



DATA SHEET



KEY BENEFITS

A Recognized Leader

VeriSign is the recognized global leader in managed security services, and has a strong heritage of being entrusted to protect the key assets of online business: consumers, brands, Web sites, and internal networks.

Operational Maturity

Managing security infrastructures for customers since 2000, VeriSign® Managed Security Services organization has the operational maturity to efficiently integrate with the high-performing organizations of leading enterprises.

Lower Total Cost of Ownership

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

Best of Breed Technology

VeriSign supports and enhances the value of market-leading security technology products with correlation and analysis, and efficiencies of operations and scale.

VeriSign® Wireless Intrusion Prevention Service

Wireless LAN implementations, both authorized and unauthorized, are increasing quickly as businesses and individual employees seek the benefits of unrestrained mobility and convenient remote productivity. But the promise of disentanglement from wires comes with strings attached, as WLANs introduce new classes of threats and risks to sensitive information and information systems.

At the same time, voice, video, and data technologies are converging as enterprises bundle them through an integrated wireless/wired networking infrastructure to support mission critical applications and enhanced network communications. No longer can WLANs be considered a separate and distinct network infrastructure. Enterprises can no longer depend solely on products that detect and block only wire-side intrusions. Enforcing policy compliance now means incorporating wireless-specific intrusion prevention technology that not only detects and alerts on policy-unfriendly events, but that can also thwart a potential wireless security breach before it impacts the business.

Wireless intrusion protection technology is complex, and the nature of the threats, attacks, and responses are quite different from their wired counterparts. However, the considerable compliance expertise and operational skills needed to meet business goals for intrusion prevention technology investments are in short supply.

Legal and industry regulations around compliance can be notoriously vague. Operational success is a core competency that is difficult to find. It requires aligning an appropriate wireless intrusion prevention strategy with solution planning, architecture, deployment, and configuration, as well as an understanding of how to implement and operate the technology to meet policy compliance. Compliant operation of wireless security infrastructures also calls for 24x7 staffing of skilled security professionals to diligently monitor wireless intrusion prevention events. Qualified staff can also filter out false positive alerts and turn qualified alerts into actionable intelligence based on correlation with the best available security event data and visibility into the global threatscape.

Companies are faced with a new level of risk—regulatory noncompliance and resulting penalties, wasted expenditures on an ineffective intrusion protection program, and distraction from core business competencies to meet compliance and security requirements.





KEY BENEFITS

Objective Advice

VeriSign is a technology- and vendor-neutral services company. VeriSign does not make or re-sell security software or hardware products.

Compliance Expertise

The VeriSign® Global Security Consulting team performs hundreds of security and compliance audits annually for some of the largest organizations in the world. Most security consulting customers are in regulated industries and include HIPAA, GLBA and other regulatory assessments. Consultants average more than ten years' experience in enterprise information security and three or more industry certifications per consultant.

Wireless Expertise

VeriSign Wireless Intrusion Prevention Service leverages VeriSign intelligence to deliver intra-enterprise, inter-enterprise, and Internet-wide security intelligence.

Unmatched Security Intelligence

VeriSign has unique insight into internal and global threats through its iDefense services and monitoring of a large number of customer security devices.

Commitment to Excellence

VeriSign continues to invest heavily in research and development and infrastructure, with multiple SOCs and a highly redundant architecture to make sure customers receive 24x7 support worldwide.

Comprehensive Deployment Services

VeriSign consultants, engineers, and program managers help ensure that the wireless intrusion prevention devices are architected, configured, staged, and tested before deployment.

+ A Solution for Managing Wireless Network Threats

VeriSign® Wireless Intrusion Prevention Service is an effective solution that helps enterprises overcome technology, regulatory, and operations pitfalls. This service capitalizes on the industry's leading team of wireless and security consultants, and on mature managed security services operations to help customers confidently, quickly, and effectively architect and set up a wireless intrusion prevention program aligned with strategy and compliance requirements. Once the service is in place, VeriSign manages and monitors the organization's wireless intrusion prevention service infrastructure, tuning and filtering out false positives, and notifying the customer of critical security or health events.

VeriSign Wireless Intrusion Prevention Service adds value to wireless intrusion prevention investments by layering on intra-customer, inter-customer, and Internet-wide correlation and intelligence analysis. It also saves customers time and money through operational efficiencies and economies of scale, and reduces the need for staffing, training, and up-front capital expenditures.

VeriSign security experts design, implement, manage, and monitor the intrusion prevention service sensors around-the-clock, monitoring for health events and security violations from attacks that originate inside or outside the network. Industry-leading service level agreements help ensure that customers are quickly notified of security and health issues so they can take prompt action to mitigate risk.

Delivered through VeriSign's information management and analysis platform, the VeriSign Wireless Intrusion Prevention Service makes the most of best-of-breed technology, operational excellence, and world-class consulting expertise to provide a flexible solution. The service includes the following components:

- VeriSign wireless deployment and logistics up-front consulting
- VeriSign compliance and security consulting
- MSS Service Activation
 - + Information gathering using purpose-built forms and tools
 - + Provisioning and installation
 - + Verification of activation (event logs on the VeriSign Enterprise Security Portal)
- Service Components – 24x7 Monitoring
 - + Baseline policy
 - + Policy tuning
 - + Sensor health monitoring
 - + Security event monitoring, alert qualification, notification
- Service Components – Management
 - + Software upgrade and patch maintenance
 - + Change control
- Intelligence and analysis
 - + Intra-wireless security event correlation
 - + Wireless – wire-side security event correlation
 - + Global threat and zero-day attack intelligence



DATA SHEET

KEY BENEFITS

24x7 Security and Device Health Monitoring

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

Guaranteed Responsiveness

VeriSign begins the escalation procedure the moment a problem is detected and then works quickly to identify its source.

Always-on Client Resource Portal

The VeriSign® Enterprise Security Portal provides a detailed view of a customer's security devices under VeriSign management. It includes reports based on device type, and access to an ad hoc query engine for sophisticated analysis of security events across multiple platforms and locations. Access is secured with token-based authentication and SSL encryption.

Customizable Review and Sign-off for Workflow and Auditing

Users can use the VeriSign Enterprise Security Portal to review and approve or flag reports, enabling companies to create a secure audit trail for compliance.

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.

+ Service Features

- Optional wireless deployment and logistics consulting services to align planning, architecture, and implementation with strategy and policy
- Optional compliance and security consulting services to help ensure legal and regulatory compliance and alignment with security-industry best practices
- 24x7 monitoring and reporting of security and sensor health events analyzed in a holistic context of customer, cross-customer, and global intelligence environments
- Security sensor and infrastructure management
- Single sign on Customer Portal for anytime viewing and reporting of security and service information
- Industry leading SLAs

+ VeriSign Teraguard

VeriSign Teraguard information management architecture 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 VeriSign Teraguard architecture 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.

+ Security Operations Centers

VeriSign security operations centers are secure, highly available environments that house VeriSign's 24x7 operations. Bunker-style construction, tiered biometric access to sensitive areas, and video surveillance are some of the features of VeriSign's physical security controls, while 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.

+ The VeriSign Difference

VeriSign leverages an extensive intelligence-gathering network, proven methodology, state-of-the-art tools, and highly skilled professionals to deliver comprehensive, multi-layered defense against network-based security threats and vulnerabilities. Using these resources, companies can gauge risk more accurately and respond rapidly and appropriately to protect business-critical data and systems. The VeriSign layered network defense ranges from security assessments and compliance consulting to context-based threat intelligence, managed firewall and intrusion prevention services with advanced event correlation, managed Domain Name System services, enterprise authentication for employees and business partners, and mobile device management. This multi-faceted approach gives companies a holistic network security solution that allows them to optimize existing resources while comprehensively managing risk.

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

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

©2007 VeriSign, Inc. All rights reserved. VeriSign, the VeriSign logo, the checkmark circle, 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.

00024751 5-30-2007