DATA SHEET

Extreme Networks Security Analytics G2 – SIEM

Boost compliance & threat protection through integrated Security Information and Event Management, Log Management, and Network Behavioral Analysis

HIGHLIGHTS

- Integrate log management and network threat protection technologies within a common database and shared dashboard user interface
- Reduce thousands of security events into a manageable list of suspected offenses
- Detect and track malicious activity over extended time periods, helping to uncover advanced threats often missed by other security solutions
- Detect insider fraud with advanced capabilities
- Help exceed regulation mandates and support compliance
- Leverages existing investments in network and security infrastructure while accelerating time to value through out-of-box functionality, rapid deployment, and staff efficiency gains
- Integrates with Extreme Networks Threat Protection G2 portfolio, Network Access Control (NAC), and Purview solutions to provide a unified, real-time view of the threat landscape and effectively detect, isolate, and automatically remediate threats
- Virtual Flow Collector allows the analysis of network behavior and enables Layer 7 visibility within virtual infrastructures
- Integrated feature-rich management web interface for all applications; Multilingual web user interface – English, French, German, Japanese, Spanish, Korean, Chinese and more

Today's networks are larger and more complex than ever before, and protecting them against malicious activity is a never-ending task. Organizations seeking to safeguard their intellectual property, protect their customer identities and avoid business disruptions need to do more than monitor logs and network flow data; they need to leverage advanced tools to detect these activities in a consumable manner. Extreme Networks Security Analytics SIEM can serve as the anchor solution within a small or large organization's security operations center to collect, normalize and correlate available network data using years' worth of contextual insights. The result is something called security intelligence

At the heart of this product sits a highly scalable database designed to capture real-time log event and network flow data, revealing the footprints of would-be attackers. Extreme Networks SIEM is an enterprise solution that consolidates log source event data from thousands of devices distributed across a network, storing every activity in its raw form, and then performing immediate correlation activities to distinguish the real threats from false positives. It also captures real-time Layer 4 network flow data and, more uniquely, Layer 7 application payloads, using deep packet inspection technology.

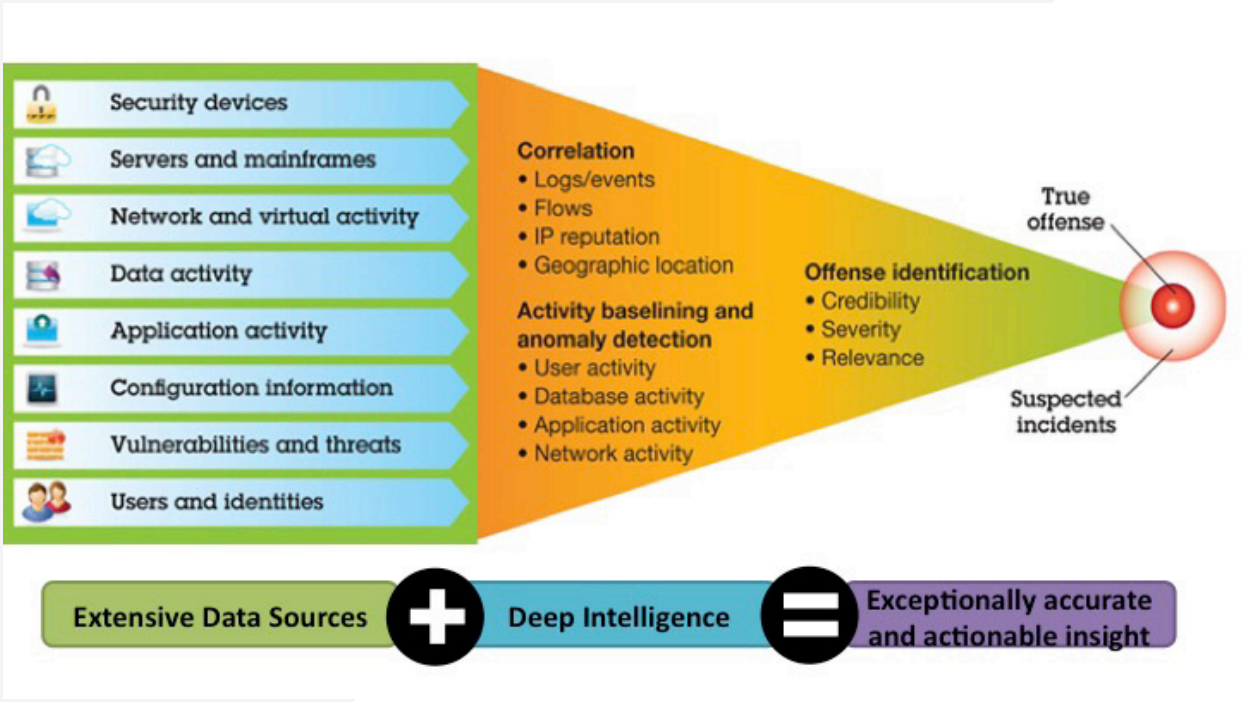
An intuitive user interface shared across all Extreme Networks Security Analytics components helps IT personnel quickly identify and remediate network attacks by rank, ordering hundreds of alerts and patterns of anomalous activity into a drastically reduced number of offenses warranting further investigation.

Providing Real-Time Visibility for Threat Detection and Prioritization

Extreme Networks SIEM provides contextual and actionable surveillance across the entire IT infrastructure, helping organizations detect and remediate threats often missed by other security solutions. These threats can include inappropriate use of applications; insider fraud; and advanced, "low and slow" threats easily lost in the "noise" of millions of events.

SIEM collects information that includes

- Security events: Events from firewalls, virtual private networks, intrusion detection systems, intrusion prevention systems and more
- Network events: Events from switches, routers, servers, hosts and more
- Network activity context: Layer 7 application context from network and application traffic
- User or asset context: Contextual data from identity and access-management products and vulnerability scanners
- Operating system information: Vendor name and version number specifics for network assets



Extreme Networks SIEM captures data across a broad range of feeds, reducing it to a manageable list of offenses using pre-existing and customer-defined rules

- Application logs: Enterprise resource planning (ERP), workflow, application databases, management platforms and more

Reducing and Prioritizing Alerts to Focus Investigations into Actionable Offenses

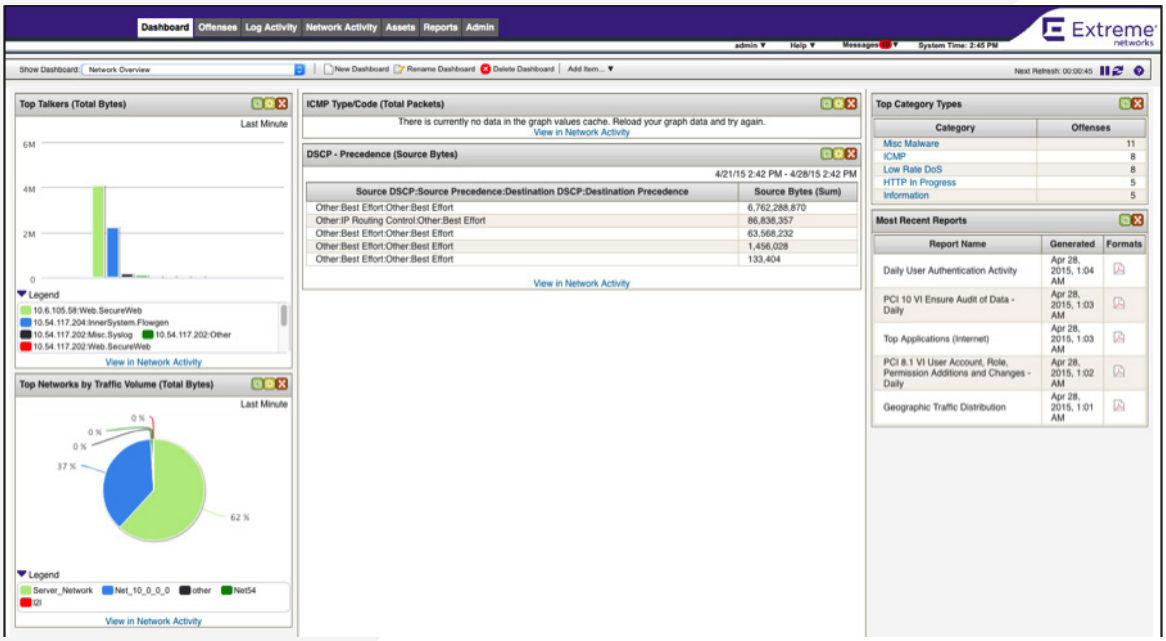
Many organizations create millions—or even billions—of events per day, and distilling that data down to a short list of priority offenses can be daunting. SIEM automatically discovers most network log source devices and inspects network flow data to find and classify valid hosts and servers (assets) on the network—tracking the applications, protocols, services and ports they use. It collects, stores and analyzes this data and performs real-time event correlation for use in threat detection and compliance reporting and auditing. Billions of events and flows can therefore be reduced and prioritized into a handful of actionable offenses, according to their business impact.

As a result, security professionals normally begin to see value from a SIEM installation in days rather than weeks, and deployments occur without a small army of expensive consultants. Automatic discovery features and out-of-the-box templates and filters mean you don't spend months teaching the system about your environment as with more generalized IT operational tools. The architecture employs multiple models of event processor appliances, event collector appliances.

Answering Key Questions for More Effective Threat Management

Security teams need to answer key questions to fully understand the nature of their potential threats: Who is attacking? What is being attacked? What is the business impact? Where do I investigate? SIEM tracks significant incidents and threats, building a history of supporting data and relevant information. Details such as attack targets, point in time, asset value, vulnerability state, offending users' identities, attacker profiles, active threats and records of previous offenses all help provide security teams with the intelligence they need to act.

Real-time, location-based and historical searching of event and flow data for analysis and forensics can greatly improve an organization's ability to assess activities and resolve incidents. With easy-to-use dashboards, time-series views, drill-down searching, packet-level content visibility and hundreds of predefined searches, users can quickly aggregate data to summarize and identify anomalies and top activity contributors. They can also perform federated searches across large, geographically distributed environments.



SIEM centralized dashboard shows log source events and network flow traffic together, helping to correlate discrete events

Gaining Application Visibility and Anomaly Detection

SIEM supports a variety of anomaly detection capabilities to identify changes in behavior affecting applications, hosts, servers and areas of the network. For example, SIEM can detect off-hours or excessive usage of an application or cloud-based service, or network activity patterns that are inconsistent with historical, moving-average profiles and seasonal usage patterns. SIEM learns to recognize these daily and weekly usage profiles, helping IT personnel to quickly identify meaningful deviations.

SIEM centralized database stores log source events and network flow traffic together, helping to correlate discrete events with bidirectional network flow activity. It also can group network flow traffic and record operations occurring within a narrow time period as a single database entry to help reduce storage consumption and conserve license requirements.

Its ability to detect application traffic at Layer 7 enables SIEM to provide accurate analysis and insight into an organization's network for policy, threat and general network activity monitoring. With the addition of an Extreme Networks Security Flow Collector appliance, SIEM can monitor the use of applications such as ERP, databases, Skype, voice over IP (VoIP) and social media from within the network. This includes insight into who is using what, analysis and alerts for content transmission, and correlation with other network and log activity to reveal inappropriate data transfers and excessive usage patterns. While SIEM ships with numerous anomaly and behavioral detection rules, security teams can also create their own through a filtering capability that enables them to apply anomaly detection against time-series data.

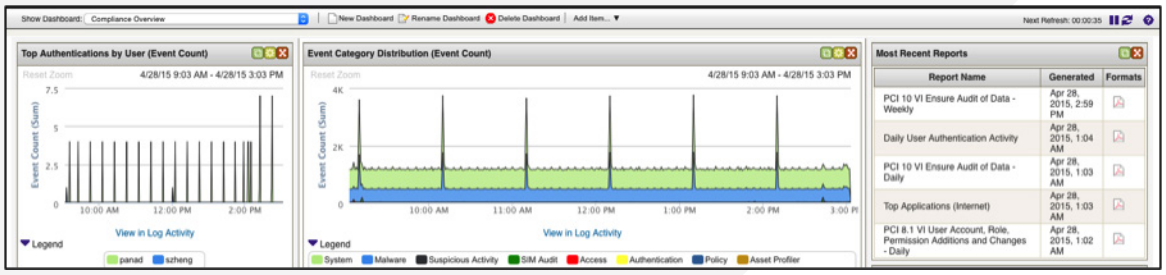
Commanding a Highly Intuitive, One Console Security Solution

SIEM provides a solid foundation for an organization's security operations center by providing a centralized user interface that offers role-based access by function and a global view to access real-time analysis, incident management and reporting. Five default dashboards are available—including threat & security, network activity, application activity, system monitoring and compliance—plus users can create and customize their own workspaces.

These dashboards make it easy to spot spikes in alert activity that may signal the beginnings of an attack. Clicking on a graph launches a drill-down capability that enables security teams to quickly investigate the highlighted events or network flows.

Extending Threat Protection to Virtual Environments

Since virtual servers are just as susceptible to security vulnerabilities as physical servers, comprehensive security intelligence solutions must also include appropriate measures to protect the applications and data residing within the virtual data center. Using VFlow Collector appliances, IT professionals gain increased visibility into the vast amount of business application activity within their virtual networks and can better identify these applications for security monitoring, application layer behavior analysis and anomaly detection. Operators can also capture application content for deeper security and policy forensics.



SIEM Compliance Dashboard.

Producing Detailed Data Access and User Activity Reports to Manage Compliance

SIEM provides the transparency, accountability and measurability critical to an organization's success in meeting regulatory mandates and reporting on compliance. The solution's ability to correlate and integrate surveillance feeds yields more complete metrics reporting on IT risks for auditors, as well as hundreds of reports and rules templates to address industry compliance requirements.

Organizations can efficiently respond to compliance-driven IT security requirements with the extensibility of SIEM to include new definitions, regulations and best practices through automatic updates. In addition, profiles of all network assets can be grouped by business function—for example, servers that are subject to Health Insurance Portability and Accountability Act (HIPAA) compliance audits. The solution's pre-built dashboards, reports and rules templates are designed for the following regulations and control frameworks: CobiT, SOX, GLBA, NERC/FERC, FISMA, PCI DSS, HIPAA, UK GSi/GCSx, GPG and more.

Extreme Networks SIEM solution features appliances as well as virtual offerings. Available Extreme Networks SIEM solution components include:

- SIEM Base All-in-One
- SIEM Console Manager
- Event Collector & Processor
- Flow Collector & Processor
- Combined Event/Flow Processor
- Data Node
- High Availability Options

SIEM BASE ALL-IN-ONE

Extreme Networks SIEM All-In-One Appliances delivers actionable security intelligence in a rack-mount, network-ready platform. With flexible deployment options, they provide on-board event collection and correlation, Layer 7 traffic analysis, aggregation of flow data from multiple network-connected devices, and a feature-rich management interface. Pre-installed software and web-based setup simplifies deployment and configuration for unified security management.

SIEM All-In-One appliances provide easy deployment and cost efficient network monitoring from small offices or enterprise branches to large and geographically dispersed organizations. The SIEM All-in-One standard appliance suits a small office or enterprise need to monitor minimal rates of network events and flows.

The SIEM Enterprise and EnterprisePlus Appliance models provide a range of options for large and geographically dispersed organizations. They are ideal for users that demand a scalable, enterprise-class solution that can be easily upgraded to support additional flow and event monitoring capacity as required. Table 1 below shows the specifications for SIEM All-in-One deployment.

All SIEM platforms capture event and flow data from a broad range of networked devices including application servers, web servers, workstations, routers, switches, firewalls, VPN tunnel servers, and IDS/IPS appliances.

SIEM CONSOLE MANAGER

For large deployments, the SIEM Console Manager distributes the collection and processing of flows and logs while maintaining a global view of the entire network. Console Manager requires a minimum of one Processor Appliance (Event Processor, Flow Processor and/or Combined Event/Flow Processor).

EVENT COLLECTOR AND PROCESSOR

The SIEM Event Collector & Processor offers an expansion unit for Extreme Networks SIEM Distributed deployment. Event Collectors can be used to collect and parse events on a remote site that have bandwidth constraints and forward those events to the Event Processors. Event Processor offloads and enhances processing of event data from the base appliances. Status events are collected from a broad array of network and security devices — including router syslogs, SNMP events, and firewall events. Multiple Event Processors may be connected to a single console manger.

FLOW COLLECTOR AND PROCESSOR

A network traffic flow is a sequence of packets that share common characteristics – such as source/destination IP address, source/destination TCP port, and IP protocol used. SIEM Flow Collectors are deployed at strategic points in the network to collect IP traffic flow information from a broad range of networked devices — including switches, routers, security appliances, servers, and applications. SIEM Flow Collectors go beyond traditional flow-based data sources to enable application-layer (L1-L7) flow analysis and anomaly detection. Deep packet and content inspection capabilities identify threats tunneled over standard protocols and ports. Flow Collectors interface with the Extreme Networks SIEM All-in-One Appliances or the SIEM Flow Processor. A SIEM Virtual Flow Collector is a virtual appliance that enables the analysis of network behavior and Layer 7 visibility within the enterprise's virtual infrastructure.

The SIEM Flow Processor is an expansion unit for Extreme Networks SIEM Distributed deployment. It offloads and enhances the processing of flow data from the Base Appliances and interfaces with Flow Collectors to collect IP traffic flow information from a broad range of devices.

COMBINED EVENT/FLOW PROCESSOR

The SIEM Combined Event/Flow Processor is an expansion unit for Extreme Networks SIEM Distributed deployment. It processes both flow data and event data. Deployment of the Combined Event/Flow Anomaly Processor enables a highly distributed enterprise to provide cost effective local event and flow collection. It is well suited as an introductory event and network activity processor for remote or branch offices.

SIEM DATA NOTE

In SIEM deployments, all data is stored on the Event or Flow processors. Data Node enhances the storage and search capability of SIEM deployments. Data Nodes can be clustered around Event and Flow Processors giving the Event and Flow Processors access to the space and processing capacity of each Data Node instance. This helps in creating data storage deployments capable of potentially 100s of TBs of data while simultaneously adding the processing capacity to handle the queries on this data. Once in place, intelligent data distribution algorithms will disperse all incoming data amongst the Data Node instance in a manner this is optimal for both query and storage.

SIEM HIGH AVAILABILITY OPTIONS

Adding SIEM high-availability solutions can help organizations take advantage of automatic failover and full disk synchronization between primary & secondary systems—a capability typically available only with costly, manually implemented software and storage solutions. Users can easily deploy high-availability data storage and analysis through advanced plug-and-play appliances. At regular intervals the secondary host sends a heartbeat ping to the primary host to detect hardware or network failure. If the secondary host detects a failure, the secondary host automatically assumes all responsibilities of the primary host.

Table 1: Technical Specification for SIEM All-in-One

	ALL-IN-ONE VIRTUAL	ALL-IN-ONE STANDARD	ALL-IN-ONE ENTERPRISE	ALL-IN-ONE ENTERPRISEPLUS
Description	Extreme Networks SIEM G2 ALL-IN-ONE Virtual	Extreme Networks SIEM G2 ALL-IN-ONE Standard Appliance	Extreme Networks SIEM G2 ALL-IN-ONE Enterprise Appliance	Extreme Networks SIEM ALL-IN-ONE EnterprisePlus Appliance
Form Factor	-	1 RU Appliance	2 RU Appliance	2 RU Appliance
Processor	4 vCPU minimum required*	Intel Xeon E5-2630 V2, 2.6GHz, 6 Core, 15MB Cache (x1)	Intel Xeon E5-2620 V2, 2.6GHz, 6 Core, 15MB Cache (x2)	Intel Xeon E5-2680 V2, 2.8GHz, 10 Core, 25MB Cache (x2)
Memory	24 GB minimum required*	32GB	64GB	128GB
Hard Drive	1 TB minimum required*	1.5TB usable	6.2TB usable	40TB usable
Base Events Per Second (EPS)	100 EPS	1000 EPS	1,000 EPS	1,000 EPS
Max Events Per Second (EPS)	5,000 EPS	1,000 EPS	5,000 EPS	15,000 EPS
Base Flows Per Minute (FPM)	15,000 FPM	25,000 FPM	25,000 FPM	25,000 FPM
Max Flows Per Minute (FPM)	200,000 FPM	50,000 FPM	200,000 FPM	300,000 FPM
Upgrade Options	None	None	Can be upgraded to distributed model (Console Manager)	Can be upgraded to distributed model (Console Manager)

**Note: Requirements may vary with high usage*

Table 2: Technical Specification for SIEM Console Manager

	CONSOLE VIRTUAL	CONSOLE ENTERPRISE	CONSOLE ENTERPRISEPLUS
Description	Extreme Networks SIEM G2 CONSOLE Virtual	Extreme Networks SIEM G2 CONSOLE Enterprise Appliance	Extreme Networks SIEM G2 CONSOLE EnterprisePlus Appliance
Form Factor	-	2 RU Appliance	2 RU Appliance
Processor	4 vCPU minimum required*	Intel Xeon E5-2620 V2, 2.6GHz, 6 Core, 15MB Cache (x2)	Intel Xeon E5-2680 V2, 2.8GHz, 10 Core, 25MB Cache (x2)
Memory	24 GB minimum required*	64GB	128GB
Hard Drive	1 TB minimum required*	6.2TB usable	40TB usable
Events Per Second (EPS)	N/A	N/A (External Event Processor)	N/A (External Event Processor)
Flows Per Minute (FPM)	N/A	N/A (External Flow Processor)	N/A (External Flow Processor)

** Note: Requirements may vary with high usage*

Table 3: Technical specification for SIEM Event & Flow Processor

	FLP VIRTUAL	FLP ENTERPRISE	FLP ENTERPRISEPLUS	EVP VIRTUAL	EVP ENTERPRISE	EVP ENTERPRISEPLUS
Description	Extreme Networks SIEM G2 Flow Processor (FLP) Virtual	Extreme Networks SIEM G2 Flow Processor (FLP) Enterprise Appliance	Extreme Networks SIEM G2 Flow Processor (FLP) EnterprisePlus Appliance	Extreme Networks SIEM G2 Event Processor (EVP) Virtual	Extreme Networks SIEM G2 Event Processor (EVP) Enterprise Appliance	Extreme Networks SIEM G2 Event Processor (EVP) EnterprisePlus Appliance
Form Factor	-	2 RU Appliance	2 RU Appliance	-	2 RU Appliance	2 RU Appliance
Processor	4 vCPU minimum required*	Intel Xeon E5-2620 V2, 2.6GHz, 6 Core, 15MB Cache (x2)	Intel Xeon E5-2680 V2, 2.8GHz, 10 Core, 25MB Cache (x2)	4 vCPU minimum required*	Intel Xeon E5-2620 V2, 2.6GHz, 6 Core, 15MB Cache (x2)	Intel Xeon E5-2680 V2, 2.8GHz, 10 Core, 25MB Cache (x2)
Memory	12GB minimum required*	64GB	128GB	12GB minimum required*	64GB	128GB
Hard Drive	-	6.2TB usable	40TB usable	-	6.2TB usable	40TB usable
Base Events Per Second (EPS)	N/A	N/A	N/A	100 EPS	2,500 EPS	2,500 EPS
Max Events Per Second (EPS)	N/A	N/A	N/A	20,000 EPS	20,000 EPS	40,000 EPS
Base Flows Per Minute (FPM)	15,000 FPM	100,000 FPM	100,000 FPM	N/A	N/A	N/A
Base Flows Per Minute (FPM)	600,000 FPM	600,000 FPM	1,200,000 FPM	N/A	N/A	N/A

** Note: Requirements may vary with high usage*

Table 4: Technical Specification for SIEM Combined Event & Flow Processor

	COMBINED EVP-FLP ENTERPRISE	COMBINED EVP-FLP ENTERPRISEPLUS
Description	Extreme Networks SIEM G2 Combined Event & Flow Processor Enterprise Appliance	Extreme Networks SIEM G2 Combined Event & Flow Processor EnterprisePlus Appliance
Form Factor	2 RU Appliance	2 RU Appliance
Processor	Intel Xeon E5-2620 V2, 2.6GHz, 6 Core, 15MB Cache (x2)	Intel Xeon E5-2680 V2, 2.8GHz, 10 Core, 25MB Cache (x2)
Memory	64GB	128GB
Hard Drive	6.2TB usable	40TB usable
Base Events Per Second (EPS)	1,000 EPS	1,000 EPS
Max Events Per Second (EPS)	5,000 EPS	15,000 EPS
Base Flows Per Minute (FPM)	25,000 FPM	25,000 FPM
Base Flows Per Minute (FPM)	200,000 FPM	300,000 FPM

Table 5: Technical Specification for SIEM Data Node

	DN VIRTUAL	DN ENTERPRISE	DN ENTERPRISEPLUS
Description	Extreme Networks SIEM G2 Data Node Virtual	Extreme Networks SIEM G2 Data Node Enterprise Appliance	Extreme Networks SIEM G2 Data Node EnterprisePlus Appliance
Form Factor	-	2 RU Appliance	2 RU Appliance
Processor	4 vCPU minimum required*	Intel Xeon E5-2620 V2, 2.6GHz, 6 Core, 15MB Cache (x2)	Intel Xeon E5-2680 V2, 2.8GHz, 10 Core, 25MB Cache (x2)
Memory	24 GB minimum required*	64GB	128GB
Hard Drive	-	6.2TB usable	40TB usable
Events Per Second (EPS)	N/A	N/A (External Event Processor)	N/A (External Event Processor)
Flows Per Minute (FPM)	N/A	N/A (External Flow Processor)	N/A (External Flow Processor)

** Note: Requirements may vary with high usage*

Table 6: Technical Specification for Event Collector

	EVENT COLLECTOR
Description	Extreme Networks SIEM G2 Event Collector Appliance
Form Factor	1 RU Appliance
Processor	Intel Xeon E5-2630 V2, 2.6GHz, 6 Core, 15MB Cache (x1)
Memory	16 GB
Hard Drive	600 GB usable
Base Events Per Second (EPS)	1,000 EPS
Max Events Per Second (EPS)	5,000 EPS
Base Flows Per Minute (FPM)	25,000 FPM
Base Flows Per Minute (FPM)	200,000 FPM

Table 5: Technical Specification for SIEM Flow Collector

	VIRTUAL FLOW COLLECTOR	FLOW COLLECTOR APPLIANCE 1G TX	FLOW COLLECTOR APPLIANCE MG TX	FLOW COLLECTOR APPLIANCE MG SX	FLOW COLLECTOR APPLIANCE MG FIBER SR/LR
Description	Extreme Networks SIEM G2 Virtual Flow Collector	Extreme Networks SIEM G2 Flow Collector Appliance 1Gbps TX	Extreme Networks SIEM G2 Flow Collector Appliance Multi-Gbps TX	Extreme Networks SIEM G2 Flow Collector Appliance Multi-Gbps SX	Extreme Networks SIEM G2 Flow Collector Appliance Multi-Gbps Fiber SR/Lr
Form Factor	1 RU Appliance	1 RU Appliance	1 RU Appliance	1 RU Appliance	1 RU Appliance
Processor	4 vCPU minimum required*	Intel Xeon E5-2630 V2, 2.6GHz, 6 Core, 15MB Cache	Intel Xeon E5-2630 V2, 2.6GHz, 6 Core, 15MB Cache	Intel Xeon E5-2630 V2, 2.6GHz, 6 Core, 15MB Cache	Intel Xeon E5-2630 V2, 2.6GHz, 6 Core, 15MB Cache
Memory	12GB minimum required*	16 GB	16 GB	16 GB	16 GB
Hard Drive	500 GB minimum required*	600 GB usable	600 GB usable	600 GB usable	600 GB usable
Network Ports	-	5x 10/100/1000 Base-T 1x 2 port 10Gbps Intel X520 SFP+ Embedded Adapter	4x 1Gbps SFP+ Copper 1x 2 port 10Gbps Intel X520 SFP+ Embedded Adapter	4x 1Gbps SFP+ Optical 1x 2 port 10Gbps Intel X520 SFP+ Embedded Adapter	2x 10Gbps SR/ LR 1x 2 port 10Gbps Intel X520 SFP+ Embedded Adapter

** Note: Requirements may vary with high usage*

Ordering Information

PART NUMBER	NAME	DESCRIPTION
89079	SIEMG2-AIO-STD	Extreme Networks SIEM G2 ALL-IN-ONE Standard Appliance
89080	SIEMG2-AIO-STD-HA	Extreme Networks SIEM G2 ALL-IN-ONE Standard HA Appliance
89081	SIEMG2-AIO-ENT	Extreme Networks SIEM G2 ALL-IN-ONE Enterprise Appliance
89082	SIEMG2-AIO-ENT-HA	Extreme Networks SIEM G2 ALL-IN-ONE Enterprise HA Appliance
89083	SIEMG2-AIO-ENTPL	Extreme Networks SIEM G2 ALL-IN-ONE Enterprise Plus Appliance
89084	SIEMG2-AIO-ENTPL-HA	Extreme Networks SIEM G2 ALL-IN-ONE Enterprise Plus HA Appliance
89085	SIEMG2-AIO-VIR	Extreme Networks SIEM G2 ALL-IN-ONE Virtual
89086	SIEMG2-AIO-VIR-HA	Extreme Networks SIEM G2 ALL-IN-ONE Virtual HA
89087	SIEMG2-CON-ENT	Extreme Networks SIEM G2 CONSOLE Enterprise Appliance
89088	SIEMG2-CON-ENT-HA	Extreme Networks SIEM G2 CONSOLE Enterprise HA Appliance
89089	SIEMG2-CON-ENTPL	Extreme Networks SIEM G2 CONSOLE Enterprise Plus Appliance
89090	SIEMG2-CON-ENTPL-HA	Extreme Networks SIEM G2 CONSOLE Enterprise Plus HA Appliance
89091	SIEMG2-CON-VIR	Extreme Networks SIEM G2 CONSOLE Virtual
89092	SIEMG2-CON-VIR-HA	Extreme Networks SIEM G2 CONSOLE Virtual HA
89093	SIEMG2-EVP-ENT	Extreme Networks SIEM G2 EVP Enterprise Appliance
89094	SIEMG2-EVP-ENT-HA	Extreme Networks SIEM G2 EVP Enterprise HA Appliance
89095	SIEMG2-EVP-ENTPL	Extreme Networks SIEM G2 EVP Enterprise Plus Appliance
89096	SIEMG2-EVP-ENTPL-HA	Extreme Networks SIEM G2 EVP Enterprise Plus HA Appliance
89097	SIEMG2-EVP-VIR	Extreme Networks SIEM G2 EVP Virtual
89098	SIEMG2-EVP-VIR-HA	Extreme Networks SIEM G2 EVP Virtual HA
89099	SIEMG2-FLP-ENT	Extreme Networks SIEM G2 FLP Enterprise Appliance
89100	SIEMG2-FLP-ENT-HA	Extreme Networks SIEM G2 FLP Enterprise HA Appliance
89101	SIEMG2-FLP-ENTPL	Extreme Networks SIEM G2 FLP Enterprise Plus Appliance
89102	SIEMG2-FLP-ENTPL-HA	Extreme Networks SIEM G2 FLP Enterprise Plus HA Appliance
89103	SIEMG2-FLP-VIR	Extreme Networks SIEM G2 FLP Virtual
89104	SIEMG2-FLP-VIR-HA	Extreme Networks SIEM G2 FLP Virtual HA
89105	SIEMG2-CEF-ENT	Extreme Networks SIEM G2 Combined EVP-FLP Enterprise Appliance
89106	SIEMG2-CEF-ENT-HA	Extreme Networks SIEM G2 Combined EVP-FLP Enterprise HA Appliance
89107	SIEMG2-CEF-ENTPL	Extreme Networks SIEM G2 Combined EVP-FLP Enterprise Plus Appliance
89108	SIEMG2-CEF-ENTPL-HA	Extreme Networks SIEM G2 Combined EVP-FLP Enterprise Plus HA Appliance
89109	SIEMG2-EVC-APL	Extreme Networks SIEM G2 Event Collector Appliance
89110	SIMEG2-EVC-VIR	Extreme Networks SIEM G2 Event Collector Virtual
89111	SIEMG2-DN-ENT	Extreme Networks SIEM G2 Data Node Enterprise Appliance
89112	SIEMG2-DN-ENT-HA	Extreme Networks SIEM G2 Data Node Enterprise HA Appliance
89113	SIEMG2-DN-ENTPL	Extreme Networks SIEM G2 Data Node Enterprise Plus Appliance
89114	SIEMG2-DN-ENTPL-HA	Extreme Networks SIEM G2 Data Node Enterprise Plus HA Appliance
89115	SIEMG2-DN-VIR	Extreme Networks SIEM G2 Data Node Virtual
89116	SIEMG2-DN-VIR-HA	Extreme Networks SIEM G2 Data Node Virtual HA
89117	SIEMG2-FC-1G-TX	Extreme Networks SIEM G2 Flow Collector Appliance 1 Gbps TX
89118	SIEMG2-FC-1G-TX-HA	Extreme Networks SIEM G2 Flow Collector HA Appliance 1 Gbps TX
89119	SIEMG2-FC-MG-TX	Extreme Networks SIEM G2 Flow Collector Appliance Multi-Gbps TX
89120	SIEMG2-FC-MG-TX-HA	Extreme Networks SIEM G2 Flow Collector HA Appliance Multi-Gbps TX
89121	SIEMG2-FC-MG-SX	Extreme Networks SIEM G2 Flow Collector Appliance Multi-Gbps SX
89122	SIEMG2-FC-MG-SX-HA	Extreme Networks SIEM G2 Flow Collector HA Appliance Multi-Gbps SX 1301)
89123	SIEMG2-FC-MG-SR	Extreme Networks SIEM G2 Flow Collector Appliance Multi-Gbps Fiber SR
89124	SIEMG2-FC-MG-SR-HA	Extreme Networks SIEM G2 Flow Collector HA Appliance Multi-Gbps Fiber SR
89125	SIEMG2-FC-MG-LR	Extreme Networks SIEM G2 Flow Collector Appliance Multi-Gbps Fiber LR
89126	SIEMG2-FC-MG-LR-HA	Extreme Networks SIEM G2 Flow Collector HA Appliance Multi-Gbps Fiber

89127	SIEMG2-vFC	Extreme Networks SIEM G2 VFlow Collector
89128	SIEMG2-vFC-HA	Extreme Networks SIEM G2 VFlow Collector HA
89129	SIEMG2-ADD-100E	Extreme Networks SIEM G2 EPS Increase 100 License
89130	SIEMG2-ADD-100E-HA	Extreme Networks SIEM G2 EPS Increase 100 HA License
89131	SIEMG2-ADD-0.5-1KE	Extreme Networks SIEM G2 EPS Increase 500 to 1000 License
89132	SIEMG2-ADD-0.5-1KE-HA	Extreme Networks SIEM G2 EPS Increase 500 to 1000 HA License
89133	SIEMG2-ADD-1-2.5KE	Extreme Networks SIEM G2 EPS Increase 1000 to 2500 License
89134	SIEMG2-ADD-1-2.5KE-HA	Extreme Networks SIEM G2 EPS Increase 1000 to 2500 HA License
89135	SIEMG2-ADD-2.5KE	Extreme Networks SIEM G2 EPS Increase 2500 License
89136	SIEMG2-ADD-2.5KE-HA	Extreme Networks SIEM G2 EPS Increase 2500 HA License
89137	SIEMG2-ADD-15-25KF	Extreme Networks SIEM G2 Flow Increase 15K to 25K VM License
89138	SIEMG2-ADD-15-25KF-HA	Extreme Networks SIEM G2 Flow Increase 15K to 25K VM HA License
89139	SIEMG2-ADD-25-50KF	Extreme Networks SIEM G2 Flow Increase 25K to 50K License
89140	SIEMG2-ADD-25-50KF-HA	Extreme Networks SIEM G2 Flow Increase 25K to 50K HA License
89141	SIEMG2-ADD-50-100KF	Extreme Networks SIEM G2 Flow Increase 50K to 100K License
89142	SIEMG2-ADD-50-100KF-HA	Extreme Networks SIEM G2 Flow Increase 50K to 100K HA License
89143	SIEMG2-ADD-100KF	Extreme Networks SIEM G2 Flow Increase 100K License
89144	SIEMG2-ADD-100KF-HA	Extreme Networks SIEM G2 Flow Increase 100K HA License
89145	SIEMG2-CON-UP-ENT	Extreme Networks SIEM G2 ALL-IN-ONE Enterprise Upgrade to CONSOLE Enterprise
89146	SIEMG2-CON-UP-ENT-HA	Extreme Networks SIEM G2 ALL-IN-ONE Enterprise HA Upgrade to CONSOLE Enterprise HA
89147	SIEMG2-CON-UP-ENTPL	Extreme Networks SIEM G2 ALL-IN-ONE Enterprise Plus Upgrade to CONSOLE Enterprise Plus
89148	SIEMG2-CON-UP-ENTPL-HA	Extreme Networks SIEM G2 ALL-IN-ONE Enterprise Plus HA Upgrade to CONSOLE Enterprise Plus HA
89156	SIEMG2-LS-ADD50	Extreme Networks SIEM G2 Log Source Increase 50
89157	SIEMG2-LS-ADD500	Extreme Networks SIEM G2 Log Source Increase 500
89158	SIEMG2-LS-ADD1K	Extreme Networks SIEM G2 Log Source Increase 1000
89159	SIEMG2-LS-ADD5K	Extreme Networks SIEM G2 Log Source Increase 5000
89160	SIEMG2-LS-ADD10K	Extreme Networks SIEM G2 Log Source Increase 10000

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 Security Analytics Appliances come with a one-year warranty against manufacturing defects. For full warranty terms and conditions please go to: http://www.extremenetworks.com/support/warranty.aspx.

Service & 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.

Extreme networks

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