Solution Brief

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 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 (TTP) can result in an inadequate and incomplete response.

As ransomware, fatigue, data breach, destruction, and fileless attacks increase in volume, a risk- centric approach to attack surface management (ASM) and 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. This means leveraging the capabilities of an AI-powered, unified, and all-empowering cybersecurity platform.

Introducing Trend Vision One

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

Empower your team with comprehensive risk insights, earlier threat detection, and automated risk and threat response options—all bolstered and made more efficient with the help of AI. 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 your 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—all 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 addressing your detection and response needs concurrently.

Figure one: overview of Trend Vision One platform capabilities and unified solutions

Trend Micro™ Zero Trust Secure Access (ZTSA)

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, ZTSA 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.

Purpose-built XDR, Attack surface risk management (ASRM), 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. Trend Vision One 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 your security operations while providing the right information at the right time. Enable the streamlined development of plans. 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.

Actionable, predictive risk insights

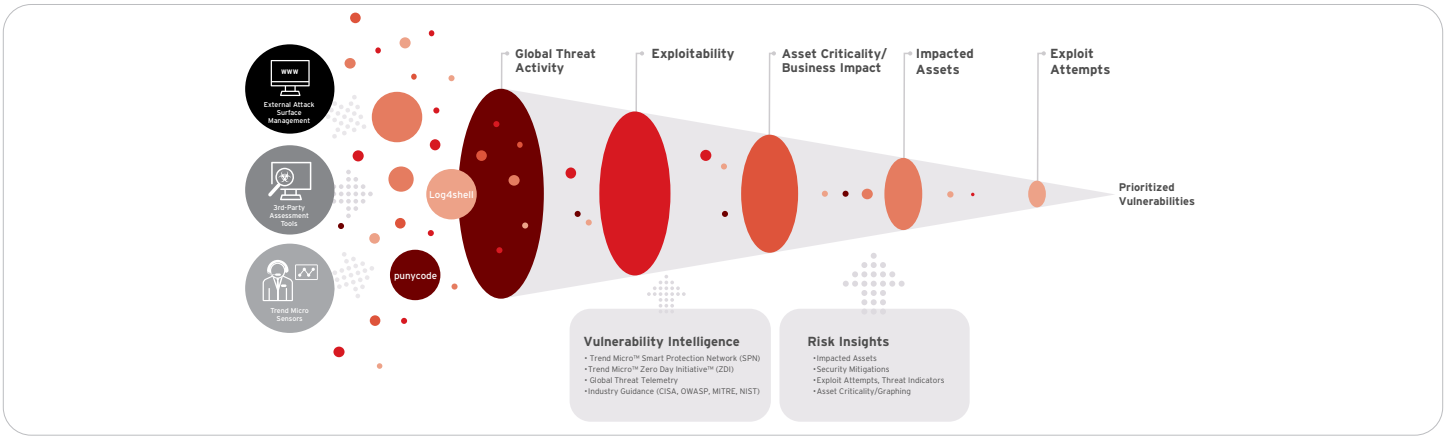
Trend Vision One™ – Attack Surface Risk Management (ASRM) synthesizes attack surface management telemetry to intuitively surface an at-a-glance understanding of your company-wide security posture, benchmarks, and trends over time. In addition, your analysts are given the opportunity to examine and filter assets, vulnerabilities, and key metrics in more detail. ASRM offers central visibility into your 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

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

Trend Vision One automatically measures and weighs different risk factors including vulnerabilities, security controls and misconfigurations, asset criticality, XDR detections, account compromise, anomalies, and cloud activity data. The information it gathers is then used to predict potential gaps for exploitation as well as automate and accelerate mitigation actions across people, processes, and technology.

Figure two: overview of protection layers



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

A Leader in the Forrester New Wave™: Extended Detection and Response, Q4 2021

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

Customers' Choice in 2024 Voice of the Customer for Network Detection and Response, Midsize Enterprise ($50M - $1B)

Supercharge your 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 XDR are 2.2 times 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 networks
- **Optimized detection modeling:** Threat intelligence incorporates more sources and research insight 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 your security team to prioritize, automate, and accelerate response actions from one location

Experience Trend Vision One

Platform trial

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

Get started today

Essential access for Trend protection customers

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

Activate your account

Essential Access includes a subset of Trend Vision One features 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
- Trend Phishing Simulation

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

Solution connector
- Protection solution connection

Threat identification and hunting
- Targeted attack detection
- Search

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

About Trend Micro

Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fueled by decades of security expertise, global threat research, and continuous innovation, our unified cybersecurity platform protects hundreds of thousands of organizations and millions of individuals across clouds, networks, devices, and endpoints.

With 7,000 employees across 65 countries, and the world's most advanced global threat research and intelligence, Trend enables organizations to simplify and secure their connected world.

TrendMicro.com