Datasheet

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. This platform will help you 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 your 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 their environment**
- **Continuously search for newly discovered IoCs via Trend Micro 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
- 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)**

Gartner Peer Insights Customers' Choice 2023

Purpose-built security for your server and cloud workload

Modern, cloud-native security for the hybrid cloud

- **Workloads, by default, are vulnerable from the moment they are instantiated. Gain built-in workload discovery capabilities, integrating with AWS, Azure, Google Cloud Platform, 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 IPS), real-time malware protection, and east-west container traffic inspection**

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, the Trend Micro™ Zero-Day Initiative™ (ZDI)..

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 (and 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.

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.

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

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		●	●
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