



DATA SHEET



KEY BENEFITS

Global Presence

VeriSign has a worldwide presence and maintains strong relationships with ISPs, registrars, Computer Emergency Response Teams (CERTs), and local law enforcement authorities all over the world. This enables the phishing team to promptly remove phishing Web sites hosted in practically any country.

Unmatched Security Intelligence

The VeriSign Anti-Phishing Solution leverages VeriSign's intelligent infrastructure 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 the Domain Name System (DNS).

Business Risk Analysis

The most effective security program is one that strikes an optimal balance between cost and business risk. VeriSign develops a custom program to ensure that systems are continually protected from hackers and malicious code, both inside and outside of the customer's network perimeter.

VeriSign® Anti-Phishing Solution

Phishing, a common con in a hacker's bag of tricks, is quickly gaining ground as an effective means for credit card fraud and identity theft. Using a social-engineering tactic that preys on the trust a company has established with its customers, phishers use email messages to pose as legitimate organizations requesting sensitive information from their patrons. Recipients, under the guise that the email has originated from a credible source, unwittingly divulge personal and financial information in their response or in online forms located on fraudulent Web sites. These counterfeit emails and Web sites are often near-perfect replicas of the originals, therefore giving consumers no real cause for concern when asked to provide personal information.

The advent of phishing techniques further demonstrates the significant growth in credit card fraud and identity theft. Although a consumer can spend months or years trying to reclaim a stolen identity or correct a credit report, businesses can face significant security risk-related damages. From loss of brand identity to erosion of consumer confidence in e-commerce, these damages can pose staggering remediation costs for any organization that is a victim of a phishing attack.

The phishing problem has evolved significantly over the past few years. This problem touches multiple points across the organization—from end users and Web sites to mail servers and networks. In addition, today's attacks come from multiple vectors.

Phishing attacks may come from any of the following sources:

- Plain-text emails, sophisticated emails, and targeted emails (spear phishing)
- Domain-based attacks (pharming style)
- Malicious code-based or Trojan-based attacks

The perpetrators of phishing attacks have also changed. Whereas attacks once originated mainly from a single hacker/phisher, today's attacks also come from organized crime groups with global syndication. For example, there have been instances in which a phishing Web site is hosted in one country, the spam attack is launched from a second country, and the financial fraud transaction occurs in a third country for a user of another country.





DATA SHEET

Always-on Enterprise Security Portal

The VeriSign® Enterprise Security Portal provides a detailed view of a customer's cases. It includes a variety of reports and access to an ad hoc query engine for sophisticated analysis of security events across multiple platforms and locations. The Enterprise Security Portal serves as primary point of contact for customer service and trouble ticketing, granting VeriSign customers access to reporting tools and timely intelligence.

24/7 Management, Monitoring, and Support

VeriSign releases an organization from the unrelenting and time-consuming responsibility of safeguarding corporate information assets. VeriSign's expert staff of security analysts is available to customers around the clock.

Trained and Dedicated Professionals

VeriSign has an extensive team of certified security professionals who are specially trained to respond to phishing attacks and other security incidents. The team keeps up with the latest phishing attack tactics and develops counter-strategies and solutions.

Lower Total Cost of Ownership

The VeriSign Anti-Phishing Solution saves organizations time and money by reducing or eliminating staffing, training, maintenance, and upfront capital expenditures.

+ Bottom Line

Phishing is a unique security, identity theft, and financial fraud problem. Frequently, large amounts of money are at stake. E-commerce sites can represent a multimillion-dollar investment, as well as a key revenue-generating infrastructure for many businesses, especially those in the financial, retail, and online auction markets, as well as Internet service providers (ISPs). To preserve customer trust and loyalty and maintain an effective e-commerce trade, organizations must integrate appropriate security measures to protect against all compromises of sensitive customer and business information.

No single technology solution completely counters phishing. To solve the phishing problem, organizations need a multi-pronged strategy, robust processes, and state-of-the-art technology. They need to work closely with industry organizations like the Anti-Phishing Working Group (www.antiphishing.org) to understand the latest phishing attack trends and to develop solutions to counter phishing at the end-user level, Web sites, mail servers, networks, and all other touch points.

A comprehensive solution should include the following components:

- **Prevention** – To prevent attacks
- **Detection** – To detect attacks and anomalies
- **Timely response** – To minimize the exposure and risk of a phishing attack
- **Reporting** – Including phishing trend analysis and high-level management reports, to understand and prioritize attacks

+ Description

VeriSign® Anti-Phishing Solution provides the most comprehensive, inclusive security program to mitigate and eliminate phishing attempts. The solution, which includes services to prevent, detect, and respond to phishing attacks, allows each organization to customize a program that meets its specific security needs.

+ Prevention Services

Phishers are taking a page from the hacker's "social engineering" book to abuse the trust relationship between the victim and the business entity spoofed by the phisher. The only antidote is a combination of policies, programs, and education, as well as strong identity-protection services.

Assessment, Education, and Policy Programs

VeriSign® Global Security Consulting services offer a full range of engagements to assess current processes and vulnerabilities; recommend optimal policies; implement educational programs for employees and end users; and, if requested, develop a response plan to help companies manage phishing attacks.

VeriSign® Identity Protection (VIP)

VeriSign Identity Protection is a comprehensive suite of identity protection and authentication services that are designed to strengthen and protect consumers' digital identities. Delivered across a trusted, shared network, VIP helps manage security risk for financial services, e-commerce companies, and enterprises that interact electronically with consumers' personal data.

The VIP suite is comprised of VIP Fraud Detection Service and VIP Authentication Service. These complementary services form a flexible, layered solution that provides both visible and invisible mechanisms for securing online transactions and preventing identity theft. VIP Fraud Detection Service provides invisible server-side monitoring capabilities. VIP Authentication Service provides a more visible, standards-based strong authentication solution for online commerce applications. Both services help ensure that a person is who he or she claims to be.

VIP Fraud Detection Service

VIP Fraud Detection Service provides intelligent fraud monitoring and fraud detection by leveraging VeriSign's extensive Internet fraud experience, state-of-the-art technology, hands-on analysts, and intelligent network to identify fraud patterns and anomalies. The service is highly scalable and extensible, supporting thousands of rules and allowing organizations to use any combination of transaction or user information. A customizable rules engine enables organizations to leverage their existing data, and includes out-of-the-box fraud detection rules that protect against well-known fraud patterns. The rules engine is complemented by a self-learning behavioral engine that automatically finds patterns of normal behavior and uses this data to identify and flag anomalies in real time. The service combines this information and other intelligence from multiple sources to create an anomaly score and when necessary intervene. Intervention mechanisms include question-and-answer processes, out-of-band verification (e.g., email, automated call, and Short Message Service (SMS)), and help desk calls. Finally, the service includes a case management interface for interacting with users and resolving fraud cases.

VIP Authentication Service

The VIP Authentication Service provides comprehensive and highly flexible security for consumer transactions. It is ideal for higher value, higher risk transactions. The open standards-based service allows any OATH-compliant device to be used for authentication, and it allows organizations to easily issue and/or accept multiple credentials from each user. VIP Authentication Service includes a number of options for supplemental factors, including standalone hardware devices such as one-time password (OTP) tokens and "soft" devices such as voice-enabled OTPs, OTP-enabled cell phones, and SMS OTP. VIP Authentication Service leverages a shared validation infrastructure that is operated by VeriSign and enables organizations to deploy strong authentication without bearing the entire burden of managing and operating a self-standing authentication infrastructure.

+ Detection Services

The numerous forms and methods of phishing continually evolve to avoid detection and dupe increasingly suspicious consumers. It is important to effectively detect newly evolved phishing schemes and attacks. VeriSign leverages its intelligent infrastructure to efficiently and accurately identify actual phishing attacks and weed out false positives.

Extensive Monitoring and Scanning Capabilities

VeriSign provides a full range of solutions to protect a company's digital assets, including services that scan millions of Web sites, Usenet newsgroups, domain names, and chat groups to search for infringement of a company's brand name, traffic-diversion tactics, and unwanted brand association with objectionable content. Brand monitoring enables companies to know where their logos and content are being used, as well as where their digital and physical goods and services might be distributed without authorization.

+ Response Services

If an organization is under phishing attack, it is very important to mitigate the potential damage of an attack by responding promptly and appropriately. Phishing response services are critical to counter phishing attacks in a timely manner and to preserve forensic evidence, if necessary.

VeriSign® Phishing Response and Brand Abuse Service

As a provider of critical Internet infrastructure, VeriSign offers a Phishing and Brand Abuse Response Service that leverages extensive experience in Internet fraud services as well as an international network of contacts in the legal, government, registrar, and ISP communities to identify sources of phishing attacks and quickly shut down Web sites and accounts. The VeriSign response team is available 24/7 and uses proprietary phishing intelligence tools to analyze and investigate attacks and bring down Web sites promptly to minimize the customer's risk. The VeriSign service also monitors previously shutdown Web sites to check whether they are re-activated. If the phishing Web site comes back up, VeriSign follows up promptly to bring down the Web site quickly and ensure removal.

Forensics

The VeriSign® Incident Response and Forensics Services team works with customers to perform post-mortem forensics and data recovery, when applicable.

Security Operations Centers

VeriSign Security Operations Centers (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, from electricity to telecommunications links to data processing, are fully redundant, thereby eliminating any single point of failure.

+ The VeriSign Difference: Expertise, Intelligence, Trust

Few companies match VeriSign's experience and expertise, depth and breadth of services, robust infrastructure, intelligence, and role as trusted advisor. VeriSign® Security Services leverage exceptional knowledge, training, and experience; best-of-breed solutions; a global network of proven technology; and VeriSign's history of stability and trust to deliver cost-effective solutions for proactively managing information security risk.

The following characteristics distinguish and differentiate VeriSign offerings:

- **Global scale and intelligent infrastructure** – With a worldwide customer base and thousands of security devices under management, VeriSign has the scale to support the largest and most demanding organizations and the flexibility to support smaller enterprises where security is also a concern. The breadth of devices that VeriSign monitors affords the company a wider and deeper view of Internet activity. It leverages this unique threat intelligence, as well as the intelligence gathered by the VeriSign® iDefense® Security Intelligence Services team to proactively identify—and alert customers to—emerging attack trends and cyber threats.



DATA SHEET

- **Seasoned practitioners** – With an average of more than ten years’ experience in enterprise information security and three or more industry certifications per consultant, the VeriSign® Global Security Consulting team boasts one of the highest concentrations of credentialed experts in the industry. The security team’s expertise, dedication, and focus on customer service help ensure that each customer not only gets a real-world solution that meets the unique requirements of its business, but also receives prompt attention when security events or other issues arise.
- **Commitment to excellence** – As a recognized leader in managed security services, VeriSign continues to experience growth well beyond the managed security services market. As a result, VeriSign continues to invest heavily in research and development (more than 15 percent of revenues annually) and in infrastructure (where we continue to add SOCs and staff in anticipation of continued growth). The company’s architecture is highly redundant to ensure that customers receive 24/7 support and availability worldwide.
- **World-class support for industry-leading technology** – VeriSign delivers world-class services to enterprise customers by leveraging industry-leading technology; skilled experts; structured processes; and unique intelligence. As a services company, VeriSign focuses solely on designing and deploying security solutions that meet the specific requirements of its customers and maximize the effectiveness of their existing security investments.
- **Trusted partner** – VeriSign has a strong heritage in providing trusted security services, and thousands of organizations benefit from this heritage every day. Together with strong authentication, security consulting, threat intelligence, and e-commerce security, VeriSign® Managed Security Services represent an unparalleled commitment to helping enterprises engage confidently in electronic commerce, communications, and collaboration.

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 the VeriSign Anti-Phishing Solution, 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, 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. 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.

00018970 06-10-2006