



VERISIGN™

DATA SHEET

# VERISIGN® IDEFENSE® VULNERABILITY INTELLIGENCE SERVICES

THE EVER-GROWING COMPLEXITY OF ENTERPRISE IT ENVIRONMENTS CONTINUES TO PUSH THE LIMITS OF INTERNAL SECURITY TEAMS. SATISFYING THE REQUIREMENTS TO DEPLOY AND SUPPORT NEW IT ASSETS IS CHALLENGING ENOUGH WITHOUT HAVING TO MANAGE AN EVOLVING SET OF SECURITY WEAKNESSES WITHIN THOSE SYSTEMS.

---

Every day, enterprises discover vulnerabilities of varying severity in software and hardware systems, making vulnerability management a critical component of each enterprise's security policies and procedures. Several vulnerability management products and services have been introduced to the market, enabling more proactive detection and remediation of security vulnerabilities. This allows security teams to address weaknesses before malicious actors exploit them and to convert their security measures from purely defensive to proactive to best protect themselves. However, these weaknesses still create a significant burden on security teams to keep up with the ever-evolving universe of new and emerging threats. Many enterprises suffer from a lack of accurate, unbiased threat intelligence, making the process of vulnerability management, prioritization and remediation very difficult. The

costs and risks of poor vulnerability management include:

- Critical application and system downtime
- Erosion of available resources driven by redundant or unnecessary patches
- Lost productivity and overtime costs due to "fire drills" for out-of-cycle patches
- Increased vulnerability to serious threats due to poor intelligence about threat severity

Verisign® iDefense® Vulnerability Intelligence Services offers an essential ingredient for vulnerability management: timely, accurate and in-depth vulnerability research.

- Frost & Sullivan recently recognized Verisign iDefense as the leading provider of exclusive vulnerability research offering zero-day threat protection.

- Verisign iDefense analysts go deeper than the competition, monitoring threats throughout their lifecycles and alerting clients of where exactly such vulnerabilities exist, the potential effects of those vulnerabilities, mitigation strategies and workarounds
- Verisign iDefense research covers all critical applications, technologies and operating systems vital to Verisign iDefense customers and does so without bias

Verisign iDefense offers added value to the enterprise vulnerability management process through the integration of deep and analytical research with leading vulnerability and threat management tools. Verisign iDefense integration services improve in-house vulnerability management efforts by enabling:

- The replacement of manual processes of vulnerability



VERISIGN™

management with automated correlation of vulnerability intelligence, scan data and IT assets on the Verisign iDefense portal

- Vulnerability prioritization based on relevance, severity and business criticality
- Better decision making, resulting in faster and smarter remediation

### **ABOUT VERISIGN® IDENSE® 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@verisign.com](mailto:learnmore@verisign.com) or visit us at [www.verisigninc.com/idefense](http://www.verisigninc.com/idefense).

### **KEY BENEFITS**

**Global Perspective** The Verisign iDefense global intelligence network includes more than 600 vulnerability researchers in more than 46 countries. A dedicated cyber intelligence team conducts threat research in more than 20 spoken languages and ongoing field operations in suspect regions of the world, all providing insight into the cyber underground, undiscovered vulnerabilities and geopolitical threats.

**Security Monitoring and Risk Management** The Verisign iDefense Vulnerability Aggregation Team (VAT) monitors security events 24 hours a day, 7 days a week. The team captures, analyzes, and correlates these events in real time, providing primary and secondary analysis of new vulnerability exploits. Therefore, the team proactively identifies suspicious and malicious events, helping to mitigate an organization's potential for security risks.

**Threats in Context** Instead of a reactive and often expensive response to vulnerabilities or suspicious activity, Verisign can assess and advise clients of the most prudent course of action based on unique geographical and contextual needs of a client's business.

### **Protection against Zero-Day Vulnerabilities**

- On average, Verisign iDefense provides original vulnerability discoveries more than 100 days prior to vendors.
- On average, Verisign iDefense warned customers of Microsoft vulnerabilities 200 days before Microsoft warned their customers of vulnerabilities related to their products.
- Verisign iDefense has discovered more than 602 exclusive vulnerabilities over the past three years.

**Automated Correlation Drives Prioritization** Correlation of Verisign iDefense vulnerabilities, vulnerability scan data and IT asset information supports automated vulnerability prioritization based on severity, business criticality and relevance to the organization.

**Smarter and Faster Remediation Support** Integration between Verisign iDefense and leading vulnerability and threat management solutions helps security teams prioritize patch deployments and remediation efforts, particularly between full vulnerability scan cycles of their environments.

---

[VerisignInc.com](http://VerisignInc.com)