DATA SHEET

Extreme Security Threat Protection G2 - Intrusion Prevention

Integrated security, visibility, and control for next- generation network protection

HIGHLIGHTS

- Delivers superior zero-day threat protection and security intelligence
- Provides critical insight and visibility into network activity, including encrypted traffic
- Integrates with the Extreme Security Analytics G2 portfolio
- Enables granular control of both web and non-web applications by users and groups
- Reduces cost and complexity through consolidation and reduces bandwidth consumption
- Industry leading intrusion prevention and response
- Leverages your existing infrastructure investments and IT expertise

Extreme Security Threat Protection platform is designed to protect your business-critical network infrastructure through a unique combination of visibility and control and prevention. Extreme extends the abilities of traditional intrusion prevention systems by offering a next-generation solution that provides network security professionals with complete security, visibility and control over their network. Extreme Security Threat Protection helps reduce cost and complexity by consolidating point solutions into a single, extensible network security platform. And by controlling and eliminating non-critical, high-bandwidth activity, organizations can achieve additional cost savings within the infrastructure.

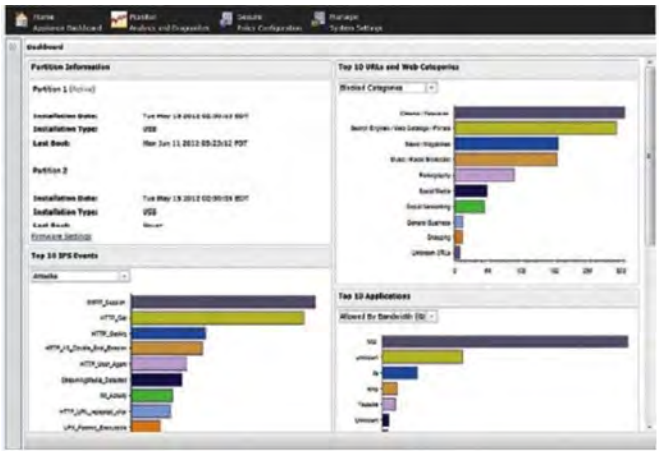
While organizations do require increasingly sophisticated security measures to address today's security threats, reducing management complexity and containing administration costs are also top priorities. Extreme Security Threat Protection is an integrated solution that can help you accomplish all of these tasks. By combining several advanced capabilities, this solution can help prevent threats, provide critical insight into network activities and enable granular application control, helping to establish a new level of integrated, simplified security.

Protection Against Evolving Threats

Security threats today are continually evolving. With the rapid growth of cutting-edge web applications and increased file sharing, activities that may have been considered harmless in the past could become potential openings for attackers. Traditional security means, such as anti-malware software and firewalls, have become easier to bypass. The need for more advanced, proactive threat protection is critical in order to help ensure productivity, data security and compliance. This means providing comprehensive security against new and emerging threats through web application protection, the ability to detect embedded shell code threats and many other advanced features. The Protocol Analysis Module (PAM) provides continuous content-and-security updates in order to help security professionals stay ahead of emerging threats. The PAM helps to drive higher protection against zero-day exploits and has the ability to accurately identify a wide range of security risks such as malware, botnets, peer-to-peer activity and many others.

Critical Insight and Visibility

By combining several key security capabilities, Extreme Security Threat Protection is able to go beyond basic threat protection and provide critical insight and visibility into network activity, such as which applications are being used, which websites are being visited and who is visiting them. To maintain security, organizations need to know exactly what is going on within their networks including which applications are being used and types of web sites being accessed from the corporate network. These activities can create opportunities for attacks, which can cause data loss, violate corporate policies or introduce compliance issues. Extreme Security Threat Protection can also provide visibility into bandwidth usage to help identify non-business-critical activities that consume high amounts of bandwidth and resources.



The Extreme Security Threat Protection dashboard provides an immediate view into the nature of traffic on the network including Web and application use by users and groups.

Granular Control Over Network Activity

Building upon high levels of threat-protection and network visibility, Extreme Security Threat Protection includes granular control functionality, which enables users to act on newly acquired insight into the network. Designed to reduce potential attack vectors and exposure to threats, these capabilities provide granular control over common attack delivery methods such as social media sites to prevent emerging attacks such as spear phishing and other advanced threats targeting users. Having the ability to create granular control policies allows organizations to reduce overall risk, as well as the bandwidth costs related to non-business use of the network. To provide maximum application coverage, Extreme Security Threat Protection includes support for more than 2,000 applications and individual actions, and leverages a database of more than 20 billion URLs. Extreme Security Threat Protection appliances can be constantly updated in order to maximize the effectiveness of use policies and protect against the latest Internet threats.

Seamless Deployment and Integration

Extreme Security Threat Protection can be seamlessly deployed into a wide variety of environments. This family of products includes flexible features such as interchangeable network modules to support a wide variety of networking standards and configurations as they change over time. It also provides flexible performance licensing to allow performance upgrades without hardware changes utilizing a simple license upgrade.

Immediate security protection is available out-of-the-box through a pre-configured default security policy. Extreme Security Threat Protection integrates tightly with the Extreme Security Analytics G2 portfolio. This includes the ability for Extreme Security Threat Protection appliances to send flow data in the standard Internet Protocol Flow Information Export (IPFIX) data format to provide a constant data feed for more sophisticated analysis and correlation. Extreme Security Threat Protection appliances can also receive quarantine commands with the ability to block traffic in the event that a security risk is detected. This provides security analytics users with the ability to take immediate action when a security threat is detected.

Centralized Policy Management and Security Updates

By combining several key security capabilities, Extreme Security Threat Protection is able to go beyond basic threat protection and provide critical insight and visibility into network activity, such as which applications are being used, which websites are being visited and who is visiting them. To maintain security, organizations need to know exactly what is going on within their networks including which applications are being used and types of web sites being accessed from the corporate network. These activities can create opportunities for attacks, which can cause data loss, violate corporate policies or introduce compliance issues. Extreme Security Threat Protection can also provide visibility into bandwidth usage to help identify non-business-critical activities that consume high amounts of bandwidth and resources.

The extensive reporting capabilities that are part of SiteProtector System enable specific and complex analysis. This means providing relevant security information to enable immediate action—from blocking an intruder to pushing an updated security policy. SiteProtector System provides the ability to analyze security information based on any number of filters, and then immediately use the analysis to create a report to share internally or prepare for auditors. The system provides a variety of default report templates and also enables template customization with very little effort. It can also quickly generate proof of compliance when needed. In the event of a disaster, resiliency capabilities are in place to help maintain security policies and settings

Taking a smarter approach to network security, Extreme Security Threat Protection provides next-generation intrusion prevention system capabilities for advanced protection against evolving security threats. By integrating several key security features into a single offering, Extreme Security Threat Protection provides a comprehensive, cost-efficient answer to the challenges faced by organizations today.

Threat Protection Appliances (Sensors) Specifications

	X-3 STANDARD APPLIANCE IPSG2-X3-PRI IPSG2-X3-SEC	X-4 ENTERPRISE APPLIANCE IPSG2-X4-PRI IPSG2-X4-SEC	X-5 ENTERPRISE PLUS APPLIANCE IPSG2-X5-PRI IPSG2-X5-SEC
PHYSICAL CHARACTERISTICS			
Form Factor	1 RU	1 RU	1 RU
Height (inch)	1.7"	1.7"	1.7"
Width (inch)	16.9"	16.9"	16.9"
Depth (inch)	21.2"	21.2"	21.2"
Weight	19 lb.	20.6 lb.	25.4 lb.
Management Interfaces	2 x 1GbE (RJ-45) IPv6 capable	2 x 1GbE (RJ-45) IPv6 capable	2 x 1GbE (RJ-45) IPv6 capable
Monitoring Interfaces (Fixed)	4 x 1GbE (RJ-45) integrated bypass	4 x 1GbE (RJ-45) integrated bypass	4 x 1GbE (RJ-45) integrated bypass
Interface Modules (Pluggable)	N/A	1	2
Monitoring Interfaces (Max.)	1 GbE – Up to 4 10 GbE – N/A	1 GbE – Up to 12 10 GbE – Up to 2	1 GbE – Up to 20 10 GbE – Up to 4
Supported Physical media types	100/1000 RJ-45	100/1000 RJ-45, 1G Fiber (SX/LX), 10G Fiber (SR/LR), 1G SFP, 10G SFP+	100/1000 RJ-45, 1G Fiber (SX/LX), 10G Fiber (SR/LR), 1G SFP, 10G SFP+
Redundant PSU	Yes – Optional	Yes – Optional	Yes – Included
PERFORMANCE CHARACTERISTICS			
Inspected Throughput	Up to 800 Mbps	Up to 1.5 Gbps	Up to 7 Gbps
Protected Segments	2	6	10
Flexible Performance Levels (FPL) All appliance comes with FPL 1 base	FPL 1: 400 Mbps FPL 2: 800 Mbps	FPL 1: 750 Mbps FPL 2: 1.5 Gbps	FPL 1: 2.5 Gbps FPL 2: 4 Gbps FPL 3: 5.5 Gbps FPL 4: 7 Gbps
Inspected SSL Throughput (inbound)	Up to 500 Mbps	Up to 900 Mbps	Up to 4.5 Gbps
Inspected SSL Throughput (outbound)	Up to 400 Mbps	Up to 700 Mbps	Up to 2.5 Gbps
Max Throughput (UDP)	3.5 Gbps	10 Gbps	15 Gbps
Connections per second (HTTP)	10K	15K	75K
Concurrent Sessions (HTTP)	500K	1M	2.2M
Average Latency	< 150 µs	< 75 µs	< 75 µs
ELECTRICAL AND ENVIRONMENTAL PARAMETERS			
AC Input Rating	460W (100-127V @ 5.6A, 200-240V @ 2.8A)		
Average Power Consumption	62W	81W	194W
Operating temperature	0°C – 40°C (32°F – 104°F)		
Safety Certification/Declaration	UL 60950-1, CAN CSA C22.2 no. 60950-1, EN 60950-1(CE Mark), IEC 60950-1, GB4943, GOST, UL-AR		
Environmental Declaration	Restriction of Hazardous Substances		

Ordering Information

PART NUMBER	NAME	DESCRIPTION
89511	IPSG2-X3-PRI	Extreme IPS G2 X3 Standard Appliance Primary, Base 400 Mbps inspected throughput, Optional ADD-ON performance license (Max 800 Mbps), Fixed 4x 1GbE RJ-45 monitoring interfaces
89512	IPSG2-X3-SEC	Extreme IPS G2 X3 Standard Appliance Secondary/Failover (Must have same configuration like Primary)
89513	IPSG2-X4-PRI	Extreme IPS G2 X4 Enterprise Appliance Primary, Base 750 Mbps inspected throughput, Optional ADD-ON performance license (Max 1.5 Gbps), Fixed 4x 1GbE RJ-45 monitoring interfaces, Optional Network Interface Module
89514	IPSG2-X4-SEC	Extreme IPS G2 X4 Enterprise Appliance Secondary/Failover (Must have same configuration like Primary)
89515	IPSG2-X5-PRI	Extreme IPS G2 X5 Enterprise Plus Appliance Primary, Base 2.5 Gbps inspected throughput, Optional ADD-ON performance license (Max 7 Gbps), Fixed 4x 1GbE RJ-45 monitoring interfaces, Optional Network Interface Modules; Redundant power supply included
89516	IPSG2-X5-SEC	Extreme IPS G2 X5 Enterprise Plus Appliance Secondary/Failover (Must have same configuration like Primary)
89519	IPSG2-X3-P-AWC-SS	Extreme IPS G2 X3 Add-on Subscription for Application/Web Control Update Primary
89520	IPSG2-X3-S-AWC-SS	Extreme IPS G2 X3 Add-on Subscription for Application/Web Control Update Failover
89521	IPSG2-X4-P-AWC-SS	Extreme IPS G2 X4 Add-on Subscription for Application/Web Control Update Primary
89522	IPSG2-X4-S-AWC-SS	Extreme IPS G2 X4 Add-on Subscription for Application/Web Control Update Failover
89523	IPSG2-X5-P-AWC-SS	Extreme IPS G2 X5 Add-on Subscription for Application/Web Control Update Primary
89524	IPSG2-X5-S-AWC-SS	Extreme IPS G2 X5 Add-on Subscription for Application/Web Control Update Failover
89527	IPSG2-X3-P-IPR-SS	Extreme IPS G2 X3 Add-on Subscription for IP Reputation Services Primary
89528	IPSG2-X3-S-IPR-SS	Extreme IPS G2 X3 Add-on Subscription for IP Reputation Services Failover
89529	IPSG2-X4-P-IPR-SS	Extreme IPS G2 X4 Add-on Subscription for IP Reputation Services Primary
89530	IPSG2-X4-S-IPR-SS	Extreme IPS G2 X4 Add-on Subscription for IP Reputation Services Failover
89531	IPSG2-X5-P-IPR-SS	Extreme IPS G2 X5 Add-on Subscription for IP Reputation Services Primary
89532	IPSG2-X5-S-IPR-SS	Extreme IPS G2 X5 Add-on Subscription for IP Reputation Services Failover
89535	IPSG2-X3-P-SSL-SW	Extreme IPS G2 X3 Add-on License for SSL Inspection Primary
89536	IPSG2-X3-S-SSL-SW	Extreme IPS G2 X3 Add-on License for SSL Inspection Failover
89537	IPSG2-X4-P-SSL-SW	Extreme IPS G2 X4 Add-on License for SSL Inspection Primary
89501	IPSG2-SMSW-STD	SiteProtector Standard Edition Software (5 Nodes)
89502	IPSG2-SMSW-ENT	SiteProtector Enterprise Edition Software (20 Nodes)
89503	IPSG2-SMSW-ENTPLUS	SiteProtector Enterprise Plus Edition Software (Unlimited Nodes)
89506	IPSG2-SMUPG-S-E	SiteProtector Upgrade from Standard to Enterprise Edition
89507	IPSG2-SMUPG-E-EPL	SiteProtector Upgrade from Enterprise to Enterprise Plus Edition
89510	IPSG2-ADD5	SiteProtector Add 5 Node License
89538	IPSG2-X4-S-SSL-SW	Extreme IPS G2 X4 Add-on License for SSL Inspection Failover
89539	IPSG2-X5-P-SSL-SW	Extreme IPS G2 X5 Add-on License for SSL Inspection Primary
89540	IPSG2-X5-S-SSL-SW	Extreme IPS G2 X5 Add-on License for SSL Inspection Failover
89543	IPSG2-X3-P-HTP-SW	Extreme IPS G2 X3 400 Mbps Inspection Throughput Increase Primary
89544	IPSG2-X3-S-HTP-SW	Extreme IPS G2 X3 400 Mbps Inspection Throughput Increase Secondary
89545	IPSG2-X4-P-HTP-SW	Extreme IPS G2 X4 750 Mbps Inspection Throughput Increase Primary
89546	IPSG2-X4-S-HTP-SW	Extreme IPS G2 X4 750 Mbps Inspection Throughput Increase Secondary
89547	IPSG2-X5-P-HTP-SW	Extreme IPS G2 X5 1500 Mbps Inspection Throughput Increase Primary
89548	IPSG2-X5-S-HTP-SW	Extreme IPS G2 X5 1500 Mbps Inspection Throughput Increase Secondary
89551	IPSG2-8PNM-1G-TX	Extreme IPS G2 Network Module 8-port 1G Copper with built-in bypass
89552	IPSG2-4PNM-1G-SX	Extreme IPS G2 Network Module 4-port 1G SX Fiber with built-in bypass
89553	IPSG2-4PNM-1G-LX	Extreme IPS G2 Network Module 4-port 1G LX Fiber with built-in bypass
89554	IPSG2-2PNM-10G-SR	Extreme IPS G2 Network Module 2-port 10GbE SR Fiber with built-in bypass
89555	IPSG2-2PNM-10G-LR	Extreme IPS G2 Network Module 2-port 10GbE LR Fiber with built-in bypass
89556	IPSG2-4PNM-1G-SFP	Extreme IPS G2 Network Module 4-port 1G SFP (requires transceivers)
89557	IPSG2-2PNM-10G-SFP+	Extreme IPS G2 Network Module 2-port 10G SFP+ (requires transceivers)

PART NUMBER	NAME	DESCRIPTION
89558	IPSG2-DTK-1G-LX	Dual Transceiver Kit 1G LX Fiber
89559	IPSG2-DTK-1G-SX	Dual Transceiver Kit 1G SX Fiber
89560	IPSG2-DTK-1G-TX	Dual Transceiver Kit 1G TX Copper
89561	IPSG2-DTK-10G-LR	Dual Transceiver Kit 10G LR Fiber
89562	IPSG2-DTK-10G-SR	Dual Transceiver Kit 10G SR Fiber
89563	IPSG2-PSU	Power Supply Unit 460 WATT

POWER CORDS
In support of its expanding Green initiatives as of July 1st 2014, Extreme Networks will no longer ship power cords with products. Power cords can be ordered separately but need to be specified at the time order. Please refer to www.extremenetworks.com/product/powercords/ for details on power cord availability for this product.

Warranty

As a customer-centric company, Extreme Networks is committed to providing quality products and solutions. In the event that one of our products fails due to a defect, we have developed a comprehensive warranty that protects you and provides a simple way to get your products repaired or media replaced as soon as possible.

Extreme Networks Intrusion Prevention System appliances come with a one year warranty against manufacturing defects. For full warranty terms and conditions please go to: http://www.extremenetworks.com/support/policies/warranty.

Service and Support

Extreme Networks provides comprehensive service offerings that range from Professional Services to design, deploy and optimize customer networks, customized technical training, to service and support tailored to individual customer needs. Please contact your Extreme Networks account executive for more information about Extreme Networks Service and Support.

Extreme®
Connect Beyond the Network

http://www.extremenetworks.com/contact / Phone +1-408-579-2800