Trellix

DATA SHEET

Trellix® Intelligent Virtual Execution

Scan objects for threats at any point in your workflow

Highlights

- Detects known and unknown malware
- Integrates with all major cloud storage solutions and many web applications
- Analyzes threats in multiple operating systems, including Windows, Mac, and Linux
- Compiles in-depth analysis details, including MITRE ATT&CK mapping, extracted objects, IOCs, and more
- Supports plug-ins for browsers and cloud storage
- Delivers contextual analysis of detected malware in JSON format

To accurately detect and stop dynamic, never-before-seen exploits and malware, organizations need intelligence-led threat detection that evolves at the speed of the threat space. They also need contextual insight to accelerate resolution of security incidents with concrete evidence, actionable intelligence, and frictionless workflow integration.

IVX is a signature-less, dynamic analysis engine that captures and confirms zero-day, and targeted APT attacks. IVX identifies attacks that evade traditional signature-based defenses by detonating suspicious files, web objects, URLs, and email attachments within a proprietary hypervisor instrumented for over 200 potential simultaneous executions. IVX accelerates incident response by enabling analysts to visualize how malware is behaving within the virtual image and securely interact with malware to test effectiveness of countermeasures.

Available on prem or as a cloud-native service Trellix IVX delivers proven, flexible analysis capabilities wherever you need to quickly inspect and verdict potentially malicious content. SOC analysts can manually submit objects for inspection and insight. Or seamlessly integrate IVX with enterprise applications— built or bought—for continuous and frictionless protection.

How Intelligent Virtual Execution works

Trellix Intelligent Virtual Execution stops incursion by revealing never-before-seen exploits and malware.

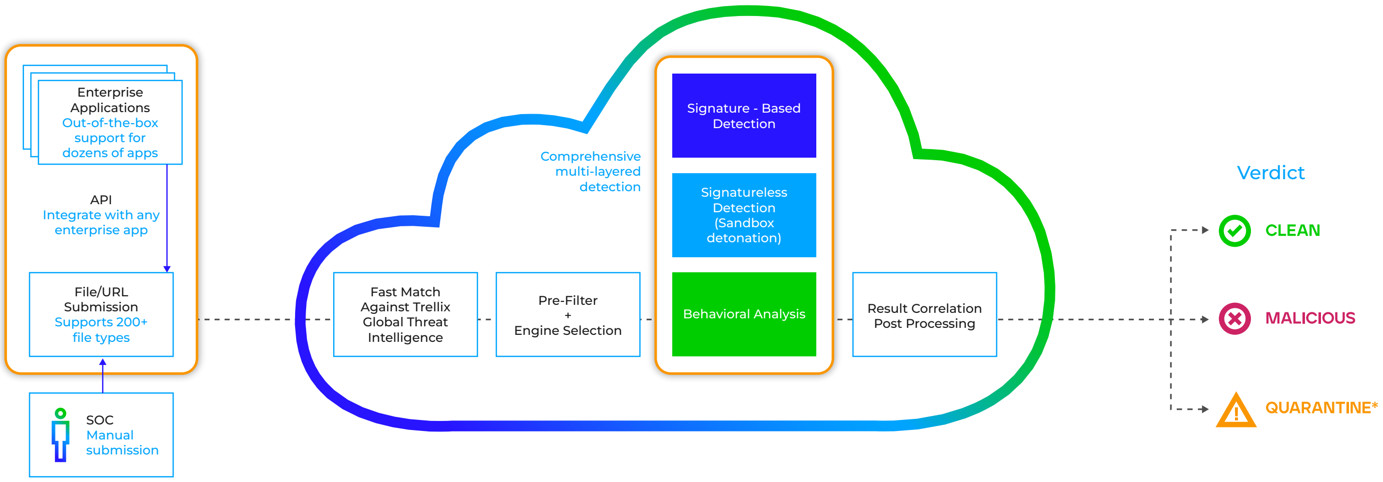
Using the same proven detection methodologies that power many of our Trellix products, the IVX engine captures and confirms zero-day, multi-flow and other evasive attacks by detonating suspicious files, web objects, URLs, and email attachments.

Intelligent Virtual Execution begins by comparing your submission to threat actors' latest known tactics and other potentially malicious behaviors using Trellix Global Threat Intelligence gleaned from over 40,000 Trellix customers and partners worldwide.

IVX then uses statistical analysis, artificial intelligence, and machine learning to conduct one-to-many analysis. At the time of analysis IVX decides how an object is to be analyzed and composes multiple unique execution environments in real time. IVX conducts over 200 simultaneous executions, covering multiple operating systems, service packs, applications, and application versions.

Unlike detection solutions that focus on a single attack object, Trellix IVX performs multi-flow analysis to break down and fully understand the full context of a multistage attack. Stateful attack analysis is critical to trigger analysis of the entire attack lifecycle, from initial exploit to data exfiltration. Trellix also determines the possibility of secondary or combinatory effects across multiple phases of the attack lifecycle to discover never-before-seen exploits and malware.

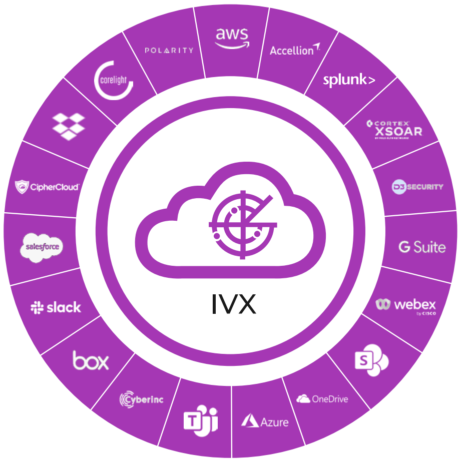
If the object is malicious, an alert is sent so you'll know that object needs attention.


Enterprise Applications
Out-of-the-box support for dozens of apps
API
Integrate with any enterprise app
File/URL Submission
Supports 200+ file types
SOC
Manual submission
Comprehensive multi-layered detection
Fast Match Against Trellix Global Threat Intelligence
Pre-Filter + Engine Selection
Signature - Based Detection
Signatureless Detection (Sandbox detonation)
Behavioral Analysis
Result Correlation Post Processing
Verdict
CLEAN
MALICIOUS
QUARANTINE*

Key technology features

- **Actively analyzes unknown code and suspicious web objects** – Objects are executed against a range of browsers, plug-ins, applications, and operating environments. The signatureless IVX engine identifies the use of zero-day exploits, confirms a Web attack is underway, and blocks callbacks and subsequent malware downloads over multiple protocols.
- **Detonates all email attachments within virtual environments** – All attachments can be safely and accurately analyzed to identify zero-day exploits. Beyond signature- and reputation- based systems, the IVX engine can detect if previously legitimate files have been weaponized and sent via spear phishing email to penetrate enterprise defenses.

- **Analyzes for weaponized files on network file shares** – The IVX engine can be used to scan CIFS-compatible file shares to detect and stop advanced targeted attacks embedded within weaponized Microsoft Office files, images, PDFs, Flash, or ZIP/RAR/TNEF archives.
- **Inspect URLs embedded** in emails, MS 365 documents, PDF, and archive files, files downloaded through URLs (including FTP links), obfuscated, spoofed, shortened and dynamically redirected URLs, and credential-phishing and typosquatting URLs.
- **Proprietary virtualization technology** – The IVX engine analyzes and confirms true, zero-day malware, such as Trojans, targeted attacks, bots, VM-aware malware, and advanced persistent threats.
- **Multi-stage inspection and blocking engine** – Verdict known and zero-day attacks while simultaneously eliminating false positives. The multi-stage inspection process unifies virtualization and network security to accurately block advanced malware that are used to penetrate networks and steal resources and sensitive data.
- **Custom-built hypervisor** with built-in countermeasures designed specifically for malware analysis. This hypervisor enables peak performance and the ability to detect sandbox aware and evasion tactics used by many sophisticated malware objects.



Accelerate investigation and response

Available on prem or as a cloud-native service, Intelligent Virtual Execution rapidly scans submitted content to identify malware.

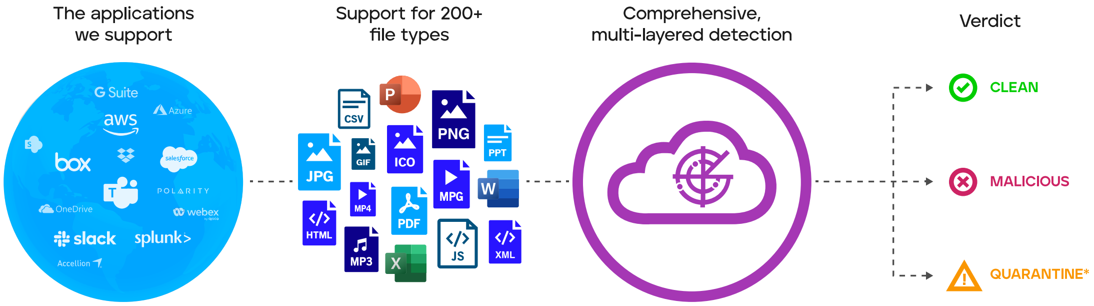
You can easily configure access to Intelligent Virtual Execution through an API for easy integration into your security operations center workflow. The applications we support The file types we support Comprehensive multi-layered detection Verdict Detection as a Service IVX

In addition to receiving a verdict, you also get supporting contextual detail, such as file, registry, process, and network changes, as well as MITRE ATT&CK mapping and other relevant findings from continually updated Trellix Global Threat Intelligence.

Protect collaboration platforms and enterprise applications

Intelligent Virtual Execution integrates with cloud services like AWS and Azure, collaboration platforms such as Slack, MS 365 and Google Workspace and cloud storage tools like Dropbox, Box, OneDrive.

It also integrates with many enterprise applications such as Salesforce, Webex, Slack, Microsoft Teams, and much more. You can easily integrate with applications that don't already have a plug-in through our easy-to-use API.



Flexible deployment options

Our cloud-native Intelligent Virtual Execution is available through Trellix channels or directly through the AWS Marketplace.

On prem options include:

Table 1. Trellix Virtual Execution models on AWS

Model	Throughput	vCPU	Memory	Network Interfaces	AWS Instance Type
Trellix VX Bare-Metal	14 Gbps (similar to VX 12550)	96	192 GB	One management port, 4 cluster ports	C5.metal

Table 2. Trellix Virtual Execution smart grid specifications

	VX 5600	VX 12600
OS support	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows
Performance	11 subs/min	85 sub/min
High availability	N+1	N+1
Management ports (rear panel)	(1) 10/100/1000BASE-T Port	1x 1G/10G Base-T
Cluster Ports (rear panel)	(3) 10/100/1000BASE-T Ports	1x 1G/10G Base-T 4x 1G/10G SFP+
IPMI Port (rear panel)	Included	Included

Table 2. Trellix Virtual Execution smart grid specifications (continued)

	VX 5600	VX 12600
Front LCD & keypad	Not available	Not available
VGA ports	Included	Included
USB ports (rear panel)	2 X USB 2.0 , 2 X USB 3.2	2x USB 3.1 ports
Serial port (rear panel)	115,200 bps, no parity, 8 bits, 1 stop bit	115,200 bps, no parity, 8 bits, 1 stop bit
Drive capacity	(2) 4TB SAS SED, RAID 1	4x 4TB 3.5 SAS3 HDD, RAID10, hot swappable, FRU
Enclosure	1 RU, fits 19-inch Rack	2RU, fits 19 inch rack
Chassis dimension WxDxH	17.2 (437 mm) X 19.98 (507 mm) X 1.7 (43 mm)	19in x 26 x 3.5 in (482.6 x 660.4 x 89 mm)
DC power supply	Not available	Not available
AC power supply	Redundant (1+1), FRU, 400W with Input 100-240VAC / 6.0-3.0A 200-240VDC / 3.4- 3.2A, 50-60 Hz IEC60320- C14 inlet	Redundant (1+1),FRU,1000W/1200W with Input 100-127/200 - 240Vac, 15-12A/8.5- 7A, 50-60 Hz IEC60320-C14 inlet
Power consumption maximum (watts)	300 watts	948 watts
Thermal dissipation maximum (BTU/h)	1024 BTU/h	3232 BTU/h
MTBF (h)	33982	30863
Appliance alone / as shipped weight lb. (kg)	24 lbs (10.9 kg) / 37 lbs (16.8 kg)	44 lbs (20 kg) / 70 lbs (31.8 kg)
Security certification	FIPS 140-2 Level 1 (pending) CC NDcPP v2.2e (pending)	FIPS 140-2 Level 1, CC NDcPP v2.2e (pending)
Regulatory compliance safety	EN IEC 62368-1:2018+A11:2020	CAN/CSA 22.2 No. 62368 UL 62368 IEC 62368, EN 62368 BS EN 62368
Regulatory compliance EMC	EN 55032:2015/A11:2020, EN 55035:2017/A11:2020, EN 61000-3-2:2014, EN 61000-3-3:2013	FCC Part 15 Class-A, CE (Class-A) CNS 13438 CISPR 32 VCCI-CISPR32 EN 55035 EN 55032 EN 61000 ICES-003 KN 32, KN 35
Environmental compliance	RoHS: Directive 2011/65/EU	RoHS REACH
Operating temperature	5°C - 35°C (41°F - 95°F)	10–35°C (50–95°F)
Non-operating temperature	-40°C - 70°C (-40°F - 158°F)	-40–70°C (-40–158°F)
Operating relative humidity	8% - 90% (non-condensing)	8%–90% non-condensing
Non-operating relative humidity	5% - 95% (non-condensing)	5%–95% non-condensing
Operating altitude	1,524 m (5,000 ft)	1,524 m (5,000 ft)

Table 3. Trellix Virtual Execution models on VMware and Nutanix

Model	Throughput	Disk	vCPU	Memory	Network Interfaces	VM Number	VM Instance Type
IVX-VM300	3 subs/min 4320 files/day	1 TB - Thick Provisioning	16	32 GB	1 management port 4 cluster ports	16	VMware ESXi Nutanix

Copyright © 2024 Musarubra US LLC