

TippingPoint Digital Vaccine® Service

IPS-Secured Networks

DATASHEET – Digital Vaccine



Digital Vaccine BY TippingPoint

The TippingPoint DV Labs team continually develops protection filters to address vulnerabilities, viruses, worms, Trojans, P2P, spyware, and other applications to incorporate them into Digital Vaccines. Digital Vaccines are packages of filters automatically delivered to customers on a regular weekly release schedule.

Key Features

Digital Vaccine Filters

- Signature
- Vulnerability
- Protocol Anomaly
- Traffic Anomaly

Automatic Security

- “Recommended Settings” for Filters
- Over 3,000 filters enabled by default in blocking mode, out of the box
- Automatic updates twice a week

The accuracy and timeliness of TippingPoint’s Digital Vaccine filters are directly related to the unsurpassed depth and experience of the DV Labs security researchers.

TippingPoint has built key relationships with vendors and organizations to get vulnerability information ahead of the public. In addition, TippingPoint’s DV Labs scours security mailing lists, monitors underground hacker chat rooms, uncovers emerging zero-day threats, and leverages an expansive honey pot network to determine the most critical vulnerabilities at any given time. In all situations, the team verifies and reproduces new vulnerability findings. The team looks closely at new vulnerabilities to determine additional potential attack vectors in a controlled security lab environment.

Consequently, Digital Vaccine packages are created for vulnerabilities to protect against all potential attack permutations rather than specific exploits. Digital Vaccines are delivered to customers twice a week, or immediately when critical vulnerabilities emerge, and can be deployed automatically with no user interaction required.

TippingPoint products provide protection across all filter types. Filters fall into four distinct categories:

Signature Filters protect against exploit attacks such as viruses and Trojans. These filters

assume knowledge of a given attack and are able to detect them in their executable form.

Vulnerability Filters protect vulnerabilities in operating systems and applications, and are not exploit specific. These filters behave like a network-based virtual software patch to protect downstream hosts from network-based attacks on unpatched vulnerabilities.

Protocol Anomaly Filters are rules that can be specified to detect conditions that violate a particular application implementation flaw (e.g., buffer overflow application anomaly) or a protocol specification (e.g., RFC anomaly).

Traffic Anomaly Filters are used to detect changes in traffic patterns. These filters are adaptive and learn about “normal” traffic patterns for the particular environment the TippingPoint IPS is placed in. Once traffic is baselined, these filters will detect statistical anomalies based on tunable thresholds. Traffic anomaly filters are effective against distributed denial of service attacks, unknown worms, rogue applications and other zero-day exploits. Of particular importance is the IPS’s ability to rate-shape traffic flows based on application types, protocols or IP addresses.

TippingPoint has demonstrated in third-party testing the best vulnerability coverage as compared to any and all competitors. In NSS Group testing, TippingPoint was the only vendor

TippingPoint

to get perfect 100% scores for attack detection, evasions, and all other security categories measured.

World-Class Vulnerability Analysis and Research

TippingPoint's DV Labs team is a premier security research organization for vulnerability analysis and discovery. Recognized in 2007 as the fastest growing discoverer of new vulnerabilities and the leader in the discovery of high-severity and Microsoft vulnerabilities by Frost & Sullivan¹, the team consists of industry recognized security researchers that apply their cutting-edge engineering, reverse engineering and analysis talents in their daily operations. The by-product of these efforts fuels the creation of vulnerability filters that are automatically delivered to TippingPoint customers' intrusion prevention systems through the Digital Vaccine® service. The DV Labs Web site (dvlabs.tippingpoint.com) serves as a portal into the research laboratories headquartered in Austin, Texas. The portal includes upcoming and published advisories as well as blogs, RSS feeds and other security resources.

TippingPoint is also the primary author of the SANS Institute @RISK e-mail newsletter, which contains the latest information on new and existing network security vulnerabilities. The newsletter summarizes newly discovered vulnerabilities, details their impact, and informs of actions large organizations have taken to protect their users. With a subscriber base of nearly 300,000 network security professionals worldwide, the newsletter is delivered every Thursday and is available for free at: <http://www.sans.org/newsletters/risk/>.

Rapid Response to Zero-Day Threats

TippingPoint's response to zero-day threats is unparalleled in the industry. Rapid response

is crucial as the window of time shrinks for exploits to emerge.

In October of 2004, Microsoft released the greatest number of security advisories in its history. TippingPoint published a Digital Vaccine to customers within 12 hours that provided protection coverage for the new critical issues. Exploits emerged for these new issues only days later.

On December 24, 2004, two new zero-day Microsoft vulnerabilities (Internet Explorer HTML Help ActiveX Code Execution and Loadimage DLL Buffer Overflow) were disclosed on the Internet. During the holiday season, TippingPoint IPS systems were automatically updated within hours with the latest protection filter against these new Windows vulnerabilities. The very same filters protected customers against the Phel Trojan that emerged one day later and widely exploited one of these new vulnerabilities.

Digital Vaccine Delivery

The Security Management System (SMS) system monitors the Threat Management Center continuously for Digital Vaccine updates. If an update is available, the system responds with a message prompt or automatically downloads and activates the update according to configured settings.

Advanced Policy Definition

Included with the TippingPoint SMS is an automated response system called Quarantine Protection that allows users to specify an action in response to a security event. This can range from directing a user to a self-remediation site, to generating a trouble ticket, or if the event is severe enough, moving them to a secure VLAN or removal from the network.

¹ Frost and Sullivan press release, "Frost & Sullivan Recognizes TippingPoint's Valuable Contribution to Vulnerability Research," 11 May 2007 *Frost & Sullivan*. <http://www.frost.com/prod/servelet/press-release.pag?docid=98552761&ctxst=FcmCtx1&ctxht=FcmCtx2&ctxhl=FcmCtx3&ctxixpLink=FcmCtx3&ctxixpLabel=FcmCtx4>

Corporate Headquarters:

7501B North Capital of Texas Hwy.
Austin, Texas 78731 USA
+1 512 681 8000
+1 888 TRUE IPS

European Headquarters:

World Trade Centre Amsterdam
Zuidplein 36, H-Toren
1077XV Amsterdam
The Netherlands
+31 20 799 7629

Asia Pacific Headquarters:

30, Cecil Street, #18-01
Prudential Tower
Singapore 049712
+65 6213 5999