



\* SOLUTION OVERVIEW



# VeriSign® iDefense® Threat Intelligence Services Overview





**CONTENTS**

+ Comprehensive, Actionable Intelligence	3
+ Four Optional Service Levels	3
+ Summary of Available Packages	5
+ Key Benefits	6
+ Learn More	6



# VeriSign® iDefense® Threat Intelligence Services Overview

Today's network threats are more numerous and more damaging than ever. Sophisticated attacks can seriously compromise an organization – not only in terms of lost productivity, data breaches and possible regulatory non-compliance penalties, but also lost trust and damaged reputation. Few organizations have the intelligence-gathering and threat-analysis capabilities to address network vulnerabilities and threats in their full context. Lack of comprehensive data can delay responses to true threats, impair threat prioritization, and incur costly and unnecessary emergency responses.

To manage risk effectively, organizations must use a holistic “threats-in-context” approach that allows proactive identification of real threats to critical business systems. VeriSign® iDefense® Threat Intelligence Services leverage an extensive intelligence-gathering network, proven methodology and highly skilled professionals to deliver comprehensive, actionable intelligence that does not merely look at the “what” and “how” of network-based security threats and vulnerabilities, but also the “who” and “why.” Using this intelligence, organizations can gauge risk more accurately and respond rapidly and appropriately to protect business-critical data and systems.

## + Comprehensive, Actionable Intelligence

VeriSign® iDefense Threat Intelligence Services are an important component of the acclaimed suite of VeriSign® Managed Security Services (MSS). Our 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 such as malicious code, zero-day exploits, and hacker groups committing cyber crime or threatening widespread cyber terror. VeriSign combines this knowledge with technical and traditional intelligence to deliver advanced warning and analysis of these threats to help protect an organization's critical infrastructure.

## + Four Optional Service Levels

VeriSign iDefense Threat Intelligence offers four optional service levels: Core, Standard, Enhanced, and Comprehensive. Every option features the unmatched capabilities of VeriSign's iDefense Threat Intelligence Services. The various service levels offer different components to meet your needs, including:

### Daily Intelligence Feed

Best-in-class intelligence content is critical to every enterprise's security practice. Daily intelligence report types include:

- **VeriSign® Public Vulnerability Reports**  
Our Vulnerability Aggregation Team (VAT) ensures around-the-clock coverage and customer notification of burgeoning vulnerabilities and exploits that target any of tens of thousands 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.
- **VeriSign® Flash Reports**  
Flash Reports are delivered as soon as VeriSign researchers identify a serious security issue that requires immediate attention. Flash Reports can be delivered for rapidly advancing worms or viruses, newly discovered severe vulnerabilities or global threats.
- **VeriSign® Malicious Code Reports**  
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 quickly and accurately.
- **VeriSign® Threat Reports**  
Multilingual analysts identify and track emerging global threats, then perform analysis and reporting to give actionable insight into incidents as they develop.
- **VeriSign® iDefense® Exclusive Vulnerability Reports**  
Research is conducted by both internal project analysts and contributors from a worldwide network of independent security researchers through the Vulnerability Contributor Program (VCP). There have been more than 2,100 submissions to the VCP in the last four years resulting in more than 1,100 exclusive vulnerability reports to customers.

**VeriSign® New Vulnerability Summary Report**  
Every week VeriSign provides customers with a report that summarizes all the newest vulnerability intelligence reports, ensuring no new issues are overlooked.

**VeriSign® iDefense® Threat Briefings**  
VeriSign holds bi-weekly customer briefings conducted by VeriSign analysts. The briefings provide 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® 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 international security issues. It is intended to assist key decision makers in pursuing policies that will help mitigate threats. Subscriptions can include archived reports.

**VeriSign® Malicious Code Summary Report**  
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.

**VeriSign® Vulnerability Summary Report**  
This report focuses on recent vulnerability exploitation trends, attack vectors and mitigation techniques. It is an invaluable resource for the security practitioner or technical manager who needs an in-depth understanding of vulnerability-related compromises and how they can be mitigated and detected in an enterprise network environment.

**VeriSign® Rapid Response Service**  
Targeted attacks are becoming ever more common and need immediate attention from experts. In response to a customer request, VeriSign will perform analysis on code related to exploits that may be impacting the customer's networks and provide detailed analysis with recommendations within three hours of the incident. 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 cases, the report may include remediation or workaround strategies.

**VeriSign® Topical Research Reports**  
Each Topical Research Report provides in-depth analysis of a specific security topic. Recent subjects include "Latest Developments in Social Engineering Techniques," "Advancements in Rootkits and Malicious Code Concealment Techniques," "Security Implications of Using Firefox versus Internet Explorer," and "Methods, Motivations and Mitigation of Insider Threats."

**VeriSign® Global Threat Research Report**  
VeriSign provides in-depth research reports about issues relating to global threats. Each report focuses on a single country or region. Countries and regions covered include Brazil, Russia, India, China, Korea, and the Middle East. Reports are published every six weeks and are delivered as a PDF attachment to an email. To ensure the most accurate and critical information, iDefense analysts spend weeks at a time performing in-country research at the source.

**VeriSign® Patch Tuesday Report**  
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.

**VeriSign® iDefense® Analyst Service**  
Customers can contact VeriSign at any time to speak directly to a VeriSign iDefense analyst. This allows direct access to authors of various intelligence reports and other specialized individuals available to answer your questions.

**VeriSign® Phishing Response Service**  
The VeriSign Phishing Response Service leverages extensive experience in Internet fraud services and an international network of contacts in legal, government, and ISP communities to help identify services of phishing attacks and get malicious Web sites and accounts shut down quickly.

**VeriSign® 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.

**VeriSign® Correlated Alerting Service**  
The VeriSign® Correlated Alerting Service may be added as an option to any VeriSign iDefense service package. VeriSign correlates newly-released alerts against customer asset data that may be derived from scanning or testing of customer hosts by VeriSign or supplied to VeriSign directly via a customer portal. If a match is found between the asset and vulnerability, VeriSign sends an email notification that directs the customer to a report that details the vulnerability, suggested remediation strategies known at the time of writing, and the IP addresses of the hosts potentially affected by the vulnerability.

**VeriSign® iDefense® Designated Analyst Service**  
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.

**+ Summary of Available Packages**

Service	Threat Protection Level			
	Core	Standard	Enhanced	Comprehensive
VeriSign® iDefense® Public Vulnerability Reports	+	+	+	+
VeriSign® Flash Reports	+	+	+	+
VeriSign® Malicious Code Reports		+	+	+
VeriSign® iDefense® Threat Reports		+	+	+
VeriSign® iDefense® Exclusive Vulnerability Reports		+	+	+
VeriSign® New Vulnerability Summary Report		+	+	+
VeriSign® iDefense® Threat Briefings			+	+
VeriSign® Weekly Threat Report			+	+
VeriSign® Malicious Code Summary Report			+	+
VeriSign® Vulnerability Summary Report			+	+
VeriSign® Rapid Response Service			+	+
VeriSign® Topical Research Reports			+	+
VeriSign® Global Threat Research Report			+	+
VeriSign® Patch Tuesday Report			+	+
VeriSign® iDefense® Analyst Service			+	+
VeriSign® Phishing Response Service				+
VeriSign® Focused Intelligence Reports				+
VeriSign® Correlated Alerting Service				+
VeriSign® iDefense® Designated Analyst Service				+

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

- VeriSign® iDefense® XML for Archer  
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 security software.
- VeriSign® iDefense® XML 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 at the customer's location. May be selected as optional add-on to any service package.
- VeriSign® iDefense® XML Web Service  
VeriSign delivers to customers the XML Web Service. 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. The application interfaces to the appliance via SQL queries, and it is delivered as a rack-mounted server that resides onsite at the customer. This may be selected as optional add-on to any service package.

## + Key Benefits

### Unmatched Threat Intelligence

VeriSign iDefense Threat Intelligence Services leverage submissions from a private, worldwide network of independent security researchers obtained through our Vulnerability Contributor Program (VCP). Intelligence researchers in more than 46 countries provide intelligence in multiple languages. VeriSign has received more than 2,100 submissions to the VCP in the last four years. Upon receipt of these submissions, VeriSign does thorough internal research to validate the submission, and upon validation, notifies both the affected vendor and VeriSign 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. In the last two years, iDefense customers received notices regarding vulnerabilities an average 122 days before they were released to the public by vendors.

### Customized Intelligence

VeriSign iDefense Threat Intelligence Services deliver the knowledge your organization needs, when it needs it.

### A Proactive Approach to a Secure Environment

The number of vulnerabilities continues to grow exponentially, while the elapsed time between vulnerability and exploit continues to shrink. VeriSign, a company that 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 Threat 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 the 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 400 research contributors in more than 42 countries offering early and unique insight into the cyber underground and previously unknown software vulnerabilities.

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 VeriSign iDefense Threat Intelligence Services, please call 650-426-5310, or email [enterprise\\_security@verisign.com](mailto:enterprise_security@verisign.com).

**Visit us at [www.Verisign.com](http://www.Verisign.com) for more information.**