Solution Brochure

Trend Vision One™

Integrated attack surface management (ASM) and extended detection and response (XDR)

Today, many organizations leverage multiple, disconnected security solutions to identify and assess risk, take inventory of assets, and detect and respond to threats across their email, endpoints, servers, cloud infrastructure, and networks. Unfortunately, this has led to limited visibility across the enterprise and an overload of uncorrelated alerts.

Market trends and security challenges like cloud migration, digital transformation, hybrid work, and shadow IT projects continue to evolve and propagate. Security teams must confront even more risk factors to prevent potential attacks and breaches from materializing.

Attacks or threats represent a critical but singular risk factor within the corporate environment. Proactively addressing additional areas of risk, including unknown and unmanaged assets, weak or misconfigured security controls, vulnerable assets (like unpatched operating systems), and cloud misconfigurations, can significantly influence the overall security posture and reduce the likelihood of an attack occurring.

Working across disparate security tools creates challenges like tedious, manual investigation processes and dangerous blind spots, which provide adversaries the opportunity to more easily hide and maneuver within the corporate environment. This limited visibility into the environment and an attacker's tactics, techniques, and procedures can result in an inadequate and incomplete response.

As ransomware, fatigue, data breach, destruction, and fileless attacks increase in volume, a Trend Vision One risk-centric approach to attack surface management (ASM) and extended detection and response (XDR) is required to strengthen security resiliency of your organization. Your SOC and security teams need advanced tools to proactively improve security posture, detect and respond faster, track and benchmark risk, and optimize overall security and IT operations.

Introducing Trend Vision One

Our cloud-native security operations platform, serving cloud, hybrid, and on-premises environments, combines ASM and XDR in a single console to effectively manage cyber risk across your organization.

Arm your team with powerful risk insights, earlier threat detection, and automated risk and threat response options. Utilize the platform's predictive machine learning and advanced security analytics for a broader perspective and advanced context.

Trend Vision One integrates with its own expansive protection platform portfolio and industry-leading global threat intelligence, in addition to a broad ecosystem of purpose-built and API-driven third-party integrations. This allows you to ingest and normalize activity and detection telemetry across the user environment.

Open or hybrid-first XDR and ASM security providers rely on other vendors. The customer receives inefficiently correlated detection logs from third parties to surface low-fidelity threat events and a more limited asset inventory and incomplete risk assessment. This strategy leads to slower detection, more blind spots, and greater potential for partial remediation.

Trend Vision One delivers the broadest native XDR sensor coverage in the cybersecurity market. The platform's native-first, hybrid approach to XDR and 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.

Security and SOC analysts, threat hunters, and senior security leaders across your organization are given the tools to contextualize risk and reduce the likelihood of attacks–while reducing false positives and noise within the environment continuously and proactively.

Anticipate your adversaries and develop more proactive and resilient programs by providing in-depth coverage across the attack surface risk management lifecycle. Trend Vision One identifies internal and internet-facing assets, assesses individual assets and company-wide risk, and provides custom, intelligent remediation recommendations while serving detection and response needs concurrently.

Purpose-Built XDR, Attack Surface Risk Management, and Zero-Trust Capabilities

The expansive threat landscape, combined with the evolving role of security within the modern enterprise, demands an integrated and proactive approach. Our platform empowers your team at every stage of the risk and threat lifecycle with intuitive applications to detect, hunt, investigate, analyze, and respond–and automatically surface prioritized risks and vulnerabilities.

This approach eases security operations while providing the right information to develop plans to reduce risk and improve key performance indicators like mean time to detect, patch, and respond–all while reducing the volume of security alerts your analysts face daily.

Solving Key Functional Issues

Enrich activity telemetry with full context and understanding

- **Open or hybrid-first ASM and XDR security providers rely on outside vendors, resulting in inefficiently correlated detection logs**
- **Working across disparate security tools creates challenges, like tedious processes and dangerous blind spots**
- **Teams require richer activity telemetry—not just detection data—across security layers**

Minimize silos and achieve central visibility

- **The exponential growth of the attack surface from shadow IT projects, hybrid work, third-party and supply chain risk, and growing use of public cloud services has made identifying internal and internet-facing assets a challenge**
- **Businesses who lack full visibility of their environment are at risk of attacks on assets of which they are unaware or misconfigured**
- **Despite deployed protection layers, the modern threat landscape makes it impossible to achieve 100% prevention**

Reduce alert fatigue with advanced correlation

- **An unmanageable volume of security alerts overwhelms and distracts security teams from building strategic, resilient plans**
- **Disconnected tools result in alert overload, resulting in manual investigation and slow and inadequate response**
- **By 2025, there will be 3.5 million open cybersecurity positions. The persistent skills gap and shortage demand that teams find solutions to do more with less full-time equivalent resources**

Address resource constraints with automated workflows

- **Lack of automated options across different security layers creates gaps in achieving a complete response**
- **Organizations are struggling to staff and adequately resource security teams with the necessary advanced skill set needed for the complexities of detection and response**

Elevating security as a critical pillar of business operations

Trend Vision One makes it easy to respond to frequently asked questions from your senior stakeholders (CEO, COO, CFO, CIO), the board, and cyber insurance carriers.

Leverage impactful reporting on risk and threat trends, asset inventory and relational graphs, and comprehensive performance report templates. Elevate cyber risk management as a critical pillar of business operations and map security investments to strategic business goals.

Company-wide risk, exposure, attack intensity, and security configuration tracking clearly identifies critical risk factors and surfaces the right data so you can build informed security strategies.

By the numbers

Lower operational costs	Improve response time	Minimize attacker dwell time	Limit threats and repeat attacks	Improve investigation speed	Reduce alert fatigue
Do more with less. Decrease your security spending by 79%	Accelerate your detection and response time by 70%	Remove silos to reduce your dwell time by 65%	Experience 55% fewer events and minimize your attack repropagation by 60%	Speed up your threat hunting and investigation efforts by 54%	Minimize alert fatigue by 99% with a single platform

Integrated Capabilities

A single source of truth to manage risk

An integrated approach to threat detection and response and risk management enables your security team to continuously assess and prioritize cyber risk across your organization. In addition, risk remediation and threat response can be easily automated and accelerated.

Our platform brings your security and IT teams together to mitigate risk before an attack occurs. Your security and SOC analysts, threat hunters, IT operations, and senior security leaders can continuously and proactively contextualize risk and reduce the likelihood of attacks while reducing false positives and noise within your environment.

- **One source of prioritized alerts enables your team to correlate and analyze data in an efficient and meaningful way**
- **One console allows you to investigate and quickly visualize the entire chain of events across your security layers or drill down into an execution profile or network traffic analysis**
- **One location lets you respond using containment actions for email, endpoints, cloud/server workloads, and networks**

A platform that fits your environment

- **Role-based custom dashboards:** Streamline the unique security functions and responsibilities of your CISO, CIO, SecOps, and IT operations
- **Custom policies with XDR-driven insight:** Proactively adjust your applicable product policy parameters to continually optimize defenses, create and modify the agent, control threat and vulnerability detection mode settings, and provision the agent
- **Custom playbooks:** Create automated remediation playbooks or leverage existing templates to remediate risk or respond to a threat event
- **Custom reports:** Communicate what is most critical to specific stakeholders and at your preferred frequency with custom or templated security and risk reports

Broad integration ecosystem

To integrate seamlessly with the existing security tools and technologies deployed in your environment, the platform offers a growing portfolio of open APIs and third-party systems. Trend Vision One fits within these ecosystems and security operations workflows, acquiring meaningful data from your infrastructure to further enrich and validate your XDR capabilities.

- **Native integrations:** Integrate with our broad cybersecurity protection portfolio for your cloud, hybrid, and on-premises environments
- **Third-party integrations:** Effortlessly integrate with purpose-built connections to cloud services, external attack surface management, firewall and network protection, IT service management, identity and access management, SIEM, SOAR, threat intelligence, ticketing communication, Microsoft 365, Microsoft Azure Active Directory, Active Directory, and unified endpoint management technologies

API automation: Leverage API cookbook templates and sample code to execute Python-based custom scripts and automate regular procedures in your SOC. This includes investigation and triage, live response, threat hunting, and user account management.

Automate and orchestrate remediation and workflows

Automate and orchestrate response across your multiple endpoints or sensor types using templated and custom security playbooks. By creating response tasks and automatically delivering detection and response results into a digestible report, your analysts can do more with less effort.

Sandbox analysis

Validate investigations, analyze suspicious objects, and keep potential threats isolated from the rest of the enterprise with sandbox analysis. Your security analysts can submit over 45 different types of files and URLs to a secure virtual environment and generate comprehensive scheduled or on-demand reports outlining the details of high-risk submissions.

Leading global threat intelligence and threat actor profiling

- **Early warning:** Trend Vision One™ XDR blocks the source of a threat—in places where most providers can't see. Get end-to-end visibility into your full attack campaign lifecycle to understand where an attack begins and respond before a breach can occur
- **Complete breach visibility:** Global threat intelligence captures both individual threat components and APT data to detail how individual malware detections and vulnerabilities contribute to a breach before, during, and after an attack occurs
- **Deep attack campaign intel:** See the MITRE ATT&CK tactics, techniques, and procedures associated with specific attack campaigns and individual attack activities

Intelligent guidance

Rapidly remediate risk across your environment with intelligent and custom mitigation recommendations to dynamically balance complexity, analyst effort, and asset criticality.

Discover, Assess, Prioritize, and Mitigate Risk with Market-Leading Attack Surface Management

Continuous verification of risk and trust is key to achieving a zero-trust strategy. ASM enables security teams to continuously identify, inventory, and assess known, unknown, managed, and unmanaged cyber assets and automatically prioritize and remediate risk and vulnerabilities associated with those assets based on the likelihood and impact of a potential attack.

ASM evaluates security gaps from the perspective of an adversary, leveling the playing field of your organization. Protect against risk across people, processes, and technology.

Internal Attack Surface Discovery	Internet-Facing (External) Attack Surface Discovery
This includes entities on your corporate network in addition to personal devices interacting with corporate assets in the cloud, workloads, and other remote tools. Integrate with Trend protection products, third-party security solutions, and IT infrastructure tools to develop a single repository for all managed or unmanaged internal assets.	These assets are significantly vulnerable due to their full exposure to the internet. Identify managed and unmanaged internet-facing assets with an agentless solution. Submit your company domain name to identify potential risks like unsupported or vulnerable application versions, expired domain certifications, and services with associated vulnerable protocols.

Internal and external attack surface discovery

With limited visibility to identify unknown assets, security teams often prioritize unmanaged, internal, and internet-facing assets.

Your security team can see more of your environment by identifying unknown assets and addressing the high-risk associated. Attack surface discovery eliminates blind spots and identifies all potential adversary entry points.

Intuitive risk assessment, analysis, and benchmarking

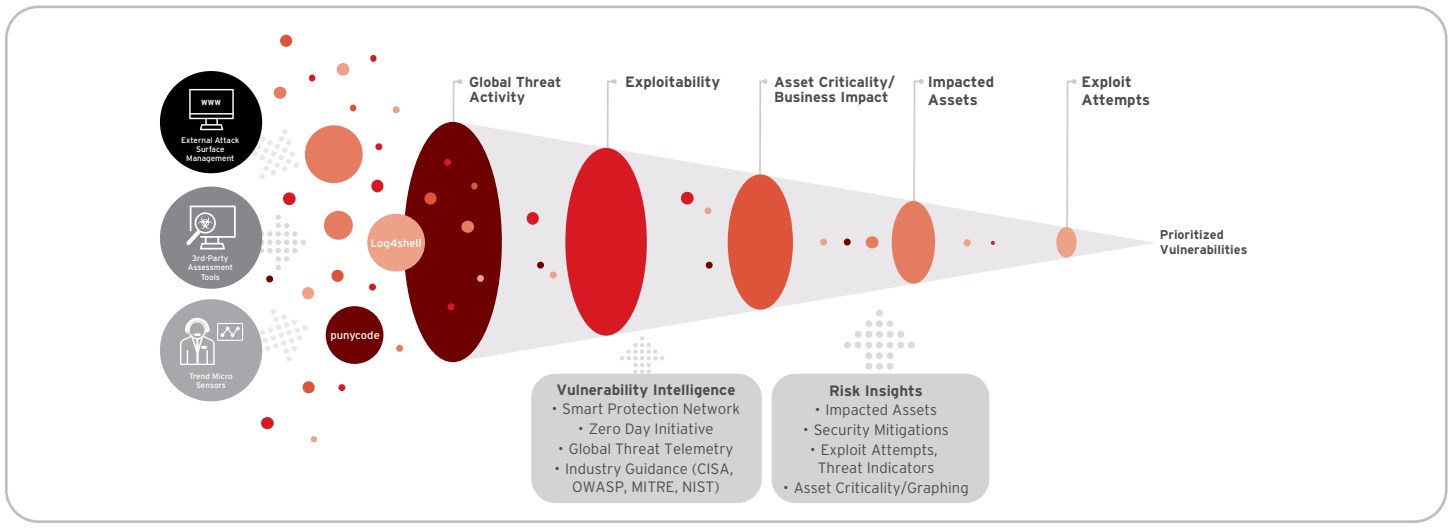
Contextualized risk assessment and analysis recognize which assets pose the highest risk to your organization with detailed information.

This risk score is a function that considers two variables: the likelihood of a threat actor entering your environment and the potential impact of an event. Using these factors, the platform presents the result as an integer between 0 and 100, representing the overall risk to an organization's individual assets at-a-glance.

The risk index represents the overall, company-wide risk of your organization using a mathematically fair methodology. It is calculated using the risk scores of a sampled set of assets.

Exposure, attack, and security control scoring provide the next layer of depth toward remediating and preventing risk in your organization. These specialized indices deliver additional visibility into your organization's security posture, enabling the development of data-informed strategies to reduce risk across your organization. With continuous assessment and prioritization, the modern SOC has complete coverage to track attack pressure, threat and exploit impact, and live misconfigurations.

- **Vulnerability and risk prioritization:** Global and local threat intelligence augment highly technical risk scoring methods, exception rules, and required effort to identify which vulnerabilities are prioritized for remediation
- **Vulnerability management metrics:** In a single pane of glass, track the number of highly exploitable unique common vulnerabilities and exposures (CVEs), mean-time to patch, average vulnerability unpatched time, vulnerable endpoint percentage, CVE density, and legacy OS usage
- **Benchmarking:** Compare and benchmark against other organizations in your industry, region, or peer group and clearly identify areas of concern and room for improvement



Actionable, predictive risk insights

Trend Micro™ Risk Insights synthesizes attack surface management telemetry to intuitively surface an at-a-glance understanding of your company-wide security posture, benchmarks, and trends over time. In addition, your analysts are given the opportunity to examine and filter assets, vulnerabilities, and key metrics in more detail. Risk Insights offers central visibility into the attack surface inventory, cyber risk score, vulnerable assets, predicted impact, operations efficiency, and recommended remediation tactics.

- **Leading ASM: Leverage first-to-market technology to deliver broad coverage for internal and internet-facing (external) attack surface discovery, risk assessment and vulnerability prioritization, and automated risk and threat remediation**
- **Complete coverage: Risk index, attack index, exposure index, and security misconfiguration trends track the attack pressure, threat and exploit impact, unpatched vulnerabilities, and misconfigurations within your environment**

Risk Insights delivers a single source for security leaders, security operations, and IT across your organization, this allows you to observe and evaluate your entire IT environment at varying and appropriate levels of detail.

The platform automatically measures and weights different risk factors (including vulnerabilities, security controls and misconfigurations, asset criticality, XDR detections, account compromise, anomalies, and cloud activity data) to predict potential gaps for exploitation as well as automate and accelerate mitigation actions across people, processes, and technology.

Proactively secure assets across the enterprise

Mitigate and contain risk across the infrastructure. Swiftly address misconfigurations, automate remediation actions for unpatched vulnerabilities, and deploy threat response actions across multiple security layers with a single action. Automate remote access control for private and network access with Trend Micro™ Zero Trust Secure Access.

Assess human risk within the environment

Proactively address human risk with manual, scheduled, and automated phishing exercises to bolster security awareness training and inform risky user behavior. Trend Micro™ Phish Insight™ enhances information security awareness for your organization by empowering people to recognize and protect themselves against targeted threats.

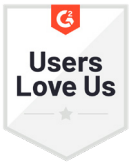
Zero Trust Secure Access follows the principles of zero-trust networking. Strengthen your overall security posture by enforcing strong access control permissions from multiple identity services across the organization.

Rather than granting access to the entire network, as a VPN does, Secure Access provides a gateway to specific applications and resources, restricting access to everything within the network that is not being employed. If valid user credentials are stolen, the level of access they will grant to the

organization can be contained, effectively reducing the blast area of any attack.

Supercharge XDR Capabilities

XDR correlates data across multiple security layers—including endpoint, server, email, identity, mobile, cloud workload, and network—from native sensors, global threat intelligence feeds, and third-party data sources. A single pane of glass allows you to detect, investigate, and respond to suspicious behavior, malware, ransomware, disruption, and other critical attacks. XDR works across different security vectors to reduce silos and detect threats that have evaded your protection technology.



According to ESG, organizations with Trend Micro XDR are 2.2x more likely to detect an attack, save up to 79% on security costs, and improve response time by 70%.

- **Earlier detection:** XDR improves your team's visibility and reduces silos to unearth threats evading detection by hiding in between security silos amid disconnected solution alerts
- **Advanced correlation:** By leveraging native and third-party data, your security team is enabled to deliver deep activity data—not just XDR detections—across endpoint, email, server, cloud workloads, and network
- **Optimized detection modeling:** Threat intelligence incorporates more sources and research to enrich detection and investigation to deliver greater context to your team
- **Faster investigation:** By quickly visualizing the full attack story, XDR automatically pieces together fragments of malicious activity across your security layers
- **Complete response:** Enacting embedded response options across multiple security layers enables security teams to prioritize, automate, and accelerate response actions from one location

Reduce time to detect and stop threats

XDR analytics surfaces fewer, prioritized alerts for action by automatically tying together a series of lower-confidence activities into a higher-confidence event. Construct powerful query strings using plain-text search to pinpoint data or objects in your environment to be examined. Automate processes when new data is found by saving query criteria, creating watchlists, and configuring email recipients.

Detect, investigate, and respond to individual events and cross-layer attacks

- **Workbench view:** Visualize the full story of an attack, run a root cause analysis, look at the execution profile, identify the scope of impact and take response actions from a single app
- **Incident view:** Group together related Workbench alerts and view the end-to-end execution profile of an incident with advanced alert correlation and machine learning techniques
- **Root cause analysis:** Understand and investigate an individual alert and advanced persistent threats (APT)

Advanced detection modelling

Specialized detection models are added and continuously updated to detect specific types of threat activity. This includes leading Trend intelligence research, MITRE ATT&CK information, filters, and rules. Leverage detection models for automatic search and identify new indicators of compromise (IoC).

Extensive response options across security layer

ENDPOINT, SERVER, AND CLOUD WORKLOAD	IDENTITY	EMAIL	NETWORK
Remote shell	Disable user account	Quarantine email	Full packet capture
Isolate endpoint	Force sign out	Delete email	Block file transfer
Terminate process	Force password reset	Restore email	Close web or access proxy connection
Collect file		Block sender	Block network access control port
Submit for sandbox analysis		Block file/process	Drop a connection in firewall
Submit for forensics		Block IP/domain/URL	New signature creation
Run remote custom script			
Memory dump			
Collect master file table (Windows)			
Collect registry (Windows)			
Restore registry (Windows)			
Collect packet capture (Windows)			

Uncover attacks faster with early warnings

Trend Vision One targeted attack detection analyzes, predicts, and sends alerts before an event occurs. By using techniques like intrusion prevention (IPS) and behavioral analysis, your security team can proactively detect and stop threats. Comprehensive MITRE ATT&CK mapping delivers visualizations for trending alerts to give you a clear understanding of the tactics, techniques, and procedures associated with suspicious activity.

Hunt with confidence

Leverage sophisticated search tools to initiate an investigation or dig deeper into specific indicators of attack (IoA) and IoC from an alert. Your threat hunters can search using simple plain-text and complex query languages to rapidly identify, visualize, categorize, automate, and retrieve results.

The API-friendly platform integrates third-party inputs to deliver more data (including firewall, vulnerability management, network, identity, SIEM, and SOAR) for analytical enrichment, as well as optimizing processes and workflows. This increases threat investigation effectiveness and efficiency across your organization.

- **Guidebook:** Ease threat hunting and search activities and pinpoint data more accurately with step-by-step guidance and query recommendations
- **Observed attack techniques:** Search a prioritized list of events—including related MITRE ATT&CK information—that may trigger an alert
- **MITRE ATT&CK mapping:** This information is deeply embedded within the platform to help your analysts map adversary tactics, techniques, and procedures to the MITRE ATT&CK framework. Easily understand, contextualize, and communicate suspicious activity

XDR forensics and analysis

From a single console, your security teams can complement detection, investigation, and response activities with advanced forensics and analytics. This improves incident response and prevents future attacks. Trend Vision One intelligently tags, categorizes, and organizes suspicious evidence records into a user-friendly timeline view so you can improve investigation efficiency, fill in missing parts of the attack story, and prevent repeat occurrences.

Managed services

Augment your security teams with 24/7 managed detection, response, and support. Trend Service One™ delivers Trend Micro™ Managed XDR to offer alert monitoring and prioritization, incident investigation, and threat hunting as a service.

Improve time to detection and time to respond by leveraging the resources and knowledge of Trend security experts. Your teams are equipped with efficient alert monitoring, in-depth investigations into advanced threats, and threat hunting via proprietary techniques.

Your threat investigators can initiate respective product response options to contain threats. A step-by-step response plan on actions needed to remediate, along with custom cleanup tools, where applicable, help you recover from the threat.

Managed XDR service can be applied to your organization's email, endpoints, network, and server/cloud workload security.

Experience Trend Vision One

Platform trial

Explore the entire Trend Vision One platform free for 30 days. Access powerful XDR capabilities, leading ASM tools, and award-winning global threat intelligence.

Get started today

Essential access for Trend protection customers

Trend customers are entitled to complimentary Essential Access to Trend Vision One for the duration of their protection product license.

Learn how to activate and access your account

Essential access includes a subset of Trend Vision One apps including:

Reporting and visibility
- Executive dashboard
- Operations dashboard

Assessment – uncover malicious activity
- At-risk mailbox
- At-risk endpoint
- At-risk users
- At-risk cloud apps
- Phish Insight

Threat Intelligence
- Intelligence report
- Suspicious object management
- Third-party intelligence (TAXII, MISP)
- Campaign intelligence
- Vulnerability intelligence

Workflow and automation
- Third-party integration
- Service gateway
- Playbooks

Product connector
- Protection product connection

Threat identification and hunting
- Targeted attack detection
- Search

Admin
- Audit logs
- Credit usage
- User accounts
- Notifications
- Console and support settings

100%

detection of **all 19 attack steps** in the evaluation - highly enriched telemetry for better investigations.

105 out of 109

provided clear visibility of attack methods providing **96.33% coverage** - this broad visibility allows customers to have a clear picture of the attack and respond faster.

100%

(#1 Performer)

of attacks against the Linux host detected and prevented, capturing attacker steps and preventing a simulated attack – especially important considering Linux is the most used OS in cloud-native applications.

Ranked #1

in the **protection category** – ensuring that attacks are prevented early in the attack lifecycle.