Global DataGuard

UNSURPASSED SECURITY RISK MANAGEMENT

The Security Risk Management Problem

Too many vendors; too many disparate security systems; too many alerts; not enough preemptive remediation information. Fact is, it takes too long to connect the dots and determine how global threats, network attacks and security vulnerabilities affect network security risks and the overall health of your organization.

Now there is an easier way.

Does Your Network Security Solution…

- Integrate true deep-threat behavioral analysis with intrusion detection, intrusion prevention, vulnerability scanning, raw packet data, vendor alerts, an asset database, event and global threat correlation and a security dashboard to control lifecycle costs while arming you with actionable information?
- Produce the intelligence required to automatically link, investigate and remediate seemingly isolated but potentially damaging events like odd connection attempts, failed attacks, scans and probes, even when they are separated by weeks or months?
- Provide on demand threat prioritization lists to identify and remediate problems based on their potential severity—enabling you to instantly focus on the most critical security issues at all times?
- Capture, continually analyze and correlate packet data 24/7 for at least six months?
- Analyze and correlate network-specific and global threats so you know instantly where the threats are from and what they're attempting to exploit?
- Conduct time-based analysis on historical data to make accurate threat assessments and predictions?

If your network security solution can't do all that, it's time to look beyond stand-alone point products or passive solutions such as Security Information Management systems (SIMs). It's time to deploy a complete, integrated and proactive Security Risk Management (SRM) solution.

Global DataGuard (GDG) is the Premier Provider of SRM Solutions for Midsize-to-Enterprise Organizations.

Global DataGuard's intelligent, turnkey ESP 3000 SRM system includes packet analysis, intrusion detection, intrusion prevention, adaptive behavioral analysis, vulnerability scanning, vendor alerts, correlation systems, an asset database and a security dashboard to provide preemptive remediation information. GDG's Security Risk Management solutions are ideal for organizations looking to implement a comprehensive network security infrastructure or those looking to improve the network security solutions they currently have in place.

GDG tells you where you're vulnerable, who's trying to attack you, how they're doing it and what you can do to shut the threats down. Simply put, looking for odd behaviors in network traffic is the best way to preemptively sniff out malicious activity *before* damage occurs.

GLOBAL DATAGUARD DIFFERENCES

- **Captures, continuously analyzes and correlates** packet data months longer than other solutions.
- **Tracks** disparate network activities and anomalies over time to isolate real threats while ignoring the "noise."
- **Provides** prioritized threat lists with links to technical, location and remediation information for individual threats/vulnerabilities.
- **Correlates** perimeter, internal and global threats, identifying vulnerable devices and threatening behaviors.
- **Integrates** vulnerability scanning, anomaly detection and truly intelligent behavioral analysis to arm you with actionable preemptive information.
- **Utilizes** advanced adaptive behavioral analytics to uncover threats that would not trigger an alert from an IDS, IPS, firewall or SIM.
- **Conducts** time-based analysis of historical data to make accurate threat assessments and predictions.

Simplify Your Security Efforts and Reduce Risk

With Global DataGuard's SRM solutions, IT professionals instantly know how to keep their network safe. One glance answers the following questions:

- What are the current vulnerabilities?
- How much damage could be done?
- How can they be remediated?
- Who's scanning or probing, and from where?
- Do any devices have a Trojan infection, or are any being used as part of a botnet?
- Are upcoming or current attempts part of a global threat with an unknown signature, or are they the work of a single hacker out to get your organization?

With GDG's integrated solutions, your staff has the answers to the most difficult network security risk questions.

Analysts who have seen GDG's new SRM solution are using words like "breakthrough."

"Based on research conducted with its customers, Global DataGuard is delivering what usually takes 20-year security veterans to accomplish, but for a lot less money."

James Hurley,
VP of Research,
Aberdeen Group

The Intelligent Difference

What sets our SRM solution apart is its ability to learn behaviors and adapt to your organization's changing network. As a result, it can protect you from internal and external threats. Our SRM solution collects more data over longer periods, and, thanks to our patent-pending technology, can analyze that data more effectively.

Threat Prioritization, Trouble Ticket and Resolution Reporting

GDG automatically analyzes your threat status with the most advanced algorithms in the industry, continually compiling reports on suspicious activity. This data is stored and continuously analyzed far longer than other solutions—for at least six months—to sniff out dangerous patterns and real threats that less sophisticated systems cannot detect. Our SRM solution even makes sure flagged vulnerabilities are resolved by providing a prioritized threat list and trouble ticket tracking system.

Cost Control

Our solutions will cost you far less than competing solutions that fail to offer the same degree of analysis and protection. Cost reductions are achieved through:

- Initial purchase of an integrated security system
- Reduced mean-time-to-repair
- Rapid deployment via plug and play technology
- Less time spent acquiring, maintaining and managing disparate security solutions
- Redeployment of IT resources for more strategic initiatives

Most importantly, your critical IT assets and data are more secure, making your organization less vulnerable to the kind of costly and publicly embarrassing security disasters appearing every day in the news.

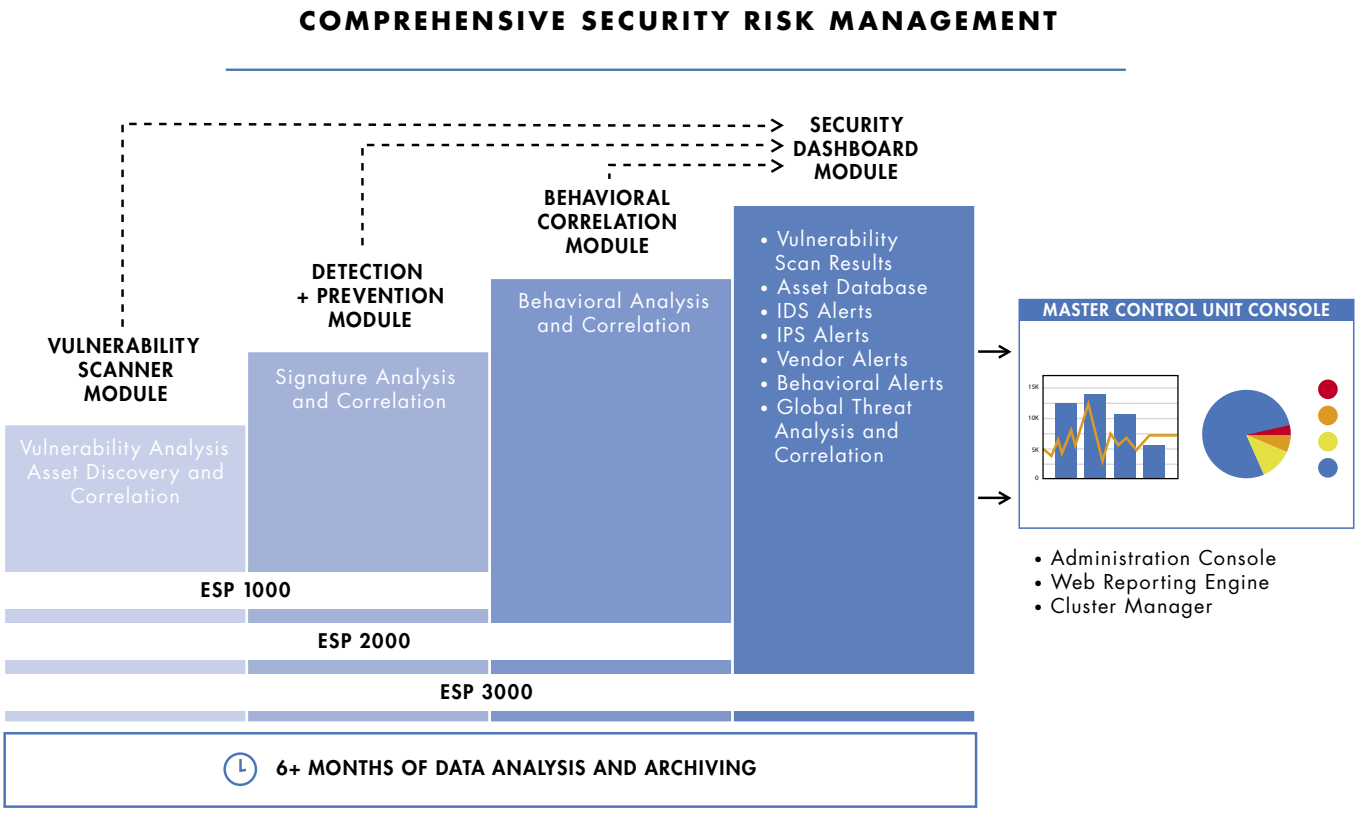
Help With Compliance

Compliance and network security are inseparable. Why not enjoy the benefits of a security solution that augments your compliance efforts? GDG's solution consistently reviews the packets that create log files for odd behaviors—similar to a security analyst reviewing millions of log files looking for what's wrong—and if forensic analysis is needed, the raw packet data provides more information to work with than log files.

Our Vulnerability Scanner Module has extensive reporting capabilities, including easily accessed individual vulnerability reports for each device (with associated risk levels and links to remediation steps) as well as summary and management reports. In addition, the Behavioral Correlation Module stores raw packet data, IDS/IPS alerts and behavioral profile information. Finally, the Security Dashboard provides direct links to the underlying data and alerts that are correlated to produce the threats to the network. All of which means GDG's solution is a valuable partner in the effort to maintain compliance.

GDG's SRM Architecture

Global DataGuard's Enterprise Security Platform (ESP) solution series consists of critical security appliance modules with plug-and-play installation that can be configured to meet your specific needs. The ESP series consists of ESP 3000, ESP 2000, and ESP 1000. The ESP 3000 is GDG's most comprehensive Security Risk Management solution and includes the following integrated layers of security technologies: IDS, IPS, behavioral analysis, event and global threat correlation, vulnerability scanning, vendor alerts, an asset database and a security dashboard. Each layer complements and augments the others, with intelligent behavioral analysis and correlation capabilities comprising the GDG technology difference. The result is early warnings of threats that other solutions cannot see, far fewer false positives, cost savings, more thorough compliance and the ability to manage your security solutions with one dashboard.



Master Control Unit

This appliance—a browser-based monitoring console, signature server, cluster manager and Web server—contains the custom Web portal housing all the reports and graphs for the appliance suite. This includes the security dashboard, intrusion detection and vulnerability scanning reports. GDG's flexible managed services can also be provisioned through the Master Control Unit (MCU) for thorough and economical risk management.

Detection + Prevention Module

Another layer in the seamless GDG solution, the Detection + Prevention Module employs signature IDS/IPS technology, deep-packet inspection of layers 1–7 and tunable signatures on a 24/7 basis. Another key component is an intelligent packet inspection and capture system that selects suspicious packets for further behavioral analysis based on a knowledge of normal network traffic. The Detection + Prevention Module offers:

- Automatic alert analysis and correlation
- Automatic alert escalation and prioritization
- Detection of unauthorized access to network resources
- Countermeasures for denial of service attacks
- Termination of attack sessions via a TCP reset or ICMP unreachable message
- Probe prevention (defeats or confuses scanning techniques with false responses)
- Enterprise threat correlation and global threat correlation

Vulnerability Scanner Module

As your systems change, GDG's Vulnerability Scanner Module allows you to keep pace, adapting and continuing to research potential security issues. This layer of the GDG solution gives you the full benefit of regular security scans, integrated and correlated with data and alerts from the other appliances, and extensive research capabilities. The Vulnerability Scanner's extensive reporting includes individual vulnerability reports for each device (with associated risk levels and links to remediation steps) as well as summary and management reports for easier vulnerability management.

Behavioral Correlation Module

The Behavioral Correlation Module (BCM) houses the patent-pending behavioral analysis and correlation tools that make GDG's solutions more thorough and preemptive than other solutions. The BCM identifies and tracks typical network traffic/packet behaviors over long periods of time and automatically alerts you to anomalies. It identifies reconnaissance activity, unknown attacks, and zero-day attacks. It also guards against threats from within, alerting you to resource violations, abuse of privileges and misuse of corporate assets. Its behavioral analytics employ raw packet information through layer 4, detecting early threat activity, maintaining alert and behavioral profile information for at least six months and constantly monitoring global attacks and vulnerabilities.

GDG PROVIDED ADVANCED WARNING:

- A 10-month warning of the arrival of SQL Spida Worm
- 5 months to prepare for the SQL Server Worm
- 3 weeks advance notice of Opaserv
- 20 hours to get ready for Code Red Worm
- A 3-hour warning of the Nimda Worm
- 3 months to lock down against the Slammer Worm
- 2 days warning of Sobig F Trojan
- A full 2 weeks to prepare for MyMail Trojan

Security Dashboard Module

The Security Dashboard Module (SDM) provides immediate single-source access to all threat data, including a single, easy and instant view of prioritized security threats and the underlying data that created them. The SDM correlates data from multiple security, network and server sources, including behavioral alerts from packet data analysis, signature IDS alerts, vulnerability scans against assets and global alerts, and prioritizes security threats. The SDM instantly shows the most critical network threats and determines the best path for remediation and gathers the data for forensic reporting. And with the SDM, there is no need to spend time attempting to integrate complex SIM software with third-party security products and then spend even more time implementing, updating and maintaining multitudes of SIM correlation rules.

Flexible Managed Security Services

With GDG's flexible Managed Security Services, you decide when internal resources are responsible for network security and when you'd prefer that GDG handle it. Outsource as much or as little as you like… 24/7/365… holidays and weekends… during lunch hours… you make the call.

Upgrades and Options Available

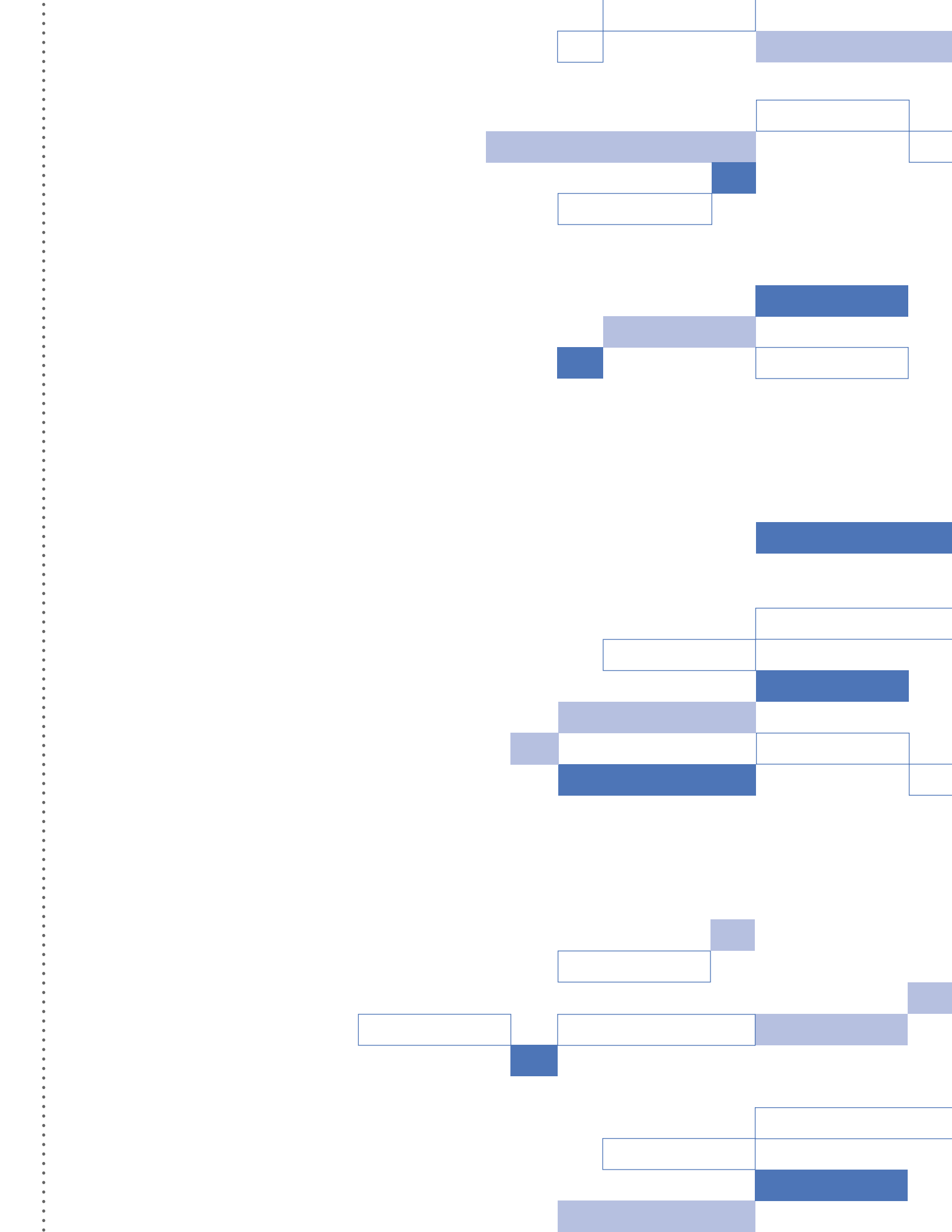
GDG provides the architectural flexibility to grow your security architecture with your enterprise. If you started with anything other than a full ESP 3000 system, or if your network infrastructure grows and you need additional coverage, you can add components as needed or as your budget allows. You have the option of starting with a basic system and then adding other components such as sensors, vulnerability scanning, global correlation or the security dashboard.

Why Global DataGuard?

- Deploy, in one day, a fully functional turnkey network SRM solution that provides the best value and the most protection.
- Enjoy the ease of a simple dashboard to preemptively identify, analyze and help manage and resolve internal and global security threats.
- Access a real-time, prioritized list of threats and vulnerabilities.
- Provide IT personnel with actionable preemptive information so they can resolve issues in a rapid and organized fashion.
- Continue to leverage your investments in your current infrastructure and third-party security solutions.
- Improve productivity and operational efficiency by redeploying resources to other critical IT projects.
- Lower overall security infrastructure and resource costs.
- Augment compliance.

About Global DataGuard

Based in Dallas, Texas, Global DataGuard is the premier provider of Security Risk Management (SRM) solutions for midsize-to-enterprise organizations. Global DataGuard's intelligent, out-of-the-box integrated SRM system includes packet analysis, intrusion detection, intrusion prevention, adaptive behavioral analysis, vulnerability scanning, vendor alerts, correlation systems, an asset database and a security dashboard to arm first responders with preemptive remediation information.



14800 Landmark Blvd, Suite 610 / Dallas, TX 75254
972.980.1444 / www.globaldataguard.com