



KEY BENEFITS

Industry-Leading Service Level Agreements (SLAs)

VeriSign delivers the industry's highest quality of service backed by industry-leading SLAs. These strict SLAs demonstrate VeriSign's strong commitment to protecting its customers' networks.

Unmatched Security Intelligence

Managed IDS gears 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. Customers gain a real-time view of the health and integrity of their security architecture as a result of VeriSign's access to and ability to correlate information from an expanded base of threat data.

Comprehensive Deployment Services

VeriSign security engineers and programme managers ensure that the IDS sensors are staged and comprehensively tested prior to deployment. This process ensures the seamless integration of new technologies into customer environments without service interruption.

VeriSign® Managed Intrusion Detection Services (IDS)

On the Internet, network intruders are sophisticated navigators. They come from outside the enterprise, attacking Internet connections, altering Web pages and launching denial-of-service attacks. They can also originate from inside the network, initiating sophisticated assaults that can circumvent or pass through firewalls, transmitting confidential information or illegally modifying network access privileges. Further complicating network security is the continuous rise in vulnerabilities, uncertain geopolitical conditions and IT budget constraints. Intrusion detection systems require constant vigilance and proactive monitoring to be effective. Security events and alerts must be reviewed and analysed on a 24/7 basis to isolate real security threats from false alarms. However, the time and effort associated with the review of security events can be a significant undertaking for any organisation.

Designing and implementing a corporate security architecture that includes proactive and continuous intrusion detection is the first step in protecting an organisation's critical assets. While many organisations deploy firewalls as central gatekeepers to prevent unauthorised access, robust protection of networks and servers can only be achieved when a layered defence is employed.

+ Bottom Line

By intelligently placing intrusion detection sensors on a network, VeriSign's team of security experts manage customers' security devices round-the-clock, monitoring for security violations or misuse that originates from inside or outside the network. VeriSign® Managed Intrusion Detection Services (IDS) enhance an organisation's firewall protection by providing a comprehensive, real-time warning system that proactively identifies and isolates real security events, helping to prevent costly downtime and potential loss of revenue.



Full Life Cycle Management

VeriSign delivers true life cycle management on an ongoing basis to ensure that the security devices within customer architectures are updated and fully operational.

Security Monitoring and Risk Management

VeriSign provides 24/7 monitoring of security events which are captured, analysed and correlated in real-time. Suspicious and malicious events are therefore proactively identified, mitigating an organisation's risk potential. When combined with VeriSign® consulting services, the company's security experts immediately execute remediation plans.

Health and Performance Monitoring

VeriSign provides 24/7 proactive monitoring for health and performance of security devices. This allows VeriSign to proactively address potential operational performance problems prior to actual service failures and provide continuous service to its customers.

Full Intrusion-Detection Capabilities Realised

VeriSign reduces the "noise" associated with false positives through fine-tuning procedures that maximise the company's ability to respond proactively to verified security events.

Due Diligence

VeriSign comprehensive Managed IDS helps address the requirement for due care and diligence mandated by industry and government regulations. Compliance both aids an organisation in protecting critical assets, as well as in assuring corporate stakeholders that the appropriate security and privacy measures have been taken to safeguard business transactions.

+ Description

VeriSign Managed IDS offers 24/7 monitoring of network traffic. The service acts as an alarm for an organisation's network, setting off necessary alerts when a potential attack is recognised. These alerts, based on the policies developed with clients, are actively monitored and managed by VeriSign certified security engineers at the company's Security Operations Centers (SOCs) and real security events are quickly identified and escalated. All intrusion attempts, regardless of severity, are logged and well-defined. Customer notification and escalation procedures are executed for each security event.

+ Service Features

- Configure and provision devices
- Notify customers of major security and health issues and provide event descriptions, context and high-level remediation
- Create initial policies
- Tune and update policies
- Upgrades and patch management
- Correlate IDS event data with information collected from other managed devices and from the Managed Vulnerability Protection Service (MVPS)
- Flexible reporting options on client portal
- Monitor health and security events 24/7
- Seamless integration with VeriSign's Incident Response and Computer Forensics team

+ Supported Platforms

- Cisco® Secure IDS
- Enterasys™ Dragon
- Intrusion SecureNet PRO™
- ISS RealSecure™
- ManHunt™
- Snort™
- Sourcefire™

+ Security Operations Centres

VeriSign Security Operations Centres (SOCs) are secure, highly available environments that provide 24/7 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 control, while a generator backup, UPS-conditioned power 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.

Guaranteed Responsiveness

VeriSign immediately commences a client-specific escalation procedure when a problem is detected and then works quickly to identify its source. VeriSign's rapid response to security incidents ensures that its customers are fully apprised of and prepared for any impending threat.

Reliable Communication/ Management Channel

The proprietary VeriSign 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 SOCs. The SDA improves security implementation efficiency, provides enhanced security and reliability and lowers capital and operational costs since VeriSign assumes all SDA hardware and management expenses. Deployment of the SDA is not required, but is highly recommended.

Negates False Alarms

VeriSign's security experts leverage industry best practices and proprietary methodologies to identify real security events before systems are compromised, thereby eliminating time-consuming false positives.

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 Secure Sockets Layer (SSL) encryption. The Client Resource Portal serves as the primary point of contact for

+ TeraGuard™

VeriSign's information management architecture, TeraGuard,™ collects a wide range of disparate data sources through its Security Defence Appliance (SDA). The VeriSign® SDA resides on the customer site and converts the data from security and network devices into a single, normalised stream of security-related events. The TeraGuard application then analyses and prioritises these events using a multi-tiered correlation process, enabling VeriSign quickly to reduce false positives, find real threats and take the appropriate action. Analysis of this wealth of threat data across clients provides VeriSign's trained security analysts with broad and real-time Internet security intelligence that would be virtually impossible for an organisation to emulate internally.

+ VeriSign Difference

Global Scale and Intelligence and Control™—VeriSign offers customers the benefit of an early warning system that gears 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 Managed Security Services (MSS) and continually invests in SOCs and support infrastructures. The company's services are highly redundant to ensure customers receive 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 organisations 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.



DATA SHEET

customer service and trouble ticketing, granting VeriSign clients access to real-time event reporting, timely intelligence and a customised vulnerability management platform.

24/7 Management, Monitoring and Support

VeriSign's expert staff of security analysts is available 24/7 to provide management, monitoring and support, thereby releasing an organisation from the unrelenting and time-consuming responsibility of safeguarding corporate information assets.

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, evaluate data collected through the TeraGuard application and promptly respond to information security threats. Relying on VeriSign's expert security staff eliminates the need for an organisation's internal staff to assess the inordinate amounts of information that today's security systems typically generate. As a result, internal security teams can refocus on other key security issues within their company.

Lower Total Cost of Ownership

VeriSign's Managed IDS saves organisations time and money by reducing or eliminating staffing, training, maintenance and upfront capital expenditures.

+ Get Started Today

For more information about VeriSign MSS and consulting services, please telephone 0800-032-2101 or send an email to sales@verisign.co.uk.

Visit us at www.verisign.co.uk for more information.

Note: In February 2004, VeriSign acquired Guardent, the recognised leader in Managed Security Services (MSSs). Guardent's security consulting and managed services are integrated into VeriSign's solution portfolio.

© 2005 VeriSign UK Ltd. All rights reserved. VeriSign, the VeriSign logo, Intelligence and Control, TeraGuard, "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. Cisco is a trademark of Cisco Systems, Inc. Enterasys is a trademark of Enterasys Networks, Inc. SecureNet PRO is a trademark of MimeStar, Inc. RealSecure is a trademark of Internet Security Systems, Inc. ManHunt is a trademark of Symantec Corporation. Snort and Sourcefire are trademarks of Sourcefire, Inc.

00018918