



DATA SHEET



KEY BENEFITS

Unmatched Security Intelligence

VeriSign® iDefense Security Intelligence Services leverages submissions from a private, worldwide network of independent security researchers obtained through our Vulnerability Contributor Program (VCP). Intelligence researchers are in over 30 countries and provide intelligence in 12 languages. VeriSign has received 1,100 submissions to the VCP in the last three 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 any 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. As a result, from the 1,100 VCP submissions over the past three years, VeriSign has reported more than 200 iDefense unique, original vulnerability reports to customers. Most important, on average, iDefense customers received notices regarding these vulnerabilities 45 days before they were released to the public by the vendors.

VeriSign® iDefense® Security Intelligence Services

As networks continue to expand to include customers, partners, remote employees, enterprises, and government must leverage the most advanced security intelligence to protect customer data and corporate assets. In today's complex threat environment, it is crucial for enterprises 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 which can help organizations proactively protect critical data and infrastructure from attacks.

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 of the iDefense Security Intelligence Services Packages offered include one or more of the following components:

VeriSign iDefense Daily Intelligence Reports

Best-in-class intelligence content which is critical to every enterprise's security practice. Intelligence Report types include:

Original Vulnerability Research

Research is conducted by both internal research projects analysts and submissions from a worldwide network of independent security researchers obtained through the Vulnerability Contributor Program (VCP). There have been more than 1,100 submissions to the VCP in the last three years resulting in more than 200 iDefense unique original vulnerability reports to customers.



Where it all comes together.™



DATA SHEET

Customized Intelligence

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

The Value of Intelligence

The cost of a security breach in terms of loss of time, data, and brand equity has grown dramatically over the last few years. At the same time, the number of vulnerabilities has grown exponentially, while the time elapsed between vulnerability and exploit continues to shrink. As a result, it is increasingly critical for enterprises to proactively protect themselves. 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

24/7 monitoring of security events, which are captured, analyzed and correlated in real-time by our Vulnerability Aggregation Team who provide primary and secondary analyses of new vulnerability exploits. Suspicious and malicious events are therefore proactively identified—helping to mitigate an organization's risk potential.

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 1,500 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.

VeriSign® iDefense® Flash Intelligence Reports

Flash Reports are delivered as soon as VeriSign researchers identify a serious security issue worthy of clients' 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.

VeriSign iDefense Weekly Threat Summary

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

VeriSign iDefense 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.

VeriSign iDefense 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.

VeriSign iDefense Rapid Response Intelligence Reports

In response to customer requests, VeriSign will perform analysis on code related to exploits that may be impacting their networks. Customers may submit code via email or they may contact VeriSign via telephone. VeriSign will deliver their 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.

VeriSign iDefense Topical Research Reports

Each iDefense Topical 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."



DATA SHEET

Global Network of Intelligence Contributors

VeriSign's multilingual network includes more than 200 research contributors in over 30 countries offering early and unique insight into the cyber underground and previously unknown software vulnerabilities.

VeriSign® iDefense® 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 and can include custom white papers, or in-person and teleconference briefings.

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.

VeriSign iDefense Directed Subscription

Subscribers at this level can suggest topics for our Topical Threat Research Reports, preview work-in-progress research, and request reports, as needed.

+ Summary of Packages Available

SUBSCRIPTIONS	TIER 1 BASIC THREAT PROTECTION	TIER 2 ENHANCED THREAT PROTECTION	TIER 3 COMPREHENSIVE THREAT PROTECTION
VeriSign® iDefense® Intelligence Reports	X	X	X
VeriSign iDefense Flash Intelligence Reports	X	X	X
VeriSign iDefense Weekly Threat Summary	X	X	X
VeriSign iDefense Bi-weekly Threat Briefings	X	X	X
VeriSign iDefense Weekly Threat Report		X	X
VeriSign iDefense Rapid Response Intelligence Reports		X	X
VeriSign iDefense Topical Research Reports (Includes MS Monthly Bulletin)		X	X
VeriSign iDefense Focused Intelligence Reports			X
Customer Analyst Desk			X
VeriSign iDefense Directed Subscriptions			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

Global Scale and Intelligence and Control – As a leading provider of critical Internet-infrastructure services, VeriSign has unique visibility into security patterns, trends and threats on the Internet by extracting and assimilating information from its worldwide customer base and network of security devices under management. Leveraging this information and intelligence, VeriSign can be first off the mark in providing companies with visibility, aggregation, and correlation of worldwide Internet-related events and proactively identify and alert customers to attack trends.

Trusted Partner – VeriSign has a strong heritage in managing trusted security services, and thousands of organizations benefit from this heritage everyday. Together with strong authentication, application security and e-commerce security, VeriSign® Managed Security Services represent an unparalleled commitment to providing services that enable organizations to engage confidently in electronic commerce, communications and collaborative computing.

Seasoned Practitioners – The VeriSign security consulting team includes one of the highest concentrations of credentialed experts in the industry. With an average of ten year's experience in enterprise information security and three or more industry certifications per consultant, VeriSign boasts expertise across the entire information-security and information-privacy spectrum. The VeriSign team has worked with entities of all sizes worldwide, from government agencies and Fortune 1000 companies to small start-ups. VeriSign customers include municipal, state and federal agencies, financial institutions, healthcare organizations, telecommunications carriers, and online retailers.

Best-of-Breed Solutions – As a vendor-neutral provider of security services, VeriSign evaluates, certifies, and supports best-of-breed security products. It is a leading proponent of open standards-based technology for identity authentication and other security solutions. The company designs and deploys security solutions based on specific needs and requirements of its customers and regularly evaluates and enhances its service offerings and support for third-party security products.

+ Get Started Today

For more information about VeriSign® iDefense® Security Intelligence Services, please call 650.426.5310 or email enterprise_security@verisign.com.

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