



## BEHAVIORAL CORRELATION MODULE

Unified Security Anywhere™

DATASHEET



**The Behavioral Correlation Module (BCM)** identifies and tracks network traffic over long periods of time and automatically generates alerts once suspicious activity is analyzed. The BCM identifies reconnaissance activity, unknown attacks and zero-day attacks – filling the gap left by traditional signature detection systems. It also guards against threats from within, providing alerts for resource violations, infections, abuse of privileges and misuse of corporate assets.

Its adaptive, predictive, behavioral analytics capability employs raw packet data to detect early threat activity. The BCM also maintains signature alert and behavioral profile information for at least six months, and features a multi-tiered correlation system that continuously analyzes stored data to assist in the detection of new enterprise and global threats.

### UNIFIED ENTERPRISE SECURITY

The Behavioral Correlation 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.



## BEHAVIORAL CORRELATION MODULE SPECIFICATIONS

MODELS	A-5000-A (Amazon EC2 License)	A-5000-V (VMware License)	A-5000-G (10/100/1000Mb)	A-5110-G (10Gb)
<b>NETWORK BEHAVIOR ANALYSIS &amp; CORRELATION</b>				
Deep-packet analysis of layers 1-4	✓	✓	✓	✓
Automatic alert analysis and correlation over 14 - 30 days worth of captured raw packet data	✓	✓	✓	✓
Automatic alert escalation and prioritization	✓	✓	✓	✓
Automatic enterprise-wide correlation	✓	✓	✓	✓
Behavioral detection of anomalous communications	✓	✓	✓	✓
Emergent behavior detection provides early detection of zero-hour attacks	✓	✓	✓	✓
Detection of unauthorized access to network resources	✓	✓	✓	✓
Frequency-based detection	✓	✓	✓	✓
Threshold-based incidents	✓	✓	✓	✓
Global threat correlation	✓	✓	✓	✓
Historical correlation of alerts up to 12 months	✓	✓	✓	✓
Correlation with detected vulnerabilities provides context to threats and reduces false positives	✓	✓	✓	✓
Global correlation provides advanced warning of threats detected across community of participating customers	✓	✓	✓	✓
Measures increasing hostility over time to provide advanced warning of pending attacks	✓	✓	✓	✓
Detects, correlates and tracks slow reconnaissance events spanning days, weeks and months	✓	✓	✓	✓
Detects foreign applications and system resources	✓	✓	✓	✓
Detects suspicious employee activities, unauthorized access attempts to protected resources	✓	✓	✓	✓
Detects new port and protocol communications on servers and system resources	✓	✓	✓	✓



**BEHAVIORAL CORRELATION MODULE SPECIFICATIONS**

MODELS	A-5000-A (Amazon EC2 License)	A-5000-V (VMware License)	A-5000-G (10/100/1000Mb)	A-5110-G (10Gb)
<b>ON-DEMAND MANAGED SECURITY SERVICES</b>				
7pm to 7am weekdays, weekends & holidays - or - FULL coverage 24/7/365	✓	✓	✓	✓
Custom Security Alert and Response Procedure (SARP)	✓	✓	✓	✓
<b>PRIVATE CUSTOMER WEB PORTAL</b>				
Unified administration, monitoring, ticketing, and reporting	✓	✓	✓	✓
View alerts, forensics tools, scans, run reports in real-time	✓	✓	✓	✓
<b>HARDWARE SPECIFICATIONS</b>				
Processors	1-4	1-4	(2) x Intel Quad-Core E5620	(2) x Intel Xeon Quad-Core X5650
Storage configuration	1 x 150Gb**	1 x 150Gb**	3 x 500Gb (Raid-5)	3 x 500Gb (Raid-5)
Memory configuration (DDR3)	4Gb	4Gb	8Gb	8Gb
Configurable ports	1	1	1	1
Passive / In-line configuration	Passive	Passive	Passive	Passive
Total 10/100/1000 interfaces	1	1	2	2
<i>** Virtual Appliance storage configuration requirements may differ based on the volume of data being stored.</i>				
<b>SYSTEM PERFORMANCE</b>				
IDS / IPS throughput	200 Mbps	200 Mbps	1000 Mbps	6000 Mbps
Network behavioral analysis (BCM) throughput	200 Mbps	200 Mbps	1000 Mbps	6000 Mbps
Network access monitoring (NSZ) throughput	200 Mbps	200 Mbps	1000 Mbps	6000 Mbps
Maximum number of BCMs per system (MCU)	1	10	10	10
Maximum number of DPMs per BCM	1	10	10	5
Unlimited user licenses	Yes	Yes	Yes	Yes
<i>* IDS/IPS performance is measured based on UDP traffic with 512 byte packet size. Actual performance may vary depends on network traffic and environment.</i>				



## BEHAVIORAL CORRELATION MODULE SPECIFICATIONS

MODELS	A-5000-A (Amazon EC2 License)	A-5000-V (VMware License)	A-5000-G (10/100/1000Mb)	A-5110-G (10Gb)
<b>PHYSICAL</b>				
Dimensions			Height: 1.7" (43mm) Width: 17.2" (437mm) Depth: 25.6" (650mm) Machine Weight: 46 lbs. (14.1kg) Shipping Weight: Approximately 51 lbs.	Height: 1.7" (43mm) Width: 17.2" (437mm) Depth: 25.6" (650mm) Machine Weight: 46 lbs. (14.1kg) Shipping Weight: Approximately 51 lbs.
Rack mountable			Yes	Yes
AC power required			AC Voltage 100-240V, 50-60Hz, 8-4 Amp	AC Voltage 100-240V, 50-60Hz, 8-4 Amp
Power consumption (AVG)			Redundant 650W 1+1 high efficiency, hot swap	Redundant 650W 1+1 high efficiency, hot swap
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			UL or CSA, FCC Class A, CE	FCC Class A, VCCI, CE, UL, 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	4200/TCP Encrypted
NTP communications	UDP-123	UDP-123	UDP-123	UDP-123
UES inter-appliance communications	9112/TCP Encrypted	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)