Solution Brief

Trend Vision One™ - Endpoint Security

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

Trend Vision One™ – Endpoint Security is the leading endpoint security solution that is purpose-built for endpoints, servers, and cloud workloads, integrating advanced threat protection, EDR/XDR, and threat intelligence. With this platform, you can streamline IT/security operations, reduce complexity, and achieve optimal security outcomes across your on-premises, cloud, multi-cloud, and hybrid environments.

As part of Trend Vision One™—a modern, cloud-native cybersecurity platform with the broadest set of native solutions complimented with third-party integration—connect endpoint and workload security with other protection products, threat intel, SIEM, orchestration, build pipeline, attack surface management, and more. Endpoint Security 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.

Integrated EDR

With 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 profile 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 your environment**
- **Continuously search for newly discovered IoCs via Trend Micro automated intelligence or custom intelligence sweeping**

Streamlined workflow for IT and security operations

Protect user endpoints, servers, and cloud workloads using a single solution with centralized visibility, management, licensing, and role-based access control. Automated protection from a single pane of glass allows you to manage endpoint inventory, detections, mitigation actions, and policies.

Protection Points

- Physical endpoints
- Microsoft Windows PCs and servers
- Mac 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)**

Endpoint Security

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

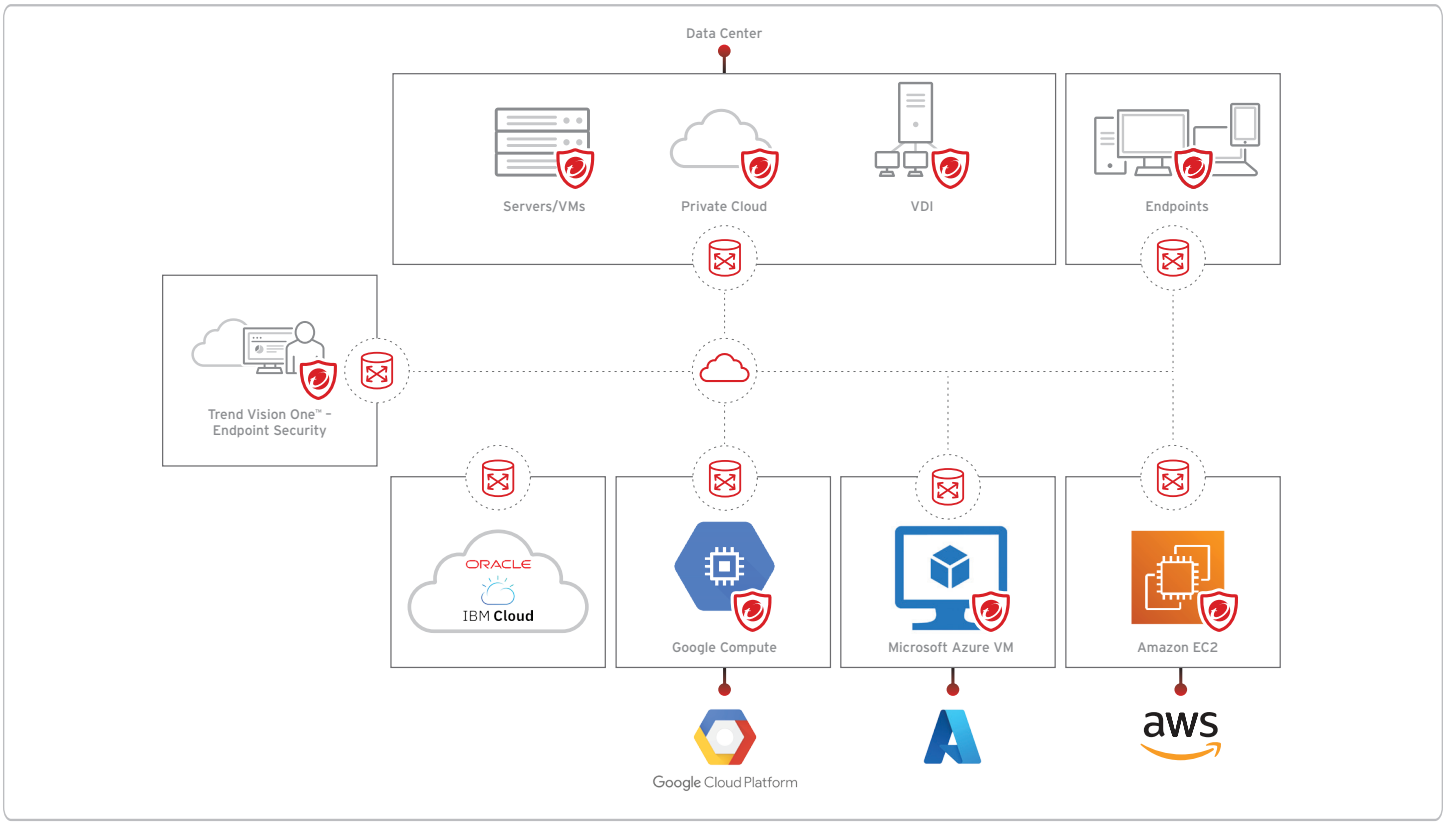
With a full range of layered prevention, detection, and response capabilities—such as modern anti-malware and ransomware protection, device control, host-based intrusion prevention, application control, machine learning/AI, and more—you can defend your endpoints, virtual desktops, servers, and cloud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

Purpose-built for server and cloud Workload Security

According to Gartner[1], "An end-user endpoint is regularly exposed to threats through email, websites, cloud services or USB drives. By contrast, threat actors target server workloads using software and configuration vulnerabilities, lateral movement, and stolen employee credentials. These differences in threat exposure create a need for distinct security requirements and protection strategies for end-user endpoints and server workloads."

Ensure your security addresses the way server and cloud workloads are deployed and attacked with Endpoint Security. Protect against vulnerabilities, malware, and unauthorized changes, and deploy advanced security capabilities specifically designed for the server and cloud workload environment.

This includes intrusion prevention system (IPS) for server applications, integrity monitoring, log inspection, and container protection. Seamlessly secure dynamic applications in the cloud, with automated discovery of workloads across cloud providers, such as AWS, Microsoft Azure, and Google Cloud Platform™.



[1]Gartner, Prioritizing Security Controls for Enterprise Servers and End-User Endpoints (Evgeny Mirolyubov, Peter Firstbrook, January 2023)

Key advantages

Advanced threat protection

- Advanced security controls such as an IPS, integrity monitoring, machine learning, and application control enable you to detect and block threats and unauthorized software execution in real time
- Shield from known and newly discovered vulnerabilities with patches delivered through an IPS, ensuring systems stay protected from existing and future threats before vendor patch is released
- Send alerts and trigger proactive prevention upon the detection of suspicious or malicious activity
- Track website credibility and protect users from infected sites with web reputation threat intelligence from our Trend global domain-reputation database
- Identify and block botnet and targeted attack C&C communications

Modern, cloud-native security for the hybrid cloud

- Workloads, by default, are vulnerable from the moment they are instantiated. Trend provides built-in workload discovery capabilities, integrating with AWS, Azure, Google Cloud Platform, VMware, and Microsoft Active Directory to provide protection 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 IPS), real-time malware protection, and east-west container traffic inspection

Tailored protection for your server and cloud workload

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

The intrusion prevention module helps you protect your environment from known and zero-day vulnerability attacks as well as against SQL injections attacks, cross-site scripting attacks, and other web application vulnerabilities.

Our vulnerability protection and intrusion prevention provides virtual patches to shield from known vulnerabilities until a patch is available from the vendor. This is backed by our world-leading bug bounty program, Trend Micro™ Zero Day Initiative™ (ZDI).

File integrity monitoring

The integrity monitoring module scans 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 performs scans on the above and logs an event (and an optional alert) if it detects any unexpected changes.

Achieve cost-effective compliance

- Address major compliance requirements for the GDPR, HIPAA, NIST, and more, with one integrated and cost- effective solution
- Provide detailed audit reports that document prevented attacks and compliance policy status
- Reduce the preparation time and effort required to support audits

Protecting your Linux platform

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

Log inspection

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

The log inspection module allows you to:

- Detect suspicious behavior
- Collect events across heterogeneous environments containing different operating systems and diverse applications
- View events such as error and informational events (disk full, service start, service shutdown, etc.)
- Create and maintain audit trails of administrator activity (administrator login or logout, account lockout, policy change, etc.)

The log inspection feature in Endpoint Security enables real-time analysis of third-party log files.

The log inspection rules and decoders provide a framework to parse, analyze, rank and correlate events across a wide variety of systems.

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		●	●
Intrusion prevention – IPS (server application)			●
Integrity monitoring/log Inspection			●
	Core	Essentials	Pro
Trend Vision One™ – Email Security	+	+	+
Trend Vision One™ – Mobile Security	+	+	+
Trend Vision One™ – Network Security	+	+	+
Trend Vision One™ – Cloud Security	+	+	+
Trend Micro™ Zero Trust Secure Access	+	+	+
MDR/Trend Service One™		+	+
Trend Vision One™ – Attack Surface Risk Management (ASRM)		+	+

+ indicates add-on option

With Trend Vision One you can have it all

- Malware and ransomware protection: Defends endpoints against threats like malware, ransomware, and malicious scripts. Advanced protection capabilities adapt to protect against unknown and stealthy new threats
- Extensive detection and response capabilities in one console: XDR goes beyond EDR with cross-layer detection and threat hunting and investigation across email, endpoints, servers, cloud workloads, and networks
- The industry's most timely virtual patching: Vulnerability protection applies virtual patches for protection before a patch is available or deployable
- Ransomware rollback: Detects ransomware with runtime machine learning and expert rules to block encryption processes in milliseconds. Rollback restores any files encrypted before the detection
- Advanced generative AI with Trend Vision One™ – Companion for analysts to search and make sense of complex threat activity
- Trend Micro™ Zero Trust Risk Insights measures risk from vulnerabilities, misconfigurations, asset criticality, XDR, anomalies, and cloud activity
- Trend Vision One delivers the broadest native XDR sensor coverage in the cybersecurity market. Our platform's native-first, hybrid approach to XDR and attack surface management (ASM) benefits security teams by delivering richer activity telemetry– not just detection data–across security layers with full context and understanding. This results in earlier, more precise risk and threat detection and more efficient investigation

Trend Vision One applies the most effective AI and expert analytics to the activity data collected from native sensors (e.g., EDR) in the environment to produce fewer, higher-fidelity alerts. Global threat intelligence from the Trend Micro™ Smart Protection Network™ combined with expert detection rules continually updated from our threat experts maximize the power of AI and analytical models in unparalleled ways.

Maximize protection with smart, layered security

Endpoint Security helps you protect your organization with a layered combination of threat protection techniques to deliver the best protection against the broadest range of threats with the most efficient performance.

All the information from each layer feeds into Trend Vision One to dramatically improve your ability to investigate, detect, and respond to threats across the environment.

Protection Layer 1

- **Signature-based techniques accurately filter out all known bad data and allow known good data to pass through**

Protection Layer 2

- **Predictive machine learning, application control, and variant protection analyzes and blocks unknown data before it has a chance to execute**

Protection Layer 3

- **Separate run-time machine learning models monitor any program, script, document or otherwise that is executing and detects threats and suspicious behavior**

Cloud sandboxing is a secure virtual environment that manages and analyzes objects submitted by integrated products and users. It provides an additional layer of protection against unknown threats that are endpoint operating system-focused.

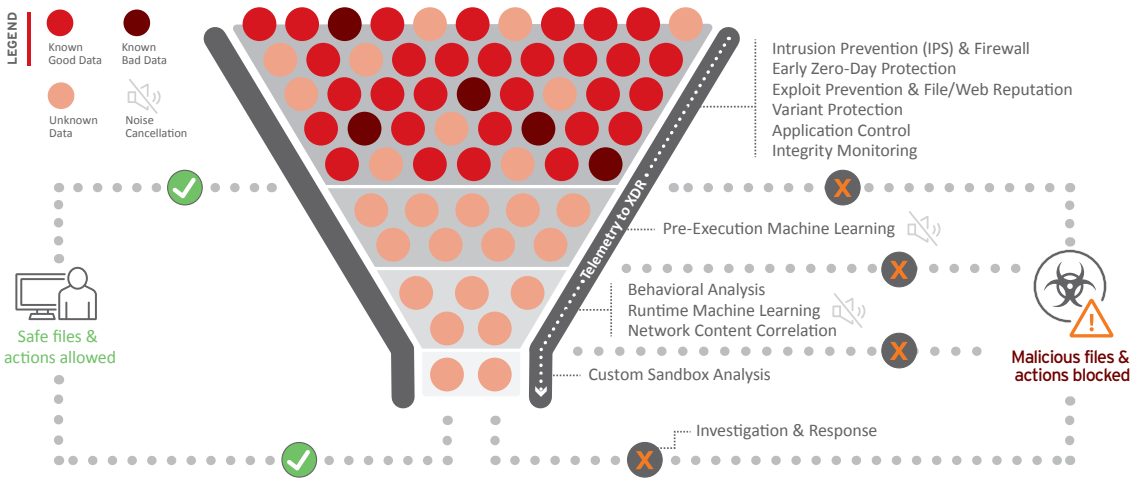


Figure 1: Trend Vision One – Endpoint Security Layers Diagram

Proven Leadership

- A leader in the Forrester New Wave™: Extended Detection and Response, Q4 2021
- Trend is a leader in Gartner Magic Quadrant for EPP since 2002. 22 times in a row

- Ranked #1 for Cloud Workload Security Market Share for the 5th consecutive year (2022)
- MITRE Engenuity ATT&CK (2023) - #1 performer in the protection, category with 100% detection of all critical attack steps in the evaluation
- A Leader in The Forrester Wave™: Endpoint Security, Q4 2023 - with the highest score in the strategy category

- Customers' Choice 2023 - Gartner® Peer Insights™ 'Voice of the Customer': EPP