



DATA SHEET



KEY BENEFITS

Unmatched Security Intelligence

VeriSign® iDefense Security Intelligence Services leverage submissions from a private, worldwide network of independent security researchers obtained through our Vulnerability Contributor Program (VCP). Intelligence researchers are in more than 42 countries and provide intelligence in multiple languages. VeriSign has received more than 1,300 submissions to the VCP in the last two years. Upon receipt of these submissions, VeriSign does thorough internal research to validate the submission, and upon validation, notifies both the affected vendor and iDefense customers. VeriSign works closely with vendors like Microsoft to help ensure that potential vulnerabilities are identified and that vendors are able to create patches as quickly as possible. Customers are also notified of these vulnerabilities, while VeriSign is working with the vendor. On average, iDefense customers receive notices regarding vulnerabilities 68 days before they are released to the public by the vendors.

Customized Intelligence

VeriSign iDefense Security Intelligence Services offer a highly customizable set of intelligence services delivering the intelligence your organization needs, when you need it.

VeriSign® iDefense® Security Intelligence Services

As networks continue to expand to include customers, partners, remote employees, enterprises, and government, organizations must leverage the most advanced security intelligence to protect customer data and corporate assets. In today's complex threat environment, it is crucial for organizations to understand the increasing number of vulnerabilities, countermeasures, exploit codes, cyber terrorist, and hacker threats, and how they relate to one another, and their potential business impact.

+ Bottom Line

The VeriSign® iDefense Security Intelligence Services are an important component of VeriSign's acclaimed suite of Managed Security Services (MSS). iDefense services deliver comprehensive, actionable intelligence regarding network-based security threats and vulnerabilities. This intelligence can help organizations proactively protect critical data and infrastructure from attacks, and thereby mitigate security risk.

Utilizing an experienced team of security experts, VeriSign scours the Internet for potential cyber threats including new malicious code, zero-day exploits, or hacker groups committing cyber crime or threatening widespread cyber terror. VeriSign combines this with technical and traditional intelligence to deliver advanced warning and analysis of these threats to help protect an organization's critical infrastructure.

+ Description

Each iDefense Security Intelligence Services Package includes one or more of the following components:

Daily Intelligence Reports

Best-in-class intelligence content is critical to every enterprise's security practice.

Intelligence Report types include:

- **Original vulnerability research** – Research is conducted by both internal research project analysts and submissions from a worldwide network of independent security researchers obtained through the Vulnerability Contributor Program (VCP). There have been more than 1,300 submissions to the VCP in the last two years resulting in more than 300 original vulnerability reports to customers.



Where it all comes together.™



The Value of Intelligence

The number of vulnerabilities continues to grow exponentially, while the elapsed time between vulnerability and exploit continues to shrink. VeriSign, which tracks security events on a global basis, delivers notification of vulnerabilities and exploits as they are identified, providing timely, actionable information and guidance to help mitigate risks before they are exploited. VeriSign iDefense Security Intelligence Services enable a proactive approach to maintaining a secure environment, while saving time and money by eliminating the hours spent searching through Web sites and emails, gathering and distributing information, and following up on the results.

Security Monitoring and Risk Management

The Vulnerability Aggregation Team (VAT) monitors security events 24/7. These events are captured, analyzed, and correlated in real time by VAT, which provides primary and secondary analyses of new vulnerability exploits. Suspicious and malicious events are therefore proactively identified—helping to mitigate an organization's potential for security risk.

Global Network of Intelligence Contributors

VeriSign's multilingual network includes more than 250 research contributors in more than 42 countries offering early and unique insight into the cyber underground and previously unknown software vulnerabilities.

- **Public vulnerability aggregation** – Our Vulnerability Aggregation Team (VAT) ensures around-the-clock coverage and customer notification of burgeoning vulnerabilities and exploits that target any of the more than 2,000 closely-monitored applications, hardware, and operating systems. VAT analysts provide primary and secondary analyses of new vulnerability exploits, working in a rapid-response system designed to ensure timely notification of exploits.
- **Malicious code research and analysis** – Malicious code analysts monitor virus-related threats, combining real-time human intelligence with focused, automated spiders and other search tools that mine the Internet. This helps VeriSign identify new threats and malicious actors.

Flash Intelligence Reports

Flash Intelligence Reports are delivered as soon as VeriSign researchers identify a serious security issue worthy of customers' immediate attention. A Flash Intelligence Report can be delivered for a rapidly advancing worm or virus (e.g., Sobig or Blaster), for a newly discovered severe vulnerability, or for a global threat issue that merits immediate analysis.

Weekly Threat Summary

Every week VeriSign provides customers with a report that summarizes all the newest Intelligence Reports, ensuring that no new issues are overlooked.

Bi-Weekly Threat Briefings

VeriSign holds bi-weekly customer briefings conducted by VeriSign analysts. The briefing is a summary of the previous two weeks' Intelligence Report activity and may highlight specific reports and/or trends seen in recent reports. Particular focus is placed on Microsoft® Security Bulletins, including workaround strategies and guidance on which bulletins should receive priority.

Weekly Threat Report

This weekly report, delivered via an authenticated portal and email, provides an overview of key trends and developments in the area of worldwide cyber threats, including terrorism and homeland security issues. It is intended to assist key decision-makers in pursuing policies that will help mitigate threats. Subscriptions can include archived reports.

Bi-Weekly Malicious Code Review

This report focuses on recent malicious code trends, spreading strategies, and mitigation techniques. It is a resource for the security practitioner or technical manager looking for an in-depth understanding of malicious code attacks and how they can be mitigated and detected in an enterprise network environment.

Rapid Response Intelligence Reports

In response to a customer request, VeriSign will perform analysis on code related to exploits that may be impacting the customer's networks. Customers may submit code via email or they may contact VeriSign via telephone. VeriSign will deliver its analysis of the code or situation via conference call with the customer. In some, but not all cases, the report may include remediation or workaround strategies.



DATA SHEET

Topical Research Reports

Each iDefense Topical Threat Research Report examines one specific security topic in depth. Recent examples of Topical Threat Research subjects include “Phishing and Pharming: A Comparison”, “Recent Developments in Key Logging,” “Security Implications of Using Firefox versus Internet Explorer,” and “Security Implications of Webmail.”

Focused Intelligence Reports

Customers can request in-depth research and investigation of specific topics of interest. Recent examples of focused intelligence reports include pre-annual meeting “chatter” monitoring, off-shore risk assessment, geographical actor profiles, and ad-hoc statistics and reporting regarding security vulnerabilities and threats. This research is highly customizable and deliverables can include custom white papers, or in-person and teleconference briefings.

Monthly Microsoft Bulletin

Once a month, VeriSign delivers a report that summarizes the preceding month’s new and revised Intelligence Reports that relate to Microsoft products. The report is delivered as a PDF attachment to an email

Customer “Analyst Desk” Designated Resource

Customers are assigned a designated analyst allowing them direct access to a VeriSign subject-matter expert. These analysts keep customers apprised of the current security trends and direct, customer-specific, research projects.

Phishing Response Service

Each month customers can request a set number of detected phishing sites to be taken down using VeriSign’s Phishing Response Service. There is no additional fee for this request.

+ Summary of Available Packages

SERVICE	THREAT PROTECTION LEVEL		
	BASIC	ENHANCED	COMPREHENSIVE
iDefense Intelligence Reports (daily alerts)	X	X	X
iDefense FLASH Reports	X	X	X
Weekly Summary of New Vulnerabilities	X	X	X
iDefense Analyst Access		X	X
iDefense Rapid Response Intelligence Reports		X	X
Bi-Monthly Threat Briefings		X	X
iDefense Weekly Threat Report		X	X
iDefense Bi-Weekly Malicious Code Review		X	X
iDefense Topical Research Reports		X	X
iDefense Focused Intelligence Reports			X
iDefense Customer Analyst Desk (designated resource)			X
Phishing Response Service			X

X = included

In addition, subscriptions are available to VeriSign iDefense Security Intelligence via the following methods:

- **Archer™ XML feed and Preventsys XML feed** – VeriSign provides customers with access to new and re-versioned Intelligence Reports via an authenticated Web service for integrated use with currently supported distributions of Archer and/or Preventsys security software. Customers have access to all Intelligence Reports in the Web service collection. Intelligence Reports are available in four types: Public Vulnerabilities, iDefense Exclusive Vulnerabilities, Malicious Code, and Geo-political Threat.
- **XML Web service appliance** – VeriSign delivers to customers the XML Web Service Appliance. The appliance manages the process of retrieving new and re-versioned Intelligence Reports from a Web Service. Reports are inserted into a relational database that is included with the appliance. Application interface to the appliance is by SQL queries. Delivered as a rack-mounted server that resides onsite at the customer. May be selected as optional add-on to any service package.

+ The VeriSign Difference

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 its iDefense Security Intelligence Services team to proactively identify—and alert customers to—emerging attack trends and cyber threats.
- **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 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 Security Operations Centers (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.



DATA SHEET

- **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.

+ Learn More

For more information about VeriSign® Managed Security Services and VeriSign® iDefense® Intelligence Services, please call 650-426-5310, email enterprise_security@verisign.com, or visit us at www.Verisign.com.

+ About VeriSign

VeriSign, Inc. (Nasdaq: VRSN) operates intelligent infrastructure services that enable and protect billions of interactions everyday across the world's voice and data networks. Additional news and information about the company is available at www.verisign.com.

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

©2006 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. Archer is a trademark of Archer Technologies. Firefox is a registered trademark of the Mozilla Foundation. Microsoft is a registered trademark of Microsoft Corporation. All other trademarks are the properties of their respective owners.

00021221 04-17-2006