Trend Vision One™- XDR for Endpoints

Detect and respond to threats faster with leading EDR and XDR

Endpoints are some of the most vulnerable points in your network. With ransomware and malware attacks becoming more frequent and aggressive, you need an endpoint detection and response (EDR) system in place. This enables you to pinpoint and investigate possible threats and investigate them is integral to organizations of every size.

Trend Vision One - XDR for Endpoints provides a complete set of EDR capabilities and mitigates threats. It continuously scans for suspicious behavior and alerts your security team to any possible threats that need to be neutralized. XDR for Endpoints allows you to monitor endpoints, servers, workloads, and host access points constantly, while perpetually searching for activities that could jeopardize your environment.

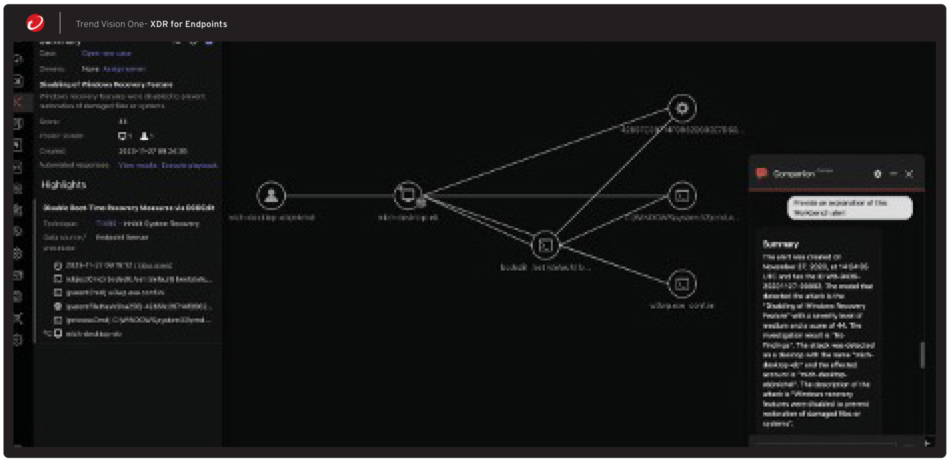
XDR for Endpoints is part of Trend Vision One™, our comprehensive platform that merges multiple security functions into a single console. It leverages the broadest set of native EDR and XDR sensors in the cybersecurity market to provide your team with activity telemetry—not just detection data—across security layers for centralized visibility, richer context, and a deepened understanding. Trend Vision One supports your diverse hybrid IT environments, helps in automating and orchestrating workflows, and delivers expert cybersecurity services, so you can stop adversaries faster and take control of your cyber risks.

Complete endpoint visibility

Receive continuous and comprehensive oversight of all your endpoint processes. Allow your security team to focus on issues in real time and observe any commands or processes that may be in use on your endpoint.

XDR for Endpoints provides you with the following information:

- User accounts that have logged in directly or through remote access
- Any changes made to ASP keys, executables, and other usage of administrative tools
- A list of process executions
- Records file creation, including .ZIP and .RAR files
- Usage of removable media, such as USB drives
- All local and external addresses that the host has connected to and vice-versa



Real XDR results

According to Enterprise Strategy Group (ESG), organizations with XDR for Endpoints:

- Are 2.2x more likely to detect an attack
- Decrease security spend by 79%
- Accelerate detection and response time by 70%
- Reduce dwell times by 65%
- Lower threat events by 55% and repeat attacks by 60%
- Speed up threat hunting and investigation by 54%
- Minimize alert overload by 99%

Proven Leadership

Trend is a Leader in Gartner Magic Quadrant for EPP since 2002, 19 times in a row

Named a Leader in The Forrester Wave™: Endpoint Security, Q4 2023 - with the highest score in the strategy category

Advantages

Accelerate investigations and respond faster with superior analytics

Real-time detections: Receive real- time alerts about unexpected activity or potential attempts to infect your endpoints with malware or ransomware.

High confidence alerts: Detections have context, correlation, and supporting threat intelligence, which reduces abundant, un-prioritized or irrelevant alerts and false positives.

Accelerate investigations: Reduce the time it takes to detect, correlate, contain, and respond to threats, minimizing the severity and scope of impact mean time to detect (MTTD), mean time to contain (MTTC), and mean time to respond (MTTR).

Respond faster: Automate and orchestrate responses across multiple endpoints or sensor types using templated and custom security playbooks.

Superior analytics: Harness a market- leading range of coverage from native sensors which, combined with third-party data inputs, feeds Trend XDR analytics and detection models. This provides more effective analytics than can be achieved via APIs to a third-party product.

Built on Trend Vision One

With XDR for Endpoints you can:

Detect threats earlier

Improve your team's visibility and reduce silos to unearth threats which evade detection by hiding in between security silos amid disconnected solution alerts.

Understand more with greater context XDR collects and correlates deep activity data for one or more vectors including email, endpoints, servers, cloud workloads, and networks. This enables a level of hunting and investigation analysis that is difficult or impossible to achieve otherwise.

Prioritize your response

By knowing the extent of an attack and its severity, you can determine which threat requires immediate response and which threats may be able to wait.

Play out attacks

With the click of a button, you can watch the entire attack play out chronologically from the initial infection point to lateral spread across the network. See every movement or scale down to view only what happened in a given time window such as this morning or over a weekend.

Take advantage of a broad integration ecosystem

With a growing portfolio of open APIs and third-party systems, XDR for Endpoints fits within a broad range of ecosystems and security operations workflows. Leverage meaningful data for infrastructure to further enrich and validate EDR and XDR capabilities.

Respond completely

One console allows you to investigate and quickly visualize the entire chain of events across your security layers. Enacting embedded response options across multiple security layers enables your security teams to prioritize, automate, and accelerate

EDR and XDR applications

Detection model management	Receive alerts based on the matched detection models and sends the alerts to Workbench.
Workbench	View, investigate, and respond to alerts and incidents in your environment.
Search app	Construct powerful query strings to pinpoint the data or objects in your environment that you want to examine.
Observed attack techniques	Displays the individual events detected in your environment that may trigger an alert and any related MITRE information.
Targeted attack detection	Review attack exposure in your environment and follow steps to mitigate or prevent attacks.
Forensics	Respond quickly to security incidents, conduct compromise assessments, threat hunting and monitoring.
Managed services	Augment your team with the expertly managed detection and response service.
Trend Companion	Analyze, investigate, and respond to incidents and alerts using the power of generative AI.
Dashboards and reports	Generate, schedule, and view reports based on security data within your environment.

Relieve constrained resources with Trend Micro™ Managed XDR

Managed XDR augments your team with Trend threat experts, giving you 24/7 full threat analysis, threat hunting and remediation capabilities, and response action plans.

Customers with Managed XDR get access to:

- **Expert threat identification and hunting: Uncover complex targeted threats using cutting-edge techniques, enriched by threats experts leveraging deep threat intelligence**
- **24/7 monitoring and detection: Proactive sweeping of endpoint, server, network, and email with continuous alert monitoring, correlation and prioritization using automation and analytics**
- **Rapid investigation and mitigation: Receive comprehensive analysis and detailed response plans with remote response actions through Trend solutions**

Customize your endpoint protection

You can install the agent program on any supported operating system alongside your existing security solutions.

Microsoft Windows Desktop

Platform	Editions	Processor	Memory	Disk space
Windows 8.1 (32/64-bit) Windows 10 (32/64-bit) November 2021 Update (21H2) Windows 11 (64-bit) October 2021 Release (21H2)	• Enterprise • Education • Pro • Home	2 CPU cores	512 MB	3 GB minimum

MacOS

Platform	Disk space
MacOS Catalina (10.15) and later	• 500 MB minimum

Linux

Platform	Memory	Disk space
AlmaLinux 8, 9 (x86_64) Amazon Linux 1, 2 (x86_64) Amazon Linux 2023 (x86_64) Amazon Linux 2 (AArch64) Amazon Linux 2023 (AArch64) CentOS Linux 6, 7, 8 (x86_64) CloudLinux 7,8 (x86_64) Debian 8, 9, 10, 11 (x86_64) Oracle Linux 6, 7, 8, 9, 10 (x86_64) Red Hat Enterprise Linux 6, 7, 8, 9 (x86_64) Red Hat Enterprise Linux 8 (AArch64) Red Hat Enterprise Linux Workstation 7 (x86_64) RockyLinux 8, 9 (x86_64) SuSE 12, 15 (x86_64) Ubuntu 16.04, 18.04, 20.04, 22.04 (x86_64) Ubuntu 18.04, 20.04, 22.04 (AArch64)	• 2 GB minimum • 5 GB recommended	• 1 GB recommended