 TFTP Protocol (revision 2) RFC 791 IP RFC 792 ICMP RFC 793 TCP RFC 826 ARP RFC 854 TELNET RFC 855 Telnet Option Specification RFC 894 IP over Ethernet RFC 925 Multi-LAN Address Resolution RFC 950 Internet Standard Subnetting Procedure RFC 951 BOOTP RFC 959 File Transfer Protocol (FTP) RFC 1027 Proxy ARP RFC 1042 IP Datagrams RFC 1058 RIPv1 RFC 1071 Computing the Internet Checksum RFC 1166 IP Addresses RFC 1122 Requirements for Internet Hosts—Communication Layers RFC 1123 Requirements for Internet Hosts RFC 1141 Incremental updating of the Internet checksum RFC 1191 Path MTU discovery RFC 1213 Management Information Base for Network Management of TCP/IP-based internets RFC 1256 ICMP Router Discovery Protocol (IRDP) RFC 1305 NTPv3	RFC 1350 TFTP Protocol (revision 2) RFC 1519 CIDR RFC 1533 DHCP Options and BOOTP Vendor Extensions RFC 1542 BOOTP Extensions RFC 1591 DNS (client only) RFC 1643 Definitions of Managed Objects for the Ethernet-like Interface Types RFC 1723 RIP v2 RFC 1812 IPv4 Routing RFC 1866 Hypertext Markup Language—2.0 RFC 1887 An Architecture for IPv6 Unicast Address Allocation RFC 1901 Introduction to Community-based SNMPv2 RFC 1902-1907 SNMPv2 RFC 2131 DHCP RFC 2236 IGMP Snooping RFC 2338 VRRP RFC 2375 IPv6 Multicast Address Assignments RFC 2462 IPv6 Stateless Address Autoconfiguration RFC 2474 Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers RFC 2475 Architecture for Differentiated Services RFC 2597 Assured Forwarding PHB Group RFC 2616 Hypertext Transfer Protocol—HTTP/1.1 RFC 2644 Directed Broadcast Control RFC 2665 Definitions of Managed Objects for the Ethernet-like Interface Types RFC 2668 Definitions of Managed Objects for IEEE 802.3 Medium Attachment Units (MAUs) RFC 2711 IPv6 Router Alert Option RFC 2784 Generic Routing Encapsulation (GRE) RFC 2865 Remote Authentication Dial In User Service (RADIUS) RFC 2866 RADIUS Accounting RFC 2868 RADIUS Attributes for Tunnel Protocol Support RFC 3046 DHCP Relay Agent Information Option RFC 3209 RSVP-TE Extensions to RSVP for LSP Tunnels RFC 3246 Expedited Forwarding PHB RFC 3410 Applicability Statements for SNMP RFC 3414 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) RFC 3415 View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP) RFC 3416 Protocol Operations for SNMP RFC 3417 Transport Mappings for the Simple Network Management Protocol (SNMP) RFC 3418 Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)	RFC 3484 Default Address Selection for Internet Protocol version 6 (IPv6) RFC 3493 Basic Socket Interface Extensions for IPv6 RFC 3542 Advanced Sockets Application Program Interface (API) for IPv6 RFC 3576 Ext to RADIUS (CoA only) RFC 3580 IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines RFC 3587 IPv6 Global Unicast Address Format RFC 3596 DNS Extensions to Support IP Version 6 RFC 3623 Graceful OSPF Restart RFC 3704 Unicast Reverse Path Forwarding (URPF) RFC 3768 Virtual Router Redundancy Protocol (VRRP) RFC 3810 Multicast Listener Discovery Version 2 (MLDv2) for IPv6 RFC 4090 Fast Reroute Extensions to RSVP-TE for LSP Tunnels RFC 4113 Management Information Base for the User Datagram Protocol (UDP) RFC 4213 Basic IPv6 Transition Mechanisms RFC 4250 The Secure Shell (SSH) Protocol Assigned Numbers RFC 4251 The Secure Shell (SSH) Protocol Architecture RFC 4252 The Secure Shell (SSH) Authentication Protocol RFC 4253 The Secure Shell (SSH) Transport Layer Protocol RFC 4254 The Secure Shell (SSH) Connection Protocol RFC 4291 IP Version 6 Addressing Architecture RFC 4443 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification RFC 4541 Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches RFC 4575 A Session Initiation Protocol (SIP) Event Package for Conference State RFC 4594 Configuration Guidelines for DiffServ Service Classes RFC 4675 RADIUS VLAN & Priority RFC 4750 OSPF Version 2 Management Information Base RFC 4762 Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling RFC 5095 Deprecation of Type 0 Routing Headers in IPv6 802.1r—GARP Proprietary Attribute Registration Protocol (GPRP)
IP multicast	RFC 1112 IGMPv1 RFC 2236 IGMPv2 RFC 2710 Multicast Listener Discovery (MLD) for IPv6	RFC 2858 Multiprotocol Extensions for BGP-4 RFC 3376 IGMPv3 RFC 3569 An Overview of Source-Specific Multicast (SSM)	RFC 3618 Multicast Source Discovery Protocol (MSDP) RFC 3973 PIM Dense Mode RFC 4601 PIM Sparse Mode

Standards and Protocols (continued)
(applies to all products in series)

IPv6	RFC 1981 IPv6 Path MTU Discovery RFC 2460 IPv6 Specification RFC 2461 IPv6 Neighbor Discovery RFC 2463 ICMPv6 RFC 2464 Transmission of IPv6 over Ethernet Networks RFC 2545 Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing	RFC 3162 RADIUS and IPv6 RFC 3306 Unicast-Prefix-based IPv6 Multicast Addresses RFC 3307 IPv6 Multicast Address Allocation RFC 3315 DHCPv6 (client and relay) RFC 3484 Default Address Selection for IPv6 RFC 3736 Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6	RFC 4291 IP Version 6 Addressing Architecture RFC 4293 MIB for IP RFC 4443 ICMPv6 RFC 4861 IPv6 Neighbor Discovery RFC 4862 IPv6 Stateless Address Auto-configuration RFC 6724 Default Address Selection for Internet Protocol Version 6 (IPv6)
MIBs	RFC 1212 Concise MIB Definitions RFC 1213 MIB II RFC 1215 A Convention for Defining Traps for use with the SNMP RFC 1493 Bridge MIB RFC 1757 Remote Network Monitoring MIB RFC 2096 IP Forwarding Table MIB RFC 2233 Interface MIB RFC 2571 SNMP Framework MIB RFC 2572 SNMP-MPD MIB RFC 2573 SNMP-Notification MIB	RFC 2573 SNMP-Target MIB RFC 2574 SNMP USM MIB RFC 2618 RADIUS Authentication Client MIB RFC 2620 RADIUS Accounting Client MIB RFC 2665 Ethernet-Like-MIB RFC 2668 802.3 MAU MIB RFC 2674 Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual Extensions	RFC 2737 Entity MIB (Version 2) RFC 2819 RMON MIB RFC 2863 The Interfaces Group MIB RFC 2925 Ping MIB RFC 3414 SNMP-User based-SM MIB RFC 3415 SNMP-View based-ACM MIB RFC 3418 MIB for SNMPv3 RFC 3621 Power Ethernet MIB
MPLS	RFC 2961 RSVP Refresh Overhead Reduction Extensions RFC 3031 Multiprotocol Label Switching Architecture	RFC 3032 MPLS Label Stack Encoding RFC 3036 LDP Specification	RFC 4762 Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling
Network management	IEEE 802.1AB Link Layer Discovery Protocol (LLDP) RFC 1215 Convention for Defining Traps for use with the SNMP RFC 2579 Textual Conventions for SMIv2 RFC 2580 Conformance Statements for SMIv2	RFC 2818 HTTP over TLS RFC 2819 Four groups of RMON: 1 (statistics), 2 (history), 3 (alarm) and 9 (events) RFC 6398 IP Router Alert Considerations and Usage	ANSI/TIA-1057 LLDP Media Endpoint Discovery (LLDP-MED) SNMPv1/v2c/v3
OSPF	RFC 1587 OSPF NSSA	RFC 1850 OSPFv2 Management Information Base (MIB), traps	RFC 2328 OSPFv2 RFC 2370 OSPF Opaque LSA Option
QoS/CoS	RFC 2474 DS Field in the IPv4 and IPv6 Headers	RFC 3260 New Terminology and Clarifications for DiffServ	
Security	IEEE 802.1X Port Based Network Access Control RFC 1492 TACACS+ RFC 2138 RADIUS Authentication	RFC 2139 RADIUS Accounting RFC 2865 RADIUS Authentication RFC 2866 RADIUS Accounting RFC 3260 New Terminology and Clarifications for DiffServ RFC 4716 SSH Public Key File Format	Secure Sockets Layer (SSL) SSHv2 Secure Shell

HPE FlexNetwork 5510 HI Switch Series accessories

Modules	**NEW** HPE 5510 QSFP+ 2-port Module (JH155A) **NEW** HPE 5130/5510 10GBASE-T 2-port Module (JH156A)[1] **NEW** HPE 5130/5510 10GbE SFP+ 2-port Module (JH157A)[1]
Transceivers	HPE X115 100M SFP LC BX 10-U Transceiver (JD100A)[2] HPE X115 100M SFP LC BX 10-D Transceiver (JD101A)[2] HPE X110 100M SFP LC FX Transceiver (JD102B)[2] HPE X110 100M SFP LC LX Transceiver (JD120B)[2] HPE X125 1G SFP LC LH40 1310nm Transceiver (JD061A)[3] HPE X120 1G SFP LC LH40 1550nm Transceiver (JD062A)[3] HPE X125 1G SFP LC LH70 Transceiver (JD063B)[3] HPE X120 1G SFP RJ45 1000BASE-T Transceiver (JD089B)[3] HPE X120 1G SFP LC BX 10-U Transceiver (JD098B)[3] HPE X120 1G SFP LC BX 10-D Transceiver (JD099B)[3] HPE X120 1G SFP LC LH100 Transceiver (JD103A)[3] HPE X120 1G SFP LC SX Transceiver (JD118B)[3] HPE X120 1G SFP LC LX Transceiver (JD119B)[3] HPE X130 10G SFP+ LC SR Transceiver (JD092B) HPE X130 10G SFP+ LC LR Transceiver (JD094B)

[1] Module supports MACsec

[2] Supported only on JH149A (HPE 5510 24G SFP 4SFP+ HI 1-Slot Switch) and only in 1G downlink configuration

[3] Transceiver cannot be used on optional module JH157A (HPE 5130/5510 10GbE SFP+ 2-port Module)

Transceivers	HPE X240 10G SFP+ SFP+ 0.65m DAC Campus-Cable (JH693A) HPE X240 10G SFP+ SFP+ 1.2m DAC Campus-Cable (JH694A) HPE X240 10G SFP+ SFP+ 3m DAC Campus-Cable (JH695A) HPE X240 10G SFP+ to SFP+ 5m Direct Attach Copper Cable (JG081C) HPE X130 10G SFP+ LC ER 40km Transceiver (JG234A)[4] HPE X130 10G SFP+ LC LH 80km Transceiver (JG915A)[4] HPE X130 10G SFP+ LC LRM Transceiver (JD093B)[4] HPE X130 10G SFP+ LC LH80 Tunable Transceiver (JL250A) HPE X140 40G QSFP+ LC BiDi 100m MM Campus-Transceiver (JH678A) HPE X140 40G QSFP+ MPO SR4 Campus-Transceiver (JH679A) HPE X240 40G QSFP+ QSFP+ 1m DAC Campus-Cable (JH697A) HPE X240 40G QSFP+ QSFP+ 3m DAC Campus-Cable (JH698A) HPE X240 40G QSFP+ QSFP+ 5m DAC Campus-Cable (JH699A) HPE X240 40G QSFP+ to 4x10G SFP+ 1m Direct Attach Copper Splitter Cable (JG329A) HPE X240 QSFP+ 4x10G SFP+ 3m DAC Campus-Cable (JH700A) HPE X240 40G QSFP+ to 4x10G SFP+ 5m Direct Attach Copper Splitter Cable (JG331A) HPE X140 40G QSFP+ LC LR4 SM 10km 1310nm Campus-Transceiver (JH677A) HPE X140 40G QSFP+ MPO MM 850nm CSR4 300m Campus-Transceiver (JH681A)
Cables	HPE 0.5 m Multimode OM3 LC/LC Optical Cable (AJ833A) HPE 1 m Multimode OM3 LC/LC Optical Cable (AJ834A) HPE 2 m Multimode OM3 LC/LC Optical Cable (AJ835A) HPE 5 m Multimode OM3 LC/LC Optical Cable (AJ836A) HPE 15 m Multimode OM3 LC/LC Optical Cable (AJ837A) HPE 30 m Multimode OM3 LC/LC Optical Cable (AJ838A) HPE 50 m Multimode OM3 LC/LC Optical Cable (AJ839A) HPE Premier Flex LC/LC Multi-mode OM4 2 fiber 1m Cable (QK732A) HPE Premier Flex LC/LC Multi-mode OM4 2 fiber 2m Cable (QK733A) HPE Premier Flex LC/LC Multi-mode OM4 2 fiber 5m Cable (QK734A) HPE Premier Flex LC/LC Multi-mode OM4 2 fiber 15m Cable (QK735A) HPE Premier Flex LC/LC Multi-mode OM4 2 fiber 30m Cable (QK736A) HPE Premier Flex LC/LC Multi-mode OM4 2 fiber 50m Cable (QK737A)
HPE 5510 24G 4SFP+ HI 1-slot Switch (JH145A)	HPE X361 150W 100-240VAC to 12VDC Power Supply (JD362B)[5] HPE X361 150W 48-60VDC to 12VDC Power Supply (JD366B)[5]
HPE 5510 48G 4SFP+ HI 1-slot Switch (JH146A)	HPE X361 150W 100-240VAC to 12VDC Power Supply (JD362B)[5] HPE X361 150W 48-60VDC to 12VDC Power Supply (JD366B)[5]
HPE 5510 24G PoE+ 4SFP+ HI 1-slot Switch (JH147A)	HPE X362 720W 100-240VAC to 56VDC PoE Power Supply (JG544A)[5] HPE X362 1110W 115-240VAC to 56VDC PoE Power Supply (JG545A)[5]
HPE 5510 48G PoE+ 4SFP+ HI 1-slot Switch (JH148A)	HPE X362 720W 100-240VAC to 56VDC PoE Power Supply (JG544A)[5] HPE X362 1110W 115-240VAC to 56VDC PoE Power Supply (JG545A)[5]
HPE 5510 24G SFP 4SFP+ HI 1-slot Switch (JH149A)	HPE X361 150W 100-240VAC to 12VDC Power Supply (JD362B)[5] HPE X361 150W 48-60VDC to 12VDC Power Supply (JD366B)[5]

[4] Supported only on optional module JH157A

[5] Products covered by 1 year warranty. See details at **hpe.com/networking/warrantyquickref**

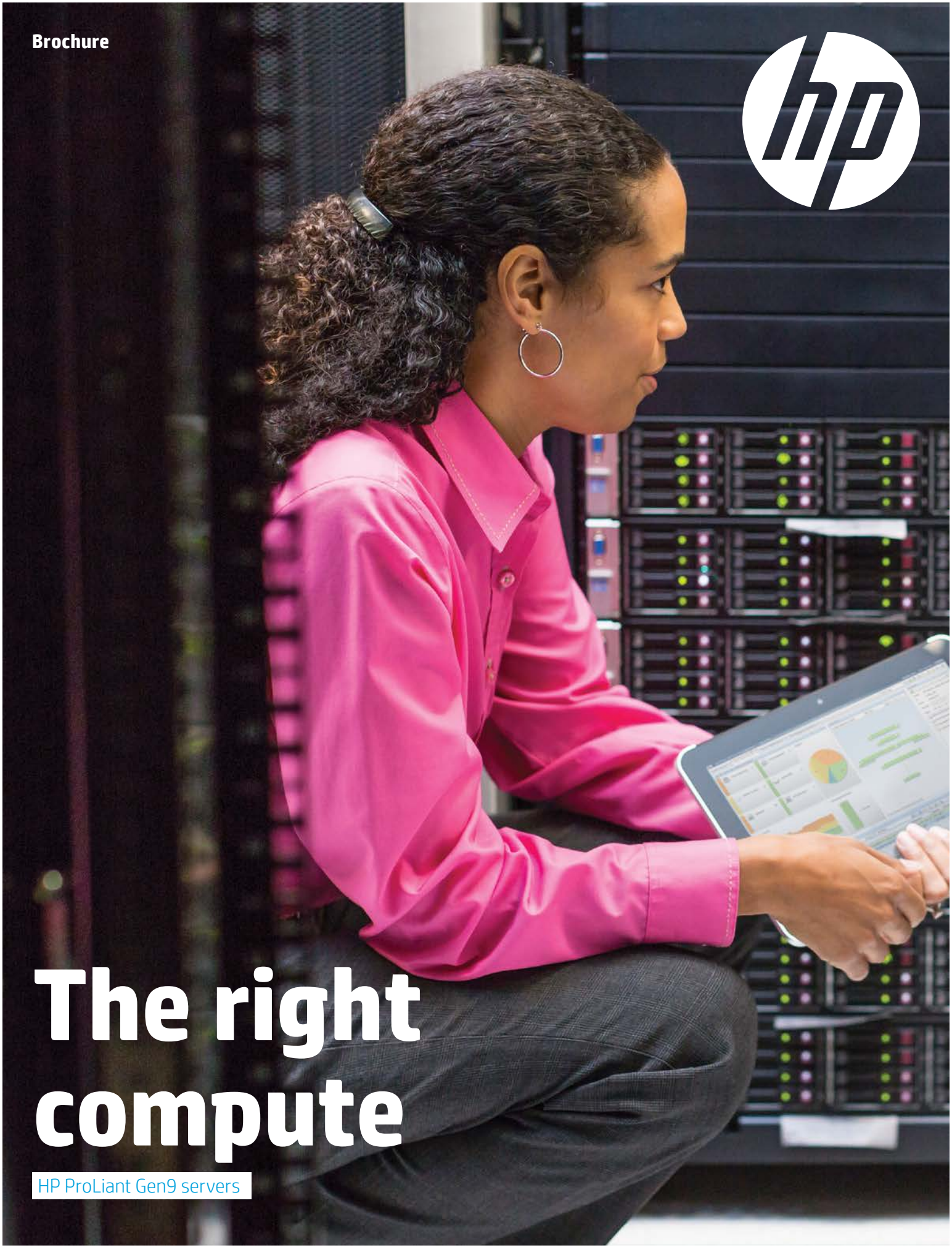
Learn more at
hpe.com/networking

Sign up for updates

4AA6-2884ENN, January 2017, Rev. 7

Hewlett Packard Enterprise

Brochure



The right compute

HP ProLiant Gen9 servers

New expectations and opportunities are here

The mega trends of cloud, mobility, Big Data, and security are generating new business opportunities—and new business challenges. Today, you need to deliver new services faster, increase operational efficiencies, and grow revenue, margin, and market share.

IT needs to lead business change, capitalizing on bold new technologies that will enable business growth. Unfortunately, today's IT infrastructure is often inefficient, sub-optimal, siloed, and slow—struggling just to meet basic business requirements, much less the need for transformation.

Intelligent HP ProLiant Gen9 servers:

- Redefine compute economics
- Accelerate service delivery
- Boost business performance

Bridging the gap between increasing business demands and IT supply will help you deliver compelling business outcomes with faster, value-added services at greater efficiency for your business. It's time to bridge the gap, by thinking about IT in an entirely new way.

A new approach is needed, starting with the heart of your infrastructure—compute—the vast pool of processing resources that can be located anywhere, scaled to any workload, and available at all times to fuel business growth. Business transformation begins with compute transformation because compute runs the applications that run your business.

The right compute for the right workload at the right economics—every time

Instead of focusing on optimizing individual systems and servers, today's new style of IT demands that you think about managing compute, storage, and networking as programmable elements that can be optimized to meet changing business needs.

HP ProLiant servers are designed with this goal in mind, delivering more compute and storage capacity, right-sized compute with flexible choices, and providing lower compute energy and floor space consumption to lower your costs of IT service.

Additionally, HP ProLiant servers help you speed your IT service delivery with faster compute, memory, and I/O performance and increased storage and networking performance, including lower latency.

They are built to excel for any size business, for any size workload, in any environment with:

- 4X compute capacity with lower total cost of ownership (TCO), maximizing data center capabilities at the lowest cost of service[1]
- 66X faster service delivery with simple automation, saving admin time and reducing errors from manual steps[2]
- 4X faster workload performance to transform the business, growing revenue, margin, and share[3]

HP ProLiant Gen9: a new approach to compute

In the compute era, processing is not defined in terms of discrete systems and silos. To move your IT infrastructure in lock-step with your business, the focus is on relentlessly driving the lowest cost, fastest time, and highest value of service delivery, period. HP ProLiant Gen9 servers are designed for this new era. Let's take a closer look at how HP gives you the simplicity and freedom to build IT that's truly the best fit for your business.

[1] Based on HP internal calculations. The HP ProLiant XL220a Server is 4X better in performance per dollar/per watt when compared to a competing Dell Blade M620 for a single threaded application per server.

[2] Anonymous customer results. The time to build and deploy infrastructure for 12 call centers was reduced from 66 days to one. Source: IDC white paper sponsored by HP, "Achieving Organizational Transformation with HP Converged Infrastructure Solutions for SDDC," January 2014, IDC #246385.

[3] HP SmartCache Performance done with equivalent controller in a controlled environment. HP Smart Storage engineers, Houston, Texas, as of 18 May 2014 posted on internal SmartCache wiki page.

Leverage HP ProLiant solutions for:

- File and print
- Infrastructure apps
- Virtualization (from low to dense)
- Mission-critical applications
- Large databases
- Monolithic applications

Compute that turns red to black

Redefining compute economics

As data centers grow, power and cooling costs take an ever larger bite out of the IT budget. Automated energy optimization features of HP ProLiant servers help you lower your use of space, power, and cooling. For example, you can:

- Get 2X more compute per watt per dollar using proven and reliable HP SmartMemory and 12 GB SAS solid-state drives (SSDs), which go through a rigorous qualification process of up to 2.4 million test hours[4]
- Use 50 percent less space and gain back 60 percent savings in energy costs with HP StoreVirtual VSA, plus co-locate apps and storage on servers to lower capital expenditures (CAPEX) by 80 percent[5]

These industry-leading innovations free up time and save money, both of which can be reallocated to other projects to drive both innovation and more efficient operations.

Compute that delivers on-site IT at cloud speed

Accelerate service delivery

Speeding up service delivery will help you keep pace with workload demands while lowering costs. Combined with the introduction of HP ProLiant Gen9 is HP Server Management, an industry-leading infrastructure management innovation. HP Server Management applies a software-defined approach to converged management, and is best suited for managing HP BladeSystem and HP ProLiant rack and tower servers. HP Server Management offers out-of-the-box integration with HP, VMware®, Microsoft®, and Red Hat® enterprise management solutions, as well as easy integration with many other management products. Architected to include open, industry-standard RESTful application programming interfaces (APIs) that enable IT staff to quickly and securely customize provisioning of the Gen9 portfolio, HP Server Management also provides a common language and interface for integrating into cloud-based environments like OpenStack. HP Server Management is designed to be:

- **Simple**—One platform for converged management leads to a 50 percent reduction in management tools to license, learn, operate, and maintain.[6] And it is simple enough to interoperate with your on-site IT management standards.
- **Automated**—Ushering in a software-defined approach to infrastructure management leads to a 66 percent increase in IT service delivery speed, enabling real competitive advantage and improved service-level agreement (SLA) performance.[7]
- **Agile**—It now takes just minutes (vs. hours) to update firmware across hundreds of servers, allowing for enterprise data center management at scale and speed.[8] And it is agile enough to scale down to meet the needs and budget of small- to medium-sized business (SMB) IT operations.

Compute that fast-forwards your success

Boost business performance

Only HP helps you deliver services at the speed your organization demands with data center infrastructure technologies that boost workload performance, thus enabling your data center for the needs of today and tomorrow.

- Faster memory performance with HP DDR4 SmartMemory up to 2,133 MHz with 14 percent better memory performance for HP ProLiant Rack and Tower servers and 33 percent better memory performance for HP ProLiant Blade servers.[9]
- One million IOPS supported with 12 GB controllers[10]

Whether you're addressing technical computing challenges, enabling cloud deployments, delivering intelligent storage, or powering design automation and data analytics, HP ProLiant servers allow you to enjoy better-than-ever performance.

[4] HP internal lab testing. 2.4 million hour test quant is derived from a combination of drive qualification test plans, specifically HDDQ spec-supplier responsibility to perform, HDDQ spec-HP responsibility to perform, RDT-Reliability Demonstration test spec, CSI integration test spec, and Pilot test requirements. Test conducted July 2014.

[5] Based on HP internal comparative analysis of publicly available data from major competitors, June 2013.

[6] Comparing HP OneView 1.10 vs. the traditional approach to server and storage management requiring eight tools. HP OneView replaces Intelligent Provisioning, Array Configuration Utility, iLO 4, Virtual Connect Manager/VCEM, HP Systems Insight Manager, HP Smart Update Manager, HP Onboard Administrator, and HP 3PAR array management. HP internal, Houston, Texas, May 2014.

[7] 66 percent faster problem resolution time for HP Insight Remote Support—initiated cases for hardware vs. traditional phone support based on HP internal call center data, Q4 2011.

[8] Performing iLO firmware updates of 200 systems in 380 seconds. Comparing it against our previous generations and competitors. Based on HP Internal estimates, Houston, Texas, U.S.A., July 2014.

[9] Up to 14 percent better performance is based on similar capacity DIMM running on HP server compared to a non-HP server with DDR4. Up to 33 percent better performance is based on similar capacity DIMM running on HP server compared to a non-HP server with DDR4.

[10] Internal performance lab testing using Iometer and the HP Smart Array P840 with RAID 0, 4k random reads, Microsoft Windows® 2012 R2; testing is ongoing with changes in firmware. Number is current as of 21 July 2014.

Maintain infrastructure health and uptime

You can't redefine compute economics, accelerate service delivery, and boost business performance if you're plagued with equipment problems. HP ProLiant servers feature multiple design innovations and tools that help you maintain server health and uptime.

Customize your IT lifecycle management, from acquisition of new IT, management of existing assets, and removal of unneeded equipment.
hp.com/go/hpfinancialservices

For example, the HP ProLiant family makes servicing easier with innovations designed to increase your productivity and confidence during setup, upgrade, and repair. Product design features allow you to confidently add or upgrade processors without the fear of bending pins, which can lead to motherboard failure and replacement. Tool-less access everywhere reduces the time to install or remove components. And the server will proactively warn you not to remove a drive if the action will cause data loss.

Developing solutions for major social and environmental challenges
hp.com/hpinfo/globalcitizenship

Issues are prevented from becoming problems through HP ProLiant software-defined lifecycle management—a converged management platform to provision, deploy, automate, monitor, and troubleshoot all your IT infrastructure resources.

HP Services

To further improve infrastructure uptime, look to HP Proactive Care Support Services—including a "direct-to-expert" support process that delivers instant access to HP server experts for faster problem resolution. You can also count on more than 2,000 HP ServiceOne partners to provide the highest levels of local expertise backed by our global resources.

Close the gap between expectation and reality

In today's data centers, small advances in technology won't solve big problems. To respond effectively to exploding demand for applications, data, and digital content, you need intelligent technology that aligns with your business demands. That's the promise of the HP ProLiant family.

Only HP has the portfolio, system management, and partner ecosystem to deliver the compute you need today and tomorrow. HP ProLiant is the one platform that you can rely on to reduce time to deliver new products and services, accelerate IT service delivery, and defer capital expenses while increasing operational efficiency to run smarter IT operations. Only HP gives you the simplicity and freedom to build IT that's the right fit for your business.

View our full portfolio of server families:

HP ProLiant Core family guide

HP BladeSystem family guide

HP Hyperscale solutions family guide

HP Moonshot System family guide

Learn more at
hp.com/go/proliant

Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document

4AA5-4292ENW, August 2014

DATASHEET

Firebox M4600 & M5600

Up to 60 Gbps firewall throughput, 11 Gbps UTM throughput
Up to 12.7 million concurrent connections and 240,000 new connections per second

TOP OF THE LINE PERFORMANCE & SECURITY

With firewall throughput of up to 60 Gbps and UTM throughput up to 11 Gbps, the Firebox® M4600 and M5600 are our fastest Firebox appliances ever. This level of performance, paired with powerful security, flexible high-port density, and affordability makes these the ideal solutions for distributed, hub-and-spoke type deployment scenarios.

M4600

M5600

Optional Modules

Choose the network interface modules that support your ideal M4600 or M5600 deployment

4 x 10 Gb Fiber

8 x 1 Gb Fiber

8 x 1 Gb Copper

2 x 40 Gb Fiber

> With WatchGuard's Firebox M4600 and M5600 appliances, we offer our customers enterprise-grade network security and the ability to maintain visibility across their entire network using the fastest, highest performing UTM solution on the market.
>
> *~ Jamison Masters, CIO, Verus Corporation*

EASILY MANAGE MANY APPLIANCES

Typically deployed at the corporate headquarters, these appliances serve as the "hub" –responsible for managing and securing all communications between the head office and all remote employee and small business sites. WatchGuard Dimension, which is included at no additional cost, provides a suite of big data visibility and reporting tools that instantly identify and distill key network security threats, issues and trends, accelerating the ability to set meaningful security policies across the entire network.

QUICK AND SIMPLE DEPLOYMENT

Cloud-based RapidDeploy technology, a configuration and deployment tool that comes standard with WatchGuard Firebox appliances, enables IT staff to create and store configuration data in the cloud – public or private – and have a new appliance directly shipped to its destination. Once the device arrives, it can connect to the cloud for a secure download of its configuration settings, saving staff travel time and money. This technology is particularly advantageous for large distributed enterprises where managing a multitude of devices efficiently across multiple locations and geographies is critical.

TOTAL NETWORK PROTECTION

Every network needs a full arsenal of scanning engines to protect against spyware, viruses, malicious apps, data leakage, botnets and more. WatchGuard's award-winning network security platform not only provides the most complete suite of unified security controls on the market today, but we have consistently been the first to offer solutions for addressing new and evolving network threats including ransomware and advanced malware.

FEATURES & BENEFITS

- Up to 60 Gbps firewall throughput. Turn on all security scanning engines and still see an amazing 11 Gbps throughput.
- All logging and reporting functions included with purchase, with over 100 dashboards and reports including PCI and HIPAA.
- Nothing could be easier than WatchGuard's drag-and-drop Branch Office VPN setup – three clicks and your remote office is connected.
- Customize your port configuration to meet current needs, knowing you have the flexibility to adapt as the network evolves. This is how to future-proof your network and eliminate costly rip-and-replace scenarios.
- To maximize port utilization, any of the ports can be configured as Internal, External, or Optional.

Firebox	M4600 base + 4 x 10 Gb interfaces	M5600 base + 4 x 10 Gb interfaces
THROUGHPUT		
Firewall throughput*	40 Gbps	60 Gbps
VPN throughput*	10 Gbps	10 Gbps
AV throughput*	9 Gbps	12 Gbps
IPS throughput*	13 Gbps	18 Gbps
UTM throughput*	8 Gbps	11 Gbps
Interfaces (installed)	8 x 1Gb	8 x 1 Gb and 4 x 10 Gb
I/O interfaces	1 serial/2 USB	1 serial/2 USB
Concurrent connections (bi-directional)	7.5 million	12.7 million
New connections per second	160,000	240,000
VLANs	1,000	unrestricted
Authenticated users limit	unrestricted	unrestricted
VPN TUNNELS		
Branch Office VPN	5,000	unrestricted
Mobile VPN IPSec	10,000	unrestricted
Mobile VPN SSL/L2TP	10,000	unrestricted

SECURITY FEATURES	
Firewall	Stateful packet inspection, deep packet inspection, proxy firewall
Application proxies	HTTP, HTTPS, SMTP, POP3, TCP-UDP, FTP, DNS
Threat protection	DoS attacks, fragmented & malformed packets, blended threats & more
VoIP	H.323, SIP, call setup and session security
Filtering options	Browser Safe Search, YouTube for Schools, Google for Business
Security subscriptions	APT Blocker, IPS, Gateway AV, WebBlocker, App Control, Data Loss Prevention, Reputation Enabled Defense, Mobile Security, Network Discovery, spamBlocker, Threat Detection & Response
MANAGEMENT	
Logging and notifications	WatchGuard, Syslog, SNMP v2/v3
User interfaces	Centralized console (WSM), Web UI, scriptable CLI
Reporting	WatchGuard Dimension includes over 100 pre-defined reports, executive summary and visibility tools
STANDARD NETWORKING	
Routing	Static, Dynamic (BGP, OSPF, RIP), Policy-based VPN
High Availability	Active/passive, active/active with load balancing
QoS	8 priority queues, DiffServ, modified strict queuing
IP address assignment	Static, DHCP (server, client, relay), PPPoE, DynDNS
NAT	Static, dynamic, 1:1, IPSec traversal, policy-based, Virtual IP for server load balancing
Link aggregation	802.3ad dynamic, static, active/backup
Other features	Port Independence, Multi-WAN failover and load balancing, server load balancing, transparent/drop-in mode
CERTIFICATIONS	
Security	ICSA Firewall, ICSA IPSec VPN Pending: CC EAL4+, FIPS 140-2
Safety	NRTL/C, CB
Network	IPv6 Ready Gold (routing)
Hazardous substance control	WEEE, RoHS, REACH
VPN & AUTHENTICATION	
Encryption	DES, 3DES, AES 128-, 192-, 256-bit
IPSec	SHA-2, IKE pre-shared key, 3rd party cert
Single sign-on	Windows, Mac OS X, mobile operating systems, RADIUS
Authentication	RADIUS, LDAP, Windows Active Directory, VASCO, RSA SecurID, internal database, Duo, SMS Passcode

PHYSICAL AND POWER SPECIFICATIONS

Product Dimensions M4600	17" x 1.8" x 18.5" (431 x 44 x 468 mm)
Product Dimensions M5600	17.4" x 1.8" x 22 (438 x 44 x 580 mm)
Shipping Dimensions M4600	32" x 8.9" x 23" (795 x 225 x 595 mm)
Shipping Dimensions M5600	23.5" x 8.9" x 31" (595 x 225 x 795 mm)
Shipping Dimensions 10G Mod.	6.3" x 3.2" x 12" (160 x 80 x 300 mm)
Shipping Weight M4600	38 lb (17 kg)
Shipping Weight M5600	46 lb (21 kg)
Shipping Weight Module	.44 lb (.2 kg)
AC Power	100-240 VAC Autosensing
Power Consumption M4600	U.S. 300 Watts (max), 1024 BTU/hr (max)
Power Consumption M5600	U.S. 400 Watts (max), 1365 BTU/hr (max)
Rack Mountable	Sliding rack rails included

ENVIRONMENT	OPERATING	STORAGE
Temperature	32° F to 104° F 0° C to 40° C	-40° F to 158° F -10° C to 70° C
Relative Humidity	10% to 90% non-condensing	10% to 90% non-condensing
Altitude	0 to 9,843 ft at 95° F (3,000 m at 35° C)	0 to 15,000 ft at 95° F (4,570 m at 35° C)
MTBF M4600	50,843 hours @ 77° F (25° C)	
MTBF M5600	68,879 hours @ 77° F (25° C)	
MTBF Module	3,863,276 hours @ 77° F (25° C)	

STRONG SECURITY AT EVERY LAYER

Uniquely architected to be the industry's smartest, fastest, and most effective network security products, WatchGuard solutions deliver in-depth defenses against advanced malware, ransomware, botnets, trojans, viruses, drive-by downloads, data loss, phishing and much more.

MULTIPLE PURCHASE OPTIONS

The flexibility of WatchGuard's integrated platform makes it easy to have exactly the security components your business network requires. Whether you choose to start with the security basics or deploy a comprehensive arsenal of network defenses, we have bundled security services to match your requirements.

EXPERT GUIDANCE AND SUPPORT

An initial Support subscription comes with every Firebox M4600 and M5600 appliance. Standard Support, included in the Basic Security Suite, provides hardware warranty with advance hardware replacement, 24 x 7 technical support, and software updates. An upgrade to Gold level support is included in WatchGuard's Total Security Suite.

For details, talk to your authorized WatchGuard reseller or visit www.watchguard.com.

*Throughput rates are dependent on network interface modules selected for your M4600 or M5600 deployment. Details available at www.watchguard.com/module.

Throughput rates are determined using multiple flows through multiple ports and will vary depending on environment and configuration. Max firewall throughput tested using 1518 byte UDP packets based on RFC 2544 methodology. UTM throughput is measured using HTTP traffic with AV, IPS, and Application Control enabled. Contact your WatchGuard reseller or call WatchGuard directly (1.800.734.9905) for help determining the right model for your network. Visit www.watchguard.com/sizing to access the online product **Sizing Tool**.

U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 www.watchguard.com

WatchGuard Total Security

Complete network protection in a single, easy-to-deploy solution.

Total Security.

A stateful packet firewall, while essential, simply isn't enough anymore. The reality is that every network needs a full arsenal of scanning engines to protect against spyware and viruses, malicious apps and data leakage – all the way through ransomware, botnets, advanced persistent threats, and zero day malware. A true network security solution will address all aspects of threat prevention, detection, correlation, and response – today, and as those threats evolve. WatchGuard's award-winning network security platform not only provides the most complete suite of unified security controls on the market today, but has consistently been the first to offer solutions for addressing new and evolving network threats including, but not limited to, advanced malware and ransomware.

Total Simplicity.

It's more than just about security scanning engines, though. At WatchGuard, we believe simplicity is the key to successful adoption of technology. As such, all of our products are not only easy to initially configure and deploy, they are also designed with an emphasis on centralized management, making ongoing policy and network management simple and straightforward. Security is complex, managing it doesn't have to be.

Total Performance.

All businesses, regardless of size, need to pay attention to performance. Slow security scanning times can cripple a network's ability to handle high-volume traffic. Some companies are forced to decrease protection to keep performance strong, but WatchGuard solutions never make you choose between security and speed. Leveraging the power of multi-core processing, WatchGuard's platform is engineered to deliver the fastest throughput when it matters – with all security controls turned on. Our platform can run all scanning engines simultaneously for maximum protection while still maintaining blazing fast throughput.

Total Visibility.

From the board room to the branch office, critical decisions about security often need to be made quickly before damage is done. Furthermore, you need to know what's happening not just in the network, but on your devices inside and outside the firewall as well. Visibility is about more than data. Visibility is achieved when that data is converted into easily consumable, actionable information. The addition of the WatchGuard Host Sensor, available through Threat Detection and Response, provides continuous event monitoring, detection and remediation of threat activity on the endpoint. WatchGuard's award-winning network visibility platform, Dimension, takes the data from all devices across your network and presents that data in the form of visually stunning, immediately actionable information. Using Dimension you can identify behavioral trends, pinpoint potential network threats, block inappropriate use, monitor network health and much more.

Enterprise-Grade Security

Simplicity

Top Performance

Threat Visibility

Future-Proofed

WatchGuard Security Services

WatchGuard offers the most comprehensive portfolio of network security services, from traditional IPS, GAV, application control, spam blocking, and web filtering to more advanced services for protecting against advanced malware, ransomware, and the loss of sensitive data. WatchGuard also offers a full suite of network visibility and management services.

FUNDAMENTAL SECURITY SERVICES

INTRUSION PREVENTION SERVICE (IPS)

IPS uses continually updated signatures to scan traffic on all major protocols to provide real-time protection against network threats, including spyware, SQL injections, cross-site scripting, and buffer overflows.

REPUTATION ENABLED DEFENSE SERVICE (RED)

A powerful, cloud-based reputation lookup service that protects web users from malicious sites and botnets, while dramatically improving web processing overhead.

NETWORK DISCOVERY

A subscription-based service for Firebox appliances that generates a visual map of all nodes on your network so you can easily see where you may be at risk.

WEBBLOCKER URL FILTERING

In addition to automatically blocking known malicious sites, WebBlocker's granular content and URL filtering tools enable you to block inappropriate content, conserve network bandwidth, and increase employee productivity.

APPLICATION CONTROL

Selectively allow, block, or restrict access to applications based on a user's department, job function, and time of day and to then see, in real-time, what's being accessed on your network and by whom.

GATEWAY ANTIVIRUS (GAV)

Leverage our continuously updated signatures to identify and block known spyware, viruses, trojans, worms, rogueware and blended threats – including new variants of known viruses. At the same time, heuristic analysis tracks down suspicious data constructions and actions to make sure unknown viruses don't slip by.

SPAMBLOCKER

Real-time spam detection for protection from outbreaks. Our spamBlocker is so fast and effective, it can review up to 4 billion messages per day.

ADVANCED SECURITY SERVICES

APT BLOCKER – ADVANCED MALWARE PROTECTION

APT Blocker uses an award-winning next-gen sandbox to detect and stop the most sophisticated attacks including ransomware, zero day threats and other advanced malware.

DATA LOSS PREVENTION (DLP)

This service prevents accidental or malicious data loss by scanning text and common file types to detect sensitive information attempting to leave the network.

DIMENSION COMMAND

Dimension translates data collected from all appliances across your network into actionable network and threat intelligence. Dimension Command gives you the power to take action to mitigate those threats instantly, from one central console.

THREAT DETECTION AND RESPONSE

Correlate network and endpoint security events with enterprise-grade threat intelligence to detect, prioritize and enable immediate action to stop malware attacks. Improve visibility by evolving your existing security model to extend past prevention, to now include correlation, detection and response.

A Unified Approach to Network Security

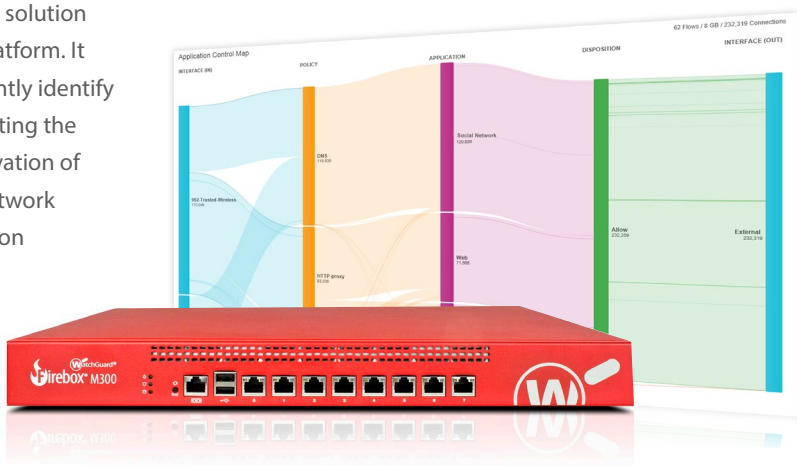
SMBs and Distributed Enterprises continue to fall victim to advanced threats that have serious impact on business operations and continuity regardless of existing security deployments. No single security control, of subset of controls, is sufficient. The more stages of an attack you're enabled to protect against, the more effective your overall defense is, even when new threats bypass one defense.

With Total Security Suite, organizations of all sizes can benefit from enterprise-grade prevention, detection, correlation and response from the perimeter to the endpoint. ThreatSync, our cloud-based threat correlation and scoring engine, collects network event data from several security services on the Firebox, including APT Blocker, Reputation Enabled Defense, Gateway AntiVirus and WebBlocker. correlated with threat activity detected via the WatchGuard Host Sensor and enterprise-grade threat intelligence to provide a unified view of your environment, and assign a comprehensive score based on threat severity.

Best of all, all of these security benefits are available through our extensive MSSP partner network via one simple offering with one SKU, one license, one appliance.

The Power of Visibility

WatchGuard Dimension is a cloud-ready network security visibility solution that comes standard with every WatchGuard's network security platform. It provides a suite of big data visibility and reporting tools that instantly identify and distill key network security threats, issues and trends, accelerating the ability to set meaningful security policies across the network. Activation of the Dimension Command feature unlocks access to a variety of network control features including, but not limited to, one-click configuration changes, the ability to jump back to previous configurations, direct access to individual appliances through a web UI, and VPN management tools. Knowledge is power and visibility provides knowledge.



"The main benefits for us have been moving from a basic stateful firewall to a full Layer 7 scanning platform. We managed to add IPS/IDS, application filtering, malware detection, Gateway AV, web filtering and all the other security features WatchGuard offers. In this one unit we have managed to combine a lot of security features, which as separate units would not make financial sense."

~ Peter Thomas
IT Manager, Roland UK

One Appliance, One Package, Total Security

Simplicity is our mission at WatchGuard and that mission extends beyond how the product is built to how it is packaged. While all of our services are offered à la carte, we have worked to develop two packages that simplify the decision-making process. The Total and Basic Security Suite packages are available on our Firebox T and M Series appliances, as well as our Firebox Cloud and FireboxV virtual models.

- The **Basic Security Suite** includes all of the traditional network security services typical to a UTM appliance: IPS, GAV, URL filtering, application control, spam blocking and reputation lookup. It also includes our centralized management and network visibility capabilities, as well as, our standard 24x7 support.
- The **Total Security Suite** includes all services offered with the Basic Security Suite plus advanced malware protection, data loss protection, enhanced network visibility capabilities, and the ability to take action against threats right from Dimension, our network visibility platform. It also includes upgraded Gold level 24x7 support.

Product	TOTAL SECURITY SUITE	Basic Security Suite
Intrusion Prevention Service (IPS)	✓	✓
App Control	✓	✓
WebBlocker	✓	✓
spamBlocker	✓	✓
Gateway AntiVirus	✓	✓
Reputation Enabled Defense (RED)	✓	✓
Network Discovery	✓	✓
APT Blocker	✓	
Data Loss Protection (DLP)	✓	
Dimension Command	✓	
Threat Detection & Response	✓	
Support	**Gold (24x7)**	Standard (24x7)

Getting Started

WatchGuard has the industry's largest network of value-added resellers and service providers. To get started, visit our website to find the best Partner for your business, or opt to contact us directly and we will answer any questions you may have and get you set up with the perfect Partner for your requirements.

- Browse our Partner network: **findpartner.watchguard.com**
- Speak with a WatchGuard security specialist: **www.watchguard.com/wgrd-sales/emailus**
- More information on How to Buy: **www.watchguard.com/totalsecurity**

About WatchGuard

WatchGuard has deployed nearly a million integrated, multi-function threat management appliances worldwide. Our signature red boxes are architected to be the industry's smartest, fastest, and meanest security devices with every scanning engine running at full throttle. Headquartered in Seattle, WA, WatchGuard has offices throughout North America, Europe, Asia Pacific, and Latin America. Visit **www.watchguard.com** for details, and check out our InfoSec blog, **Secplicity**, for real-time information about the latest threats and how to cope with them – in an easily understood and actionable way. Go to: **www.watchguard.com/secplicity**.

Datasheet

WatchGuard APT Blocker

DEFEND AGAINST ADVANCED MALWARE INCLUDING CRYPTOWALL AND CRYPTOLOCKER

Businesses that rely on antivirus software alone are no longer protected. What makes today's threats so dangerous is that they can easily morph into code that will slip by signature-based products looking for a recognizable malware pattern.

Next-Generation Sandbox for Full System Emulation

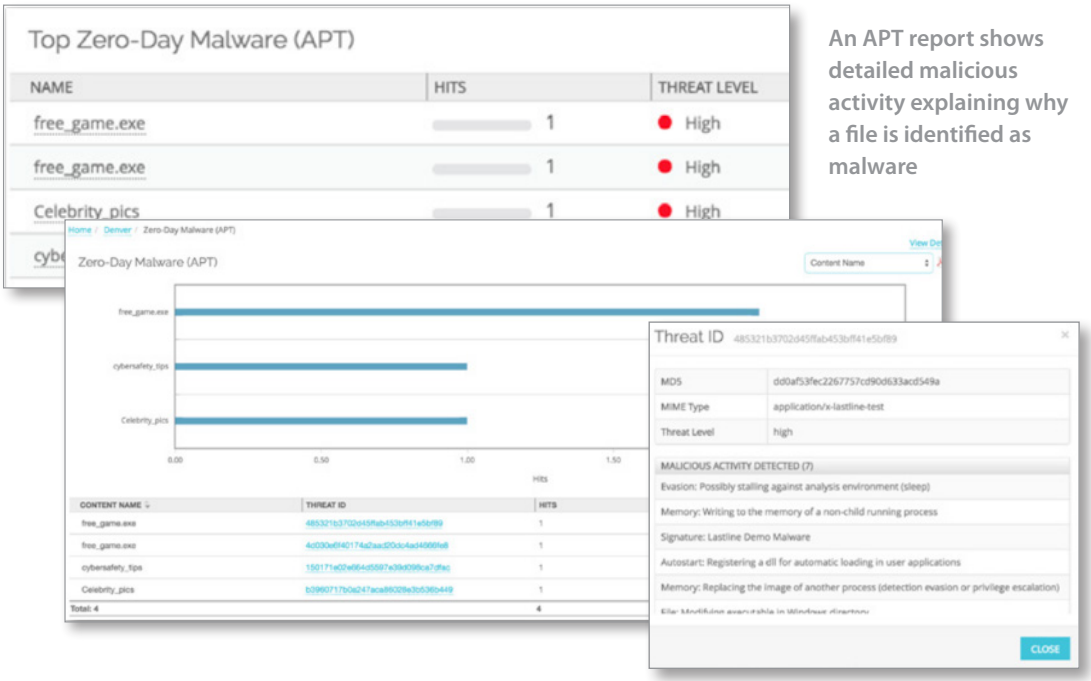
WatchGuard APT Blocker focuses on behavior analysis to determine if a file is malicious. APT Blocker identifies and submits suspicious files to a cloud-based next-generation sandbox, a virtual environment where code is analyzed, emulated, and executed to determine its threat potential.

Modern malware including Advanced Persistent Threats (APTs) is designed to recognized and evade traditional defenses. APT Blocker's full system emulation – which simulates the physical hardware including CPU and memory – provides the most comprehensive level of protection against malware. WatchGuard has partnered with Lastline Technology as the best-in-class partner for the APT Blocker service.

File Types Analyzed by APT Blocker

- Adobe PDF
- Rich Text Format
- Microsoft Office
- All Windows executable files
- Android executable files (.apk)
- Proxies including POP3

Not Just Detection, But Unparalleled Visibility



An APT report shows detailed malicious activity explaining why a file is identified as malware

ZERO DAY IS THE NEW BATTLEGROUND

Zero day attacks are those for which no software patch is available and no signature exists.

Signature-based antivirus solutions are still important as a first line of defense, eliminating known threats at the gateway.

APT Blocker extends protection from the universe of known malware to the unknown, securing your business from today's constantly evolving threats.

As far as attackers are concerned, **size doesn't matter**: **it's all about the information**.

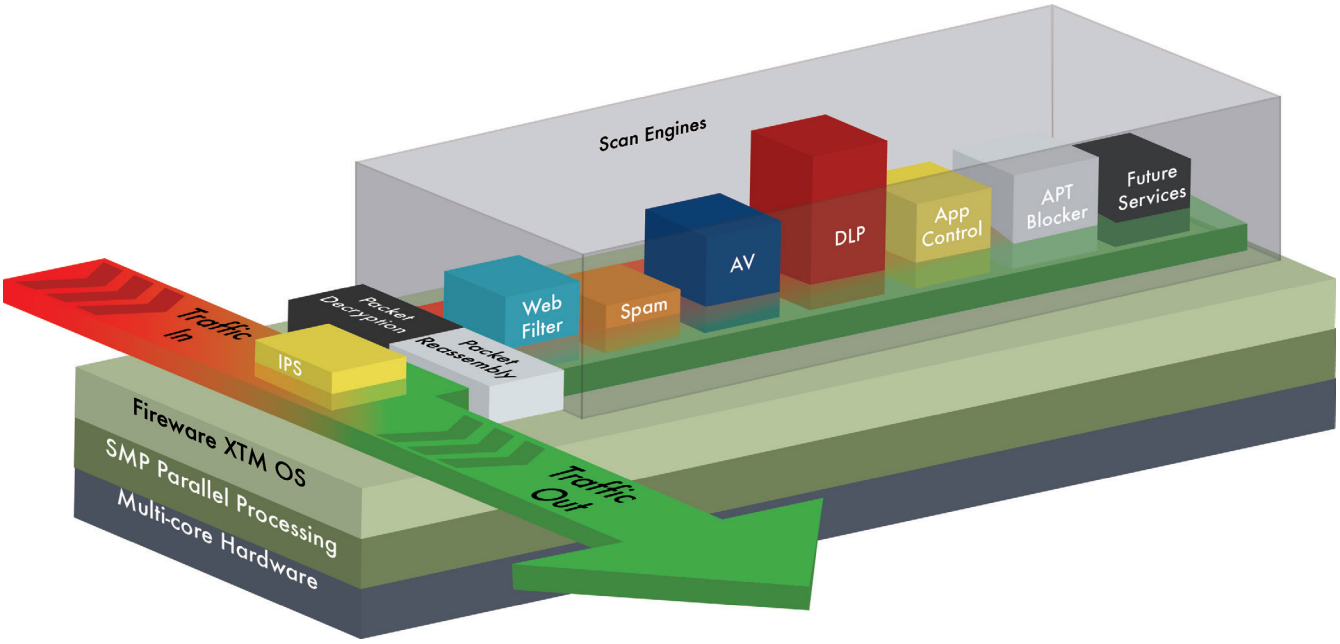
Securelist.com

FROST & SULLIVAN

2015 Global APT Protection for SMB New Product Innovation Award

APT Blocker not only provides a new level of protection against advanced malware, it does it in a way that's simple and intuitive. Thanks to WatchGuard Dimension™, which is included at no additional cost in every WatchGuard XTM and Firebox® solution, you have strong zero day protection, plus real-time visibility with easy-to-understand information about threats impacting your networks..

WATCHGUARD UTM PLATFORM



Flexible architecture blocks network threats while optimizing performance

WatchGuard's UTM (unified threat management) platform is designed to allow network traffic to pass through a full suite of security services — from anti-spam protection to Data Loss Prevention — at top performance levels. Leveraging the power of multi-core processing, the platform runs all scanning engines simultaneously for maximum protection and blazing fast throughput. Resources are allocated based on the flow of data and the security services that data requires. For example, if web filtering needs more horsepower, additional processors are automatically applied so web traffic keeps moving and your business stays secure.

MANAGING SUBSCRIPTIONS IS EASY

All security functionality on your WatchGuard Firebox or XTM solution, including security subscriptions, can be managed from a single intuitive console.

KNOW WHAT'S HAPPENING ON YOUR NETWORK AT ALL TIMES

- Any security activity identified by a service is logged and stored for easy reporting so you can take immediate preventive or corrective action.
- All management tools, including rich reporting and monitoring, are included with your WatchGuard firewall purchase. There is no additional hardware or software to buy.

HOW TO PURCHASE

WatchGuard security services are available in single and multi-year subscriptions. Contact your local authorized WatchGuard reseller for more information on how to add best-of-class defenses to your WatchGuard appliance, including bundled services and special promotions.

BEST-IN-CLASS UTM

WatchGuard uses a best-in-class strategy to create the most reliable security solutions on the market. By partnering with industry-leading technology vendors, WatchGuard delivers an all-star family of network security services.

- **AVG**—A consistently high performer in independent Virus Bulletin testing provides the engine for Gateway AntiVirus.
- **Cyren**—Patented RPD® technology in the Cloud provides spamBlocker with the only effective anti-spam solution for low footprint UTM appliances. Up to 4 billion messages per day reviewed.
- **Websense**—Supplies the cloud-based URL database for WebBlocker. Security coverage is supplemented by Websense Security Labs and their ThreatSeeker Network.
- **Trend Micro**—Leading provider of IPS and Application signatures, delivering comprehensive protection against the latest threats.
- **Sophos**—Leading provider of email and endpoint security, including DLP, for enterprises worldwide.
- **Lastline**—Provides the cloud-based, full system emulation analysis and advanced evasion detection that powers APT Blocker.

U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 www.watchguard.com

Threat Detection & Response

Correlate. Prioritize. Respond.

Cyber criminals are mounting attacks with increasing complexity and sophistication, using coordinated means to gain access to your network from any and every connection. Security measures must keep pace by adding detection capabilities across networks and endpoints, as well as the ability to correlate this event activity into targeted action. WatchGuard's Threat Detection and Response (TDR) service correlates network and endpoint security events with threat intelligence to detect, prioritize and enable immediate action to stop malware attacks. TDR enables small and midsize businesses and the Managed Security Service Providers (MSSPs) that support them to confidently remediate advanced malware attacks before business-critical data or organizational productivity is compromised.

Network and Endpoint Event Correlation

ThreatSync is WatchGuard's new cloud-based correlation and threat scoring engine, improving security awareness and response across the network to the endpoint. ThreatSync collects event data from the WatchGuard Firebox, WatchGuard Host Sensor and cloud threat intelligence feeds, and correlates this data to generate a comprehensive threat score to guide remediation.

Enterprise-grade Threat Intelligence

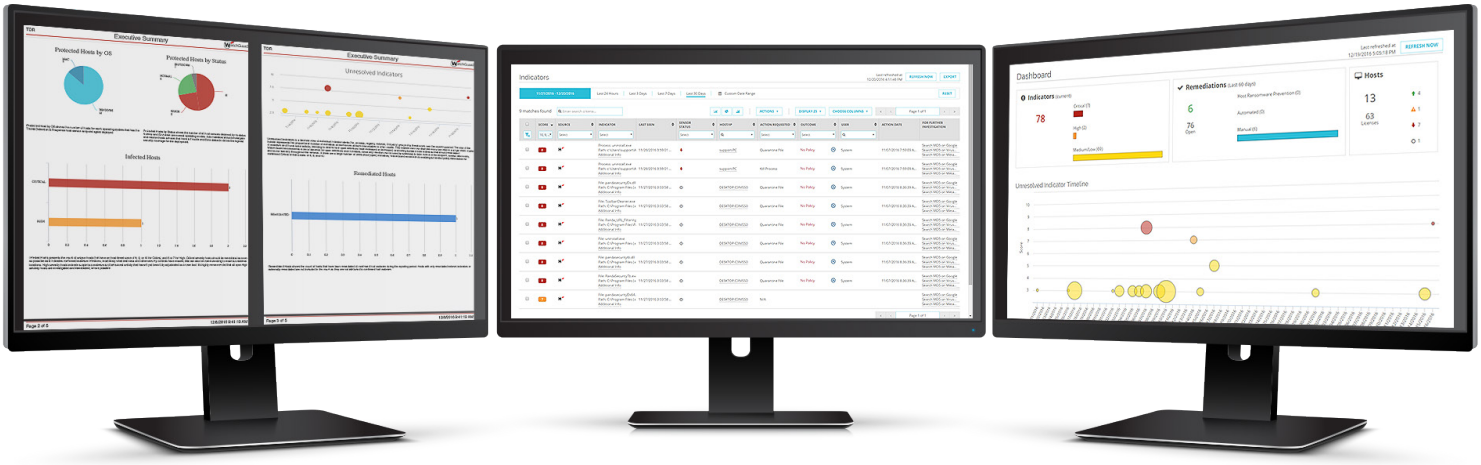
Threat Intelligence gathered from third-party vendors was previously only a benefit available to enterprise organizations with big budgets and even bigger security teams. With Threat Detection and Response, WatchGuard consumes and analyzes threat intelligence – delivering the security benefits without passing down the associated complexities or cost.

Extend Visibility to the Endpoint

The lightweight WatchGuard Host Sensor monitors and detects threat activity on your devices. The Host Sensor continuously sends these events to ThreatSync for correlation and scoring, receiving and executing the instructions for tactical remediation. Host Sensors are centrally managed from the cloud, making it easy for MSSPs and IT admins to deploy, update and manage host sensors anywhere in the world.

Advanced Ransomware Prevention

Host Ransomware Prevention (HRP) is a ransomware-specific module within the WatchGuard Host Sensor. HRP leverages a behavioral analytics engine and a decoy directory honeypot to monitor a wide array of characteristics that determine if a given action is associated with a ransomware attack or not. If the threat is malicious, HRP can automatically prevent a ransomware attack before file encryption on the endpoint takes place.



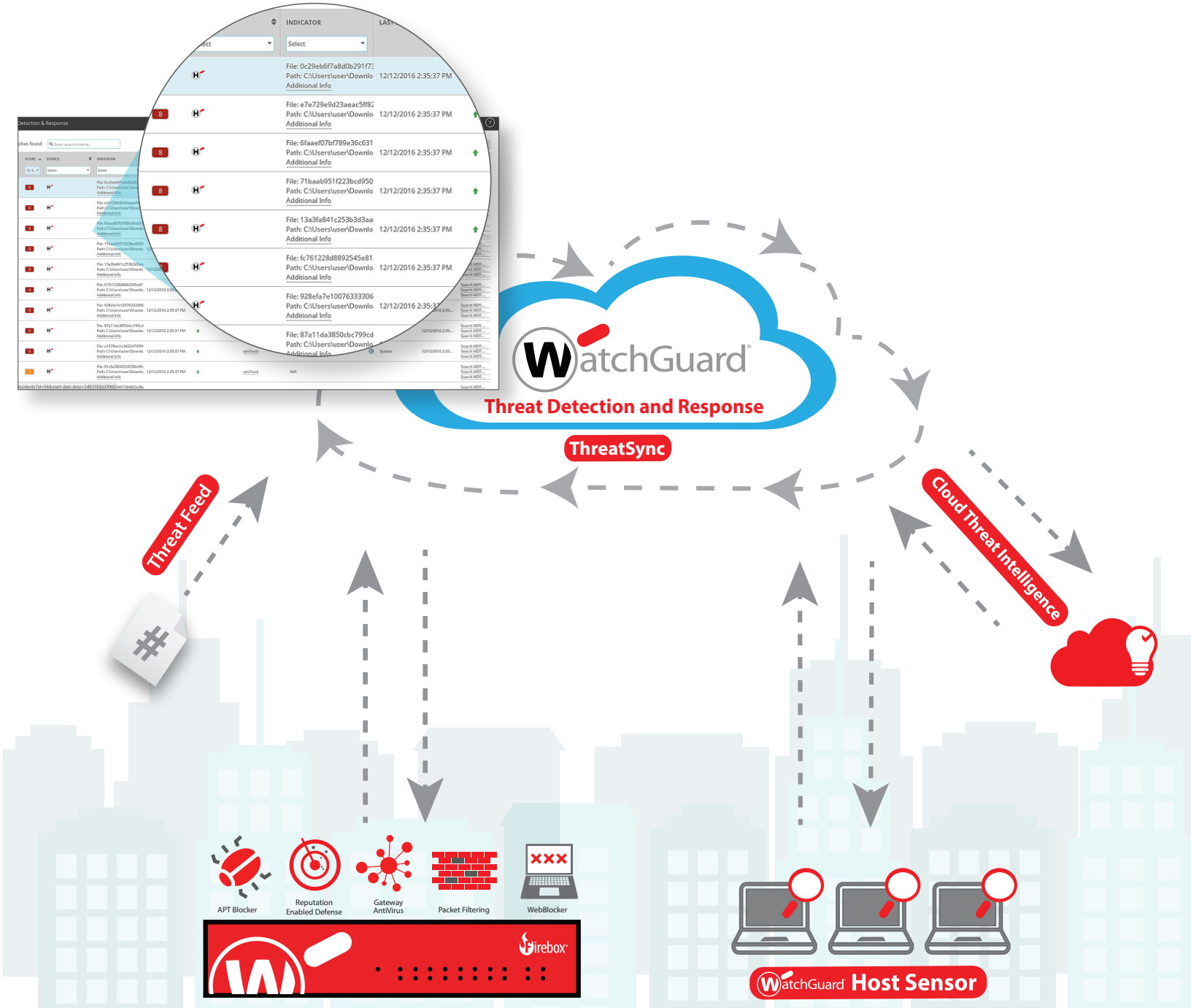
Improved Security with Correlation

ThreatSync, TDR's cloud-based correlation and threat scoring engine, improves security awareness and response across the network to the endpoint.

ThreatSync can collect network event data from several other security services on the Firebox, including APT Blocker, Reputation Enabled Defense (RED), Gateway AntiVirus and WebBlocker. These events are correlated with threat activity detected via the WatchGuard Host Sensor and enterprise-grade threat intelligence.

ThreatSync then analyzes this threat data to provide a comprehensive threat score and rank overall severity. Specific response actions will be transmitted back to the Host Sensor including quarantine file, kill process or delete registry value.

This proprietary technology not only decreases time to detection by enhancing visibility into threats on both the network and the endpoint, but ultimately empowers confident response by generating a comprehensive threat score to improve time to remediation.



One Appliance, One Package, Total Security

Threat Detection and Response is available through WatchGuard Total Security Suite, which also includes advanced security solutions like APT Blocker, WebBlocker, Gateway AntiVirus, Intrusion Prevention Service and Reputation Enabled Defense.

While each of these security solutions can defend against advanced threats, users benefit most when security defenses work in tandem, providing the strongest protection and maximum efficiency without impacting performance on the Firebox.

Product	Support	TOTAL SECURITY	Basic Security
Stateful Firewall	✓	✓	✓
Mobile VPN	✓	✓	✓
Branch Office VPN	✓	✓	✓
Application Proxies	✓	✓	✓
Intrusion Prevention Service (IPS)		✓	✓
App Control		✓	✓
WebBlocker		✓	✓
spamBlocker		✓	✓
Gateway AntiVirus		✓	✓
Reputation Enabled Defense (RED)		✓	✓
Network Discovery		✓	✓
APT Blocker		✓	
Data Loss Protection (DLP)		✓	
Dimension Command		✓	
Threat Detection & Response		✓	
Support	Standard (24x7)	**Gold (24x7)**	Standard (24x7)

Firebox Model	Included Host Sensors
T10	5
T30	20
T50	35
T70 / M200	60
M300	150
M400 / M440 / M500 / M4600 / M5600	250
Firebox Cloud / FireboxV S	50
Firebox Cloud / FireboxV M	250
Firebox Cloud / FireboxV L	250
Firebox Cloud / FireboxV XL	250

Need More Host Sensors?

Threat Detection and Response includes a set number of Host Sensors based on your Firebox M Series, T Series, Firebox Cloud or FireboxV model. Additional Host Sensors are available through an upgrade offering, as needed.

Host Sensor Add-On Options
10 Host Sensors
25 Host Sensors
50 Host Sensors
100 Host Sensors
250 Host Sensors
500 Host Sensors

Threat Detection and Response service includes a set number of Host Sensors, based on appliance model. Additional Host Sensors are available for purchase and add to overall host sensor quantity available to the account.

Manageable, Scalable Security

Threat Detection and Response enables users to easily scale and manage their security. The cloud-based service makes it easy for administrators and operators to quickly deploy Host Sensors across their entire organization, create policies and perform one-click remediation.

TDR can easily scale and grow with your business. While each instance of TDR includes a set number of Host Sensors based on an existing appliance, upgrade packages make it easy to add more Host Sensors to meet your organizational needs.

If managing security services isn't the best option for your organization's valuable time and resources, our extensive network of MSSP Partners enables you to leverage the benefits of Threat Detection and Response while they take care of the day-to-day operations.

Learn more about Threat Detection and Response. For more information on WatchGuard's newest security service, please visit our website at **www.watchguard.com/TDR**.

How to Get Started

WatchGuard has the industry's largest network of value-added resellers and service providers. To get started, visit our website to find the best partner for your business, or opt to contact us directly and we will answer any questions you may have and get you set up with the perfect partner for your requirements.

- Visit our "Find a Reseller" page to find a partner near you: **http://findpartner.watchguard.com**
- Speak with a WatchGuard security specialist: **www.watchguard.com/wgrd-sales/emailus**

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in network security, secure Wi-Fi, and network intelligence products and services to more than 75,000 customers worldwide. The company's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for Distributed Enterprises and SMBs. WatchGuard is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit watchguard.com.

DATASHEET

HOST SENSOR

Threat Detection and Response accessory for endpoint monitoring and remediation

As threats continue to evolve, it becomes increasingly important to protect every attack vector from the network to the endpoint. Part of WatchGuard's Total Security Suite, Threat Detection and Response (TDR) correlates network and endpoint security events with threat intelligence to detect, prioritize and enable immediate action to stop malware attacks. Visibility into the network is provided through WatchGuard Firebox® appliance, while endpoint event data is collected through the WatchGuard Host Sensor.

The WatchGuard Host Sensor continuously detects threats on the endpoint, receiving and executing response commands. Host Ransomware Prevention (HRP), a feature of the WatchGuard Host Sensor, along with the advanced malware protection provided through APT Blocker, enables industry-leading prevention against ransomware attacks. Host Ransomware Prevention blocks the execution of ransomware before file encryption on the endpoint takes place, mitigating the ransomware attack before any damage is done.

EXTEND VISIBILITY TO THE ENDPOINT

The lightweight WatchGuard Host Sensor monitors and detects threat activity on devices using heuristics and behavioral analytics. The Host Sensor continuously sends these events to TDR's ThreatSync to be correlated with events from the Firebox appliance, developing a comprehensive threat score prioritization.

AUTOMATED THREAT REMEDIATION

The WatchGuard Host Sensor enables users to automate threat remediation through the creation of policies. Based on the comprehensive threat score generated by ThreatSync, these pre-defined policies determine the response tactics triggered – including kill the process, quarantine file, or delete the registry value. Automated threat remediation can not only decrease the time it takes to remedy the problem, but also helps to minimize the demand on scarce resources.

ADVANCED RANSOMWARE PREVENTION

Host Ransomware Prevention is a ransomware-specific module within the WatchGuard Host Sensor. HRP leverages a behavioral analytics engine and a decoy directory honeypot to monitor a wide array of characteristics that determine if a given action is associated with a ransomware attack or not. If the threat is malicious, HRP can automatically prevent a ransomware attack before file encryption takes place.

FEATURES & BENEFITS

- Continuously monitors and detects endpoint threat events
- Decreases time to detection and remediation through automation
- Improves prevention of advanced malware attacks, including ransomware
- Pre-defined policies run automatically to kill the process, quarantine files, or delete the registry value
- The lightweight software agent consumes minimal processing resources
- Works alongside existing antivirus solutions already deployed

DATASHEET

Host Sensor Licensing

With a subscription for Total Security Suite, each appliance includes a set number of Host Sensors. These Host Sensors are managed and distributed within Threat Detection and Response, where they are aggregated for use throughout the account. To meet organizational needs, additional Host Sensors are available through an add-on offering.

Firebox Model	Included Host Sensors
T10	5
T30	20
T50	35
T70 / M200	60
M300	150
M400 / M440 / M500 / M4600 / M5600	250
Firebox Cloud / FireboxV S	50
Firebox Cloud / FireboxV M	250
Firebox Cloud / FireboxV L	250
Firebox Cloud / FireboxV XL	250

Host Sensor Add-On Options
10 Host Sensors
25 Host Sensors
50 Host Sensors
100 Host Sensors
250 Host Sensors
500 Host Sensors

HOST SENSOR SPECIFICATIONS:

Compatible operating systems –

- Windows 7, 8, 8.1, 10
- Windows Server 2008, 2012, 2016
- Linux RedHat/CentOS 6, 7

Compatible with Firebox T Series, M Series, Firebox Cloud, and FireboxV appliances.

WatchGuard Security Services

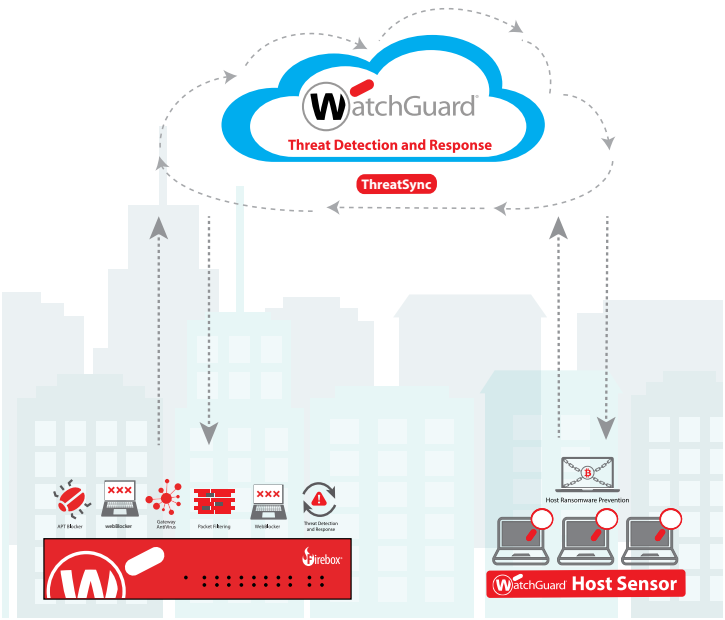
One Appliance, One Package, Total Security

Customers benefit most when security defenses work in tandem, providing the strongest protection, maximum efficiency and lightning-fast performance. WatchGuard's Total Security Suite provides customers traditional network security services, as well as advanced security offerings including APT Blocker, Data Loss Prevention and Threat Detection and Response (TDR).

TDR takes this philosophy a step further, by correlating event data from the network, endpoint and threat intelligence feeds to create a comprehensive threat score and rank. Our threat correlation and scoring engine, ThreatSync, collects input from advanced network security service, including WebBlocker, APT Blocker, Gateway AntiVirus and spamBlocker. It then correlates this network data with endpoint event data collected via the WatchGuard Host Sensor to generate a threat score and rank based on severity.

With WatchGuard Total Security Suite, organizations can benefit from advanced network security, robust endpoint visibility and remediation, as well as enterprise-grade threat intelligence through one complete offering.

Services	TOTAL SECURITY	Basic Security
Intrusion Prevention Service (IPS)	✓	✓
Application Control	✓	✓
WebBlocker (URL/Content Filtering)	✓	✓
spamBlocker (Anti-Spam)	✓	✓
Gateway AntiVirus (GAV)	✓	✓
Reputation Enabled Defense (RED)	✓	✓
Network Discovery	✓	✓
APT Blocker	✓	
Data Loss Prevention	✓	
Dimension Command	✓	
Threat Detection and Response (with WatchGuard Host Sensor)	✓	
Support	Gold (24x7)	Standard (24x7)



WatchGuard has the industry's largest network of value-added resellers and service providers. Browse our network of certified partners at **findpartner.watchguard.com. Learn more about Threat Detection and Response with WatchGuard Host Sensor at watchguard.com/TDR.**

U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 www.watchguard.com

DATASHEET

Support Program Overview

24 X 7 TECHNICAL SUPPORT

No matter which WatchGuard network security appliance you buy, your support needs will be covered 24 x 7 by our in-house team of highly trained technical experts.

HARDWARE WARRANTY

WatchGuard's hardware warranty includes advance hardware replacement to ensure that a replacement appliance is shipped immediately if a fault is identified.

SOFTWARE UPDATES

WatchGuard continually enhances the capabilities of its operating system software and services. Your Support license gives you access to all new releases at no cost.

Product	Standard Support	Gold Support	Platinum Support
Hours Per Day/Days Per Week	24 x 7	24 x 7	24 x 7
Cases Per Year of Service	unlimited	unlimited	unlimited
Targeted Response Time	4 Hour – Critical, High 8 Hours – Medium 24 Hours – Low	Live Call – Critical 1 Hour – High 4 Hour – Medium, Low	Live Call – All Phone Cases 1 Hour – All Web Cases All Cases Given Highest Priority
Advance Hardware Replacement	✓	✓	✓
Software Updates and Patches	✓	✓	✓
Technical Accounts Manager	–	–	✓
Quarterly Account Review	–	–	✓

PROBLEMS SOLVED

At WatchGuard we understand just how important support is when you are trying to secure your network with limited resources. You require greater knowledge and assistance in a world where security is becoming ever more critical and complex, and downtime can spell disaster.

Our Support program gives you the backup you need, starting with an initial subscription that supports you from the moment you activate your WatchGuard appliance.

HOW TO PURCHASE

All WatchGuard products come with a Support subscription. With three support levels available, you have the flexibility to select the level that best suits your business needs. Talk to your reseller for help choosing, or visit www.watchguard.com/support.

SECURITY SIMPLIFIED

Want to see WatchGuard's commitment to network security in action? Check out *Secplicity*, our InfoSec blog, dedicated to bringing security, IT, and business professionals real-time information about the latest threats and how to cope with them – and in an easily understood and actionable way. We invite you to visit the Secplicity community at www.watchguard.com/secplicity.

BENEFITS

- **Round-the-clock technical support** comes standard with all appliances.
- **There are no limits** on the number of Support cases allowed.
- **Important software updates.** Receive more than just the standard fixes and minor software patches. The Support program delivers feature enhancements, full-rev updates, and new capabilities as long as your Support subscription is active.
- **Platinum level support** allows enterprises with complex environments to have personalized service from a Technical Account Manager to help them achieve strategic goals with WatchGuard products.
- **Minimize downtime** in the rare case of a hardware failure. WatchGuard will ship a replacement via pre-paid, next-day airfreight in advance of receiving the returned appliance.
- **You never have to go it alone.** Additional Support offerings include Remote Installation Services and Premium 4-Hour RMA with continuous replacement coverage.

U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 www.watchguard.com

Datasheet

WatchGuard Dimension™

BRINGING BIG DATA VISIBILITY TO NETWORK SECURITY

From the board room to the branch office, the pace and complexity of decision-making about network security has been increasing. How can you ensure that your decisions are timely, effective, and better informed? You need **Visibility**.

DATA ANALYSIS IS THE KEY

Businesses are drowning in oceans of data, including network security data, making it nearly impossible to identify important security issues and make better policy decisions. The impact on regulatory compliance status can be devastating.

WatchGuard Dimension resolves these challenges by instantly turning raw network data into actionable security intelligence – in the big data visualization style today's users have come to expect.

"**Data in itself is not valuable** at all. The **value is in the analyses** done on that data and how the data is turned into information..."

Mark van Rijmenam, Big-Data Strategist

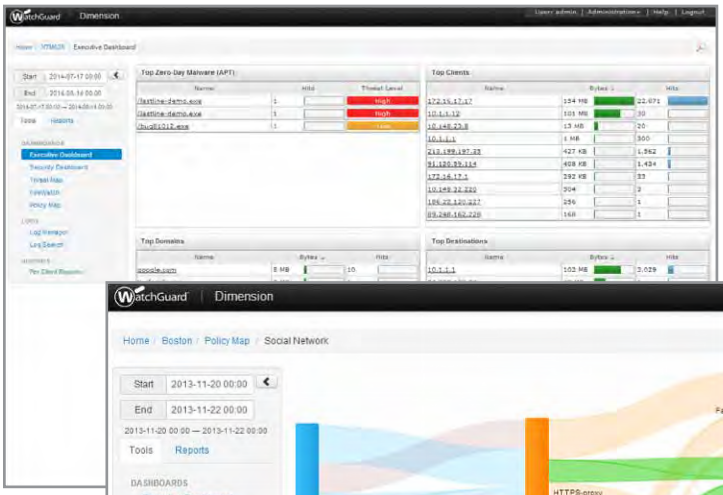
PUBLIC AND PRIVATE CLOUD-READY

WatchGuard Dimension™ is a cloud-ready network security visibility solution that comes standard with WatchGuard's flagship Unified Threat Management and Next Generation Firewall platform. It provides a suite of big data visibility and reporting tools that instantly identify and distill key security issues and trends, and deliver valuable insights to set meaningful security policies across the network.

The solution can be up and running in a few minutes and is easy to use and understand. You can quickly see any unusual network activity related to malware and threats, Internet usage, and bandwidth consumption at any time from anywhere using a web browser.

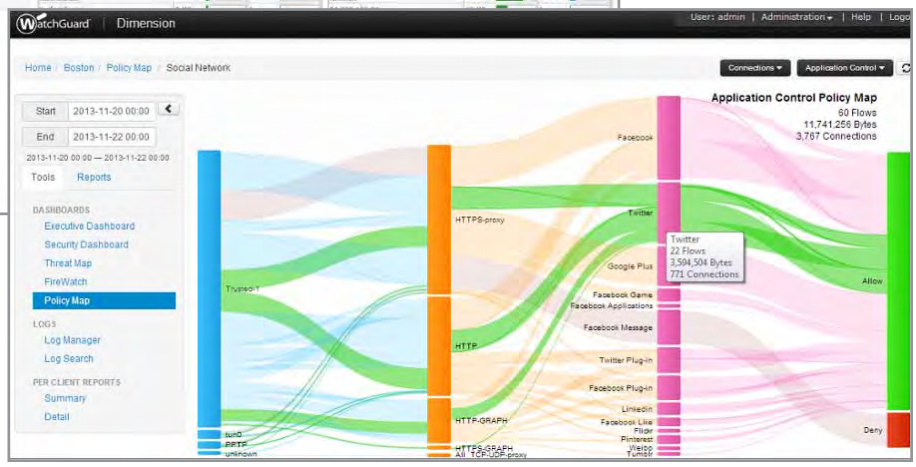
START WITH THE BIG PICTURE

Get a high-level view of network activity that pinpoints top trends, top clients, and correlated views of top users and applications. Then with just a click, you can drill all the way down to individual log data that reveals key details.



Executive Dashboard

Reviewing massive amounts of data makes effective analysis impossible. Organize your thoughts around crystal clear data points in the dashboard.



Policy Map

Policies are the brains of the firewall. Use Policy Map's integrated big picture views to find what policies are used, how they impact traffic flows, and whether they are as effective as intended. Policy Map makes it easier to find active and misconfigured policies and drill down as needed.

THE POWER OF VISUALIZATION

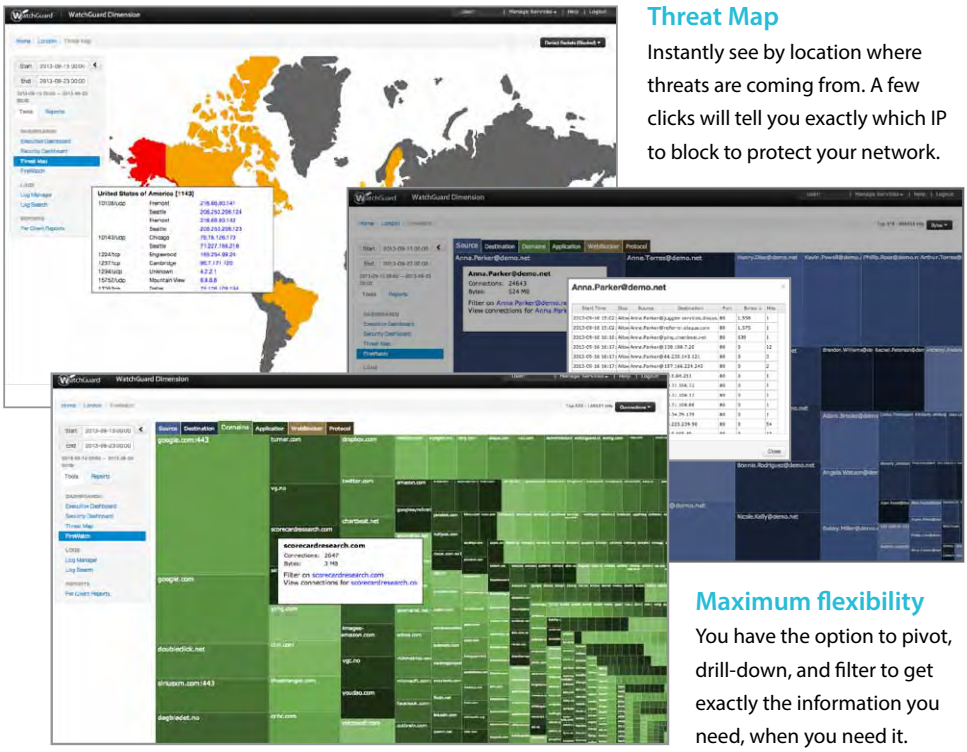
FireWatch filters traffic in a way that instantly highlights the most critical information on active users and connections.

FireWatch easily answers

- Who consumes the most bandwidth?
- Are there unusual traffic patterns?
- What is the most popular website visited?
- Which applications are used by specific workers?
- Which applications consume the most bandwidth?

ZERO INSTALL

No complicated setup required. Simply deploy a virtual appliance – includes OS, database, utilities, and WatchGuard server software.

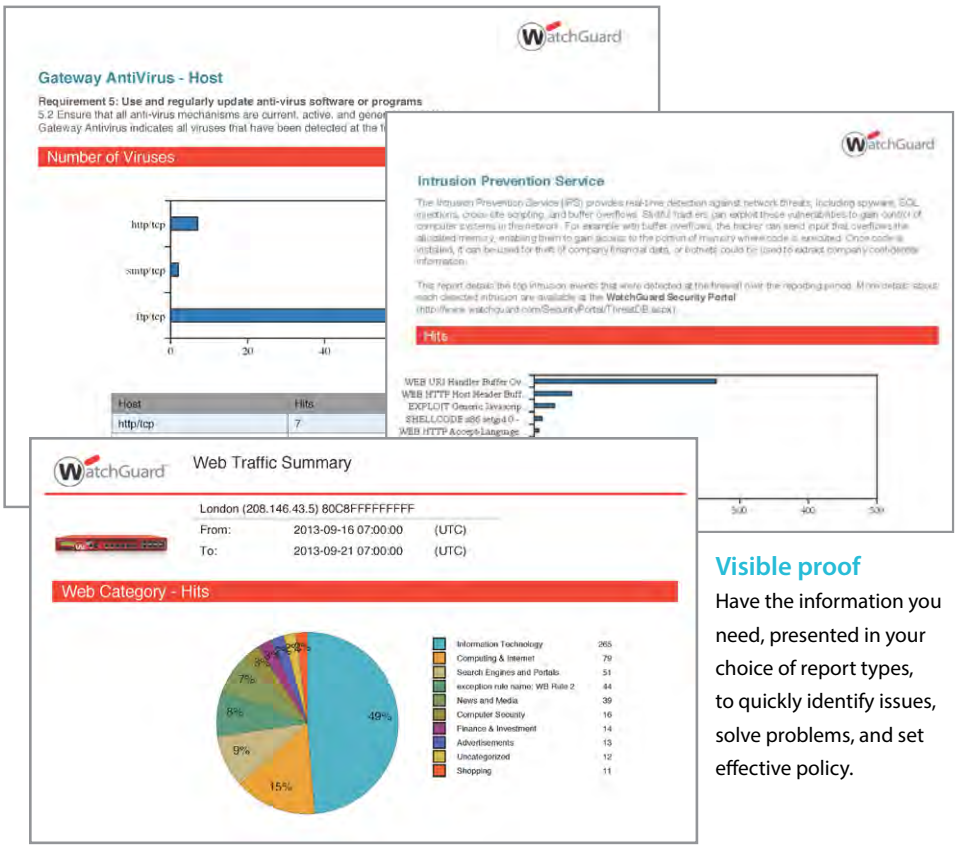


Threat Map

Instantly see by location where threats are coming from. A few clicks will tell you exactly which IP to block to protect your network.

Maximum flexibility

You have the option to pivot, drill-down, and filter to get exactly the information you need, when you need it.



Visible proof

Have the information you need, presented in your choice of report types, to quickly identify issues, solve problems, and set effective policy.

SPOT PATTERNS, MAKE BETTER DECISIONS

You can choose from more than 70 comprehensive reports, with the ability to pre-schedule reports for email delivery to key stakeholders in your organization. Options include summary and detail views, and special reports for HIPAA and PCI compliance. The Executive Report is a high-level summary tailored for C-level executives, IT directors, compliance officers, and small business owners.

NEW! DIMENSION COMMAND

Dimension Command is the new suite of management tools for WatchGuard Dimension. With it, IT pros don't just see what's happening on the network, they can take immediate action right from the dashboard. Contact your authorized WatchGuard reseller to see a demo and get details on an introductory one-year subscription promotion.

Seeing is believing.
Visit www.watchguard.com/dimension today to see more.

U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 www.watchguard.com

Secure, Cloud-Managed Wi-Fi

Secure, Simple, Intelligent.

Offering basic Wi-Fi access doesn't give you a competitive advantage, it offers you a chance to compete. With benefits ranging from increased productivity to improved customer satisfaction, implementing a wireless network for your employees and guests has become the table stakes of doing business. But Wi-Fi also opens your business to significant security risks, and can be complicated to deploy and manage, not to mention expensive. WatchGuard's Secure Wi-Fi Solution, a true game-changer in today's market, is engineered to provide a safe, protected airspace for your Wi-Fi environments, while eliminating administrative headaches and greatly reducing costs. With expansive engagement tools and visibility into business analytics, it delivers the competitive advantage your business needs to succeed.

Enterprise-Grade Wireless Intrusion Prevention System (WIPS)

Our cloud-managed access points have built-in WIPS to help ensure you have the protection you need. Using patented Marker Packet technology, WatchGuard WIPS defends your airspace from unauthorized devices, man-in-the-middle and denial-of-service attacks, rogue APs and more – and with close to zero false positives. For even greater protection, deploy our APs with a WatchGuard Firebox® to extend the Firebox's best-in-class UTM defenses, like application control and zero day malware protection, to your WLAN.

Management That Scales

With the WatchGuard Wi-Fi Cloud, IT pros can enjoy an entirely controller-less Wi-Fi management experience including setup, configuration, monitoring, troubleshooting, and improving corporate and guest Wi-Fi access, without worrying about the limitations of legacy controller infrastructure. Wi-Fi Cloud environments easily scale from one to an unlimited number of APs across multiple locations. APs can be grouped in many ways including location, building, floor, and customer to maintain consistent policies.

Performance Without Compromise

Incorporating the latest IEEE WLAN standards such as band steering, fast roaming, and quality of service (QoS) features, you'll have the most reliable and fast Wi-Fi experience, without sacrificing security. When managed by the Wi-Fi Cloud, WatchGuard APs come standard with RF optimization, spectrum monitoring, and trouble-shooting built in.

Engage with People and Gain Visibility into Business Analytics

The WatchGuard Wi-Fi Cloud delivers unprecedented visibility into every corner of your wireless environment, and beyond. Customizable dashboards and alerts provide a comprehensive overview and the ability to drill down for a more granular view. Business owners, now more than ever, need to leverage technology to get the most bang from their marketing budgets and have concrete data around site metrics like footfall, dwell time, and conversion to drive business decisions. Don't waste money on three separate products (for Wi-Fi access, splash pages, analytics), when WatchGuard's Wi-Fi Cloud gives you all three in one interface for all the business metrics you need to make the best decisions to grow.

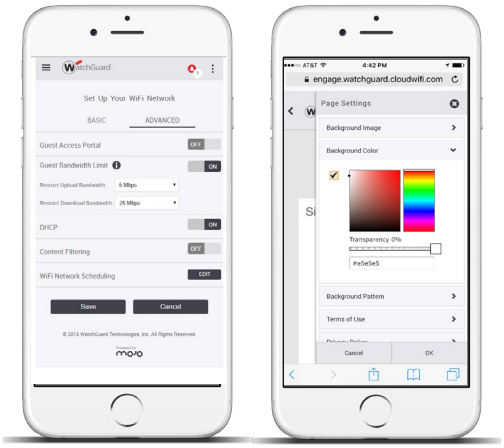
Flexible Management Options

WatchGuard offers two management scenarios to meet the needs of SMBs and distributed enterprises. You can manage all access points with either a Firebox®, via the Gateway Wireless Controller with lightweight feature set, or with WatchGuard's Wi-Fi Cloud. And with the Wi-Fi Cloud you get an expanded set of features including strong WIPS security, marketing tools, and location-based analytics for optimal business insights. And for ultimate peace of mind, rely on a Firebox UTM-protected network with WatchGuard Wi-Fi Cloud-managed APs to realize the full marketing and security potential of a cloud-managed access point solution.

	Features	Wi-Fi Cloud +UTM	Wi-Fi Cloud	UTM Wi-Fi
SECURITY	Total UTM Protection	✓		✓
	Patented Wireless Security and Threat Prevention	✓	✓	
	Friendly Wi-Fi Compliant (URL FIltering)	✓	✓	✓
	Location of Client Devices, Rogue APs	✓	✓	
ENGAGEMENT	Analytics (Footfall, VIsit History, Frequency, Dwell Time)	✓	✓	
	Mobile-Friendly Captive Portals	✓	✓	
	Social Wi-FI	✓	✓	
SIMPLIFIED MANAGEMENT	Cloud-Managed 'controllerless'	✓	✓	
	GO Mobile Web App	✓	✓	
	Location-based Templates	✓	✓	

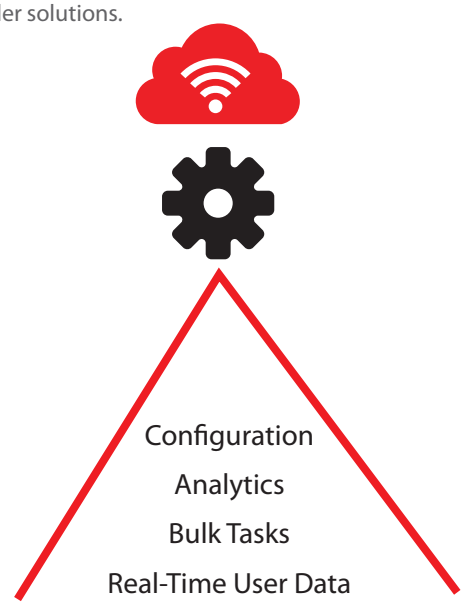
GO Mobile Web App

The GO mobile web experience allows you to manage your wireless networks using any mobile device. Managing customer engagement is entirely integrated with standard features enabling simple setup of customized splash pages and personalized customer promotions.



RESTful API

WatchGuard Wi-Fi Cloud is built from the ground up on RESTful APIs to handle even the largest WLAN networks that, until now, would need to be served by on-premises WLAN controller solutions.



WatchGuard Access Points

AP120

The AP120 is the affordable option when optimum performance is needed in a small space or where fewer devices are connected. It is an indoor 2x2 MIMO 802.11ac access point with dual concurrent radios, two spatial streams, and data rates up to 866 Mbps. This is a great alternative for small branch offices, stores, and classrooms.

AP320

This is a high-horsepower access point that can support critical applications like voice, video and cloud with ease. The AP320 is an indoor 3x3 MIMO 802.11ac access point with dual concurrent band radios, three spatial streams, and data rates up to 1.3 Gbps. It's the natural choice when deploying in offices, classrooms and meeting spaces.

AP322

The AP322 is a ruggedized 3x3 MIMO 802.11ac outdoor access point with dual concurrent 5 GHz and 2.4 GHz band radios supporting 802.11a/n/ac, 802.11b/g/n, three spatial streams, and data rates of up to 1.3 Gbps and 450 Mbps, respectively. The AP322 delivers broad, fast, and reliable Wi-Fi coverage – making it ideal for stadiums and sports fields, schools/universities, malls, parks, hotel pool areas and open air cafes, shipping docks, warehouses and other harsh or outdoor locations.

Manage any of these AP models for expanded features including strong WIPS security, marketing tools and location based analytics for enhanced business insights.

"We've found that the dashboard within the WatchGuard Wi-Fi Cloud product has made it much easier for our limited IT staff to deploy new access points, to understand the functionality of the existing access points, and to understand the true needs of our guests."

~ Hunter Hughes, Director of IT, Museum of Flight

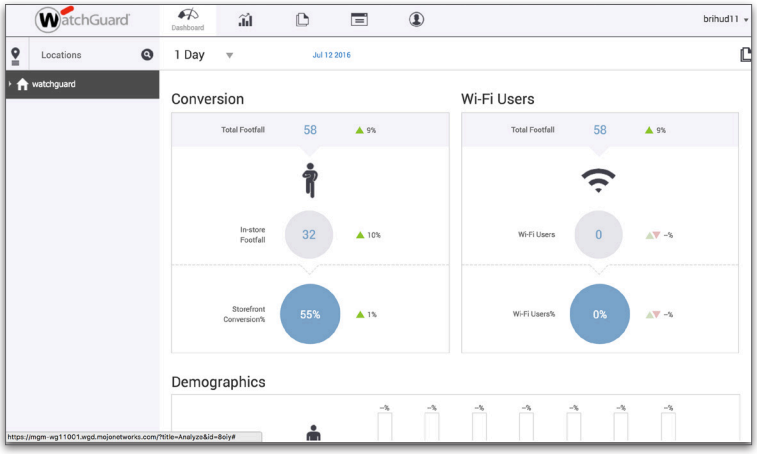
WATCHGUARD SECURE, CLOUD-MANAGED WI-FI

Reach Out to Mobile Users

Turn your Wi-Fi environment into a potent source of revenue and customer loyalty by leveraging the combined benefits of secure cloud-managed Wi-Fi, captive portal technology, and social media interaction. Use splash pages like the one at right to grab the attention of today's mobile and connected consumers, engage them with videos, polls and surveys, and then take advantage of built-in analytics tools to better understand their habits and preferences.

Powerful Engagement & Analytics Tools

Gain actionable insights into customers with social login analytics. In combination with the social Wi-Fi features, data can be used to analyze demographic information including gender, age, and customer buying tendencies. Wi-Fi device location, customer dwell time, footfall, and new vs. repeat users can be captured with zone-based analytics. Dashboards and reports allow administrators to quickly view analytics at all levels, from the highest to the most granular view, across time segments and location groups - and there are no hidden third party costs.



Find out more

WatchGuard has the industry's largest network of value-added resellers and service providers. To get started, visit our website to find the best Partner for your business, or opt to contact us directly and we will answer any questions you may have and get you set up with the perfect Partner for your requirements.

- Browse our Partner network: **findpartner.watchguard.com**
- Speak with a WatchGuard security specialist: **www.watchguard.com/wgrd-sales/emailus**

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in network security, providing best-in-class Unified Threat Management, Next Generation Firewall, secure Wi-Fi, and network intelligence products and services to more than 75,000 customers worldwide. The company's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for Distributed Enterprises and SMBs. WatchGuard is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit **watchguard.com**.

DATASHEET

AP322 OUTDOOR ACCESS POINT

IP67-rated enclosure, 3x3 MIMO, 802.11ac wave 1 support

6 integrated antennas, 2 GbE ports, PoE+

WatchGuard's AP322 brings secure, cloud-managed Wi-Fi to the outdoors. Its rugged, IP67-rated enclosure protects the wireless access point from the wind, rain, and cold weather, while six integrated omnidirectional antennas operate with three spatial streams per radio (3x3 MIMO) to deliver broad, fast, and reliable Wi-Fi coverage. The AP322 is ideal for stadiums and sports fields, schools/universities, malls, parks, hotel pool areas and open air cafes, shipping docks, warehouses, and other harsh environments or outdoor locations.

"We've found that the dashboard within the WatchGuard Wi-Fi Cloud product has made it much easier for our limited IT staff to deploy new access points, to understand the functionality of the existing access points, and to understand the true needs of our guests."

~ Hunter Hughes, Director of IT, Museum of Flight

FLEXIBLE MANAGEMENT OPTIONS

You can manage AP322 access points with either a Firebox®, via the Gateway Wireless Controller with lightweight feature set, or with WatchGuard's Wi-Fi Cloud. And with the Wi-Fi Cloud you get an expanded set of features including strong WIPS security, marketing tools, and location-based analytics for optimal business insights.

PERFORMANCE WITHOUT COMPROMISE

Incorporating the latest 802.11ac standards, you'll have speeds of up to 1.3 Gbps over the air, without sacrificing security. When managed by the Wi-Fi Cloud, WatchGuard APs come standard with RF optimization, spectrum monitoring, and trouble-shooting built in.

UNIQUELY EFFECTIVE APPROACH TO SECURITY

Using patented Marker Packet technology, WatchGuard's cloud-managed WIPS (Wireless Intrusion Prevention System) defends your airspace from unauthorized devices, man-in-the-middle and denial-of-service attacks, rogue APs and more. As a dedicated WIPS sensor, the AP322 can be added to any existing Wi-Fi network for a powerful layer of patented security features simply unavailable in most AP devices.

ADVANTAGES OF CLOUD-BASED MANAGEMENT

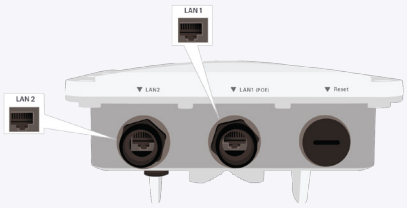
WatchGuard's secure cloud-managed APs deliver the most comprehensive set of features for the price – including marketing tools for customizable user engagement and location-based analytics for enhanced business insights. With the WatchGuard Wi-Fi Cloud, IT pros can enjoy an entirely controller-less Wi-Fi management experience including setup, configuration, monitoring, troubleshooting, and improving corporate and guest Wi-Fi access, without worrying about the limitations of legacy controller infrastructure. Wi-Fi Cloud environments easily scale from one to an unlimited number of APs across multiple locations. APs can be grouped in many ways including location, building, floor, and customer to maintain consistent policies.

FEATURES & BENEFITS

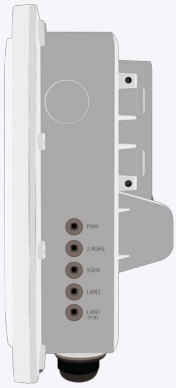
- Support for up to 8 individual SSIDs per radio allows for maximum flexibility in network design.
- The IP67 sealed enclosure protects APs in harsh, wet outdoor environments so they can be mounted with direct exposure to the elements – no overhang or shelter required.
- AP322 devices can be converted to a dedicated security sensor with a single click for maximum wireless protection.
- Manage with Wi-Fi Cloud for expanded features including strong WIPS security, marketing tools and location-based analytics for enhanced business insights.
- Patented Marker Packet technology is used to accurately detect authorized, unauthorized, and external access points on any network with the fewest false positives in the industry.
- Supports self-healing and bridge-mode wireless meshing for optimal installation scenarios.

PHYSICAL SPECIFICATIONS

Property	Specification
Physical Dimensions	8.26" x 8.26" x 2.6378" (210 mm x 210 mm x 67 mm)
Weight	3.22 lb. (1.46 kg)
Operating Temperature	-20°C to 55°C (-4°F to 131°F)
Storage Temperature	-40°C to 70°C (-40°F to 158°F)
Humidity	5% to 95% non-condensing
Max power consumption	17.4W (DC plug) | 19W (802.3at)



Bottom View



Side View

Port	Description	Connector Type	Speed/Protocol
LAN1	Gigabit Ethernet port that enables the device to connect to the wired LAN and communicate with the WatchGuard Cloud or Server. This port is also used to power the device using the 802.3at Power over Ethernet Plus (PoE+) standard.	IP67 rated weatherproof RJ-45	10/100/1000 Mbps Gigabit Ethernet 802.3at PoE+
LAN2	Gigabit Ethernet port that can be used for wired extension of an SSID	IP67 rated weatherproof RJ-45	10/100/1000 Mbps Gigabit Ethernet
Reset	Reset to factory default settings	Push button	Hold down an power cycle the device to reset

WI-FI SPECIFICATIONS – Frequency, Modulation, and Data Rates

IEEE 802.11b/g/n			
Frequency Band	Scanning	Transmission	
	All regions	USA & Canada (FCC/IC)	Europe (ETSI)
	2400 ~ 2483.5 MHz	2400 ~ 2473.5 MHz	2400 ~ 2483.5 MHz
Modulation Type	DSSS, OFDM		
Data Rates	Up to 450 Mbps (MCS 0-23) with automatic rate adaptation		
Antenna	Integrated modular high efficiency PIFA omnidirectional antenna with peak gain up to 7.5dBi		

IEEE 802.11a/n/ac			
Frequency Band	Scanning	Transmission	
	All regions	USA & Canada (FCC/IC)	Europe (ETSI)
	5.15 ~ 5.25 GHz 5.25 ~ 5.35 GHz 5.47~ 5.725 GHz 5.725~ 5.825 GHz	5.15 ~ 5.25 GHz 5.25 ~ 5.35 GHz 5.725~ 5.825GHz	5.15 ~ 5.25 GHz 5.25 ~ 5.35 GHz 5.47~ 5.725 GHz
Dynamic Frequency Selection	DFS and DFS2		
Modulation Type	OFDM		
Data Rates	Up to 1.3 Gbps (MCS 0-23) with automatic rate adaptation		
Antenna	Integrated modular high efficiency PIFA omnidirectional antenna with peak gain up to 10.2dBi		

MAXIMUM TRANSMIT POWER – FOR 2.4TGHZ

Transmitter	Target Power(Bm)
802.11b	
1 ~ 2 Mbps	24
5.5 ~ 11 Mbps	24
802.11g	
6 ~ 24 Mbps	24
36 Mbps	23
48 Mbps	22
54 Mbps	22
802.11n HT20	
MCS 0,8,16	24
MCS 1,2,3,4,5,9,10,11,12,13,17,18,19,20,21	23
MCS 6,7,14,15,22,23	22
802.11n HT40	
MCS 0,1,2,3,4,5,8,9,10,11,12,13,16,17,18,19,20,21	23
MCS 6,7,14,15,22	22
MCS 23	21

COUNTRY-WISE MAX TRANSMIT POWERS (DBM)

Countries	2.4GHz	5Ghz
Australia	20	23
Canada	30	23
India	20	20
Israel	20	20
Japan	20	20
UAE	20	17
USA	20	23

Note:
The actual transmit power will be the lowest of:

- Value specified in the Device Template
- Maximum value allowed in the regulatory domain
- Maximum power supported by the radio

For 5GHz

Transmitter	Target Power(dBm)
802.11a	
6 ~ 24 Mbps	24
36 Mbps	23
48 Mbps	22
54 Mbps	22
802.11n HT20	
MCS 0,8,16	24
MCS 1,2,9,10,17,18	23
MCS 3,4,5,11,12,13,19,20,21	22
MCS 6,14,22	21
MCS 7,15,23	20
802.11n HT40	
MCS 0,8,16	23
MCS 1,2,9,10,17,18	22
MCS 3,4,5,6,11,12,13,14,19, 20,21	21
MCS 7,15,22	20
MCS 23	19
802.11ac VHT20/VHT40	
MCS 0,1,2	23
MCS 3,4,5	22
MCS 6	21
MCS 7	20
MCS 8	18
MCS 9	17
802.11ac VHT80	
MCS 0,1,2	22
MCS 3,4,5	21
MCS 6	20
MCS 7	19
MCS 8	17
MCS 9	16

Receive Sensitivity – For 5GHz

MCS Index	Receive Sensitivity
802.11a (legacy)	
6Mbps	-91
36Mbps	-78
48Mbps	-75
54Mbps	-73
802.11n HT20 (legacy)	
MCS 0,8	-91
MCS 1,9	-88
MCS 2,10	-85
MCS 3,11	-81
MCS 4,12	-77
MCS 5,13	-74
MCS 6,14	-72
MCS 7,15	-71
802.11n HT40	
MCS 0,8	-87
MCS 1,9	-85
MCS 2 ,10	-82
MCS 3,11	-78
MCS 4,12	-74
MCS 5,13	-70
MCS 6,14	-69
MCS 7,15	-68
802.11ac 256QAM VHT80	
MCS 0	-84
MCS 1	-82
MCS 2	-79
MCS 3	-75
MCS 4	-71
MCS 5	-67
MCS 6	-66
MCS 7	-65
MCS 8	-60
MCS 9	-58

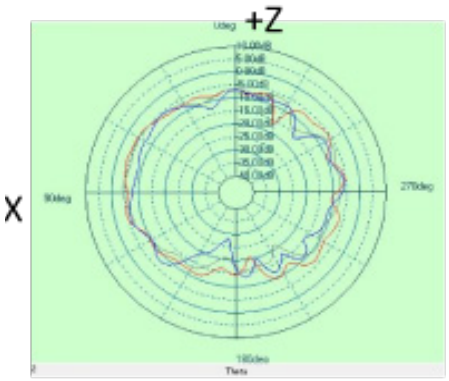
For 2.4GHz

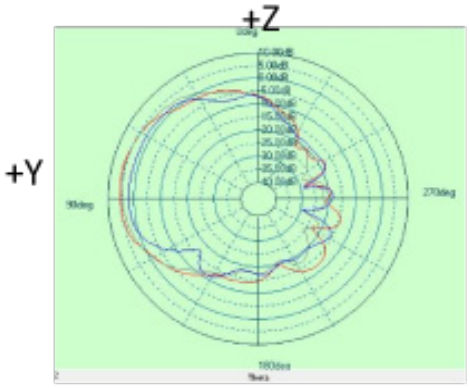
MCS Index	Receive Sensitivity
802.11b	
1Mbps	-94
11Mbps	-86
802.11g	
6Mbps	-90
24Mbps	-81
36Mbps	-78
48Mbps	-74
54Mbps	-73
802.11n HT20	
MCS 0,8	-90
MCS 1,9	-87
MCS 2,10	-84
MCS 3,11	-80
MCS 4,12	-77
MCS 5,13	-73
MCS 6,14	-71
MCS 7,15	-69
802.11n HT40	
MCS 0,8	-86
MCS 1,9	-84
MCS 2,10	-81
MCS 3,11	-77
MCS 4,12	-74
MCS 5,13	-70
MCS 6,14	-68
MCS 7,15	-66

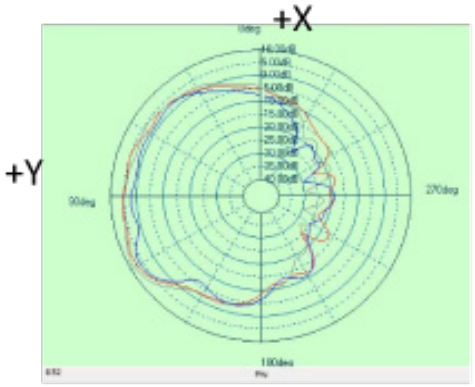
INTERNAL ANTENNA RADIATION PATTERNS

5 GHz

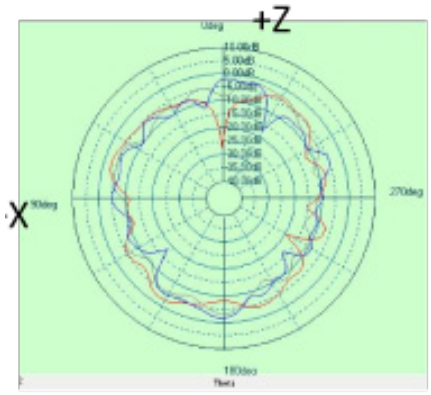
Antenna 1

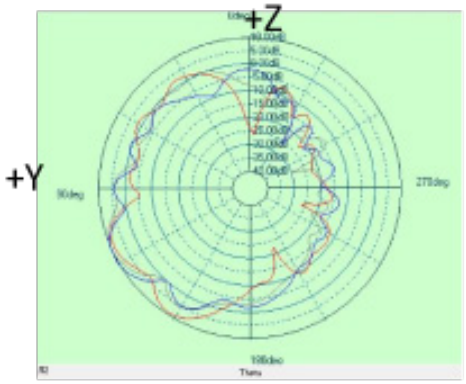


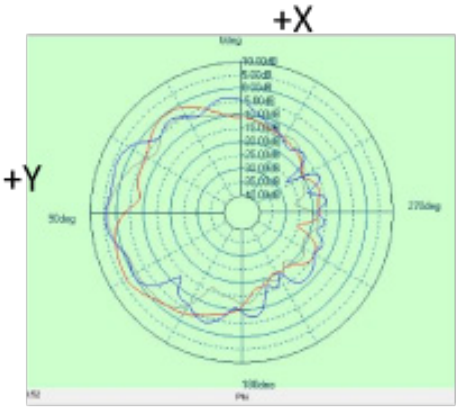




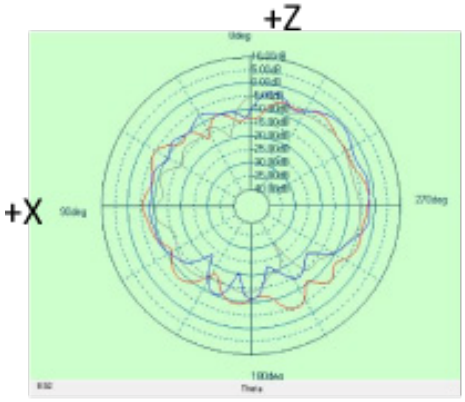
Antenna 2

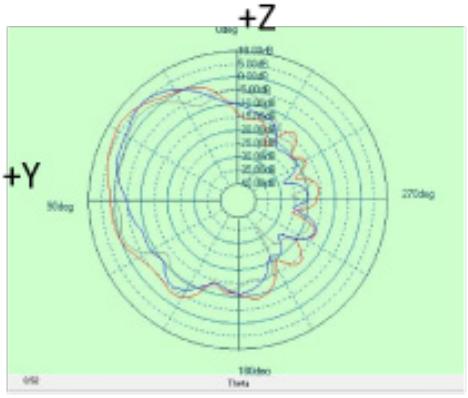


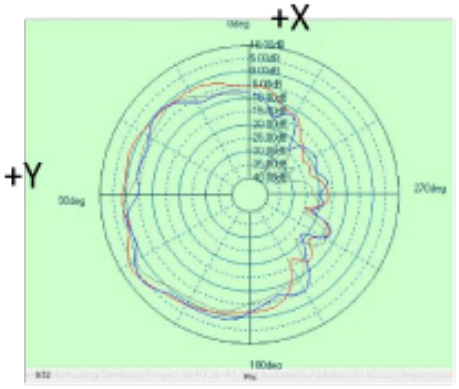




Antenna 3

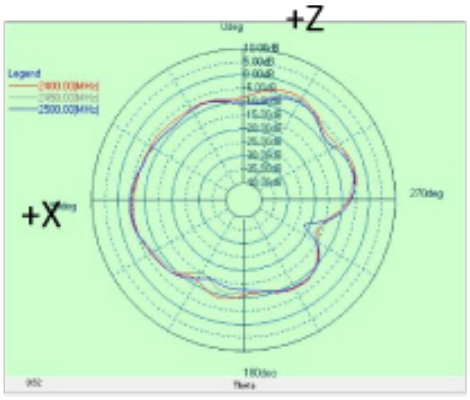


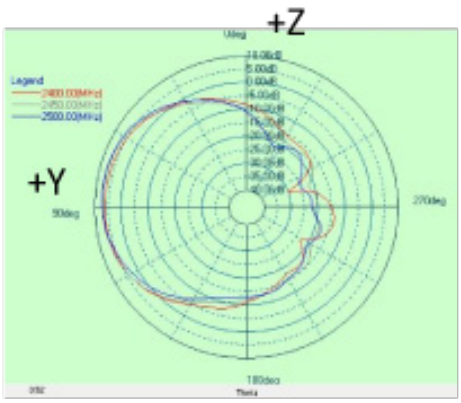


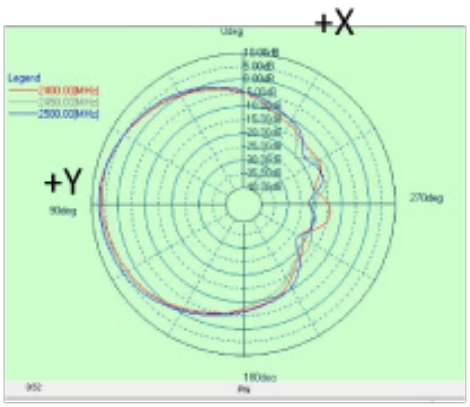


2.4 GHz

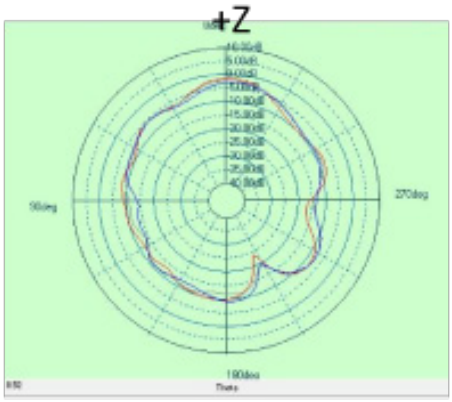
Antenna 1

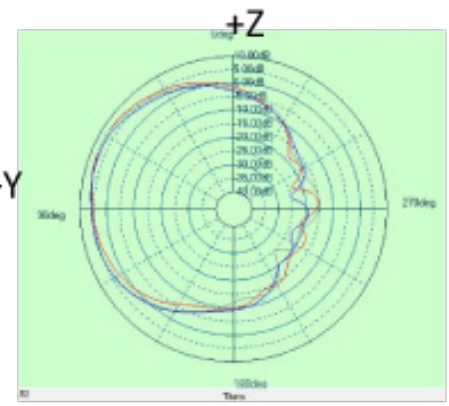


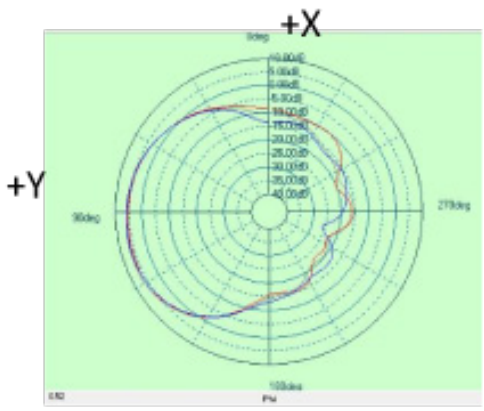




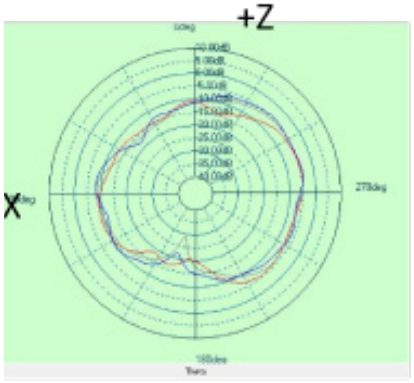
Antenna 2

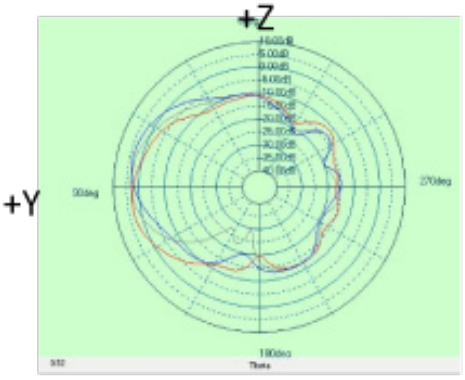


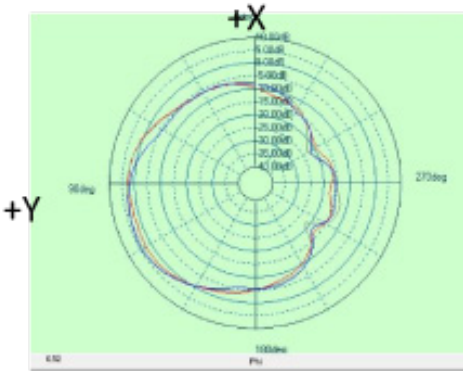




Antenna 3







Access Point Security Modes:

- WPA/WPA2 (802.11i) with TKIP or AES-CCMP encryption and PSK or 802.1x authentication
- Integrated WIPS background wireless scanning and Rogue AP prevention

WIPS Sensor Mode:

- Dedicated dual-band WIPS scanning for complete 24/7 protection from wireless threats

REGULATORY SPECIFICATIONS

RF and Electromagnetic

Country	Certification
USA	FCC Part 15.247, 15.407
Canada	IC
Europe	CE EN300.328, EN301.893 Countries covered under Europe certification: Austria, Belgium, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Iceland, Luxembourg, Latvia, Lithuania, Malta, Netherlands, Norway, Poland, Portugal, Spain, Sweden, Slovakia, Slovenia, Switzerland, The Czech Republic, UK.

Safety

Country	Certification
USA	UL 60950
Canada	cUL 60950
European Union (EU)	EN 60950, RoHS

WATCHGUARD HAS YOU COVERED, INDOORS AND OUT

Secure, Simple, Intelligent Wi-Fi Solution

A full suite of cloud-ready secure wireless access points for delivering blazing fast Wi-Fi, without compromising your network.

The **AP322** is your ideal solution for the outdoors. This access point features a rugged IP67-compliant exterior and delivers broad, fast, and reliable Wi-Fi coverage. Designed to bring Wi-Fi to stadiums, schools, outdoor cafes, shipping docks, warehouses, and more, AP322 has you covered.

The **AP320** is perfect for busy environments with diverse client ecosystem and Wi-Fi requirements. This high-horsepower AP can support critical applications like voice, video, and cloud with ease. Common deployment scenarios include offices, classrooms, and meeting spaces.

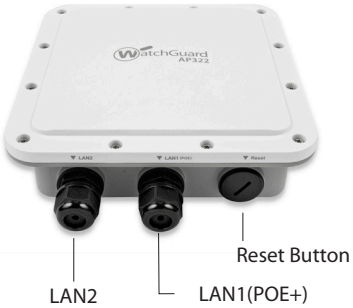
The **AP120** is built for networks with heavy smartphone and tablet access such as guest or public Wi-Fi environments, or smaller-footprint locations that support limited devices. Common deployment scenarios include branch offices, stores, and small classrooms.

For details, talk to your authorized WatchGuard reseller or visit **www.watchguard.com**.

About WatchGuard Technologies, Inc.

WatchGuard® Technologies, Inc. is a global leader in network security, providing best-in-class Unified Threat Management, Next Generation Firewall, secure Wi-Fi, and network intelligence products and services to more than 75,000 customers worldwide. The company's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for Distributed Enterprises and SMBs. WatchGuard is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit **watchguard.com**.

AP322



DATASHEET

AP320 INDOOR ACCESS POINT

3x3 MIMO, 802.11ac wave 1 support, 6 integrated antennas

2 Gigabit Ethernet ports, PoE power

WatchGuard's AP320 is perfect for busy environments and diverse client ecosystem and Wi-Fi requirement. This high-horsepower AP solution can support critical applications like voice, video, and cloud with ease. The AP320 has concurrent 5 GHz and 2.4 GHz band radios, 3 spatial streams, and data rates of up to 1.3 Gbps. Ideal for offices, classrooms, and meeting spaces.

"We've found that the dashboard within the WatchGuard Wi-Fi Cloud product has made it much easier for our limited IT staff to deploy new access points, to understand the functionality of the existing access points, and to understand the true needs of our guests."

~ Hunter Hughes, Director of IT, Museum of Flight

FLEXIBLE MANAGEMENT OPTIONS

You can manage AP320 access points with either a Firebox®, via the Gateway Wireless Controller with lightweight feature set, or with WatchGuard's Wi-Fi Cloud. And with the Wi-Fi Cloud you get an expanded set of features including strong WIPS security, marketing tools, and location-based analytics for optimal business insights.

PERFORMANCE WITHOUT COMPROMISE

Incorporating the latest 802.11ac standards, you'll have speeds of up to 1.3 Gbps over the air, without sacrificing security. When managed by the Wi-Fi Cloud, WatchGuard APs come standard with RF optimization, spectrum monitoring, and trouble-shooting built in.

UNIQUELY EFFECTIVE APPROACH TO SECURITY

Using patented Marker Packet technology, WatchGuard's cloud-managed WIPS (Wireless Intrusion Prevention System) defends your airspace from unauthorized devices, man-in-the-middle and denial-of-service attacks, rogue APs and more. As a dedicated WIPS sensor, the AP320 can be added to any existing Wi-Fi network for a powerful layer of patented security features simply unavailable in most AP devices.

ADVANTAGES OF CLOUD-BASED MANAGEMENT

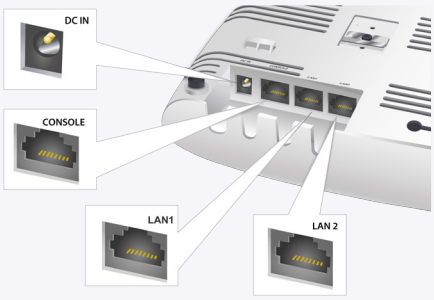
WatchGuard's secure cloud-managed APs deliver the most comprehensive set of features for the price – including marketing tools for customizable user engagement and location-based analytics for enhanced business insights. With the WatchGuard Wi-Fi Cloud, IT pros can enjoy an entirely controller-less Wi-Fi management experience including setup, configuration, monitoring, troubleshooting, and improving corporate and guest Wi-Fi access, without worrying about the limitations of legacy controller infrastructure. Wi-Fi Cloud environments easily scale from one to an unlimited number of APs across multiple locations. APs can be grouped in many ways including location, building, floor, and customer to maintain consistent policies.

FEATURES & BENEFITS

- Horizontal (ceiling) or vertical (wall) mounting support included at no additional cost.
- Wi-Fi Cloud-enabled APs include integrated firewall, traffic shaping, QoS and BYOD controls per SSID
- Support for up to 8 individual SSIDs per radio allows for maximum flexibility in network design.
- AP320 devices can be converted to a dedicated security sensor with a single click for maximum wireless protection.
- Manage with Wi-Fi Cloud for expanded features including strong WIPS security, marketing tools and location-based analytics for enhanced business insights.
- Patented Marker Packet technology is used to accurately detect authorized, unauthorized, and external access points on any network with the fewest false positives in the industry.
- Supports self-healing and bridge-mode wireless meshing for optimal installation scenarios.

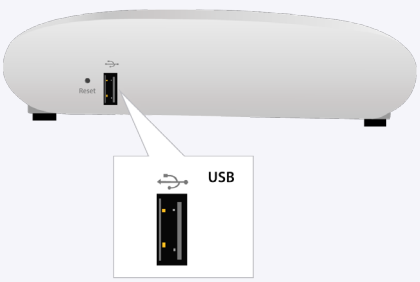
PHYSICAL SPECIFICATIONS

Property	Specification
Physical Dimensions	177mm × 155mm × 42mm
Weight	0.82 lb. (0.37 kg)
Operating Temperature	0°C to 40°C (32°F to 104°F)
Storage Temperature	-40°C to 70°C (-40°F to 158°F)
Humidity	5% to 95% non-condensing



Rear View

Port	Description	Connector Type	Speed/Protocol
Power	This is a 12V DC input jack that can be used to power the device.	3.5 mm barrel	N/A
Console	To establish 'Config Shell' terminal session via serial connection.	RJ-45	RS 232 Serial Bits per second: 115200 Data Bits: 8, Stop Bits: 1 Parity: None Flow Control: None
LAN1	Gigabit Ethernet port used to connect to the wired LAN and communicate with the WatchGuard Cloud or Server. This port can also be used to power the device using the 802.3af Power over Ethernet (PoE) standard.	RJ-45	10/100/1000 Mbps Gigabit Ethernet 802.3af Class 0 PoE PoE input voltage: 48V
LAN2	Gigabit Ethernet port that can be used for wired extension for an SSID.	RJ-45	10/100/1000 Mbps Gigabit Ethernet



Port	Description	Connector Type	Speed/Protocol
Reset	Reset to factory default settings	Pin-hole push-button	Hold down and power cycle the device to reset
USB	Not in use	Not in use	Not in use

WI-FI SPECIFICATIONS – Frequency, Modulation, and Data Rates

IEEE 802.11b/g/n			
Frequency Band	Scanning	Transmission	
	All regions	USA & Canada (FCC/IC)	Europe (ETSI)
	2400 ~ 2483.5 MHz	2400 ~ 2473.5 MHz	2400 ~ 2483.5 MHz
Modulation Type	DSSS, OFDM		
Data Rates	Up to 450 Mbps (MCS 0-23) with automatic rate adaptation		
Antenna	Integrated modular high efficiency PIFA omnidirectional antenna		

IEEE 802.11a/n/ac			
Frequency Band	Scanning	Transmission	
	All regions	USA & Canada (FCC/IC)	Europe (ETSI)
	4.92 ~ 5.08 GHz 5.15 ~ 5.25 GHz 5.25 ~ 5.35 GHz 5.47~ 5.725 GHz 5.725~ 5.825 GHz	5.15 ~ 5.25 GHz 5.25 ~ 5.35 GHz 5.725~ 5.82 5GHz	5.15 ~ 5.25 GHz 5.25 ~ 5.35 GHz 5.47~ 5.725 GHz
Dynamic Frequency Selection	DFS and DFS2		
Modulation Type	OFDM		
Data Rates	Up to 1.3 Gbps (MCS 0-9) for 11ac with automatic rate adaptation Up to 450 Mbps (MCS 0-23) for 11n with automatic rate adaptation		
Antenna	Integrated modular high efficiency PIFA omnidirectional antenna		

Maximum Transmit Power

For 5GHz

MCS Index	Transmit Power(dBm)
802.11a (legacy)	
6Mbps	18
36Mbps	18
48Mbps	18
54Mbps	17
802.11n HT20 (legacy)	
MCS 0,1,2,3,4,8,9,10,11,12,16,17,18,19,20	18
MCS 5,13,21	18
MCS 6,14,22	18
MCS 7,15,23	17
802.11n HT40	
MCS 0,1,2,3,4,8,9,10,11,12,16,17,18,19,20	18
MCS 5,13,21	18
MCS 6,14,22	18
MCS 7,15,23	17
802.11ac 256QAM VHT80	
3/4 Code Rate	15
5/6 Code Rate	14

For 2.4GHz

MCS Index	Transmit Power(dBm)
802.11g (legacy)	
6Mbps	20
54Mbps	18
802.11n HT20 (legacy)	
MCS 0/8/16	20
MCS 7/15	18
MCS 23	17
802.11n HT40	
MCS 0/8/16	20
MCS 7/15	17
MCS 23	16

Note:
The actual transmit power will be the lowest of:

- Value specified in the Device Template
- Maximum value allowed in the regulatory domain
- Maximum power supported by the radio

Country-Wise Max Transmit Powers (dBm)

Countries	2.4GHz	5Ghz
Australia	20	23
Canada	30	23
India	20	20
Israel	20	20
Japan	20	20
UAE	20	17
USA	20	23

Receive Sensitivity

For 5GHz

MCS Index	Receive Sensitivity
802.11a (legacy)	
6Mbps	-90
36Mbps	-77
48Mbps	-74
54Mbps	-72
802.11n HT20 (legacy)	
MCS 0,1,2,3,4,8,9,10,11,12,16,17,18,19,20	-90
MCS 5,13,21	-73
MCS 6,14,22	-71
MCS 7,15,23	-70
802.11n HT40	
MCS 0,1,2,3,4,8,9,10,11,12,16,17,18,19,20	-86
MCS 5,13,21	-69
MCS 6,14,22	-68
MCS 7,15,23	-67
802.11ac 256QAM VHT80	
HT20 MCS 8 @ 3/4 Code rate	-59
HT20 MCS 9 @ 5/6 Code Rate	-57
HT40 MCS 8 @ 3/4 Code Rate	-56
HT40 MCS 9 @ 5/6 Code Rate	-54
HT80 MCS 8 @ 3/4 Code rate	-53
HT80 MCS 9 @ 5/6 Code Rate	-51

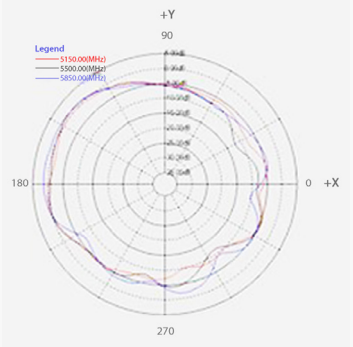
For 2.4GHz

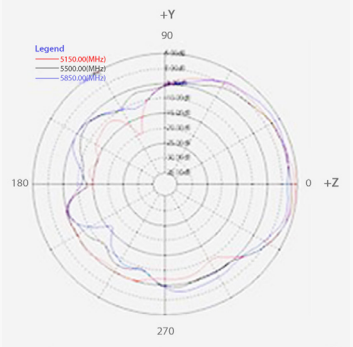
MCS Index	Receive Sensitivity
802.11g (legacy)	
1Mbps	-95
6Mbps	-91
11Mbps	-87
54Mbps	-74
802.11n HT20 (legacy)	
MCS 0/8/16	-91
MCS 7/15/23	-70
802.11n HT40	
MCS 0/8/16	-87
MCS 7/15/23	-67

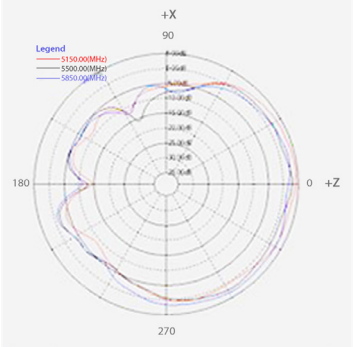
INTERNAL ANTENNA RADIATION PATTERNS

5 GHz

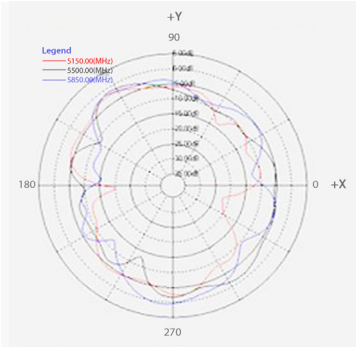
Antenna 1

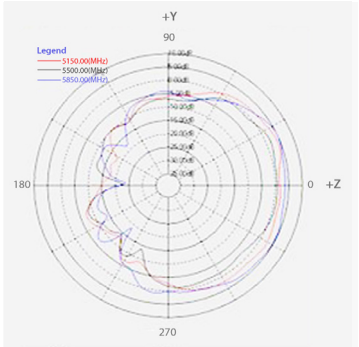


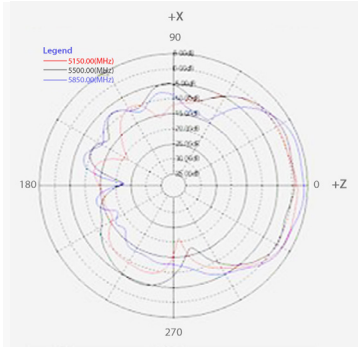




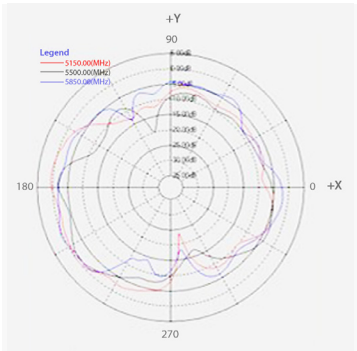
Antenna 2

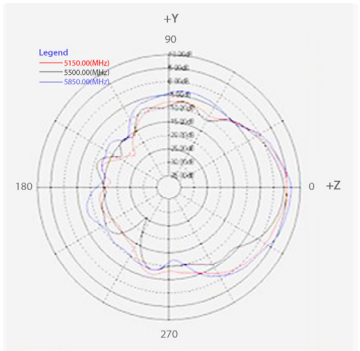


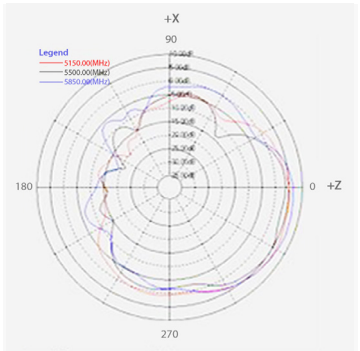




Antenna 3

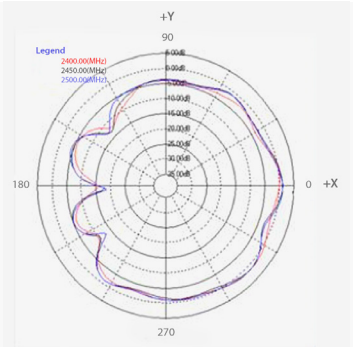


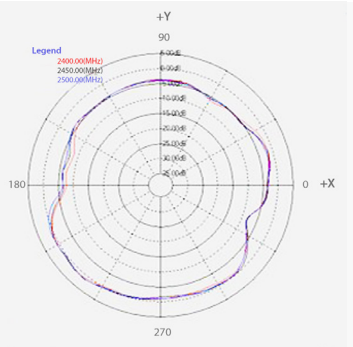


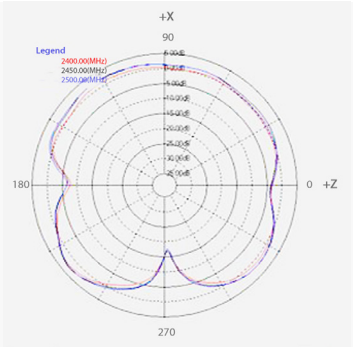


2.4 GHz

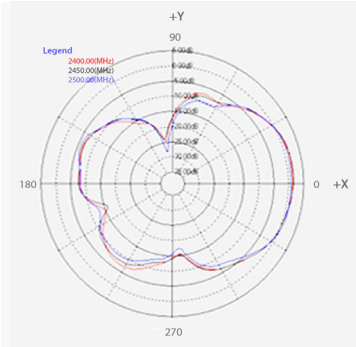
Antenna 1

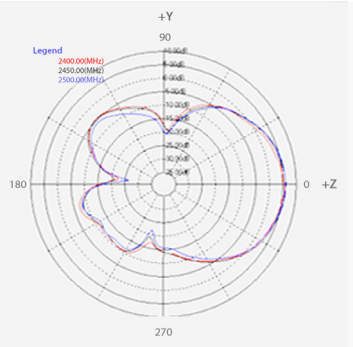


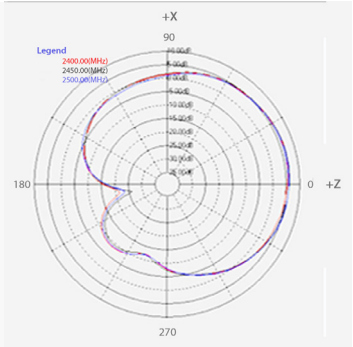




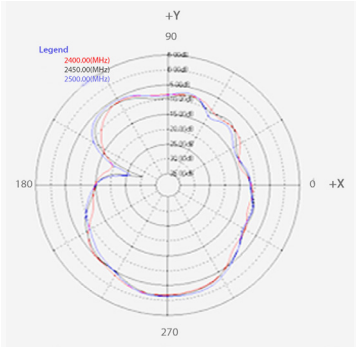
Antenna 2

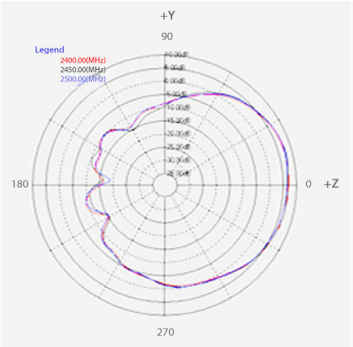


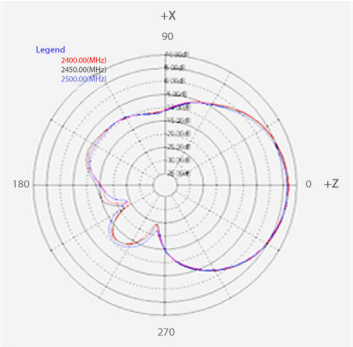




Antenna 3







Access Point Security Modes:

- WPA/WPA2 (802.11i) with TKIP or AES-CCMP encryption and PSK or 802.1x authentication
- Integrated WIPS background wireless scanning and Rogue AP prevention

WIPS Sensor Mode:

- Dedicated dual-band WIPS scanning for complete 24/7 protection from wireless threats

REGULATORY SPECIFICATIONS

RF and Electromagnetic

Country	Certification
USA	FCC Part 15.247, 15.407
Canada	IC
Europe	CE EN300.328, EN301.893 Countries covered under Europe certification: Austria, Belgium, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Iceland, Luxembourg, Latvia, Lithuania, Malta, Netherlands, Norway, Poland, Portugal, Spain, Sweden, Slovakia, Slovenia, Switzerland, The Czech Republic, UK.

Safety

Country	Certification
USA	UL 60950
Canada	cUL 60950
European Union (EU)	EN 60950, RoHS

WATCHGUARD HAS YOU COVERED, INDOORS AND OUT

Secure, Simple, Intelligent Wi-Fi Access Point Family

WatchGuard offers a full suite of cloud-ready secure wireless access points for delivering blazing fast Wi-Fi, without compromising your network.

The **AP322** is your ideal solution for the outdoors. This access point features a rugged IP67-compliant exterior and delivers broad, fast, and reliable Wi-Fi coverage. Designed to bring Wi-Fi to stadiums, schools, outdoor cafes, shipping docks, warehouses, and more, AP322 has you covered.

The **AP320** is perfect for busy environments with diverse client ecosystem and Wi-Fi requirements. This high-horsepower AP can support critical applications like voice, video, and cloud with ease. Common deployment scenarios include offices, classrooms, and meeting spaces.

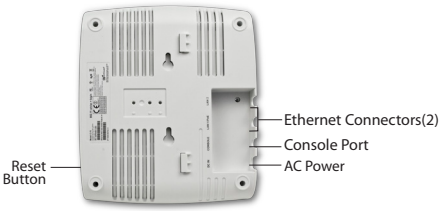
The **AP120** is built for networks with heavy smartphone and tablet access such as guest or public Wi-Fi environments, or smaller-footprint locations that support limited devices. Common deployment scenarios include branch offices, stores, and small classrooms.

For details, talk to your authorized WatchGuard reseller or visit **www.watchguard.com**.

About WatchGuard Technologies, Inc.

WatchGuard® Technologies, Inc. is a global leader in network security, providing best-in-class Unified Threat Management, Next Generation Firewall, secure Wi-Fi, and network intelligence products and services to more than 75,000 customers worldwide. The company's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for Distributed Enterprises and SMBs. WatchGuard is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit **watchguard.com**.

AP320



DATASHEET

FIREBOX CLOUD

Extending the WatchGuard Security Perimeter to the Public Cloud

It's a fact – businesses are migrating services from on-premises servers into the cloud. Email servers, web servers, customer relationship management systems (CRMs), and file storage are migrating to cloud services. With so much sensitive data moving to the cloud, security is essential. WatchGuard's Firebox Cloud allows network administrators to extend their security perimeter to protect servers running in public cloud environments.

While cloud service providers are responsible for the security of the cloud, protecting your sensitive data as it moves to and from the cloud falls to you. Under this shared responsibility model, it is crucial that administrators take every step possible to defend their data and deflect cyber criminals. WatchGuard Firebox Cloud brings the protection of WatchGuard's leading Firebox® Unified Threat Management (UTM) appliances to public cloud environments. Firebox Cloud can quickly and easily be deployed to protect servers in a public cloud from attacks such as botnets, cross-site scripting, SQL injection attempts, and other intrusion vectors.

BUILT FOR THE CLOUD ENVIRONMENT

Unlike many UTM services in the cloud, WatchGuard's Firebox Cloud was built specifically to run within each cloud environment and provides a streamlined user interface (UI) that removes elements that aren't relevant. Firebox Cloud also simplifies the process of establishing secure connections to your public cloud environment by enabling WatchGuard-to-WatchGuard VPN tunnels.

EXTENDING THE WATCHGUARD SECURITY PERIMETER

Small-to-midsize businesses and distributed enterprises with portions of their infrastructure running in the cloud can streamline their configuration and maintenance efforts by extending their security perimeter with Firebox Cloud. Using Firebox Cloud in conjunction with physical Firebox appliances eliminates the need to become familiar with a separate product line to protect a Virtual Private Cloud (VPC).

BIG DATA VISIBILITY

WatchGuard Firebox Cloud is completely compatible with WatchGuard Dimension, a cloud-ready network security visibility solution that comes standard with WatchGuard's flagship Unified Threat Management and Next Generation Firewall platform. Dimension provides a suite of big data visibility and reporting tools that instantly identify and distill key security issues and trends, and deliver actionable insights to set meaningful security policies across all of your environments.

MULTIPLE PURCHASING OPTIONS

WatchGuard has made it easy to get your Firebox Cloud instance up and running by providing multiple ways to purchase. You can purchase a Bring-Your-Own-License (BYOL) from a WatchGuard Partner to ensure you benefit from the skills and expertise of the Partner you trust. It is also possible to purchase a metered (e.g. pay by the hour) instance directly from the marketplace.

FEATURES & BENEFITS

- Quickly and easily protect VPCs from attacks such as botnets, cross-site scripting, SQL injection attempts, and other intrusion vectors
- Save time with a streamlined UI built for each cloud platform
- Simplify the process of establishing secure connections to your public cloud environment
- Increase visibility with WatchGuard's leading network visibility solution, Dimension
- Purchase your way, with multiple purchasing options available

Model Name	CPU Core Limit	User Count	TDR Host Sensors	Firewall (Gbps)	VPN (Gbps)	VPN Users
Small	2	50	50	2	0.4	50
Medium	4	250	250	4	1.5	600
Large	8	750	250	8	3	6,000
XLarge	16	1,500	250	Unrestricted	Unrestricted	10,000

Note: Specification values apply to BYOL subscription model only.

CLOUD FEATURES

Supported environments	Amazon Web Services (AWS)
Subscription models	Bring Your Own License, On-Demand

SECURITY FEATURES

Firewall	Stateful packet inspection, deep packet inspection, proxy firewall
Application proxies	HTTP, HTTPS, SMTP, FTP, DNS, TCP-UDP, POP3
Threat protection	DoS attacks, fragmented packets, blended threats and more
Filtering options	Browser Safe Search, YouTube for Schools, Google for Business
Security subscriptions	APT Blocker, IPS, Gateway AV, WebBlocker, App Control, Data Loss Prevention, Reputation Enabled Defense, Threat Detection and Response

MANAGEMENT

Logging and notifications	WatchGuard, Syslog, SNMP v2/v3
User interfaces	Web UI, scriptable CLI
Reporting	WatchGuard Dimension includes over 100 pre-defined reports, executive summary and visibility tools

STANDARD NETWORKING

QoS	8 priority queues, DiffServ, modified strict queuing
IP address assignment	DHCP (client)
NAT	Static, dynamic, 1:1, IPSec traversal
Other features	Static routing, port Independence

VPN & AUTHENTICATION

Encryption	DES, 3DES, AES 128-, 192-, 256-bit
IPSec	SHA-2, IKE pre-shared key, 3rd party cert
Single sign-on	Windows, Mac OS X, mobile operating systems, RADIUS
Authentication	RADIUS, LDAP, Windows Active Directory, RSA SecurID, internal database

STRONG SECURITY AT EVERY LAYER

Uniquely architected to be the industry's smartest, fastest, and most effective network security products, WatchGuard solutions deliver in-depth defenses against advanced malware, ransomware, botnets, trojans, viruses, drive-by downloads, data loss, phishing and much more.

Features & Services	TOTAL SECURITY SUITE	Basic Security Suite
Intrusion Prevention Service (IPS)	✓	✓
Application Control	✓	✓
WebBlocker (URL/Content Filtering)	✓	✓
Gateway AntiVirus (GAV)	✓	✓
Reputation Enabled Defense (RED)	✓	✓
APT Blocker	✓	
Data Loss Prevention	✓	
Threat Detection and Response (with WatchGuard Host Sensor)	✓	
Support	Gold (24x7)	Standard (24x7)

ONE PACKAGE. TOTAL SECURITY.

The flexibility of WatchGuard's integrated platform makes it easy to have exactly the security components your business network requires. Whether you choose to start with the security basics or deploy a comprehensive arsenal of network defenses, we have bundled security services to match your requirements.

EXPERT GUIDANCE AND SUPPORT

An initial Support subscription comes with every Firebox Cloud model. Standard Support, which is included in the Basic Security Suite, provides 24 x 7 technical support and software updates. An upgrade to Gold level support is included in WatchGuard's Total Security Suite.

For details, talk to your authorized WatchGuard reseller or visit www.watchguard.com.

U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 www.watchguard.com

sovergence

107 Main Street, Ste 500
Richardson, Texas 75280
Main - 469 631 3849
https://www.sovergence.com