TREND ™ MICRO

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

Trend Vision One – Email and Collaboration Security

- Protection for Microsoft 365 and Google Workspace
- Protection for email gateway
- Protection for collaboration applications
- Visibility into on-premises email solutions
- Email XDR and ASRM

Microsoft 365

Google Workspace

Dropbox

box

Unified experience for better understanding of the full attack story.

Instant access to advanced capabilities to stop phishing, ransomware, and BEC attacks.

Centralized visibility and management across API + inline + gateway email protection.

XDR for Email for advanced analytics with automated remediation and response.

ASRM for continuous risk assessment, prioritize and mitigate risks in real time.

TREND MICRO™

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
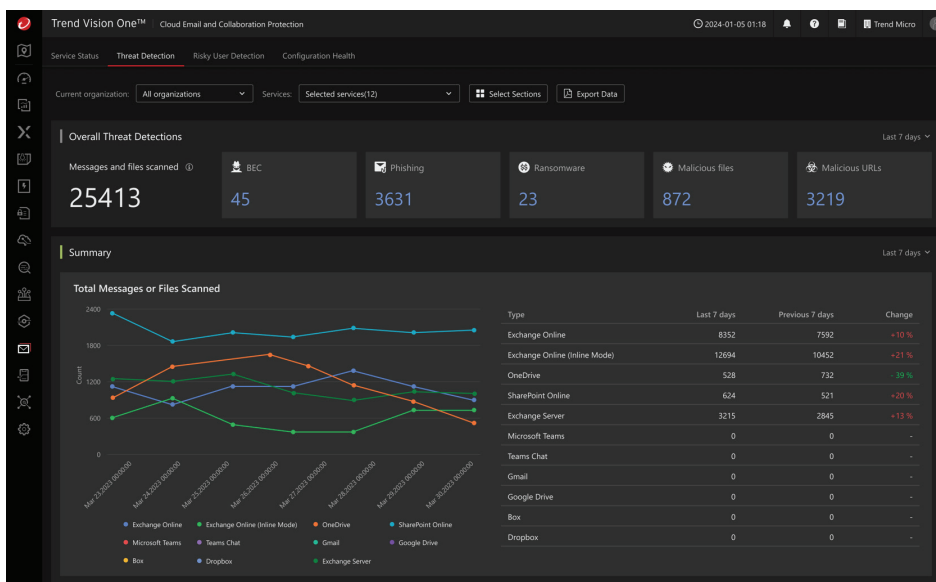
Solution architecture

Email Inline and Mailbox Protection

TREND™ MICRO
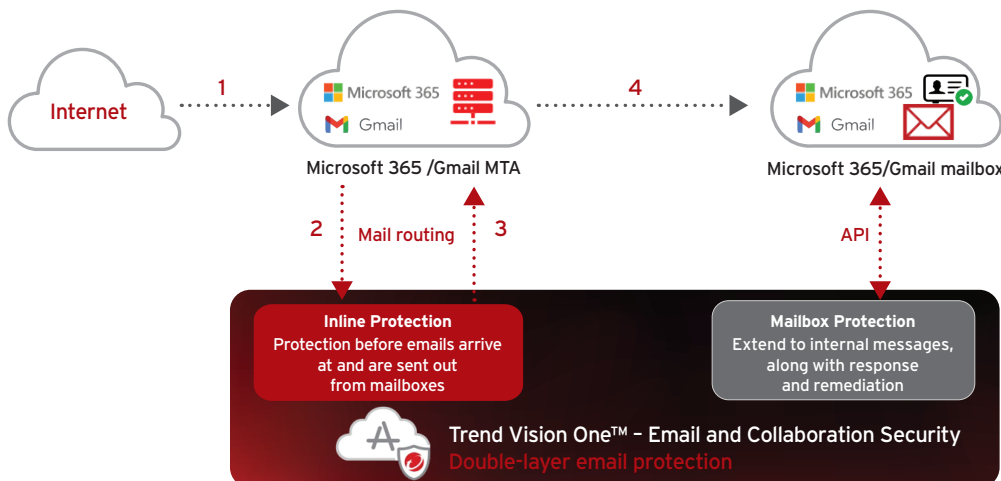
Features and specifications:

	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	✓	

TREND™ MICRO

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.

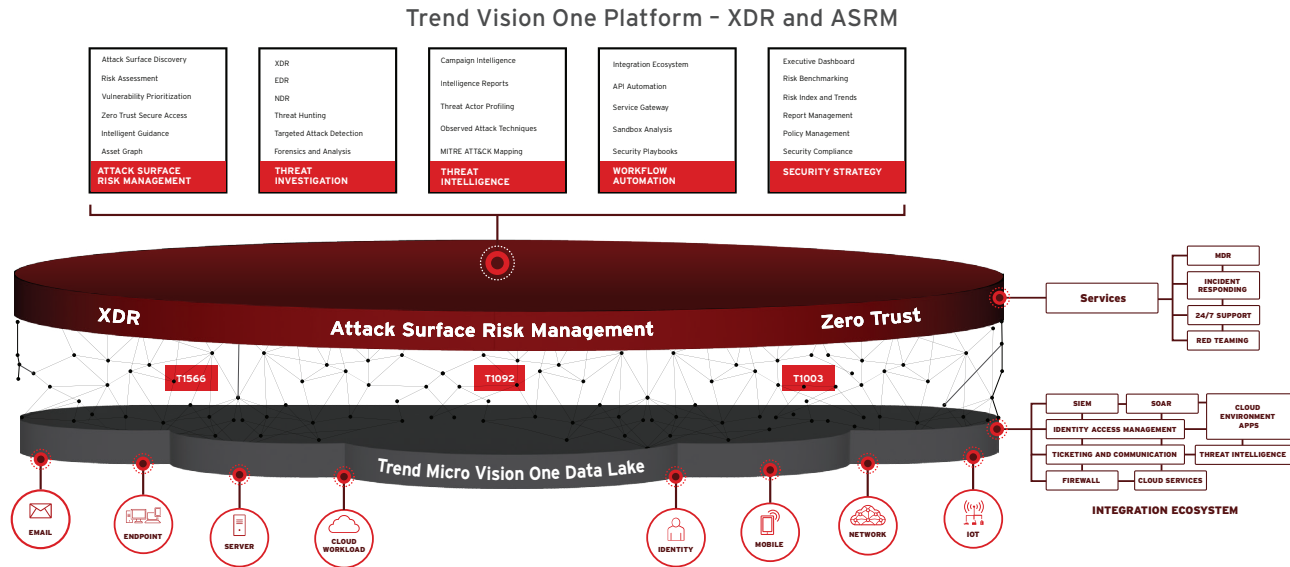### Prioritize your response with XDR for Email

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

Attack Surface Discovery	XDR	Campaign Intelligence	Integration Ecosystem	Executive Dashboard
Risk Assessment	EDR	Intelligence Reports	API Automation	Risk Benchmarking
Vulnerability Prioritization	NDR	Threat Actor Profiling	Service Gateway	Risk Index and Trends
Zero Trust Secure Access	Threat Hunting	Observed Attack Techniques	Sandbox Analysis	Report Management
Intelligent Guidance	Targeted Attack Detection	MITRE ATT&CK Mapping	Security Playbooks	Policy Management
Asset Graph	Forensics and Analysis			Security Compliance
ATTACK SURFACE RISK MANAGEMENT	**THREAT INVESTIGATION**	**THREAT INTELLIGENCE**	**WORKFLOW AUTOMATION**	**SECURITY STRATEGY**

XDR · **Attack Surface Risk Management** · **Zero Trust**

T1566 · T1092 · T1003

Trend Micro Vision One Data Lake

EMAIL · ENDPOINT · SERVER · CLOUD WORKLOAD · IDENTITY · MOBILE · NETWORK · IOT

Services — MDR / INCIDENT RESPONDING / 24/7 SUPPORT / RED TEAMING

SIEM · SOAR · CLOUD ENVIRONMENT APPS
IDENTITY ACCESS MANAGEMENT
TICKETING AND COMMUNICATION · THREAT INTELLIGENCE
FIREWALL · CLOUD SERVICES
INTEGRATION ECOSYSTEM

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.