



VERISIGN™

SOLUTION OVERVIEW



VERISIGN® IDEFENSE® SECURITY INTELLIGENCE SERVICES

SOLUTION OVERVIEW

VerisignInc.com



VERISIGN™

CONTENTS

COMPREHENSIVE, ACTIONABLE INTELLIGENCE	3
INTELLIGENCE DRIVES IMPROVED SECURITY OPERATIONS	3
INTEGRATED INTELLIGENCE YIELDS EFFICIENCY AND ACCURACY	4
FOUR OPTIONAL REPORT AND RESEARCH SERVICE PACKAGES	4
SUMMARY OF VERISIGN IDEFENSE SECURITY INTELLIGENCE SERVICES	5
ABOUT VERISIGN IDEFENSE SECURITY INTELLIGENCE SERVICES	8
LEARN MORE	8



VERISIGN™

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 NONCOMPLIANCE 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.

Enterprise security teams need a reliable, accurate view of serious threats delivered in context of their environment, geographic, and organizational needs to know what's relevant and critical. To help prioritize threat management, organizations are integrating threat intelligence as an essential part of their strategy for mitigating enterprise risk around cyber security threats.

The outcome will result in informed decisions and a sound, cost-effective risk mitigation strategy based on the potential impact that any one threat can have on an organization's IT assets, sensitive data, and critical production systems.

**COMPREHENSIVE,
ACTIONABLE INTELLIGENCE**

Security practitioners rely on Verisign® iDefense® Security Intelligence Services to collect, analyze, and package intelligence that matters to provide them with situational

awareness and mitigation strategies pertaining to enterprise cyber threats. Verisign iDefense Security Intelligence Services leverages an extensive intelligence-gathering network, proven methodology, and highly skilled professionals. This powerful combination puts security teams in control with proactive, accurate intelligence and informed recommendations for threat mitigation with insights into the cyber underground, malicious attack methods, undiscovered vulnerabilities, and global threats.

**INTELLIGENCE
DRIVES IMPROVED
SECURITY OPERATIONS**

Today, security teams recognize the value of integrating Verisign iDefense Security intelligence into daily security operations to drive increased global threat awareness; improve vulnerability and patch management; expand their bench and extend incident response capabilities; and effectively manage risk around online fraud.

Verisign iDefense provides packaged intelligence that addresses the specific and daily needs of key security operations:

**Verisign® iDefense® Global
Threat Intelligence Services**

is fundamental to critical decision making and increased global threat awareness within an enterprise to protect critical infrastructure, reputation, and trust.

**Verisign® iDefense® Vulnerability
Intelligence Services**

offers an essential ingredient for vulnerability management: timely, accurate and in-depth vulnerability research to address the significant burden on security teams to keep up with the ever-evolving universe of new and emerging vulnerabilities.



VERISIGN™

Verisign® iDefense® Incident Response Services provides access to a dedicated team of security engineers with advanced expertise around malicious code analysis and response strategies to compliment and extend an enterprise security team that most companies cannot afford to staff only for incidents.

Verisign® iDefense® Fraud Mitigation Services offers malware intelligence and mitigation solutions that assist security practitioners in quickly identifying and managing risk around online fraud.

INTEGRATED INTELLIGENCE YIELDS EFFICIENCY AND ACCURACY

Enterprise security organizations benefit from deep research analysis from Verisign iDefense. Our expert analysis adds value to the landscape of security management tools and platforms upon which security organizations rely each day for effective threat and vulnerability management.

Verisign iDefense Intelligence Feed for Archer™, ArcSight™, Agilience®, and Skybox®

Any Verisign iDefense service package can be integrated into the Archer, ArcSight, Agilience, and Skybox® security management platforms. Customers have access to view re-versioned Verisign iDefense Intelligence Reports via an authenticated Web service for integrated use with currently supported distributions of Archer,

ArcSight, Agilience, and Skybox security software. Customers have access to all Intelligence Reports in the Web service collection.

Verisign iDefense® Integration Service: QualysGuard® VM

The Verisign iDefense security intelligence feed is integrated with QualysGuard® Vulnerability Management (VM) through the Verisign iDefense portal, enabling customers to manage Verisign iDefense vulnerability reports with Qualys scan data. The service correlates against IT assets to prioritize vulnerabilities based on severity, business criticality, and relevance to the organization. This integration helps security teams prioritize patch deployments and remediation efforts particularly between full vulnerability scan cycles of their environments.

Verisign iDefense® Integration Service: Skybox® Threat Alert Manager

The Verisign iDefense Security Intelligence Feed seamlessly integrates with Skybox Threat Alert Manager, providing a centralized platform to normalize, correlate, and analyze security data from vulnerability scanners, patch management systems, and asset repositories. When data is compared against Verisign iDefense threat alerts, the integrated service supports automated prioritization of high-severity vulnerabilities to critical IT assets. Through the Skybox built-in remediation workflow system, designed specifically for managing the life cycle of security threats, Verisign

iDefense Threat Manager enables security organizations to automate the vulnerability remediation process with increased efficiency and accuracy compared to a manual vulnerability management process.

FOUR OPTIONAL REPORT AND RESEARCH SERVICE PACKAGES

Verisign iDefense Security Intelligence Services offers four optional report and research packages to address specific requirements and meet the unique cyber security needs of a business enterprise or government entity. These include Core, Standard, Enhanced, and Comprehensive Threat Protection Levels.

The foundation of Verisign iDefense's optional service packages is the vulnerability intelligence feed that provides best-in-class intelligence content critical to every enterprise's security practice and includes the following intelligence report types:

- **Verisign iDefense® 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 the more than ten thousand 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™

- **Verisign iDefense® 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 iDefense® Threat Reports** Multilingual analysts identify and track emerging global threats, then perform analysis and reporting to give actionable insight into incidents as they develop.

SUMMARY OF VERISIGN iDEFENSE SECURITY INTELLIGENCE SERVICES

Verisign iDefense® Threat Briefings

Verisign holds semi-monthly customer briefings conducted by Verisign analysts. The briefings provide a summary of the previous month's Intelligence Report activity and may highlight specific reports and/or trends seen in recent reports. Particular focus is placed on Microsoft® Corp. 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 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 iDefense® Exclusive Vulnerability Report

Research is conducted by both internal project analysts and contributors from a worldwide network of independent security researchers through the Vulnerability Contributor Program (VCP). iDefense has provided clients with in-depth reporting and analysis on more than 10,000 vulnerabilities over the past 3 years, of which about 650 were exclusive vulnerabilities identified by the iDefense team.

Verisign iDefense® Vulnerability Summary Report

Every week, Verisign provides customers a summary report that focuses on recent vulnerability exploitation trends and attack vectors to ensure that no new issues are overlooked.

Verisign iDefense® 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 and its products. The report is delivered as a PDF attachment to an email.

Verisign iDefense® Malicious Code Intelligence Report

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 iDefense® 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 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 iDefense® Designated Analyst Service

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



VERISIGN™

Verisign iDefense® Malcode Rapid Report Service

Verisign has the ability to quickly process malicious code and provide a summary report back to the customer. Code can be submitted by the customer directly to the analytic engine that will generate a report back to the customer generally within one hour. Reports may include: code distribution URLs, anti-virus effectiveness, and drop site information.

Verisign iDefense® 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 iDefense® Artifact Analysis On-Demand Service

The Verisign iDefense® Artifact Analysis On-Demand Service provides a trusted and independent malicious code analysis resource. Security organizations may submit various malware artifacts for extended

analysis for up to two weeks per submission. Examples of analysis may include, but are not limited to, server log file analysis, extended malicious code reverse engineering, forensically analyzing contents, and memory dumps from an infected computer.

Verisign iDefense® IP Reputation Service

Verisign maintains an IP list of known malicious URLs and domains. This service provides daily updates to the IP list, allowing customers to alert and/or block traffic from these locations.

Verisign iDefense® Cyber Threat Brief

Verisign delivers a cyber intelligence review on a bi-weekly basis that highlights, but is not limited to, cyber crime, cyber terrorism, US and world cyber security policy and law, critical infrastructure protection, information warfare, cyber espionage, and the latest vulnerability news. This summary provides a high-level picture of the cyber security marketplace over the given time period while covering hot security topics affecting security decisions.

Verisign iDefense® Topical Research Report

Each Topical Research Report provides in-depth analysis of a specific security topic. Recent subjects include banking Trojans, an update of the Russian Business Network, IPv6, and vulnerability disclosure methodology.

Verisign iDefense® Global Threat Research Report

Verisign provides customers with in-depth research reports about issues relating to global threats. Each report will focus on a single country or region chosen by Verisign. Global Threat Research Reports are published and available in various report formats, including an in-depth and comprehensive report, mini country brief, and a one-page summary. To provide accurate and critical information, Verisign iDefense analysts spend weeks at a time performing in-country research at the source. Global Threat Research Reports are updated regularly to maintain accuracy and relevance.

Verisign iDefense® Focused Intelligence Report

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, 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™

VERISIGN IDEFENSE INTELLIGENCE SOLUTION PACKAGES								
VERISIGN IDEFENSE SECURITY INTELLIGENCE SERVICES	CORE	STANDARD	ENHANCED	COMPREHENSIVE	GLOBAL THREAT INTELLIGENCE	VULNERABILITY INTELLIGENCE	INCIDENT RESPONSE	FRAUD MITIGATION
Verisign iDefense® Public Vulnerability Reports	✓	✓	✓	✓		✓		
Verisign iDefense® Flash Reports	✓	✓	✓	✓		✓		
Verisign iDefense® Threat Reports	✓	✓	✓	✓		✓	✓	
Verisign iDefense® Exclusive Vulnerability Reports		✓	✓	✓		✓		
Verisign iDefense® Threat Briefings			✓	✓	✓			
Verisign iDefense® Weekly Threat Report			✓	✓	✓			
Verisign iDefense® Cyber Threat Brief		✓						
Verisign iDefense® Malicious Code Reports		✓	✓	✓		✓	✓	
Verisign iDefense® Malicious Code Summary Report			✓	✓	✓		✓	
Verisign iDefense® Vulnerability Summary Report			✓	✓	✓	✓		
Verisign iDefense® Patch Tuesday Report			✓	✓		✓		
Verisign iDefense® Global Threat Research Reports				✓	✓			
Verisign iDefense® Topical Research Reports			✓	✓	✓			
Verisign iDefense® Analyst Service			✓	✓	✓	✓	✓	✓
Verisign iDefense® Designated Analyst Service				✓				



VERISIGN™

VERISIGN IDEFENSE INTELLIGENCE SOLUTION PACKAGES								
VERISIGN IDEFENSE SECURITY INTELLIGENCE SERVICES	CORE	STANDARD	ENHANCED	COMPREHENSIVE	GLOBAL THREAT INTELLIGENCE	VULNERABILITY INTELLIGENCE	INCIDENT RESPONSE	FRAUD MITIGATION
Verisign iDefense® Rapid Response Service								
Verisign iDefense® Malcode Rapid Report Service								
Verisign iDefense® Artifact Analysis On-Demand Service							Optional	
Verisign iDefense® IP Reputation Service								
Phishing Shutdown Service								Optional
Malcode Shutdown Service								Optional
Verisign iDefense® Integration Service for QualysGuard® VM						Optional		

ABOUT VERISIGN® IDEFENSE® SECURITY INTELLIGENCE SERVICES

Verisign iDefense Security Intelligence Services gives information security executives access to accurate and actionable cyber intelligence related to vulnerabilities, malicious code, and global threats 24 hours a day, 7 days a week. Verisign iDefense in-depth analysis, insight, and

response recommendations help keep businesses and government organizations ahead of new and evolving threats and vulnerabilities.

LEARN MORE

For more information about Verisign iDefense Security Intelligence Services, please e-mail learnmore@verisigninc.com or visit us at www.verisigninc.com/idefense.

VerisignInc.com