



## SECURITY DASHBOARD MODULE

Unified Security Anywhere™

DATASHEET



**The Security Dashboard Module (SDM)™** provides immediate single-source access to threat data, including an easy-to-use, instant view of prioritized security threats and the underlying data that created them, so an organization can get ahead of the threat curve and prevent security issues. A security event and threat manager, the SDM™ correlates and prioritizes threats from multiple security, network and server sources, including signature-based analysis, logs, network zone or policy violations, vulnerability scans, asset information, and vendor and global threats. The SDM automatically links these threats to the network assets they target. This makes alert and remediation recommendations more relevant and useful to network administrators and management, who can not only identify threats before they compromise network resources, but also gain an overall view of security threat status.

Further, the SDM continuously monitors and updates a repository of all known assets, threats, vulnerabilities, logs, and behavioral and signature IDS alerts, which are then updated, integrated, correlated and normalized for each organization. It instantly displays the most critical threats in a clear and simple format and provides remediation information or open ports to check. Utilizing an innovative minimal maintenance approach, the SDM requires no agents, tuning or creation of complex correlation rules, so critical IT resources can focus on more important tasks.

### UNIFIED ENTERPRISE SECURITY

The Security Dashboard Module is a fully integrated component within Global DataGuard's Unified Enterprise Security™ (UES) and Unified Enterprise Cloud Security™ (UECS) portfolio. These are the only truly unified offerings on the market today that combine the unique integration properties of a security architecture with the adaptive and predictive data sharing, tracking and analysis capabilities of a network behavior analysis and correlation engine. Global DataGuard's UES and UECS solutions provide true subsystem integration of industry-proven security applications – network behavior analysis and correlation; intrusion detection and prevention; vulnerability scanning and management; security and event log management, analysis and monitoring; network access and policy monitoring; prioritized threat management for network, global and vendor threats and vulnerabilities, and a unified service-enabled console– within a multi-layered, 21st century security architecture that spans premise-based, cloud and cloud/on-premise network environments.



**SECURITY DASHBOARD MODULE SPECIFICATIONS**

MODELS	I-6000-A (Amazon EC2 License)	I-6000-V (VMware License)	I-6000-G (10/100/1000Mb)
<b>THREAT MANAGEMENT PORTAL</b>			
Threat management correlation engine	✓	✓	✓
Prioritized Threat List (global, network, vendor, & vulnerability) with detailed analysis and remediation steps	✓	✓	✓
Real-time security alert feed	✓	✓	✓
Network alert integration & correlation	✓	✓	✓
Global internet alert integration & correlation	✓	✓	✓
Vulnerability scanning integration & correlation	✓	✓	✓
Asset management database	✓	✓	✓
Posted vendor alerts	✓	✓	✓
Rolling 30-day threat remediation graph (global, network, vendor, & vulnerability)	✓	✓	✓
Geographic origin of attacker radar	✓	✓	✓
Security risk breakdown graph (pie chart)	✓	✓	✓
Primary attack types ( by name)	✓	✓	✓
Network access policy violation indication	✓	✓	✓
<b>REGULATORY COMPLIANCE ENABLED</b>			
Collects packet data, log file and event data from multiple security, network and server sources	✓	✓	✓
Normalizes and correlates events in real-time to identify threats before they become security breaches	✓	✓	✓
Prioritizes threats according to risk-based event weighting, target vulnerability, asset value and historical activity	✓	✓	✓
Maintains internal threat database, including a taxonomy of known threats, vulnerabilities and exploits	✓	✓	✓
Provides extensive threat, attack and forensic reporting and analysis capabilities	✓	✓	✓
Enables automated and guided operator actions for consistent incident responses	✓	✓	✓



## SECURITY DASHBOARD MODULE SPECIFICATIONS

MODELS	I-6000-A (Amazon EC2 License)	I-6000-V (VMware License)	I-6000-G (10/100/1000Mb)
<b>THREAT MANAGEMENT REPORTS</b>			
Prioritized threat remediation list	✓	✓	✓
Global threats	✓	✓	✓
Network threats	✓	✓	✓
Vendor threats	✓	✓	✓
Vulnerability threats	✓	✓	✓
<b>ON-DEMAND MANAGED SECURITY SERVICE</b>			
7pm to 7am weekdays, weekends & holidays - or - FULL coverage 24/7/365	✓	✓	✓
Custom Security Alert and Response Procedure (SARP)	✓	✓	✓
<b>HARDWARE SPECIFICATIONS</b>			
Processors	1	1	(1) x Intel Xeon Quad-Core X3430
Storage configuration	1 x 30Gb	1 x 30Gb	2 x 250Gb (Raid-1)
Memory configuration (DDR3)	2Gb	2Gb	4Gb
Configurable ports	1	1	1
Passive / In-line configuration	Passive	Passive	Passive
Total 10/100/1000 interfaces	1	1	2
1Gb SFP interfaces (Fiber)*	n/a	n/a	n/a
10Gb CX4 Interfaces	n/a	n/a	n/a
<i>* SX transceivers are standard; LX transceivers are available as an additional option</i>			
<b>SYSTEM PERFORMANCE</b>			
Maximum number of Security Dashboard Modules per system (MCU)	1	1	1
Unlimited user licenses	Yes	Yes	Yes



## SECURITY DASHBOARD MODULE SPECIFICATIONS

MODELS	I-6000-A (Amazon EC2 License)	I-6000-V (VMware License)	I-6000-G (10/100/1000Mb)
<b>PHYSICAL</b>			
Dimensions			Height: 1.7" (43mm) Width: 17.2" (437mm) Depth: 19.8" (503mm) Machine Weight: 36 lbs. (14.1kg) Shipping Weight: Approximately 41 lbs.
Rack mountable			Yes
AC power required			AC Voltage 100-240V, 50-60Hz, 1.2-1.8 Amp
Power consumption (AVG)			350W AC
Environmental			Operating temperature: 10 to 35C (50 to 95F) Non-operating temperature: -40 to +70C (-40 to 158F) Operating relative humidity: 8% to 90% (non-condensing) Non-operating relative humidity: 5% to 95% (non-condensing)
Compliance			cUL or CSA, FCC Class A, CE, RoHS
Warranty	Standard three-year limited warranty, return to factory. Optional extended warranty and advance replacement service.		
<b>COMMUNICATION PORTS</b>			
MSSP monitoring / configuration	4200/TCP Encrypted	4200/TCP Encrypted	4200/TCP Encrypted
NTP communications	UDP-123	UDP-123	UDP-123
UES inter-appliance communications	9112/TCP Encrypted	9112/TCP Encrypted	9112/TCP Encrypted



Global DataGuard

[www.globaldataguard.com](http://www.globaldataguard.com)**ABOUT GLOBAL DATAGUARD**

Based in Addison, Texas, Global DataGuard is the premier provider of Unified Enterprise Security™ (UES), Unified Enterprise Cloud Security™ (UECS), and world-class managed and professional services for small/medium businesses up to large enterprise organizations. Global DataGuard's intelligent, out-of-the-box UES™ portfolio and VMware-based Cloud Guard™ for private cloud environments provide comprehensive and preemptive remediation information through a unified suite of industrial-strength applications that include packet analysis, intrusion detection and prevention, adaptive network behavior analysis and correlation, network access and policy monitoring, vulnerability scanning and management, prioritized threat management for network, global and vendor threats and vulnerabilities, security and event log management and monitoring, and a unified service-enabled console.

**CONTACT GLOBAL DATAGUARD TODAY**

For more information regarding our Unified Enterprise Security solutions, contact us at 972.980.1444 or visit us online at [www.globaldataguard.com](http://www.globaldataguard.com)