Data sheet

Stop today's advanced cyber threats with proactive network security

HP N Platform Next-Generation Intrusion Prevention System (NGIPS)

Product overview

HP N Platform Next-Generation Intrusion Prevention System (NGIPS) achieves a new level of in-line, real-time protection, providing proactive network security for today's and tomorrow's real-world network traffic and data centers. The N Platform NGIPS's next-generation architecture adds significant capacity for deep packet traffic inspection, and its modular software design enables the addition of valuable network protection services to its proven intrusion prevention solution. This industry-leading NGIPS platform redefines intrusion prevention as a foundation for comprehensive network security.

Key features

- Industry-proven proactive network security
- Up-to-date and broad NGIPS protection
- Industry-leading security research team—DVLabs
- Reduced overall security costs and complexity
- Security compliance best practices

Features and benefits

Technical features

- **Next-Generation Intrusion Prevention System:** The N Platform NGIPS provides a new level of in-line, real-time protection, enabling proactive network security for real-world network traffic and data centers. Its architecture adds significant capacity for deep packet traffic inspection and its modular software design enables the convergence of additional security services.
- **Proven in-line threat protection:** Since 2001, we have been focused on creating NGIPS solutions that provide proactive, in-line network protection while supporting high network performance and availability. No network security solution remains in-line if it compromises network performance or uptime.
- **Extensible security framework provides a foundation for growth:** The N Platform NGIPS includes an extensible security framework that has a modular software design built to support faster development and deployment of new NGIPS filter packages, security services, and partner security solution integrations.
- **NGIPS security services:** The N Platform NGIPS enables the convergence of new security services such as customer-defined IP DNS reputation entries, HP TippingPoint Reputation Digital Vaccine Service (Rep DV Service), HP TippingPoint Web Application Digital Vaccine Service, HP TippingPoint Application Digital Vaccine (AppDV), location-based policies (perimeter, core, and more), and customer-developed protection filters.
- **Modular design for solutions integration:** The modular design of the N Platform NGIPS enables integrations with partner security solutions such as vulnerability assessment and vulnerability management (VA and VM) products, forensics solutions, security information and event management (SIEM), and network-based anomaly detection (NBAD) products.
- **Support for a broad set of traffic types:** The N Platform NGIPS supports a wide variety of traffic types and protocols. It provides uncompromising IPv4 and IPv6 simultaneous payload inspection and support for related tunneling variants (4in6, 6in4, 6in6). It also supports inspection of IPv4 and IPv6 traffic with VLAN and MPLS tags, mobile IPv4 traffic, GRE and GTP (GPRS tunneling), and jumbo frames. This breadth of coverage gives IT administrators the flexibility to deploy NGIPS protection wherever it is needed.
- **Powered by X-Armour:** HP TippingPoint's X-Armour software architecture performs total packet flow inspection at Layers 2-7, executing thousands of checks on each packet flow simultaneously, and delivering high performance deep-packet inspection working in with conjunction the N platform's custom ASICs and high-performance network processors. Unlike traditional security appliances, X-Armour, running on the N platform, automates the security protection you can install our appliances throughout the network without the worry of daily management. The X-Armour architecture automatically adjusts to new attacks at a very rapid rate. In fact, X-Armour has built-in capabilities to update itself every two hours with no impact to network performance.

- **Proven reliability and redundancy:** The N Platform NGIPS is designed to deliver unparalleled high availability. This helps ensure that network traffic always flows at wire speed in the event of network error, internal device error, or even complete power loss. There are two complementary high availability modes of operation—intrinsic high availability and stateful network redundancy—that enable higher uptime and availability for both the NGIPS platform and the security management system (SMS) devices.

- **Built-in high availability features:** The N Platform NGIPS has multiple features for Intrinsic High Availability, including dual hot-swappable power supplies and watchdog timers to continuously monitor the security and management engines. In case an internal error is detected, the NGIPS automatically fails open; and Zero Power High Availability (ZPHA) options, so in the event of a power loss, the IPS interfaces can switch over to the ZPHA relay, allowing all traffic to pass unimpeded.

- **Redundant configuration options:** Two N platforms can be provisioned using redundant links in a transparent "Active-Active" or "Active-Passive" high-availability mode. The N platform acts as a "bump in the wire," does not have an IP address, and does not participate in routing protocols. It can be deployed in existing network designs without changing network configurations, including high-availability routing protocols such as VRRP, OSPF, and HSRP, which are passed transparently by the NGIPS.

- **High throughput inspection for data center and core network deployments:** The N Platform NGIPS is designed for data center and network core protection. For these mission-critical network areas, our HP core controller solution combined with a pool of N platforms delivers automated, in-line inspection (up to 20 Gb/s) to protect network devices, virtualization software, operating systems, and applications from attack without impeding performance.

- **Low application latency enables zero degradation of end-user experience:** Based on purpose-built hardware, the N platform inspects all packet flows with typical latency of less than 80 microseconds, independent of the number of filters or security protections that are enabled. This prevents any noticeable application performance impact from an end-user perspective.

- **Advanced filter accuracy facilitates smooth legitimate traffic:** We use two simple filter writing rules to provide filter accuracy—no false positives and no false negatives. That's why our DVLabs security research team focuses on creating filters to guard entire vulnerabilities, not just known exploits. Vulnerability filters block all exploits for a software vulnerability and provide unmatched levels of accuracy so the N Platform NGIPS does not block legitimate traffic while protecting the network.

- **Virtual patching protects unpatched systems:** DVLabs creates vulnerability filters that block all exploits for a given software vulnerability, creating a "virtual patch." These vulnerability filters protect vulnerabilities in virtualization software, operation systems, and applications and are not exploit specific. They behave like a network-based virtual software patch to protect downstream hosts from network-based attacks on unpatched vulnerabilities.

- **Purpose-built hardware and software:** Blocking cyber attacks at multi-gigabit speeds with extremely low latency requires purpose-built hardware and software. While others' solutions use general-purpose hardware and processors that are simply unable to perform without degrading network performance, our N platform provides thorough threat protection at multi-gigabit speeds, with very low latency.

- **Leading security research team—DVLabs:** DVLabs is the premier security research team for vulnerability discovery in the security industry. The team consists of industry-recognized researchers who apply cutting-edge engineering and analysis in their daily operations. DVLabs is a leader in annual vulnerability discoveries, and the result is the creation of vulnerability filters that are delivered to customers' N Platform NGIPS through the Digital Vaccine (DV) Service.

- **ThreatLinQ security portal:** ThreatLinQ is a service that allows our NGIPS customers to view the latest threats across the globe. This data is collected from a global network of Lighthouse monitoring devices and from thousands of N Platform NGIPS customers. ThreatLinQ is available to all our customers and provides valuable data that can enable enterprises to more effectively hone their network security policies to meet the demands of the latest threat trends.

- **Industry's fastest threat protection keeps ahead of threats:** Our DV Service provides up-to-date protection against emerging threats. DVs are delivered to customers twice a week or immediately when critical vulnerabilities emerge, and they can be deployed automatically with no IT interaction required. These vaccines are created not only to address specific exploits, but also potential attack permutations, protecting customers from zero-day threats.

- **Leading zero-day threat protection:** DVLabs manages the zero-day initiative (ZDI) program, which is designed to reward worldwide researchers for responsibly disclosing vulnerabilities they discover. Whether from DVLabs internal vulnerability research or the ZDI program, DVLabs passes all vulnerability discoveries to affected software vendors and creates NGIPS filters to protect customers from potential zero-day attacks before vulnerabilities are disclosed to the public.

- **Comprehensive NGIPS threat and vulnerability coverage for the most advanced protection:** The combination of talent, research, and security intelligence from the world-class DVLabs research team; over 1,200 researchers in the ZDI program; ThreatLinQ global threat monitoring from thousands of sites; and security community partners such as SANS Institute, CERT, and NIST—all these combine to provide the broadest threat and vulnerability coverage for the industry-leading protection available today.

- **Full attack surface threat protection:** The N platform provides comprehensive vulnerability coverage in the NGIPS industry, including protection of network devices, virtualization software, operating systems, enterprise and Web applications, and industrial control system networks. From Microsoft® operating systems to SCADA and VoIP filters, and many more, HP TippingPoint solutions provide true network protection for today's complex enterprise IT environments.

- **Rep DV Service removes "known bad" traffic:** The optional Rep DV Service provides IPv4, IPv6, and Domain Name System (DNS) security intelligence feeds from a DVLabs global reputation database, so customers can actively enforce and manage reputation security policies using the N platform. The platform acts as an enforcement point, inspecting traffic in real time, identifying "known bad" traffic, and enforcing Rep DV security policies.

- **NGIPS automated, proactive protection reduces most manual event follow-up:** Automated policy enforcement reduces the need to respond to myriad alerts (some real and some false), or to clean up after cyber attacks have compromised network resources. IT security costs are reduced by lowered ad-hoc patching and alert response, while simultaneously increasing IT productivity and profitability through bandwidth savings and protection of critical applications.

- **Prevent the need to emergency patching and protect systems from zero-day events:** Our vulnerability filters helps eliminate the need for ad-hoc and emergency patching. By protecting software vulnerabilities, IT staff can implement software patches using a regular, scheduled process instead of costly, disruptive emergency patching. The N Platform NGIPS blocks attacks and allows IT staff to test security patches before deployment.

- **Improve control of end-user desktops:** Most IT teams cannot adequately control end-user desktops. Many client-side applications were shown to be increasingly difficult to keep patched due to the growing number of vulnerabilities. The N platform improves IT control through vulnerability protection for unpatched systems and network segmentation to stop the spread of malicious traffic from infected users, all while notifying the administrator where attacks originate.

- **Enhance network performance by recapturing misused bandwidth:** The N Platform NGIPS's bandwidth management capabilities stop rogue applications like peer-to-peer and streaming media from running rampant throughout the network. By continually cleansing the network of malicious and unwanted traffic, network performance is accelerated for mission-critical applications. And rate-shaping rogue applications can increase bandwidth and network availability by significant amounts.

- **Easy to install in just minutes, reducing IT burdens:** The N platform significantly reduces the amount of time and resources needed to maintain a healthy network. The NGIPS and security management system (SMS) can both be easily installed in the network, typically in 30 minutes to two hours. The NGIPS is designed for network transparency and is deployed seamlessly into the network with no IP address or MAC address, so it can immediately begin filtering out malicious and unwanted traffic.

- **Easy-to-manage solutions reduce IT staff workload:** The SMS easily discovers, monitors, configures, diagnoses, and reports on multiple N Platform NGIPSs. It features a simple, state-of-the-art secure Java client interface that enables "big picture" analysis with trending reports, correlation and real-time graphs on traffic statistics, filtered attacks, network hosts and services, as well as NGIPS inventory and health.

- **Flexible local management options:** Every NGIPS unit also has an embedded local security manager (LSM) and CLI. The LSM is a Web GUI management application that provides administration, configuration, and reporting capabilities in an easy-to-use, secure Web interface.

- **Automated DV updates reduce ongoing management time:** Automated DV download and distribution capabilities reduce the time required to manage the N platform. The SMS allows for manual DV download and distribution, or automated DV download and manual distribution.

- **Simple but powerful security policies:** The N Platform NGIPS allows security administrators to manage security policy with fine granularity. Administrators can set specific network security policies by network segment, by VLAN, or by Classless Inter-Domain Routing (CIDR). In addition, by utilizing the N Platform NGIPS's reputation capabilities and the Rep DV, customers can now incorporate the use of IP addresses and DNS names into their security policy management.

- **Automated enforcement of security policies for compliance:** The N Platform NGIPS can be a critical component in any IT compliance program. It addresses many compliance program objectives, including vulnerability management with the DV Service and network monitoring objectives with the security management system. In addition, the NGIPS may provide a "compensating control" where a requirement is not specifically satisfied with other solutions or processes.

- **Robust security reporting provides auditor details:** Reporting from the NGIPS and SMS allows administrators to show internal and external auditors how the network is protected from the latest threats. In addition to meeting regulatory and internal compliance requirements, organizations can have sophisticated security enforcement available for their networks.

Warranty and support

- **1-year warranty:** With advance replacement and 30-calendar-day delivery (available in most countries)

- **Electronic and telephone support:** Limited electronic and telephone support is available from HP; refer to **hp.com/networking/warranty** for details on the support provided and the period during which support is available

- **Software releases:** Refer to **hp.com/networking/warranty** for details on the software releases provided and the period during which software releases are available for your product(s)

HP N Platform Next-Generation Intrusion Prevention System (NGIPS)

Specifications

	HP S660N 750 Mb/s 5 Gig-T/5 1Gb Copper or Fiber Segments NGIPS (JC019A)	HP S1400N 1.5 Gb/s 5 Gig-T/5 1Gb Copper or Fiber Segments NGIPS (JC020A)
Ports	10 RJ-45 auto-sensing 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T); Duplex: 10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only 10 fixed Gigabit Ethernet SFP ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T); Duplex: 10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only	10 RJ-45 auto-sensing 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T); Duplex: 10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only 10 fixed Gigabit Ethernet SFP ports
Physical characteristics		
Dimensions	24 (d) x 16.87 (w) x 3.42 (h) in. (60.96 x 42.86 x 8.69 cm) (2U height)	24 (d) x 16.8 (w) x 3.42 (h) in. (60.96 x 42.67 x 8.69 cm) (2U height)
Weight	29.1 lb. (13.2 kg)	28.99 lb. (13.15 kg)
Mounting	19-or 23-inch wide rack—ears provided	19-or 23-inch wide rack—ears provided
Performance		
Latency	< 80 µs	< 80 µs
NGIPS/IDS throughput	750 Mb/s	1.5 Gb/s
Network throughput	750 Mb/s	1.5 Gb/s
Security contexts	1,200,000	1,200,000
Connections per second	115,000	115,000
Concurrent sessions	6,500,000	6,500,000
Environment		
Operating temperature	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C)
Operating relative humidity	5% to 95%, non-condensing	5% to 95%, non-condensing
Non-operating/Storage temperature	-4°F to 158°F (-20°C to 70°C)	4°F to 158°F (-20°C to 70°C)
Non-operating/Storage relative humidity	5% to 95%, non-condensing	5% to 95%, non-condensing
Electrical characteristics		
Voltage	100-240 Vac	100-240 Vac
Current	8/5 A	8/5 A
Frequency	50/60 Hz	50/60 Hz
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; CSA 22.2 60950-1; ROHS Compliance	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; CSA 22.2 60950-1; ROHS Compliance
Emissions	FCC Class A; VCCI Class A; EN 55022 Class A; AS/NZS 3548 Class A; ICES-003 Class A	FCC Class A; VCCI Class A; EN 55022 Class A; AS/NZS 3548 Class A; ICES-003 Class A
Immunity		
ESD	EN 61000-4-2	EN 61000-4-2
Radiated	EN 61000-4-3	EN 61000-4-3
EFT/Burst	EN 61000-4-4	EN 61000-4-4
Surge	EN 61000-4-5	EN 61000-4-5
Conducted	EN 61000-4-6	EN 61000-4-6
Voltage dips and interruptions	EN 61000-4-11	EN 61000-4-11
Harmonics	EN 61000-3-2	EN 61000-3-2
Flicker	EN 61000-3-3	EN 61000-3-3

Specifications (continued)

	HP S660N 750 Mb/s 5 Gig-T/5 1Gb Fiber Segments NGIPS (JC019A)	HP S1400N 1.5 Gb/s 5 Gig-T/5 1Gb Fiber Segments NGIPS (JC020A)
Management	SMS; command-line interface; Web browser; HP TippingPoint IPS MIB	SMS; command-line interface; Web browser; HP TippingPoint IPS MIB
Notes	Performance footnotes: • NGIPS/IDS throughput represents the inspection throughput levels measured with recommended security profiles. • Network throughput represents the maximum throughput levels that can be achieved with the use of traffic forwarding. • Typical latency is measured on packet sizes up to 1518 bytes. • Concurrent network sessions are the maximum number of concurrent network sessions that can be supported by the NGIPS. • Security contexts are the maximum number of sessions with security state that can be supported by the NGIPS.	Performance footnotes: • NGIPS/IDS throughput represents the inspection throughput levels measured with recommended security profiles. • Network throughput represents maximum throughput levels that can be achieved with the use of traffic forwarding. • Typical latency is measured on packet sizes up to 1518 bytes. • Concurrent network sessions are the maximum number of concurrent network sessions that can be supported by the NGIPS. • Security contexts are the maximum number of sessions with security state that can be supported by the NGIPS.
Services	3-year, 24x7 next-business-day hardware advance exchange, 24x7 software phone support and software updates (UX067E) Refer to the HP website at **hp.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 HP sales office.	3-year, 24x7 next-business-day hardware advance exchange, 24x7 software phone support and software updates (UX068E) Refer to the HP website at **hp.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 HP sales office.

Specifications (continued)

	HP S2500N 3 Gb/s 5 Gig-T/1 10GbE/5 1GbE Copper or Fiber Segments NGIPS (JC021A)	HP S5100N 5 Gb/s 5 Gig-T/1 10GbE/5 1GbE Copper or Fiber Segments NGIPS (JC022A)
Ports	10 RJ-45 auto-sensing 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T); Duplex: 10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only 10 fixed Gigabit Ethernet SFP ports 2 XFP 10GbE ports (IEEE 802.3ae Type 10GBASE-LR); Duplex: full only	10 RJ-45 auto-sensing 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T); Duplex: 10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only 10 fixed Gigabit Ethernet SFP ports 2 XFP 10GbE ports (IEEE 802.3ae Type 10GBASE-LR); Duplex: full only
Physical characteristics		
Dimensions	24 (d) x 16.88 (w) x 3.42 (h) in. (60.96 x 42.88 x 8.69 cm) (2U height)	24 (d) x 16.88 (w) x 3.42 (h) in. (60.96 x 42.88 x 8.69 cm) (2U height)
Weight	31.5 lb. (14.29 kg)	31.5 lb. (14.29 kg)
Mounting	19-or 23-inch wide rack—ears provided	19-or 23-inch wide rack—ears provided
Performance		
Latency	< 80 µs	< 80 µs
NGIPS/IDS throughput	3 Gb/s	5 Gb/s
Network throughput	15 Gb/s	15 Gb/s
Security contexts	2,600,000	2,600,000
Connections per second	230,000	230,000
Concurrent sessions	10,000,000	10,000,000
Environment		
Operating temperature	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C)
Operating relative humidity	5% to 95%, non-condensing	5% to 95%, non-condensing
Non-operating/Storage temperature	-4°F to 158°F (-20°C to 70°C)	-4°F to 158°F (-20°C to 70°C)
Non-operating/Storage relative humidity	5% to 95%, non-condensing	5% to 95%, non-condensing
Electrical characteristics		
Voltage	100-240 Vac	100-240 Vac
Current	8/5 A	8/5 A
Frequency	50/60 Hz	50/60 Hz
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; CSA 22.2 60950-1; ROHS Compliance	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; CSA 22.2 60950-1; ROHS Compliance
Emissions	FCC Class A; VCCI Class A; EN 55022 Class A; AS/NZS 3548 Class A; ICES-003 Class A	FCC Class A; VCCI Class A; EN 55022 Class A; AS/NZS 3548 Class A; ICES-003 Class A
Immunity		
ESD	EN 61000-4-2	EN 61000-4-2
Radiated	EN 61000-4-3	EN 61000-4-3
EFT/Burst	EN 61000-4-4	EN 61000-4-4
Surge	EN 61000-4-5	EN 61000-4-5
Conducted	EN 61000-4-6	EN 61000-4-6
Voltage dips and interruptions	EN 61000-4-11	EN 61000-4-11
Harmonics	EN 61000-3-2	EN 61000-3-2
Flicker	EN 61000-3-3	EN 61000-3-3

Specifications (continued)

	HP S2500N 3 Gb/s 5 Gig-T/1 10GbE/5 1GbE Fiber Segments NGIPS (JC021A)	HP S5100N 5 Gb/s 5 Gig-T/1 10GbE/5 1GbE Fiber Segments NGIPS (JC022A)
Management	SMS; command-line interface; Web browser; HP TippingPoint IPS MIB	SMS; command-line interface; Web browser; HP TippingPoint IPS MIB
Notes	Performance footnotes: • NGIPS/IDS throughput represents the inspection throughput levels measured with recommended security profiles. • Network throughput represents the maximum throughput levels that can be achieved with the use of traffic forwarding. • Typical latency is measured on packet sizes up to 1518 bytes. • Concurrent network sessions are the maximum number of concurrent network sessions that can be supported by the NGIPS. The measured number was limited by the available test equipment. • Security contexts are the maximum number of sessions with security state that can be supported by the NGIPS.	Performance footnotes: • NGIPS/IDS throughput represents the inspection throughput levels measured with recommended security profiles. • Network throughput represents the maximum throughput levels that can be achieved with the use of traffic forwarding. • Typical latency is measured on packet sizes up to 1518 bytes. • Concurrent network sessions are the maximum number of concurrent network sessions that can be supported by the NGIPS. The measured number was limited by available test equipment. • Security contexts are the maximum number of sessions with security state that can be supported by the NGIPS.
Services	3-year, 24x7 next-business-day hardware advance exchange, 24x7 software phone support and software updates (UX069E) Refer to the HP website at **hp.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 HP sales office.	3-year, 24x7 next-business-day hardware advance exchange, 24x7 software phone support and software updates (UX070E) Refer to the HP website at **hp.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 HP sales office.

HP N Platform Next-Generation Intrusion Prevention System (NGIPS)

Mounting Kit

HP Slide Kit Quick Release (JC017A)

About HP Enterprise Security

HP is a leading provider of security and compliance solutions for the modern enterprise that wants to mitigate risk in their hybrid environment and defend against advanced threats. Based on market-leading products from HP ArcSight, HP Fortify, and HP TippingPoint, the HP Security Intelligence Platform uniquely delivers the advanced correlation, application protection, and network defenses to protect today's hybrid IT infrastructure from sophisticated cyber threats.

HP Services

HP ESP Global Services take a holistic approach to building and operating cyber security and response solutions and capabilities that support the cyber threat management and regulatory compliance needs of the world's largest enterprises. We use a combination of operational expertise—yours and ours—and proven methodologies to deliver fast, effective results and demonstrate ROI. Our proven, use-case driven solutions combine market leading technology together with sustainable business and technical process executed by trained and organized people.

Learn more about HP ESP Global Services at **hpenterprisesecurity.com**.

For more information

Find out how HP N platform Next-Generation Intrusion Prevention System (NGIPS) real-time protection and proactive network security for networks and data centers. Visit **hpenterprisesecurity.com/products/hp-tippingpoint-network-security/**.

Get connected

hp.com/go/getconnected

Current HP driver, support, and security alerts delivered directly to your desktop

4AA3-0819ENW, Created August 2010; Updated September 2012, Rev. 2