

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. The TippingPoint Digital Vaccines are packages of filters automatically delivered to customers on a regular weekly release schedule that are at the heart of all TippingPoint IPS solutions. When it comes to filter development, TippingPoint is an industry leader in the three most important filter metrics: (1) filter accuracy, (2) breadth of filter coverage, and (3) speed and timeliness of filter releases.

Digital Vaccine Filters

- Signature
- Vulnerability
- Protocol Anomaly
- Traffic Anomaly

Automatic Security

- “Recommended Settings” for Filters
- Over 3,000 security filters available, with 1,000 filters enabled by default in blocking mode out of the box
- Automatic updates twice a week

“Thanks to the Digital Vaccine service, we have defenses against the most current threats, without any IT intervention. This is precisely the robust and economical security we wanted.”
NCSOFT

“The Digital Vaccine service is fantastic. By blocking threats from entering our network before any damage occurs, the update service is the reason why Vejen’s network has not been infected once since the TippingPoint IPS was installed. Without it, we would almost assuredly be infected on a constant basis.”
Vejen Kommune

“A superior product combined with TippingPoint’s Digital Vaccine update service made this an easy choice. Out of all products tested, no signature/rule update service even compared to Digital Vaccine.”
MaximumASP

The accuracy, breath of coverage and timeliness of TippingPoint’s Digital Vaccine filters are directly related to the unsurpassed depth and experience of the TippingPoint DV Labs security research team.

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.

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

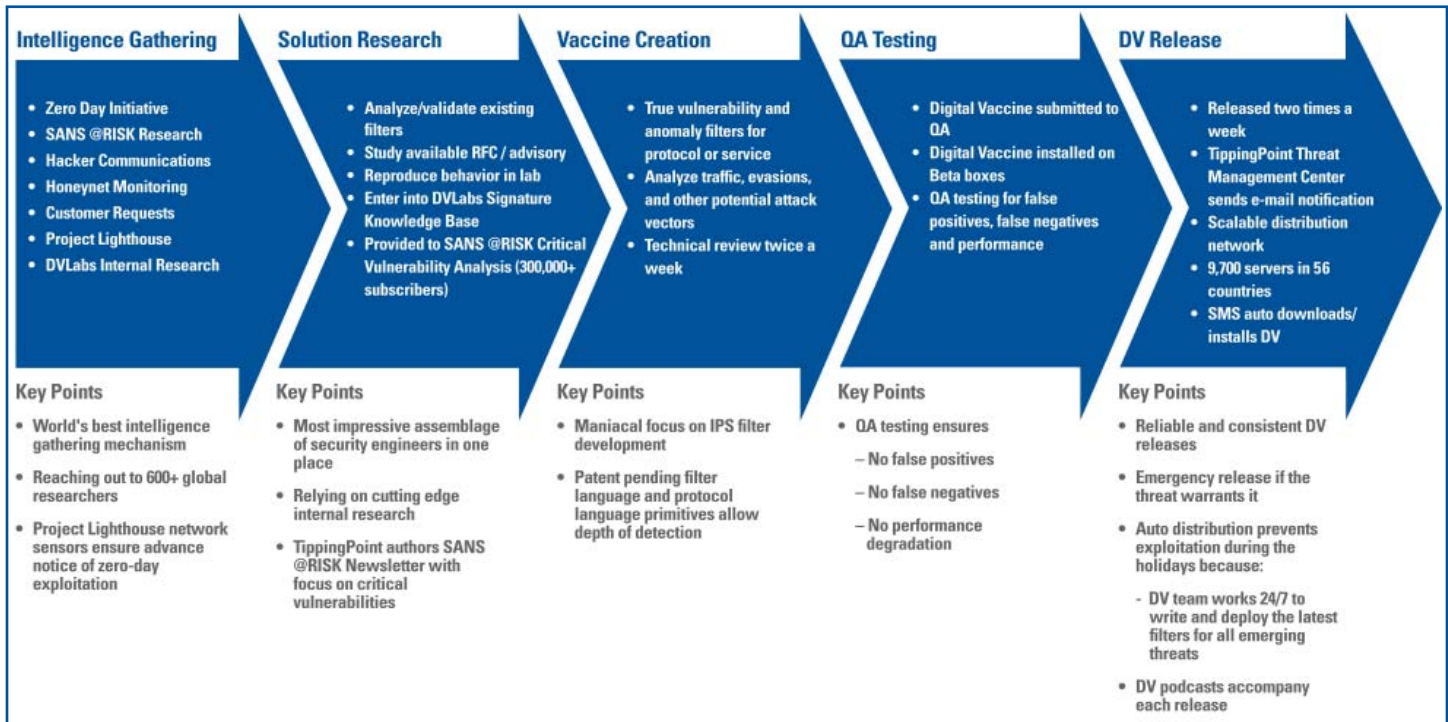
as the fastest growing discoverer of new vulnerabilities and the leader in the discovery of high-severity and Microsoft vulnerabilities by Frost & Sullivan¹, the team consists of industry recognized security researchers that apply their cutting-edge engineering, reverse engineering and analysis talents 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

TippingPoint®



is crucial as the window of time shrinks for exploits to emerge. This is specifically why TippingPoint created and continues to manage the Zero Day Initiative (www.zerodayinitiative.com). With this program, TippingPoint receives vulnerability research from hundreds of benevolent researchers worldwide. Once this research is received and validated, TippingPoint notifies the affected vendor and releases Digital Vaccine filters to cover the vulnerabilities providing customers protection to vulnerabilities that have not even been publicly disclosed.

Digital Vaccine Filters

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 Labs group testing, TippingPoint was the only vendor to get perfect 100% scores for attack detection, evasions, and all other security categories measured.

Digital Vaccine Delivery

The TippingPoint 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.

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&ctxpLink=FcmCtx3&ctxpLabel=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

TippingPoint®

www.tippingpoint.com