VeriSign®

DATA SHEET

VeriSign® Managed Incident Response and Forensics

KEY BENEFITS

Industry-Leading service level agreements (SLAs)
VeriSign offers full lifecycle management of its Managed Incident Response and Forensics service backed by industry-leading SLAs. These strict SLAs demonstrate a strong commitment to protecting its customers networks.

Unmatched Security Intelligence
VeriSign has unique visibility into Internet security threats, by managing critical Internet infrastructure services such as the Domain Name System (DNS).

Always-on Client Resource Portal
The VeriSign Internet portal provides a detailed view of a client's security devices under VeriSign management. It includes a variety of reports per device type, and access to an ad hoc query engine for sophisticated analysis of security events across multiple platforms and locations. Access to the system is secured with token-based authentication and SSL encryption.

The initial minutes following a network attack are the most crucial; therefore, a calculated and planned response is an organization's best line of defense to prevent the compromise of critical business systems. Establishing a plan will enable an organization to quickly stabilize its network and data, analyze options to prevent further damage, preserve forensic evidence, and strategize for full containment and recovery.

The VeriSign® Managed Incident Response and Forensics service benefits organizations that lack an internal team of cyber forensics investigators and are seeking to establish a best-practices program for incident management.

+ Bottom Line

With a powerful combination of proactive planning and 24/7 handling of security incidents, VeriSign's services enable organizations to quickly and confidently respond to computer-related security situations. Responding appropriately to events such as system compromise, virus infection, and denial-of-service attacks helps minimize downtime and lost revenue.

+ Description

VeriSign employs a detailed and comprehensive methodology for responding to computer security occurrences using law-enforcement evidence-handling standards and taking into account the availability requirements of the client's organization. Based on the five cornerstones of effective incident management and response—detection, assessment, forensics, containment, and recovery—Managed Incident Response and Forensics services leverage industry best practices to provide a complete and measured response to any security breach.

+ Service Features

- **Strategic planning**—VeriSign customizes an incident response methodology guide (based on industry-leading policies, guidelines, and processes) to provide a step-by-step process for detecting and reacting to incidents. Serving as a customer's roadmap for effective incident response, the methodology guide includes decision matrices for establishing incident severity, escalation areas, and management decision points.

24/7 Management, Monitoring and Support

When a client calls, VeriSign is there. VeriSign security analysts work nights, weekends and holidays so clients don't have to.

Trained and Dedicated Professionals

VeriSign's certified security professionals undergo extensive security training and rigorous background checks prior to managing or monitoring a client's equipment.

Lower Cost of Ownership

Whether outsourcing a single device or an entire security infrastructure, VeriSign reduces a company's operational costs while increasing the effectiveness of your security program.

- **Infrastructure development**—VeriSign helps customers handle security incidents effectively. By conducting an extensive review of each customer's infrastructure, VeriSign identifies critical technology and staffing resources. This ensures that the appropriate management structure and plans are in place to handle network-security-related incidents.
- **Hands-on training**—VeriSign ensures that new incident response processes are put into practice. In addition, the company provides awareness training and workshops to help customers' employees understand their critical role in the incident management process and their contribution to a security-aware business environment.
- **Thorough detection**—Detecting "real" security events is as difficult as combating them. Led by the industry's leading experts in intrusion and incident detection, VeriSign's incident response team can quickly and reliably identify events that threaten an organization's security posture.
- **Impact assessment**—VeriSign's detailed triage process reveals extensive information about the scope, impact, and severity of security events, enabling a faster and more complete prioritization of response activities. Data is reviewed to determine whether, and to what extent, critical business systems have been compromised.
- **Forensic analysis**—Using legally sound scientific and analytical techniques, VeriSign identifies, gathers, preserves, and presents evidence that details the root cause and effect of an incident. Regardless of whether legal action is taken, forensic data is leveraged to drive effective containment, recovery, and system improvement activities.
- **Systematic containment**—Based on the identified root cause, VeriSign deploys countermeasures to quickly halt the spread of the threat, minimize its damage, and avoid adverse impact on an organization's critical business functions.
- **Proactive recovery**—VeriSign helps restore damaged systems to a more secure operational state and provides recommendations for system hardening, as well as enterprise policy decisions, to prevent damage from future episodes.

+ Security Operations Centers

VeriSign's Security Operations Centers (SOCs) are secure, highly available environments that house 24/7 operations. Bunker-style construction, tiered biometric access to sensitive areas, and video surveillance are select features of the physical security control, while a generator backup, uninterruptible power supply (UPS), and state-of-the-art fire suppression systems ensure 24/7 availability. All mission critical systems are fully redundant, from electricity to telecom links to data processing, thereby eliminating any single point of failure.

+ TeraGuard™

VeriSign's information management architecture, TeraGuard,™ takes a wide range of disparate data sources from security and network devices and converts the information into a single, normalized stream of security-related events. The TeraGuard application then analyzes and prioritizes these events using a multitiered correlation process. This enables VeriSign to quickly eliminate false positives, find real threats, and take the appropriate action.

+ The VeriSign Difference

Global Scale and Intelligence and Control™—VeriSign offers customers the benefit of an early warning system that leverages a comprehensive base of threat data available only to VeriSign and its customers through its Intelligence and Control™ Services. With a worldwide customer base and over 2,600 network security devices under management, VeriSign has a wider and deeper view of Internet activity and therefore can proactively identify and alert customers to emerging attack trends and cyber threats.

Commitment to excellence—VeriSign is focused on the continued growth and enhancement of VeriSign® Managed Security Services (MSS) and continually invests in SOCs and support infrastructures. The company's services are designed to be highly redundant to continually provide 24/7 support and availability.

Best-of-breed support for third-party devices—VeriSign is vendor-agnostic and supports a wide variety of best-of-breed security products. The company designs and deploys security solutions based on the specific needs and requirements of its customers and regularly evaluates and enhances its service offerings to support third-party security products. Customers are assured that their infrastructures are protected by the right combination of a trained 24/7 security staff managing and monitoring the industries top technologies.

Trusted partner—VeriSign has a strong heritage in managing trusted security services, and thousands of organizations benefit from this heritage every day. Together with strong authentication, application security, and e-commerce security, VeriSign® MSS represents an unparalleled commitment to providing services that enable enterprises to engage in electronic commerce, communications, and collaborative computing with confidence.

+ Get Started Today

For more information about VeriSign Global Security Consulting Services, please call 650-426-5310 or send an email to enterprise_security@verisign.com.

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

Note: In February 2004, VeriSign acquired Guardent,® a recognized leader[1] in Managed Security Services. Guardent security consulting and managed services are integrated into VeriSign's solution portfolio.

[1]See *http://www.gartner.com/reprints/guardent/118599.html* for more information.

00017400 05-20-2005