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 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 (TTP) 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 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 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—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, 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. 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.

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 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

ASRM delivers a single source for security leaders, security operations, and IT operations 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.

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.

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.

FORRESTER® WAVE LEADER 2023 Endpoint Security

FORRESTER® WAVE LEADER 2023 Network Analysis And Visibility

TREND MICRO Named a LEADER in 2023 Gartner Magic Quadrant for Endpoint Protection Platforms

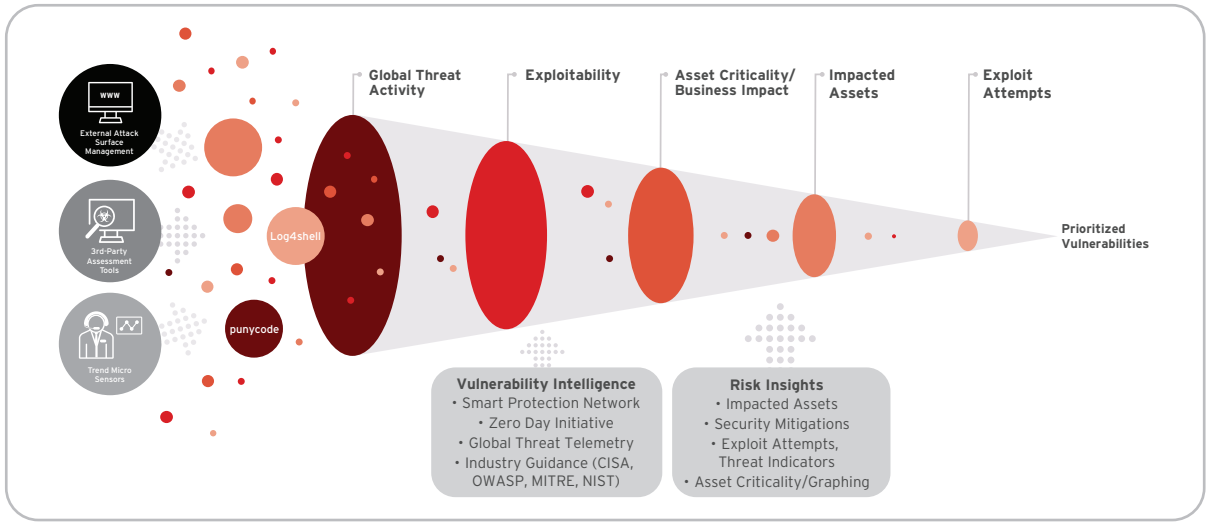
G2 Best Results Enterprise SPRING 2024

G2 Best Usability Enterprise SPRING 2024

G2 Best Relationship Enterprise SPRING 2024

G2 Leader SPRING 2024

G2 Users Love Us



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.

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
- 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

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

Trend Vision One™ – Email and Collaboration Security

Centralized visibility and management with unified protection, detection, and response

Threat actors are using advanced tactics to penetrate email. Phishing remains the top attack vector with **92% of organizations** falling victim through modern attack techniques that have expanded beyond email to collaboration tools.

You need to protect users from business email compromise (BEC), ransomware, phishing, social engineering, and malware. However, traditional email security protection offers a limited view—often only reactive to known threats—without understanding the full attack story.

Blind spot for IT administrators

With workforces across the globe, businesses are utilizing collaboration tools to engage and boost productivity. This new norm of communication often remains unprotected, putting you at risk.

Without skills to stop evolving attacks or training to educate employees on handling events and reporting malicious emails, the chance of falling victim will continue.

Introducing Trend Vision One – Email and Collaboration Security

Our cloud-native fully integrated solution helps modernize protection for email and collaboration applications by leveraging our unified cybersecurity platform to withstand and rapidly recover from evolving threats.

Centralized visibility and management for API + inline + gateway

Through our Trend Vision One™ platform, gain access to:

- **Cloud email and collaboration protection.** Manage inbound, outbound, and internal email threats in real-time and secure your collaboration services (messaging and file storage in Microsoft 365, Google Workspace™, Box™, and Dropbox™)
- **Cloud email gateway protection.** Analyze incoming/outgoing emails and prevent sensitive information from leaving the organization by encrypting emails and providing auto remediation for potential threats and anomalous behavior
- **Trend Vision One™ – XDR for Email:** Gain holistic insight into an attack through correlation detection and investigation across multiple security layers. Leverage the email activity data collected via the email sensor in the platform.
- **Trend Vision One™ – Attack Surface Risk Management (ASRM):** Prioritize and mitigate risks in real-time, powered by ASRM, for continuous risk assessment.

Key benefits:

- Protection against account takeover (ATO)
- Real-time protection for email and collaboration apps against phishing and business email compromise (BEC)
- Multi-layer security across API + inline + gateway
- Removing silos and visibility gaps with central visibility, analysis, and deep insights
- Improving security posture across email and collaboration environments
- Organizations can embrace cloud efficiency while maintaining the security of their employees, unifying analyst experience, and optimizing protection of email and collaboration environments

Email and Collaboration Security Overview

Key capabilities:

Complete protection of your email and collaboration apps

Leverage advanced threat and data protection against BEC, ATO, and phishing attacks with market-leading cloud email and collaboration protection. Enforce compliance for cloud-file sharing and collaboration services (Microsoft 365, Google Workspace, Box, and Dropbox).

Stopping attacks using AI, machine learning, and modern innovations

Utilize the ability to discover known, unknown, and highly sophisticated attack tactics with cloud email gateway protection. Analyze writing styles of suspicious emails, end-to-end encryption for sensitive data, and utilize retro-scan to uncover attacks in progress.

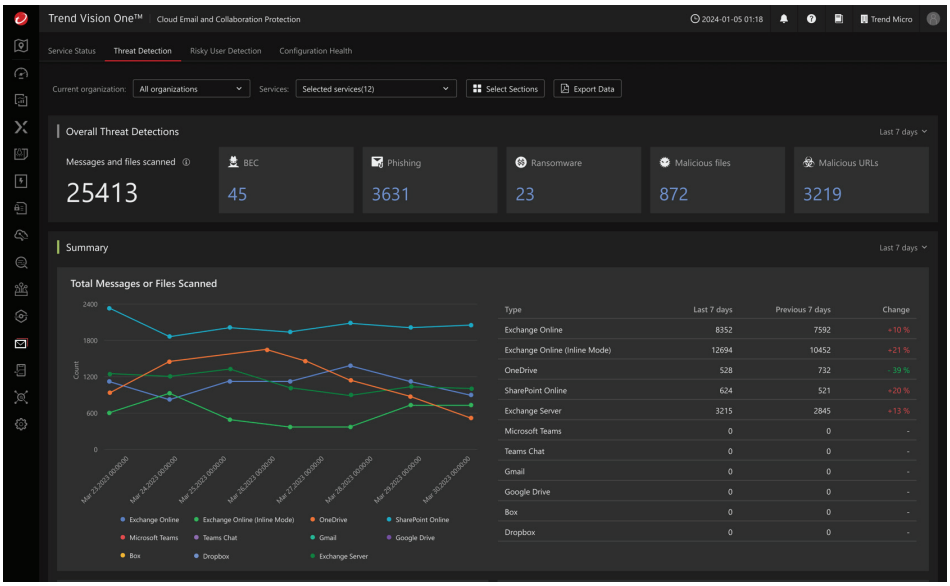
Full visibility into the "what", "who", and "where"

Get built-in capabilities for SecOps through XDR for Email with its advanced analytics for securing email and collaboration environments. Leverage email activity data, enriched with cross-layer extended detection and response (XDR) data telemetry, all in a single place.

Deep insight of latest threats, vulnerabilities, and risks

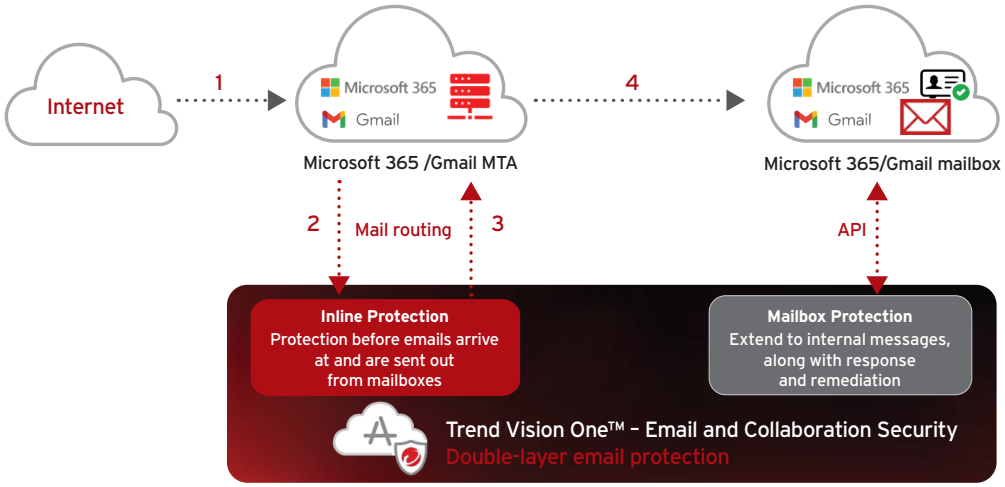
Gain central visibility for business and technology leaders with ASRM. Allow for continuous identity-based risk verification and the prioritization of risks. Take remediation action for internal users, top targeted employees, and users with high-risk events.

Trend Vision One platform – Cloud Email and Collaboration Protection



Solution architecture

Email Inline and Mailbox Protection



Features and specifications:

	CLOUD EMAIL AND COLLABORATION PROTECTION	CLOUD EMAIL GATEWAY PROTECTION
Deployment	API and Inline	MX
Malware Scanning, Anti-Spam, Web Reputation, ATP	✓	✓
Data Loss Prevention	✓	✓
End User Quarantine	✓	✓
IP Reputation	✓	✓
Domain Authentication		✓
Email Continuity		✓
Email Encryption		✓
DMARC Monitoring		✓
Cloud Sandboxing	✓	✓
BEC Protection	✓	✓
Writing Style Analysis	✓	✓
QR Code Detection	✓	✓
Password Guessing	✓	✓
Suspicious Objects	✓	✓
Retro Scan	✓	
Integration with MS MIP	✓	
Collaboration Apps Protection	✓	
(Microsoft 365, Google Workspace, Box, Dropbox)	✓	
Manual Scan	✓	
API Remediation	✓	
End User Feedback Management	✓	
Target Attack User Visibility	✓	
Account Takeover Visibility	✓	
Account Block	✓	
	XDR FOR EMAIL	
Filter and Search	✓	
Workbench for Email and Cross-Layer Advanced Detection	✓	
Email Response	✓	
Email Account Response	✓	
Observed Attack Techniques: MITRE Att&ck™ Matrix Mapping	✓	
Event Data Retention	✓	
Threat Intelligence Sweeping in Email Telemetry	✓	
	ASRM	
Executive Dashboard	✓	
Risk User Assessment (risk score and risk event)	✓	
Security Configuration	✓	
Security Dashboard	✓	

Enhance email with Trend Vision One:

Deliver XDR across email, endpoint, server, cloud workload, identity, network, and IoT.

Get broader visibility for greater understanding

XDR collects and correlates deep activity data across multiple security layers from the initial infection point to the lateral spread across the network—enabling hunting and investigation analysis and improving your SOC team's visibility.

Prioritize your response with XDR for Email

By knowing the extent of a phishing attack and its severity, you can determine which threat requires immediate response and enact automated response options to break the attack chain (for example, quarantine an email across multiple mail accounts or block an IP address across email, endpoint, servers, cloud).

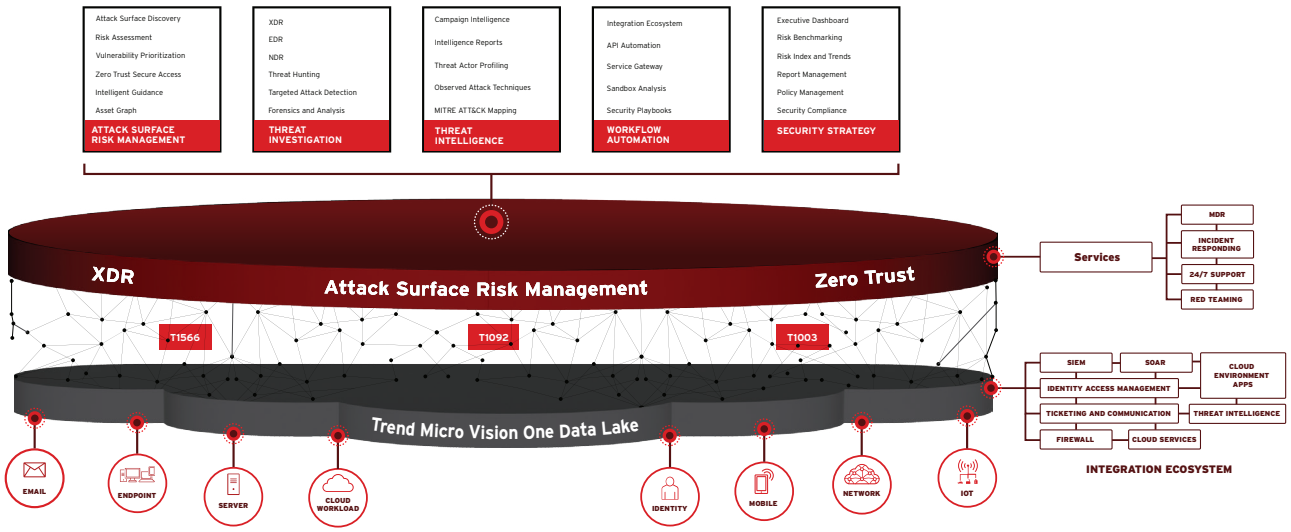
Dig deeper into each step of an attack quickly

With the ability to zoom-in on an email attack event, you can immediately see the details of a threat exposure. This includes related assets, score, impact scope, suspicious links, user details, attack phase, initial access, severity level, and more.

Broad integration ecosystem

With 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 abilities.

Trend Vision One platform – XDR and ASRM



Enrich email with Trend Vision One – Attack Surface Risk Management (ASRM):

Trend Micro helps your organization gain the continuous visibility and analysis needed across your attack surface risk management lifecycle to understand, prioritize, and actively mitigate your cyber risk.

Discover unknown and unmanaged cyber assets.

Your digital attack surface is expanding, making exploitation easier and protection difficult. Attack surface discovery continuously identifies known and unknown assets to inform your attack exposure and status of your security configurations.

Dynamically assess your cyber risk.

Continuous organization-wide risk assessment includes risk scoring based on the dynamic assessment of risk vectors in your network. Risk assessment integrates the status of vulnerabilities, configuration of existing security controls, and types/stages of threat activity being seen in the environment.

Mitigate cyber risk.

With in-depth attack surface risk knowledge, you can apply the right preventative controls to mitigate and remediate risks across the enterprise. Receive recommendations and automated actions to harden defenses, reduce vulnerabilities, and avoid breaches.

Integrate with XDR for Email

Detection data collected by XDR provides valuable insight into your attack surface threat activity and provides you with a snapshot of how current defenses are coping. Inform risk assessments and response recommendations on how to proactively mitigate against identity-based risks.

Trend Vision One™ – Cloud Security

Unify. Simplify. Standardize.

As your business continues to navigate its cloud journey, moving from migration and optimization to cloud-native application development, the security challenges you face continue to evolve. We know how important it is to have a solution that helps bridge the gap between developers and security teams, all while breaking down silos within your security operations.

Trend Vision One – Cloud Security enables your organization to connect SecOps and cloud security teams across the entire hybrid cloud journey. We can meet you at any stage your security journey, helping to stop adversaries faster and take charge of risk. Our powerful enterprise cybersecurity platform is purpose-built to facilitate earlier detection, faster response, and ultimately reduce risk across a diverse range of hybrid IT environments.

Hybrid focus

Like many others, perhaps your organization retains a hybrid environment, adding an additional layer of complexity when it comes to security. Such operations need to implement a proactive approach to application and workload protection across ever-evolving, dispersed environments. With Cloud Security, you can apply modern security tooling to any hybrid workload, regardless of whether it is on-premises or in the cloud.

Multi-cloud support

Achieving visibility and consistent security policy management across the cloud can be complex—often as much as managing these cloud environments through their native controls. Cloud Security enables you to provide consistent policy, risk assessment, and security controls regardless of where workloads are running. This includes within AWS, Microsoft Azure, and Google Cloud Platform™ (GCP) services, multi-cloud, or on-premises. Integrating with cloud-native applications, development, and orchestration platforms further extends the reach of your vulnerability management and risk assessment to containers and serverless environments.

Key benefits

- Proactively identify cloud threats, visualize risk, and prioritize vulnerabilities
- Quickly respond to security threats and mitigate breaches
- Manage agent/agentless and run-time/on-demand services
- Reduce complexity and create a viable path towards tool consolidation
- Gain richer insight to asset discovery, security policy management, licensing, and more
- Easily roll up operational metrics for executive reporting and compliance requirements
- Support orchestration, automation, and cloud best practices
- Protect, investigate, and remediate security incidents via connected platform workflows

Trend Cloud Security Posture Assessment

Utilize our free assessment to scan your organization's cloud infrastructure to identify misconfigurations, compliance, and security risks based on common standards and practices.

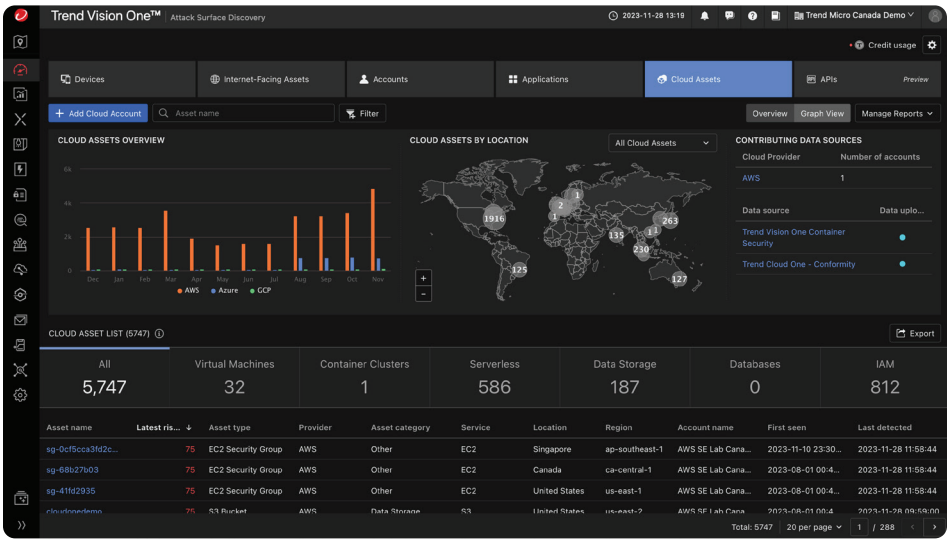
Trend Vision One™ – Attack Surface Risk Management for Cloud (ASRM for Cloud)

Take charge of your cyber risk with cloud-focused internal and external attack surface discovery, assessment, risk prioritization, and remediation. ASRM for Cloud delivers bespoke hybrid cloud telemetry correlation, facilitating faster detection and response while empowering cloud and security teams to consistently uncover, identify, and prioritize risks. These capabilities enable you to take swift, data-driven actions to proactively mitigate risk and reduce your attack surface.

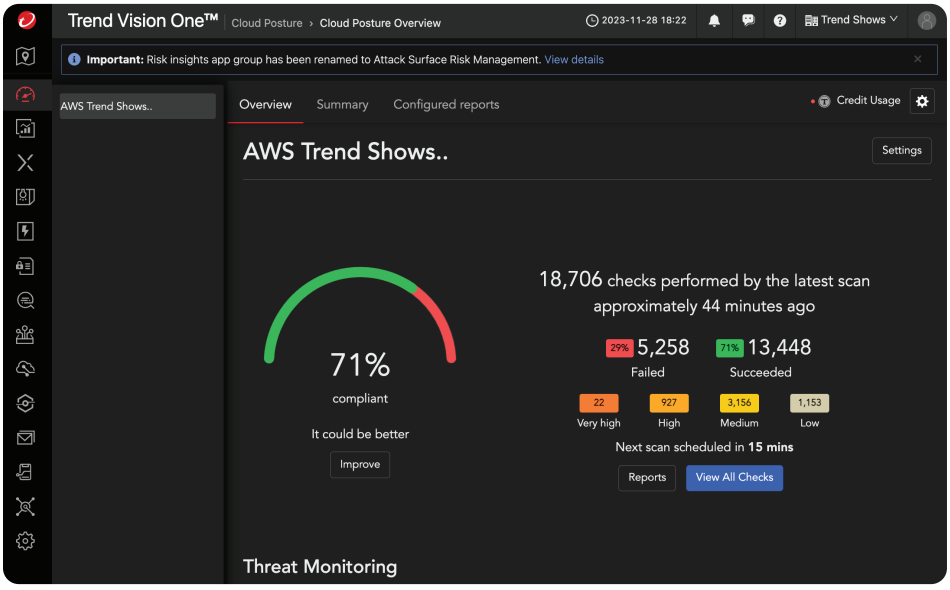
Turn visibility into decisions

- Obtain a high-level view of your organization's overall security posture, scanning against 900+ AWS and Azure rules
- Identify, prioritize, and remediate high-risk violations, misconfigurations, overly permissive identity and access management (IAM) policies, and compliance risks
- Customize regular infrastructure checks and directly apply them to over 30 compliance regulations and best practices, complete with exportable reports for audits
- Infrastructure as code (IaC) template scanning shifts security and compliance checking left, improving code and enabling innovation
- Graph asset connections to one another to analyze potential attack paths, helping to mitigate potential breaches

Cloud attack surface discovery in Trend Vision One™



Cloud posture overview in Trend Vision One



> Trend Micro focuses broadly on all security aspects of multi-cloud, not just one small piece which is really important to us.

René Joosten

Enterprise Architect
at KNMI

Trend Vision One™ – XDR for Cloud

Stop adversaries faster with a broader perspective, improved contextual awareness, and the ability to hunt, detect, investigate, and respond to threats from a single platform. XDR for Cloud extends detection and response to your customer cloud accounts by examining user, service, and resource log activity for suspicious behavior and by providing remediation and response actions.

Enhanced by our global threat intelligence, this solution is the perfect complement to Trend Vision One™ – XDR for Endpoints running either on-premises or in AWS, Azure, and GCP. In addition, you can detect, track, and investigate suspicious container activity and cross-layer threats with Trend Vision One™ – Container Security.

Streamline hybrid cloud investigations

Benefit from an expanding list of advanced cloud security models and response action across all your AWS environments. Integrate XDR for Cloud with AWS CloudTrail logs to gain insights into all user, service, and resource activity, including:

- Who or what took which action
- Which resources were acted upon
- When the event occurred

In addition, stay in front of privilege escalation attempts, policy rollbacks, master password modifications, Amazon Simple Storage Service (S3) data exfiltration attempts, multi-factor authentication (MFA) deactivations, and more. CloudTrail detection models include:

- AWS Identity and Access Management (IAM) privilege escalation through policy rollback
- AWS Relational Database Service (RDS) master password modification
- Amazon S3 bucket data exfiltration
- AWS IAM user login MFA deactivation

Empower analysts with automated response actions

- CloudTrail alerts trigger workbench activities for investigation and response
- Response actions can be automated via playbooks to revoke access to AWS resources under attack

Protection in the Cloud

Quickly identify, mitigate, and block security threats across your hybrid cloud environment by leveraging on-demand and runtime protection techniques for VMs, containers, storage, databases, and APIs.

Trend Vision One™ – Workload Security

A market-leading solution, Workload Security is purpose-built for servers and cloud workloads. Integrating advanced threat protection, detection and response, and threat intelligence, it enables you to streamline IT and security operations, reduce complexity, and achieve optimal security outcomes across your on-premises, cloud, multi-cloud, and hybrid environments.

Trend Vision One – Container Security

Container Security delivers container image security, admission control policy, runtime protection, and detection and response capabilities, ensuring the security of your containers from build to termination.

Trend Vision One™ – File Storage Security (public preview)

Get instant scanning capabilities for any file size or type. File Storage Security protects your downstream workflows from malware, integrating into your custom cloud-native processes, providing broad cloud storage platform support.

Trend Cloud Security Posture Assessment

Utilize our free assessment to scan your organization's cloud infrastructure to identify misconfigurations, compliance, and security risks based on common standards and practices.

Trend Vision One is available on AWS Marketplace, Azure Marketplace, and Google Cloud Marketplace.

Solution Overview

Trend Vision One™ – Network Security

Detect the unknown, protect the unmanaged

Network Security is More Relevant Than Ever

Your network is the foundation of your IT environment, acting as the fabric that connects users, applications, customers, and overall operations. In turn, your network is foundational for effective cybersecurity strategy, as assessing the cyber risk of your environment across all layers and defenses relies on the cyber health of your network.

According to **Verizon's 2023 Data Breach Investigation Report,** phishing makes up 44% of social engineering incidents. Unfortunately, it doesn't stop at the mailbox or endpoint. Insecure networks can then be abused to spread malware throughout your environment making the situation worse.

Network security has long been thought of as a silo of deeply technical tools, often saddling both network and security operations. With the rise of extended detection and response (XDR), a new opportunity is presented where such tools can effectively sit in both camps– delivering rich detection telemetry to advanced platforms and affecting response orchestrations, without sacrificing network performance or introducing complexity.

This combination is critical as we consider XDR as a subset. To effectively mitigate cyber risk across your entire environment both are needed. Only tightly integrated sensors and platforms across endpoints, email, cloud applications, and networks can deliver this.

Trend Vision One – Network Security

As a part of our Trend Vision One™ cybersecurity platform, Trend Vision One – Network Security delivers powerful network security capabilities that detect unknown cyber assets and protect unmanaged entities in your environment. Unlike point solutions that leave gaps in between siloed products, Network Security combines risk analysis and XDR methodologies with Trend Vision One. Your team can seamlessly surface events and orchestrate the response actions across the entire network fabric–alongside other sensors such as endpoint and email.

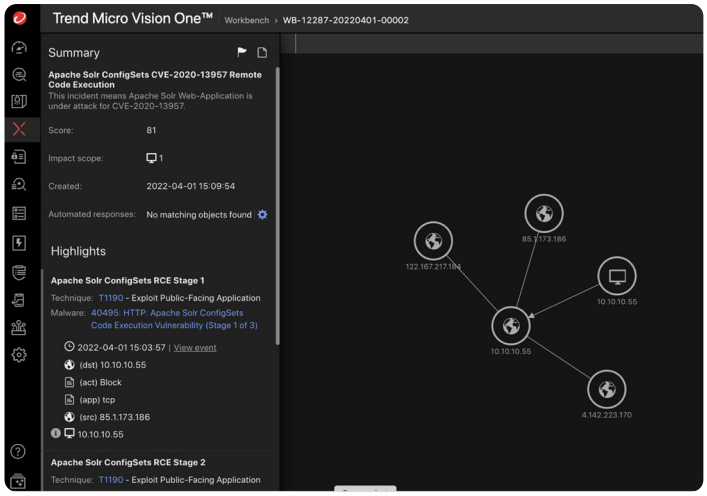
FORRESTER®
WAVE LEADER 2023
Network Analysis And Visibility

Network Security Focuses on Three Key Areas:

1. Enterprise Network

The nature of networks is changing, with control of the network fabric used to connect assets together becoming more dynamic and often less controllable. The enterprise network focuses capabilities on these new challenges in places such as public clouds (IaaS) while continuing to provide strong protection for the more well-known challenges of operating a network in the data center.

ise network begins on the strong base of vulnerability-based protection that can be performed in real-time, at line rates. Through Trend Vision One, the network telemetry from an enterprise network sensor is then analyzed alongside other sensor telemetry to surface actionable information. Tying this together is the seamless sharing of dynamic threat intelligence to provide protection at all stages of a threat's lifecycle through the network.

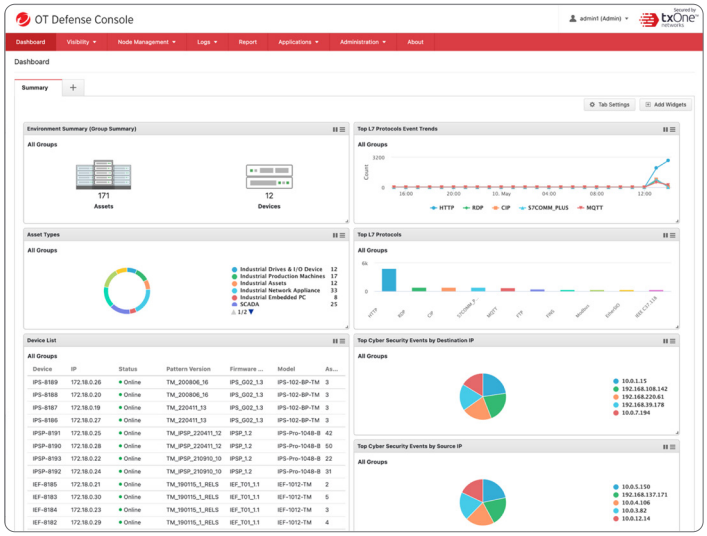


As is the nature of many networks though, standalone operations using best-of-breed technologies is a common use case where Enterprise Network continues to excel. When high performance, highly accurate network protections are needed and tight scrutiny may limit the use of SaaS solutions, you can rest assured that industry-leading capabilities are available and ready to protect your organization.

2.ICS/OT Network

Operational Technology, which includes industrial control system (ICS), communication infrastructure, and the industrial internet of things (IIoT) spans wide, requiring specialized protection. As an example, an MRI machine must be regularly updated to patch vulnerabilities. But patches are not always available, or the machine does not allow for timely updates. IIoT security can provide non-intrusive coverage until a permanent fix can be applied, leaving the organization's risk posture stronger through mitigating controls.

These types of scenarios equally apply to industrial shop floors, connected cars, private 5G networks and critical infrastructure, where downtime must be avoided. With an ICS/OT control in place, updates can more safely be incorporated into regular maintenance cycles and security posture improvements without unacceptable impacts to plant operations.

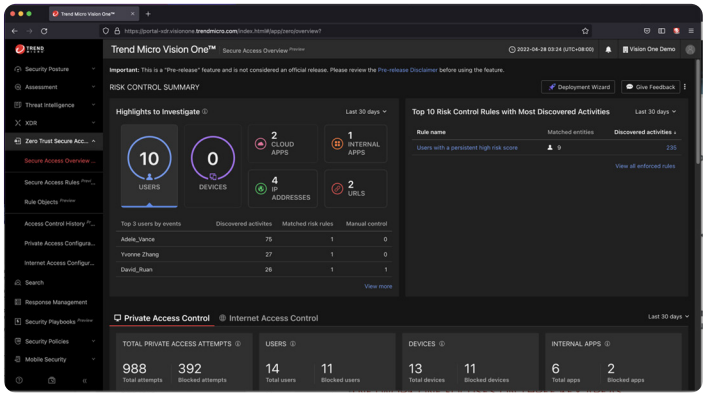


3. Secure Access Service Edge (SASE)

SASE, and industry names for similar capabilities like Security Service Edge (SSE) and Zero Trust Edge (ZTE), all drive towards the re-envisioning of trust as a part of a zero-trust architectures and methodologies.

The zero-trust methodology flips the concept of trust to assume that devices and users are untrusted until proven 'all clear'. SASE introduces continuous assessment for users and devices, automatically altering or revoking permissions dynamically if the nature of the connection or risk profiles change. With this capability, the security analyst benefits from significantly improved contextual information, and an automated solution to maintain security at the network connection level.

This risk evaluation and visibility capability is surfaced in Trend Vision One, leveraging Risk Insights and XDR. SASE components gather telemetry and limits the activity of suspicious and nefarious attempts to circumvent point product controls and the gaps that exist within them.



Building the Network Security Foundation

In the rapidly changing digital world we operate in, it is required that security strategies include the network not as a silo, but as an innate and essential component in proactive protection. As network boundaries continue to blur, protections will benefit from the underpinning network understandings being applied in new ways including in cloud environments, service edges, and organizational application edges.

As existing network controls are assessed, a view of how your organization's assets, applications, and users will interact with one another will drive projects that provide more streamlined, higher performance, and more secure connectivity. For these projects, the availability of detection and response, adoption of IoT and connectivity of OT, and workforce office locations should be contributing factors when determining how best to manage cyber security risk.

North-South, East-West Detection and Response

Enterprise network capabilities provide a strong base to block known, unknown, and undisclosed threats and monitor network segmentation implementations, reducing the blast radius if a breach does occur. Network Security offers layered and early warning defenses to protect the environment from high risks such as unmanaged endpoints–which, when compromised, spreads to higher-value managed targets. This visibility and active response capabilities help ensure that if an incident does occur, it will not cripple the entire business.

The Right Protection in the Right Place

Organizations who conflate IT and OT protection under the same product capabilities often find one or the other lacking. This is not because the products are not feature-rich and capable, it's just the nature of the infrastructure is simply different.

Taking these specially tuned, simplistically designed tools that focus on advanced security problems without disrupting business operations is a guiding principle for this capability area. Network Security and TXOne Networks allow security teams to easily take a holistic view of the entire organization across IT and OT zones, building confidence that your business is well protected and built on a solid foundation.

As Workforces Change, Maintaining Protection is a Challenge

Across the diverse network landscape, the concept of a network boundary is becoming more blurred. Existing network security capabilities can no longer provide the complete protection needed to allow access to internal network resources from users outside its boundary–because the boundary is gone. The new architecture based on zero-trust methodologies is effective but should not be viewed as a silver bullet to solve all challenges that have arisen from a shift to remote workforces.

While organizations should move towards a zero-trust strategy, early projects in this space should focus on tactical problems being faced, such as VPN overload, unsanctioned app usage, and performance issues related to network doglegs. By completing such projects over time, the journey towards zero trust becomes achievable, with meaningful security improvements along the path.

Bringing Information to the Surface to Focus Efforts and Provide Automated Action

The network sees a lot of data, including any data that is not entirely self-contained within an endpoint. Even though this data can be a source of increased visibility and context for events, the sheer volume of data would leave security teams overwhelmed. This is where XDR comes into play.

XDR ingests data from across the environment and distills it down to critical events. With network telemetry included, Trend Vision One delivers insights far beyond the limitations of endpoint detection and response (EDR) by enriching other sensor data with network context. Bringing this network telemetry to XDR can feel like a complex and expensive undertaking, even in smaller networks. Network Security combats this problem by making smart decisions on what data should be sent, and how much context is needed for it to be actionable.

Network Security, as part of our Trend Vision One cybersecurity platform, delivers intelligent detection and powerful response capabilities. As your organization migrates from point solution-based security to an XDR focus, greater resiliency against new vulnerabilities and threats will be seen and risk management-focused security strategy will be within reach.

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

Trend Vision One™ – Mobile Security

Manage Android™, Chromebook™, and iOS devices. Deploy next-generation security to safeguard against malware, malicious apps, and credential attacks

Even the savviest user can mistakenly click on a malicious link or download a malicious app, exposing your enterprise to threats. Trend Vision One™ – Mobile Security™ gives you advanced mobile threat detection and prevention, centralized visibility and management, advanced risk telemetry, and corporate data protection.

With Mobile Security, you get more

Advanced threat detection and prevention

- Protect mobile devices and detect threats faster with techniques from the MITRE ATT&CK® Matrices for Mobile
- Identify ransomware and other types of zero-day malware with pre-execution machine learning
- Share threat information with other security layers to guard against persistent and targeted attacks
- Block access to malicious and phishing websites, preventing access to malicious code and potential data leaks
- Allow IT to assess the use of risky mobile apps based on up-to-the-minute data from the MARS database
- Provide flexible management options for easy removal of apps identified as malicious or potentially risky

Reduced cost and complexity

- Manage mobile security, applications, and data protection in a single solution
- Deploy with just one click
- Unlock centralized visibility and control of all endpoint security

Improved visibility and control

- Enable IT teams to track, monitor, and manage mobile devices, apps, and data through a single console
- Gain visibility on the number, types, and configuration of devices accessing corporate resources, whether they are enrolled or not
- Determine risk level of devices and users by correlating mobile telemetry with endpoint, network, email, and directory services in the same console

Mobile Device Director

- Gain easy deployment and control without the need for a third-party MDM solution
- Improve mobile device control, visibility, and security via access permissions and security policies management, monitoring, and enforcement
- Combine deployment, enforcement, and security solution for mobile devices

Key features

- **Centralized management and policy enforcement:** Reduce silos and streamline administration with a single view for enterprise users, device location tracking, inventory management, and deployment of data protection policies in just one click.
- **Greater visibility:** Get instant summary views of compliance, inventory protection, and the health of all devices. Mobile Security also provides visibility into the number, types, and configuration of devices that are accessing corporate resources.
- **Threat prevention and detection:** Add leading malware and phishing protection, powered by the Trend Micro™ Smart Protection Network™, to identify access to malicious codes and websites.
- **Mobile Application Reputation Service (MARS):** Identify and block apps that pose security, privacy, and vulnerability risks by correlating installed app data with the MARS database.
- **Integration with mobile device management (MDM) solutions:** Mobile Security provides flexible and centralized unified endpoint management options. Integrate with your third-party MDM solution or use our MDD for easy deployment and control without the need for a third-party MDM.
- **Advanced risk telemetry:** Automatically pull risk data from mobile devices for threat detection and response, as well as continuous risk assessment of devices and users. Correlate risk data across email, endpoint, network, cloud, and identity.

Part of our unified cybersecurity platform

Mobile Security is part of Trend Vision One™, giving your organization the ability to holistically manage security with comprehensive prevention, detection, and response capabilities—powered by AI and leading threat research and intelligence.

- **Attack surface risk management (ASRM):** Mobile Security sends mobile device posture, application rating, and user behavior to Trend Vision One™ Risk Insights. Get a centralized view of your organization's attack surface. View your inventory, check detections, take risk mitigation actions, and manage policies for your endpoints all in one place.
- **Extended detection and response (XDR):** Extend XDR to mobile, including Android, iOS, and ChromeOS devices. Mobile device information feeds into Trend Vision One XDR to dramatically improve your ability to detect, investigate, and respond to threats across your environment. One consolidated and centralized view to uncover events and the attack path across endpoints, servers, cloud workloads, and other security layers enables your organization to respond faster and limit the impact of events.
- **Zero trust:** Introduce trust-based access for sanctioned and unsanctioned apps. Trend Micro™ Zero Trust Secure Access uses device posture from Mobile Security to continuously assess risk and automatically block risky users.

Trend is the only vendor that natively integrates XDR, ASRM, and security for endpoint, email, mobile, cloud, network, and OT in one platform—managed through a single console.

Feature Summary – Trend Vision One™ – Mobile Security™

Centralized Management	• Via Trend Vision One console
Advanced Protection	• Known threats • Phishing attempts • Malware • Wi-fi vulnerabilities • Malicious apps and websites
Operating System Posture and Support	• Support for Android, ChromeOS, iOS • Out-of-date OS notifications • OS vulnerability mapping
Integration with Mobile Device Management Solutions	• Microsoft Intune • VMWare Workspace One • Google Workspace Endpoint Management • And more
Advanced Security and Management Capabilities	• XDR • ASRM • Zero Trust Secure Access • Mobile Device Director

Proven leadership

- AV-Test Awards. First place in Android protection for the fifth consecutive year (2023)
- A Leader in Gartner© Magic Quadrant™ for EPP since 2002, 18 times in a row
- A Leader in The Forrester Wave™: Endpoint Security, Q4 2023. Five times in a row
- A Leader in The Forrester New Wave™: XDR, Q4 2021 with the highest score in Current Offering category