Trend Vision One™ – Endpoint Security

Optimized prevention, detection, and response for endpoints, servers, and cloud workloads

In the face of an ever-changing threat landscape, organizations must keep endpoints secure—no matter where they are—to help stay ahead of adversaries. The right endpoint detection and response (EDR) solution is one that is not only up to the task, but easy to integrate, capable of reducing loads on your security teams with smarter alerts and AI-bolstered data analysis. In a sense, less is more, enabling your teams to prioritize—and mitigate—the most urgent threats across endpoints and environments.

Discover the capabilities of Endpoint Security

Our Endpoint Security solution is purpose-built for endpoints, servers, and cloud workloads, integrating advanced threat protection, EDR/XDR, and threat intelligence. Leveraging the unified, AI-powered architecture of our Trend Vision One™ platform, it will help you streamline IT and security operations, reduce complexity, and achieve optimal security outcomes across your on-premises, cloud, multi-cloud, and hybrid environments.

Connect your endpoint and workload security with other protection solutions seamlessly, including those from Trend Micro and third parties. In addition, leverage threat intel, security information and event management (SIEM), attack surface management (ASM), and more. Endpoint Security supports your diverse hybrid IT environments, helps automate and orchestrate workflows, and delivers expert cybersecurity services, so you can stop adversaries faster and take control of your cyber risk.

Integrated EDR

Through Trend Vision One, you get the XDR advantage with integrated EDR capabilities.

- **Receive prioritized, actionable alerts and comprehensive incident views**
- **Investigate root cause and execution profiles across Linux and Windows system attacks to uncover their scope and initiate direct response**
- **Hunt for threats via multiple methods—from powerful queries to simple text search— to proactively pinpoint tactics or techniques and validate suspicious activity in their environment**
- **Continuously search for newly discovered indicators of compromise (IoCs) via automated intelligence or custom intelligence sweeping**

Comprehensive threat protection from layered prevention to detection and response

Get timely protection against an ever-growing variety of threats by leveraging automated and advanced security controls, and the latest industry-leading threat intelligence.

With a full range of layered prevention, detection, and response capabilities—such as modern anti-malware and ransomware protection, device control, host-based intrusion prevention, application control, machine learning/AI, and more—you can defend your endpoints, virtual desktops, servers and cloud workloads in real time.

Protection points

- Physical endpoints
- Microsoft Windows PCs and servers
- Apple MacOS computers
- Point-of-sale (POS) and ATM endpoints
- Server
- Cloud workload
- Virtual machines

Threat detection capabilities

- **High-fidelity machine learning (pre-execution and runtime)**
- **Behavioral analysis (against scripts, injection, ransomware, memory, and browser attacks)**
- **In-memory analysis for identification of fileless malware**
- **Variant protection**
- **Census check**
- **Web reputation**
- **Exploit prevention (host firewall, exploit protection)**
- **Command and control (C&C) blocking**
- **Data loss prevention (DLP)**
- **Device and application control**
- **Ransomware rollback**
- **Sandbox and breach detection integration**
- **Extended detection and response (XDR)**

Modern, cloud-native security for your hybrid cloud deployments

- Workloads, by default, are vulnerable from the moment they are instantiated; gain built-in workload discovery capabilities, integrating with AWS, Microsoft Azure, Google Cloud Platform™ (GCP), VMware, and Microsoft Active Directory to provide protections from the moment they are created
- Eliminate the cost of deploying multiple point solutions and achieve consistent security across physical, virtualized, cloud, container, and user endpoint environments with a single management console
- Monitor for changes and attacks on Docker and Kubernetes platforms with integrity monitoring and log inspection capabilities
- Protect runtime containers through container vulnerability shielding via intrusion prevention, real-time malware protection, and east-west container traffic inspection

Intrusion and vulnerability prevention for endpoints, servers, and their applications

The intrusion prevention module within Endpoint Security helps you protect your environment from known and zero-day vulnerabilities. In addition, it safeguards against structured query language (SQL) injection attacks, cross-site scripting attacks, and other web application vulnerabilities. In addition, our vulnerability protection and intrusion prevention includes virtual patches to shield your organization from known vulnerabilities until a patch is available from the vendor. This is backed by the Trend Micro™ Zero-Day Initiative™ (ZDI), the world's largest bug bounty program.

File integrity monitoring

The integrity monitoring module allows you to scan for unexpected changes to registry values, registry keys, services, processes, installed software, ports, and files. Using a baseline secure state as a reference, the integrity monitoring module helps you perform scans on the above and logs an event (as well as an optional alert) if it detects any unexpected changes.

Log inspection

The log inspection protection module enables you to identify important events that might be buried in your operating system and application logs.

This module allows you to:

- Detect suspicious behavior
- Collect events across heterogeneous environments containing different operating systems and diverse applications
- View error and informational events, such as "disk full," "service start," and "service shutdown"
- Create and maintain audit trails of administrator activity, including administrator logins or logouts, account lockouts, and policy changes

In addition, the log inspection feature within Endpoint Security enables the real-time analysis of third-party log files. The log inspection rules and decoders provide a framework to help you parse, analyze, rank and correlate events across a wide variety of systems.

Proven Leadership

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

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

MITRE Engenuity ATT&CK (2023) #1 performer in the protection, category with 100% detection of all critical attack steps in the evaluation

Ranked #1 for Cloud Workload Security Market Share for the 6th consecutive year (2023)

Protecting your Linux platform

Our platform provides support for extensive Linux builds and hundreds of Linux kernels, Solaris™, AIX, and HP-UX.

Achieve cost-effective compliance

Address major compliance requirements for the GDPR, HIPAA, NIST, and more, with one integrated and cost-effective platform.

Trend Vision One – Endpoint Security offerings

	Core	Essentials	Pro
Primary endpoint type	User endpoints and basic servers	User endpoints and basic servers	Critical endpoints including servers and workloads
Windows, Linux, and Mac OS	●	●	●
Anti-malware, behavioral analysis, machine learning, web reputation	●	●	●
Device control	●	●	●
DLP	●	●	
Firewall	●	●	●
App control	●	●	●
Intrusion prevention – IPS (OS)	●	●	●
Virtualization protection	●	●	●
EDR-XDR		●	●
IPS (OS)			●
Integrity monitoring/log Inspection			●
	Core	**Essentials**	**Pro**
Trend Vision One™ – Email and Collaboration Security	+	+	+
Trend Vision One™ – Mobile Security	+	+	+
Trend Vision One™ – Network Security	+	+	+
Trend Vision One™ – Cloud Security	+	+	+
Trend Micro™ Zero Trust Secure Access (ZTSA)	+	+	+
Managed detection and response/Trend Service One™		+	+
Trend Vision One™ – Attack Surface Risk Management (ASRM)		+	+

+ indicates add-on option

Interested in learning more about how you can leverage our platform and solutions to secure your endpoints?

Explore Trend Vision One

Learn more at TrendMicro.com