



DATA SHEET

KEY BENEFITS

Unmatched Security Intelligence

VeriSign Managed Intrusion Prevention Service leverages VeriSign intelligence to deliver intra-enterprise, inter-enterprise and Internet-wide security intelligence. VeriSign has unique visibility into Internet security threats, by managing critical Internet infrastructure services such as DNS.

Industry Leading Service Level Agreements (SLAs)

VeriSign delivers the industry's highest quality of service backed by stringent SLAs.

Comprehensive Deployment Services

VeriSign security engineers and program managers ensure that the intrusion prevention devices are staged and comprehensively tested prior to deployment.

Full Life-Cycle Management

VeriSign delivers true life-cycle management on an ongoing basis.

Security Monitoring and Risk Management

24x7 monitoring of security events, which are captured, analyzed and correlated in real-time. Suspicious and malicious events are therefore proactively identified, mitigating an organization's risk potential. When combined with VeriSign's consulting services, the company's security experts immediately execute remediation plans.

VeriSign® Managed Intrusion Prevention Service

The increasing sophistication of Internet attacks and the speed at which they propagate requires a smarter breed of technologies that are better able to prevent intrusions. Enterprises can no longer rely on products that merely notify of attacks. They require technology that can thwart a potential security breach before it can adversely impact their business. In response, security vendors have built prevention technologies into their existing products as well as created a new line of intrusion prevention devices. Today, intrusion prevention technologies deploy a wide range of techniques, including signature matching as well as protocol and traffic anomaly detection, to effectively monitor and block malicious traffic.

The adoption of intrusion prevention technologies has created a unique challenge for security professionals. Creating and maintaining effective device policies requires extensive security expertise and time. If policies are incorrectly tuned to the customer's environment and not regularly updated, malicious traffic may be permitted and benign traffic blocked. In addition to managing intrusion prevention policies, security professionals must also monitor events generated from, and the health of, the devices on a continual basis. Because these technologies are often deployed via inline devices, downtime can result in either all traffic being blocked or malicious traffic being permitted into the customer's environment.

+ Bottom Line

VeriSign Managed Intrusion Prevention Service (MIPS) is a component of VeriSign's acclaimed suite of Managed Security Services (MSS). This service allows enterprises to maximize their return on investment for intrusion prevention technologies while reducing their operational and capital costs. VeriSign's team of security experts manage and monitor the device around-the-clock, monitoring for health events and security violations from attacks that originate inside or outside the network. VeriSign's industry leading Service Level Agreements (SLAs) ensure that customers are quickly notified of security and health issues so that they can take timely action to mitigate risk.

+ Description

VeriSign Managed Intrusion Prevention Service offers 24x7 management and monitoring of a wide range of intrusion prevention technologies. Creating and maintaining effective policies is the most challenging aspect of managing intrusion prevention technologies. Given our extensive security experience and unmatched



Where it all comes together.™

Health and Performance Monitoring

24x7 proactive monitoring for health and performance of devices. This allows VeriSign to proactively address developing operational problems prior to actual service failures.

Guaranteed Responsiveness

VeriSign commences a client-specific escalation procedure the moment a problem is detected and then works quickly to identify its source.

Reliable Communication/ Management Channel

VeriSign's proprietary Security Defense Appliance (SDA) provides a secure, fault-tolerant communication and management channel. The SDA, located behind a customer's security devices, provides secure, event store-and-forward capabilities via an encrypted connection to the Security Operations Centers (SOCs). Deployment of the SDA is not required, but highly recommended.

Always-On Client Resource Portal

The Client Resource Portal provides a detailed view of a customer'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.

24x7 Management, Monitoring and Support

VeriSign's expert staff of security analysts are available to customers around-the-clock.

security intelligence, VeriSign is in a unique position to create a policy that is appropriate for the customer's environment.

During the initial tuning period, VeriSign runs policies in simulation mode and works closely with the customer to determine what traffic should be blocked. After extensive tuning and customer approval, the active blocking mode is enabled. These policies are augmented as vendors release updates and as new threats emerge. The status of the device's health as well as all intrusion attempts are logged and reported on VeriSign's Client Resource Portal. Customers are notified of major security and health issues via phone, email or pager. In addition, VeriSign patches and upgrades all devices under management.

+ Service Features

- Configure and provision device
- Create initial policy; update and tune policy on an ongoing basis
- Monitor and report on health and security events 24x7
- Report all security events on the Client Resource Portal
- Flexible reporting options on Client Resource Portal
- Notify customers of major security and health issues
- Upgrade and patch devices
- Seamless integration with VeriSign Incident Response and Computer Forensics team

+ Security Operations Centers

VeriSign Security Operations Centers are secure, highly available environments that provide 24x7 monitoring and management of security infrastructures for Global 2000 companies. Bunker-style construction, tiered biometric access to sensitive areas and video surveillance are select features of the physical security controls, while a generator backup, UPS-conditioned power and state-of-the-art fire suppression systems ensure 24x7 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, collects a wide range of disparate data sources through its SDA. The SDA resides on the customer site and converts the data from security and network devices into a single, normalized stream of security-related events. TeraGuard then analyzes and prioritizes these events using a multi-tiered correlation process. This enables VeriSign to quickly eliminate false positives, find real threats and take the appropriate action.

+ VeriSign Difference

Global Scale and Intelligence and Control – VeriSign offers customers the benefit of an early warning system that leverages the expanded base of threat data available through its Intelligence and Control Services. With a worldwide customer base and thousands of network security devices under management, VeriSign has a wider and deeper view of Internet activity and therefore can proactively identify and alert customers to attack trends.

Commitment to Excellence – VeriSign is focused on the continued growth and enhancement of its Managed Security Services and continually invests in its SOC expertise, unmatched infrastructure, and advanced correlation and intelligence.



DATA SHEET

Trained and Dedicated Professionals

VeriSign has an extensive team of certified security professionals who are specially trained to manage security products of leading industry vendors.

Lower Total Cost of Ownership

VeriSign Managed Intrusion Prevention Service saves organizations time and money by reducing staffing, training, maintenance and upfront capital expenditures.

The company's services are designed to be highly redundant to continually provide 24x7 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 and supported third party security products.

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's MSS represent an unparalleled commitment to providing services that enable enterprises to engage confidently in electronic commerce, communications and collaborative computing.

+ Get Started Today

For more information about VeriSign MSS and consulting services, please call 650.426.5310 or send an email to mss_ips@verisign.com.

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

Note: Gartner, Inc. (NYSE: IT and ITB) positioned VeriSign in the Leader quadrant in the 1H04 Managed Security Services Provider (MSSP) Magic Quadrant report for North America. A full copy of the report is available at: <https://www.verisign.com/cgi-bin/go.cgi?a=068050192724827000>.

©2004 VeriSign, Inc. All rights reserved. VeriSign, the VeriSign logo, "Where it all comes together," 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.

00017813