DATASHEET

Trend Micro

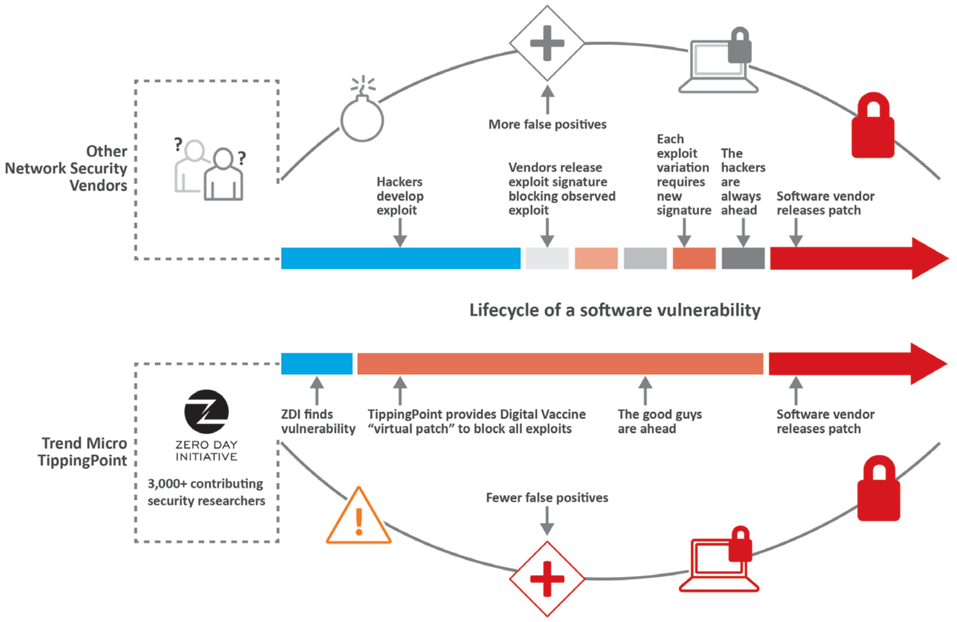
TIPPINGPOINT® DIGITAL VACCINE® LABS THREAT INTELLIGENCE OFFERINGS

Network security is only as effective as the security and threat intelligence that powers it. Trend Micro TippingPoint Digital Vaccine Labs (DVLabs) provides cutting-edge threat analysis and security filters that cover an entire vulnerability to protect against all potential attack permutations, not just specific exploits. TippingPoint is powered by XGen™ security, and offers ongoing threat prevention against emerging vulnerabilities through the Digital Vaccine service.

Digital Vaccine filters help you gain control of your organization's patch management life cycle by providing pre-emptive coverage between the discovery of a vulnerability and the availability of a patch, as well as added protection for legacy, out-of-support software. Digital Vaccine packages are delivered to customers weekly, or immediately when critical vulnerabilities emerge, and can be deployed automatically with no user interaction required. In addition to weekly Digital Vaccine packages, DVLabs offers several products including ThreatDV and DVToolkit.

DIGITAL VACCINE PACKAGE HIGHLIGHTS

- Weekly subscription service of updated vulnerability filters
- Security coverage filters are written to cover the entire footprint of a vulnerability and are not exploit-specific
- Filters are not prone to false positives because of the rigorous QA process and DVLabs research experience
- The DV package includes zero-day protection to customers via filters developed from Zero Day Initiative (ZDI) vulnerability information
- Emergency Digital Vaccine updates may be provided on a prioritized basis as critical vulnerabilities are identified
- DVLabs team provides information on every filter, as well as information on attack events occurring globally via the TippingPoint ThreatLinQ website, which can be used to fine-tune configurations for more comprehensive protection


More false positives
Other Network Security Vendors
Hackers develop exploit
Vendors release exploit signature blocking observed exploit
Each exploit variation requires new signature
The hackers are always ahead
Software vendor releases patch
Lifecycle of a software vulnerability
ZDI finds vulnerability
TippingPoint provides Digital Vaccine "virtual patch" to block all exploits
The good guys are ahead
Software vendor releases patch
Trend Micro TippingPoint
ZERO DAY INITIATIVE
3,000+ contributing security researchers
Fewer false positives

Powered by XGen™ security

Trend Micro TippingPoint products and solutions are powered by XGen™ security, a smart, optimized and connected security approach

STOP MALWARE AND PROTECT SENSITIVE DATA WITH THREATDV

Threat Digital Vaccine (ThreatDV) is a subscription service that enables organizations to prevent and disrupt malware activity. The combination of reputation feeds and malware filters allow customers to leverage ThreatDV to protect their sensitive data and optimize network performance.

The malware filters are designed to detect infiltration, exfiltration, phone-home, command and control (C&C), and mobile traffic. The malware filters are delivered weekly through an Auxiliary Digital Vaccine (DV) package to keep customers protected from the latest advanced threats.

ThreatDV also includes an intelligence feed that is a global database of malicious or undesirable IPv4, IPv6, and Domain Name System (DNS) names. The reputation database collects data from the TippingPoint ThreatLinQ global intelligence network, DVLabs malware repository and honeypot network, third-party commercial sources, and open source black lists. A threat score of 1 to 100 is assigned to each entry based on DVLabs analysis of the activity, source, category, and threat. This intelligence feed is updated multiple times a day.

THREATDV HIGHLIGHTS

- Block drive-by downloads of malware from known malware depots
- Disrupt malware activity and prevent its goals such as ransomware, data exfiltration, espionage, click fraud, etc.
- Detect C&C activity such as configuration download, version checking, remote access, instructions, etc.
- Intercept targeted phishing attacks and prevent them from infiltrating your enterprise
- Block zero-day exploits from known attackers before signatures are available
- Block sites that use fast-fluxing IP addresses by blocking DNS host names
- Detect DNS requests from malware-infected hosts attempting to contact their C&C hosts using domain generation algorithms (DGAs)
- Detect and mitigate exploit kits in real-time with filters focused on statistical analysis using machine learning primitives

> **"[ThreatDV] is the single greatest security and performance benefit ever implemented across any security control to date."**
>
> - Sr. Network Security Engineer,
> Americas Financial Services Institution

CREATE CUSTOM FILTERS WITH TIPPINGPOINT DVTOOLKIT

Digital Vaccine Toolkit (DVToolkit) is a downloadable application from the TippingPoint Threat Management Center that enables TippingPoint customers to create custom filters to extend threat coverage. Using analysis and development techniques from DVLabs, users can quickly develop and implement filters to block events unique to their network. DVToolkit also supports the use of regular expressions, which are frequently used in the industry when crafting customer filters. DVToolkit enables customers to expedite time to market for a particular filter if they are under constant attack. DVToolkit key benefits include:

- Broad protection with custom filters for proprietary or user-developed applications
- Import open source rules (e.g. Snort signatures); extended support for Snort primitives, options, and modifiers
- Define filter triggers or support triggerless filters
- Create custom filters in IPv4 and IPv6 environments
- Single point of deployment and management for custom-developed and Digital Vaccine filters

THREATLINQ

The TippingPoint ThreatLinQ security intelligence portal gives you an effective way to evaluate the changing threat landscape and connect the intelligence you gather to specific policy changes. Your team can proactively optimize network security and reduce business risks thanks to full, real-time analysis. ThreatLinQ is available to all TippingPoint customers through the TippingPoint Threat Management Center at **http://threatlinq.tippingpoint.com**.

ZERO DAY INITIATIVE

TippingPoint launched the Zero Day Initiative (ZDI) to reward security researchers for responsibly disclosing vulnerabilities.

- Largest vendor-agnostic bug bounty program
- Over a 10-year track record of securing the ecosystem of critical enterprise-class vulnerabilities
- Unique insight into the latest threats
- Strong partnership with affected vendors resulting in more timely patching
- For more information, **visit www.zerodayinitiative.com**

PREREQUISITES

Digital Vaccine packages, ThreatDV, and DVToolkit require a TippingPoint next-generation network security device and a TippingPoint Security Management System (SMS) with access to the Trend Micro TippingPoint Threat Management Center (TMC) web site. ThreatDV requires a separate subscription to be enabled on your TippingPoint network security device. The TippingPoint SMS is optional for downloading DV packages and for using DVToolkit. It is only required for downloading and distributing ThreatDV.

TREND MICRO™

Securing Your Journey to the Cloud