



WHITE PAPER

VeriSign[®] Teraguard

Securing Critical Information Assets Through
Intelligent Data Collection, Expert Monitoring,
and Analysis





CONTENTS

+ Teraguard Overview	3
+ Monitoring	4
+ The VeriSign Security Defense Appliance (SDA)	5
+ Multi-Context Event Correlation	7
+ Ticket Management	7
+ The VeriSign® Enterprise Security Portal	8
+ VeriSign Security Operations Centers (SOCs)	8
Operational Support Systems	8
Facility Attributes	9
+ Business Continuity and Disaster Recovery	9
+ Learn More	9



+ Teraguard Overview

With the increasing complexity of today's technology environment and the continued growth of the hacker community, companies are experiencing difficulty in establishing the appropriate levels of security. Many organizations that have invested in the latest hardware and software solutions to contend with this increased threat are finding that strong perimeter security only provides a temporary and fractional fix. Technology investments will only prove fruitful when combined with a trained security staff who can provide 24/7 management and monitoring. At the end of the day, what matters most is the act of monitoring, not the deployment of monitoring technology. Responding appropriately to detected incidents requires a strong understanding of the issue and of current Internet attack activity so events can be put in perspective. With a dedicated team in place, the team can continually monitor and manage security systems such as intrusion detection systems (IDSs), intrusion prevention systems (IPSs), and firewalls. The team can conduct regular upgrades, security assessments, auditing, and change control, as well as respond to emergency incidents, among other obligatory functions. Although necessary, operating an around-the clock monitoring and management security program internally is an expensive, time-consuming, and onerous task that can seriously detract from an organization's core business focus and profitability.

Additionally, for an organization trying to internally manage its security program, the amount of information collected represents a double-edged sword. A company can gain a better understanding of the current security climate through analyzing large amounts of collected data. However, this type of detailed analysis requires a significant time and financial investment as well as access to a wide range of data beyond what an organization can collect from its own network activity. This data is not generally available, and privacy interests and other confidentiality concerns make it difficult, if not impossible, to acquire it from other organizations.

Conversely, VeriSign® Managed Security Services (MSS) customers benefit from the wealth of threat data collected through the VeriSign® Teraguard architecture and the 24/7 expert analysis of that information. Across a customer base representing thousands of devices, Teraguard collects security information from a range of sources, including all major firewalls, IDSs, IPSs, host security logs, vulnerability scanners, and intelligence sources. Information travels from client sites across highly secure virtual private networks (VPNs), and the built-in correlation technology filters, normalizes, correlates, and prioritizes collected events into major and minor classifications, giving VeriSign's trained security analysts a virtually real-time view of the health and integrity of a client's security architecture.

This monitoring capability, and the associated analysis, allows VeriSign to sort through large amounts of inconsequential information to cost- and time-effectively identify serious threats. Teraguard also allows VeriSign to log non-critical information, which offers clients the benefit of long-term analysis of archived data. Additionally, security experts at VeriSign cross-reference threat data with activity collected across its large, global, and industry-diverse customer base and VeriSign-operated critical Internet infrastructure services such as the Domain Name System (DNS). This allows VeriSign to proactively identify, track, and respond to threat trends, an advantage that is near impossible to emulate through the management of network devices at a single site.

This paper will delve into the specific components of the Teraguard architecture, offering the reader a detailed view of how VeriSign technology, combined with expert management and monitoring, helps organizations mitigate their risk potential.

+ Monitoring

Today's complex security systems; rapidly expanding and evolving information architectures; and extended network access to partners, suppliers, customers, and mobile employees presents a complex information management challenge. Having an internal team in place to contend with this volatile security climate is a difficult objective for any organization to meet. Recruiting, hiring, and retaining qualified security employees and maintaining a solid training program to keep an internal staff apprised of the latest technological advances are major hurdles for an organization. With the current security climate showing no sign of a decrease in threat level, no organization can risk its internal team being at less than optimal performance. From a technology perspective, today's security solutions generate tremendous amounts of data. This overload of information raises the "noise floor" to the point of obscuring the identification of real security incidents.

As previously stated, even the best security technology is rendered ineffective without the experts on hand to manage the products and monitor the information gathered. VeriSign security experts act as technical authorities for corporations and government entities on a global scale. They include former analysts from various military branches, private-sector enterprises, financial services, and Computer Emergency Response Teams (CERTs), as well as more than 30 Certified Information Systems Security Professionals (CISSPs). VeriSign security and network analysts have a wide range of certifications from leading manufacturers including Cisco Systems, Microsoft, Sun Microsystems™, and Check Point®. Each member of the VeriSign team of certified security professionals undergoes extensive security training and rigorous background checks prior to managing or monitoring any VeriSign client.

Outsourcing the management and monitoring of network devices to VeriSign releases an organization from the unrelenting and time-consuming responsibility of safeguarding corporate information assets. VeriSign's expert staff can evaluate data collected through the Teraguard architecture's advanced correlation and analysis technologies and promptly respond to any real information-security threat. Additionally, this evaluation by VeriSign security experts negates the need for an organization's internal staff to assess inordinate amounts of information that today's security systems typically generate.

Further, to maximize the Teraguard architecture's efficacy, VeriSign logically classifies and correlates collected information into "meta events," which may include the output of various data sources. VeriSign meta events are assigned to one of the following five Teraguard categories:

- **Severity Level 5: Large-scale incident** – Cross-customer correlation indicates a widespread security threat. This priority level is not used for baseline event prioritization; it is applicable only to meta events such as the Nimda virus or MSBLAST worm.
- **Severity Level 4: Critical** – VeriSign has observed malicious activity that it has confidence was or will be successful. The client will automatically be notified immediately regarding the event, and a trouble-ticket transaction will be generated at the VeriSign Security Operation Center (SOC) for immediate action. A VeriSign security analyst will call the client to review the threat and provide counsel on next steps and threat remediation. Information regarding the event will also be made available on the Teraguard Client Portal.

- **Severity Level 3: Threat** – VeriSign has observed malicious activity that it does not have high confidence was or will be successful, or has intelligence about a relevant threat. The event information will be included in the Teraguard Client Portal for reporting purposes.
- **Severity Level 2: Suspicious** – VeriSign has observed reconnaissance activity that warrants visibility, but is not believed to represent an immediate threat. The event information will be included in the Teraguard Client Portal for reporting purposes.
- **Severity Level 1: Informational** – VeriSign has identified useful contextual information that will be included in the Teraguard Client Portal reporting capabilities.

This method enables the Teraguard architecture to identify any patterns and alert VeriSign security analysts of all potential threats. The security analysts can then validate or discount the alert according to each specific customer's environment. Correlating and validating customer data both reduces expensive "false positive" events and enables VeriSign to analyze the collected, non-critical information to determine the appropriate threat level. The benefit of this evaluation is passed on to the client, providing a comprehensive view of the incident with relevant remediation guidance.

The Teraguard architecture correlates data across customer sites to find trends and emerging threats. It accomplishes this distillation through a process that begins on the Security Defense Appliance (SDA) and ends at the VeriSign SOC.

+ The VeriSign Security Defense Appliance (SDA)

The VeriSign proprietary SDA is an integral part of the VeriSign overall value proposition. It improves security implementation efficiency, provides enhanced security and reliability and, because VeriSign assumes all hardware and management expenses, the SDA lowers capital and operational costs.

As the Teraguard architecture's remote eyes and ears, the SDA captures security event logs, provides an encrypted communications channel for device management, and becomes an active security agent, running a variety of security protection software. This multi-purpose device provides a communication and management channel between the client's site and the VeriSign SOC, collecting data from firewalls, IDSs, IPSs, host logs, and other data sources. The SDA then normalizes and correlates the data into meaningful meta events, while limiting the amount of customer bandwidth used by the monitoring service.

Furthermore, the SDA provides a single, highly secure VPN tunnel through which all customer network devices are managed and monitored. This limits the number of "holes" needed in a perimeter firewall for VeriSign to manage its customer's network devices. Having fewer openings in a firewall helps prevent sensitive security information falling into the wrong hands.

The SDA can be configured to accept event data from numerous security and non-security devices via the VeriSign event acquisition framework. Supported devices include those using SYSLOG, SMTP, remote databases, and XML, as well as those using popular native protocols such as Check Point's OPSEC™ and Cisco's IDIOM (XML-based) protocols. This approach enables VeriSign to rapidly support new devices while abstracting device-specific data formats from the SOC.

The Teraguard architecture uses a distributed computing model, and with the CPU power of the SDA, it performs the first steps of data processing locally. This includes the following steps:

- **Data normalization** – The SDA translates the information into a single, consolidated device-independent data model that becomes the basis for the first level of event correlation.
- **Data de-duplication** – The SDA reduces events with the same source and destination hosts and ports into de-duplicated events within a specific time frame.
- **Event linking** – After the data is de-duplicated, it can often be linked to other de-duplicated events that originated from the same source within a given time frame. The SDA links appropriate events locally without losing any resolution or important information.
- **Rule-based event reprioritization** – The SDA can reset the initial priority of the meta event through a list of client-specific rules that is regularly updated on the SDA. This type of local reprioritization allows VeriSign customers to define certain types of attacks, or certain hosts, as being more or less critical, depending on their environment, and therefore greatly increases the accuracy of the meta event, which is transmitted back to the centralized correlation engine.
- **Event qualification** – Normalized events are qualified through a process of examining the qualifying attributes of a target and an attack to determine confidence and reduce false positives.

The SDA is also capable of running its own Snort-based IDS and vulnerability scanner as part of the VeriSign® Vulnerability Management Service. (See data sheet for a description of the Vulnerability Management Service.)

As a purpose-built, highly secured appliance, the SDA has a virtually invisible network footprint. It is available in high-availability (HA) configurations and comes equipped with dial-up, out-of-band (OOB) access, and 80 gigabytes (GB) of local storage in the event of network failure. The VeriSign SDA comes equipped with a “phone home” capability that ensures the SDA software and supporting configuration files (e.g., IDS, correlation rules, and so on) are up to date. This eliminates the need for service interruptions, which ensures that VeriSign clients are not distracted by frequent upgrades and updates. Consequently, clients are assured that they will always have the most up-to-date and relevant security protection running on their SDA.

Using a standardized platform, the SDA can also be configured and deployed in a centralized or satellite model to support higher device-to-node ratios. This is ideal for a hosting or data center environment because it provides a scalable and cost-effective solution for supporting multiple devices or customers while leveraging the full capabilities of the SDA.

The SDA can be deployed in a variety of logical placements in order to gain visibility of attack traffic for IDSs, or access to devices for vulnerability assessment. The SDA can also be deployed behind firewalls or on internal segments for monitoring or scanning of internal systems.

+ Multi-Context Event Correlation

By comparing normalized security-related data with other variables, including host-specific considerations and cross-customer correlation, the Teraguard architecture uses a variety of techniques to corroborate and prioritize event information. Once the SDA transmits this meta event back to VeriSign, the proprietary correlation engine performs further analysis, including the following steps:

- **Event qualification** – Meta events are analyzed and compared with other meta events, and other data, such as scanning data from the VeriSign Vulnerability Management Service to determine the relevance of the event.
- **Cross-customer correlation** – Individual meta events are compared with global Teraguard meta events in order to determine whether activity is part of a larger trend, such as a new worm outbreak.
- **Dynamic reprioritization** – Based on all the information available at the time of the receipt of the event, the Teraguard architecture uses proprietary algorithms to dynamically alter the priority of the meta event, ensuring that every meaningful event is investigated.
- **Anomaly detection** – The Teraguard architecture performs statistical analysis of customer information to identify abnormal traffic patterns and thereby detect infected hosts and misuse.

+ Ticket Management

The Teraguard architecture supports the VeriSign SOC transaction-based model for managing security events. By using this model, system-created trouble tickets are kept at a manageable level as a result of the Teraguard data reduction and correlation engine. With the Teraguard transaction-based approach, security-related events automatically generate a prioritized trouble ticket populated with relevant supporting information. The trouble ticket is then queued for handling by a VeriSign security analyst who takes ownership of the ticket and works it to completion. During this process, the analyst may access information stored in the Teraguard system, including log information from other client devices, or the analyst may use the Teraguard global query engine to determine whether the problem exists with other client systems or other geographies.

Based on the priority of the security event and the review of the trouble ticket by a security analyst, VeriSign initiates an appropriate response. This response may include blocking the attack; contacting the client for live support and to discuss response and remediation; or generating a report on the Teraguard Client Portal for customer review.

In the event of a major incident, VeriSign will engage its incident response and forensics team, preserving data and evidence for use in the legal arena. VeriSign will further help the client contain and recover from the problem. The VeriSign transaction model is an improvement over the more reactionary approach employed by most MSS providers. In the reactionary model, technicians watch monitors, waiting for lights to switch from green to red before investigating a client issue. This can lead to inconsistent performance and the inaccurate measurement of service-level compliance. The VeriSign model uses the Teraguard architecture to resolve this issue.

+ The VeriSign® Enterprise Security Portal

The VeriSign® Enterprise Security Portal is an integral element of the Teraguard platform. It provides customers with relevant, actionable information that enables them to continually assess and improve their security and compliance posture. Customers can use VeriSign® Unified Authentication services to gain secure, virtually real-time access to event and ticket information. A rich authentication, authorization, and auditing model controls the information that users can view.

The Enterprise Security Portal includes more than 100 pre-built executive and in-depth reports with comprehensive templates that can be customized to provide maximum insight into the network environment. The portal's Event Viewer enables precise control over which event information is displayed. Customers can sort and filter data, and select the data fields to display. The Event Viewer also allows customers to easily search real-time and historical events. All reports can be run in real time or scheduled according to customer preferences. In addition, reports can be filtered using customer-defined groups (e.g., critical assets, business units, and regions).

The portal provides access to the following information and features:

- Executive and trend analysis
- Comprehensive risk analysis
- Intelligence information on the latest vulnerabilities, threats, and malicious code
- Event log viewer
- Ticket information
- Reports and other documents uploaded by VeriSign for customer review
- More than 100 pre-built reports
- Report scheduling
- Localized language support

+ VeriSign Security Operations Centers (SOCs)

The management and monitoring of security devices transpires in the VeriSign SOC's. These secure, highly available environments are staffed around the clock by security, customer care, and networking specialists. Within the walls of these VeriSign MSS nerve centers, experts monitor the health, status, and availability of security devices; run vulnerability scans; manage and monitor intrusion detection systems and firewalls; manage and update each client's security devices; respond to security events; and store client data. VeriSign maintains SOC's in Providence, Rhode Island; Mountain View, California; Sterling, Virginia; and Australia, Switzerland, and Japan; and it expands its facilities on a regular basis.

Operational Support Systems

The Teraguard Virtual SOC (vSOC) and Customer Access Jump (CAJ) systems are designed to automate and simplify the management of security and non-security devices by providing an automated mechanism for distributed, scheduled, and on-demand device interaction. The systems are used to update products; facilitate secure file transfer; enable device configuration management; and support out-of-band, dial-out/dial-back access. The systems also provide session information including keystroke-logging and auditing for all interactions with each device. Access restrictions are handled via analyst/user profiles, with the principle that VeriSign employees will have access only to the information required to safeguard our clients' networks.

Facility Attributes

The VeriSign SOC's feature bunker-style construction with multiple layers of security and redundancy. Authorized VeriSign staff gains entry to areas of the center through tiered levels of access, including biometric, card-key, and PIN-based authentication, and are under constant video surveillance. The SOC's provide multiple layers of backup and provisions to secure all physical infrastructure, including redundant power grids, dry nitrogen fire suppression systems, independent HVAC, armored fiber backbone connectivity from multiple service providers, and a power generator supplemented by battery backup.

+ Business Continuity and Disaster Recovery

Disaster recovery and business continuity processes are critical components to ensuring 24/7 security vigilance for VeriSign clients. All VeriSign clients are safeguarded by a triple-level disaster recovery and continuity process that provides some of the highest levels of non-stop operations in the industry. In addition to multiple layers of physical infrastructure redundancy, including redundant, high-speed Internet connections and utility infrastructures, VeriSign also maintains a backup operations center within a 45-minute drive of its main facility in Providence, Rhode Island. The proximity of the secondary facility allows VeriSign security analysts to provide full services in less than one hour of the primary facility becoming unavailable. The current sites are linked via a “meshed” network, removing single points of failure and minimizing the total number of connections required. The telecommunications system in the VeriSign primary SOC is also mirrored in the backup facility.

VeriSign is positioned in the Leaders Quadrant of the August 2007 “Magic Quadrant for MSSPs, North America, 1H07” Gartner report.

+ Learn More

For more information about VeriSign Managed Security Services and VeriSign® Global Security Consulting, please call 650-426-5310, email enterprise_security@verisign.com, or visit us at www.Verisign.com.

Visit us at www.Verisign.com for more information.

©2007 VeriSign, Inc. All rights reserved. VeriSign, the VeriSign logo, the checkmark circle, Teraguard, and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign and its subsidiaries in the United States and in foreign countries. Cisco is a trademark of Cisco Systems, Inc. Check Point and OPSEC are trademarks of Check Point Software Technologies Ltd. Microsoft is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries. Sun Microsystems is a trademark and service mark of Sun Microsystems, Inc. All other trademarks are the properties of their respective owners. The Magic Quadrant is copyrighted August 2007 by Gartner, Inc. and is reused with permission. The Magic Quadrant is a graphical representation of a marketplace at and for a specific time period. It depicts Gartner's analysis of how certain vendors measure against criteria for that marketplace, as defined by Gartner. Gartner does not endorse any vendor, product or service depicted in the Magic Quadrant, and does not advise technology users to select only those vendors placed in the “Leaders” quadrant. The Magic Quadrant is intended solely as a research tool, and is not meant to be a specific guide to action. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

00017410 04-27-2006