Trend Micro™

TippingPoint™ Threat Intelligence Offerings

Network security is only as effective as the threat intelligence that powers it. The Trend Micro™ Digital Vaccine™ (DV) service includes security filters that cover an entire vulnerability, protecting against all potential attack permutations, not just specific exploits.

DV filters help you gain control of your organization's patch management lifecycle by providing coverage between the discovery of a vulnerability and the availability of a patch, as well as added protection for legacy, out-of-support software. DV filter packages are delivered weekly, or immediately when critical vulnerabilities emerge, and can be deployed automatically with no user interaction required.

DIGITAL VACCINE SERVICE HIGHLIGHTS

- Weekly distribution of threat intelligence through DV filters are written to cover the entire footprint of a vulnerability, not just specific exploits, resulting in minimal false positives.
- Pre-emptive protection for undisclosed and zero-day vulnerabilities through exclusive access to vulnerability information from the Trend Micro™ Zero Day Initiative™ (ZDI) bug bounty program.
- Emergency DV filter distributions that may be provided on a prioritized basis as critical vulnerabilities are identified.
- Detailed information on every DV filter, as well as information on attack events occurring globally via the ThreatLinQ website; which can be used to fine-tune configurations for more comprehensive protection

ZERO DAY INITIATIVE

1,604
vulnerabilities published in 2021

9,000+
vulnerabilities published since inception

Over US $30 million
awarded since inception

102 days
average preemptive protection for Trend Micro™ TippingPoint™ customers ahead of vendor patch in 2021

A top provider
of vulnerabilities to ICS-CERT, Adobe, and Microsoft

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 available to customers that enables the prevention and disruption of malware activity. The combination of reputation feeds and malware filters gives customers added protection for their sensitive data and helps 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 (Auxiliary DV) package to keep customers protected from the latest advanced threats.

ThreatDV also includes an intelligence feed that works as a global database of malicious or undesirable IPv4, IPv6, and Domain

Name System (DNS) names. The reputation database collects data from the Trend Micro™ Smart Protection Network™, the ThreatLinQ global intelligence network, an internal malware repository and honeypot network, third-party commercial

sources, and open source blocklists. A threat score of 1 to 100 is assigned to each entry based on analysis of the activity, source, category, and threat. This feed is updated multiple times a day.

In addition, ThreatDV includes a URL reputation feed. Websites on the list are compiled based on their reputation rating from various sources. Targeted websites can come from the ThreatDV feed, a user-defined list of sites or both. In addition, the integration of TippingPoint+ and Trend Micro™ Deep Discovery™ solutions provides seamless detection and enforcement of detected URL suspicious objects.

ThreatDV Highlights

- Blocks drive-by downloads of malware from known malware depots.
- Disrupts malware activity and prevents its goals such as ransomware, data exfiltration, espionage, click fraud, etc.
- Detects C&C activity such as configuration download, version checking, remote access, instructions, etc.
- Intercepts targeted phishing attacks and prevents them from infiltrating your enterprise.
- Detects and mitigates exploit kits in real time with filters focused on statistical analysis using machine learning primitives.
- Prevents users from accessing inappropriate or high-security-risk sites.
- Blocks sites that use fast-fluxing IP addresses by blocking DNS host names.
- Detects DNS requests from malware-infected hosts attempting to contact their C&C hosts using domain generation algorithms (DGAs).

> [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 an application that enables you to create custom DV filters to extend your threat coverage. Using analysis and development techniques leveraged in DV filters, you can quickly develop and implement custom DV filters to block events unique to your network environment. DVToolkit supports the use of regular expressions frequently used in the industry and enables customers to expedite time to market for a particular filter if they are under constant attack.

DVToolkit Key Benefits

- Provides broad protection with custom filters for proprietary or user-developed applications.
- Supports the import of open source rules (for example, Snort signatures); with extended support for Snort primitives, options, and modifiers.
- Enables customers to define filter triggers or support triggerless filters.
- Allows for the creation of custom filters in IPv4 and IPv6 environments.
- Provides centralized management and single point of deployment for both 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**.

Prerequisites

Digital Vaccine packages, ThreatDV, and DVToolkit require a TippingPoint network security device and a TippingPoint Security Management System (SMS) with account access to the Trend Micro TippingPoint Threat Management Center (TMC) website. 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, but is required for downloading and distributing ThreatDV.