Trellix

DATASHEET

Trellix Email Security – Cloud

Comprehensive enterprise communication and collaboration security

Email connects customers, suppliers, partners, and coworkers—and continues to be the most successful attack vector. Over 90 % of cyberattacks begin with phishing. Cybercriminals use targeted social engineering to trick users into clicking malicious URLs and opening compromised attachments. And as companies extend collaborative platforms and enterprise applications to transform partner relationships, threat actors are already exploiting this largely unprotected attack vector.

Solution Overview

Trellix provides the industry's most comprehensive enterprise communication and collaboration security solution. Our flexible deployment models offer both secure email gateway (SEG) and

Highlights

- Comprehensive inbound and outbound email security
- Cloud-native API-enabled integration with Microsoft 365 and Google Workspace
- Automatically extract emails weaponized post-delivery
- Deployed in inline, hygiene (ASAV) or out-of-band modes.
- Metadata streaming to third party SIEM solutions
- Carrier-grade reliability with 99.995% availability
- Supports custom YARA rules to enhance threat detection efficacy
- Meets the FedRAMP security and SOC2 requirements
- Ability to monitor email queues and advanced debugging options using email trace

integrated cloud email security (ICES) solutions to secure email infrastructure and collaboration tools to minimize the risk of costly breaches.

Trellix Email Security – Cloud offers industry-leading detection to identify, isolate, and immediately stop ransomware, business email compromise, spear phishing, impersonation, and attachment-based attacks before they enter your environment. Email Security – Cloud also scans outgoing email traffic for advanced threats, spam, and viruses.

Integrated investigation and response ensure alignment with your overall security operations program. Features like auto remediation for Microsoft 365 and Google Workspace, automatically extract emails weaponized post-delivery.

Use the Trellix portal to view real-time alerts, create smart custom rules and generate reports. Email Security – Cloud offers over 1,000 smart custom rules so you can customize policies and rules based on multiple granular conditions.

Trellix Email Security-Cloud is carrier grade resilient providing 99.995% availability and an average email processing time of less than 10 seconds. Active-active AWS deployment ensures against individual AWS region failures. The FedRAMP Moderate certification assures public sector customers their sensitive data is properly protected.

Trellix Email Security, paired with Trellix Intelligent Virtual Execution (IVX) provides a comprehensive enterprise communication and collaboration security solution, spanning email infrastructure, enterprise applications, and collaboration platforms ensuring people can work together securely across the extended enterprise.

Email Security – Cloud is an integral part of the Trellix learning and adaptive ecosystem. Trellix continuously monitors the threat landscape, correlating threat data gathered from more than 40k enterprise customers, technology partners, and service provider networks around the world, ensuring you stay ahead of known and emerging threats.

Key capabilities

Superior threat detection

Attackers use multi-stage campaigns, designed to evade email infrastructure providers. For example, in multi-staged phishing campaigns, attackers first steal credentials then use the stolen credentials to login to Microsoft 365 and distribute phishing emails throughout the organization. While ransomware attacks start with an email, a callback to a command-and-control server is required to encrypt the data.

Figure 1. Trellix Email Security – Cloud as a secure email gateway

Email Security – Cloud offers multiple detection techniques, powered by cutting-edge machine learning, artificial intelligence, and security analytics, providing unparalleled defense against multi-stage campaigns.

Email Security – Cloud analyzes every email attachment and URL to identify threats hidden in:

- All attachment types, including EXE, DLL, PDF, SWF, DOC/ DOCX, XLS/XLSX, PPT/PPTX, JPG, PNG, MP3, MP4, and ZIP/RAR/TNEF archives
- Password-protected and encrypted attachments
- Credential-phishing and typo squatting URLs
- URLs embedded in emails, PDFs, and Microsoft Office documents
- OS, browser, and application vulnerabilities
- Malicious code embedded in spear-phishing emails

Advanced URL Defense

Phishing is popular among attackers because cybercriminals can use targeted social engineering to trick almost any user into clicking a URL. Email Security – Cloud offers multiple advanced URL defense techniques to identify malicious URLs, protecting your organization from credential harvesting and spear-phishing attacks.

PhishVision is an image classification engine that uses deep learning to compile and compare screenshots of trusted and commonly targeted brands against web and login pages referenced by URLs in an email.

Working in tandem with PhishVision, Kraken is a phishing detection plug-in that applies domain and page content analytics to augment machine learning. While PhishVision looks at screenshots from a comparison perspective, Kraken performs extensive inspection and analysis of new page content compared to known phishing knowledge base.

Skyfeed is a successful intelligence gathering system that collects social

media accounts, blogs, forums, and threat feeds for malware-based attacks. Skyfeed tracks these sites for malicious URLs that point to objects with malware payloads, command and control domains and black listed URLs for malware.

Attackers use deferred phishing to send benign emails that pass inspection, then update the emails with malicious URLs once delivered. Trellix protects users from deferred phishing by rescanning emails to identify URLs weaponized post-delivery. Malicious emails are automatically extracted from users' inboxes using an auto remediate policy and Microsoft 365 and Google Workspace APIs.

Impersonation protection

CEO fraud and impersonation attacks also rely on social engineering techniques, rather than malicious attachments or links. Therefore, Trellix offers dedicated detection engines specializing in impersonation detection and defense.

A common indicator of an email attack is the age of the sender's domain. When creating an impersonation campaign, adversaries send attack emails from a domain similar to that of the person or company they are impersonating, usually within a few hours of that domain's creation. Email Security – Cloud labels newly existing and newly observed domains as suspicious and further inspect emails for other attack indicators, such as typo-squatting.

Spoofing is when adversaries change the sender display name, so the email appears to come from a trusted source. Trellix defends against email spoofing by checking the authenticity of sender display names and email addresses in addition to examining content for other malware-less impersonation tactics.

Malware protection

Trellix Intelligent Virtual Execution (IVX) helps further defend your organization from phishing and ransomware by detonating all email attachments and URLs to determine if previously legitimate files have been weaponized.

> Email is fundamental to all collaborative environments, so deploying [Trellix] Email Security – Cloud gives us the ability to mitigate the risks of compromise from this highly exploited channel using a single solution. ”
>
> — Nils Göldner, Managing Partner and Cloud Advisor Blackboat GmbH

IVX is a signature-less, dynamic intelligence-driven analysis engine that inspects suspicious objects using real-time multi-flow, multi-vector analysis to identify and block targeted, evasive and emerging threats.

Email Security – Cloud is also available with anti-spam and antivirus (AVAS) protection to detect both common attacks that use conventional signature matching and impersonation techniques.

Outbound email protection

Email Security – Cloud detects unknown advanced threats, including malicious attachments and phishing URLs delivered via outbound email messages. It also scans outgoing email traffic for malware and spam to protect your organization's domains from being blacklisted.

Integrated Detection, Investigation, and Response

Security threats are more dynamic and sophisticated than ever. Static, siloed solutions are simply not enough to protect your businesses.

Email Security – Cloud is an integral part of the Trellix learning and adaptive ecosystem. The Trellix ecosystem continuously monitors the threat landscape, correlating threat data gathered from customer, technology partner, and service provider networks around the world.

Our artificial intelligence algorithms, machine learning models, and security analytics use this threat intelligence to strengthen threat prevention and detection at the speed of the adversary, so you stay ahead of known and emerging email-borne threats.

Trellix Email Security – Cloud enables integrated investigation and response to align with your larger security operations program. Analysts can perform retrospective analysis by searching for newly identified IOCs in previously received emails to quickly identify the source of a compromise. Analysts can also claw back emails weaponized post-delivery, simplify and accelerating incident response.

Elite intel analysts from Trellix's Advanced Research Center actively track vulnerabilities and malware campaigns—and the nation-states and malicious actors behind them—providing rich contextual intelligence to inform and accelerate response.

Trellix threat intelligence helps:

- Identify and block known, and emerging email-borne threats with minimal false positives
- Identify specific capabilities and features of detected malware and malicious attachments
- Provide contextual insights to prioritize and accelerate response
- Determine the probable identity and motives of an attacker so you can track their activities within your organization
- Retroactively identify spear phishing attacks and prevent access to phishing sites by rewriting malicious URLs

Gain real-time protection from multi-vector, multi-staged attack using Trellix XDR, or other third party SIEM/XDR providers, to correlate email alerts with rich metadata with signals from endpoint, network and other security controls.

Easy deployment and resilient protection

Trellix Email Security offers flexible deployment models including both secure email gateway (SEG) and integrated cloud email security solution (please note, Gartner uses the acronym ICES, while Forrester prefers cloud-native, API-enabled solution (CAPES)).

Email Security – Cloud simplifies migration to the cloud, integrating natively with cloud-based enterprise email infrastructure solutions such as Microsoft Office 365 with Exchange Online Protection and Google Workspace.

To protect against malicious emails organizations simply route messages to Email Security – Cloud, which analyzes the emails for spam, known malware and impersonation tactics first. Then uses advance URL defense techniques and IVX signature-less, dynamic intelligence-driven analysis to inspect URLs and attachments to stop advanced attacks in real time.

Organization may select to deploy Email Security – Cloud in active protection or monitor-only mode. For active protection simply update your mail exchanger (MX) records to route messages to Trellix. For monitor-only deployments, set up a transparent BCC rule to send copies of emails to Trellix for analysis.

Trellix offers email journaling for organizations working under compliance regulations that require recording and retention of communication records.

Trellix Email Security-Cloud is carrier grade resilient providing 99.995% availability and an average email processing time of less than 10 seconds. Active-active AWS deployment ensures against individual AWS region failures. FedRAMP Moderate certification assures public sector customers their sensitive data is protected.

Extend protection with Collaboration Security

Collaboration platforms such as slack, box, Microsoft Teams and Google Workspace have transformed both the nature and velocity of collaboration. We now freely share information with co-workers and external partners — increasing an organization's risk exposure by providing attackers an easy on-ramp to the network.

Trellix Email Security, paired with Trellix Intelligent Virtual Execution (IVX) provides a comprehensive enterprise communication and collaboration security solution, spanning enterprise email infrastructure, collaboration

Authorization and compliance certifications

ISO 27001

Trellix Email Security – Cloud meets the ISO 27001 information security standard that ensures data centers are securely managed.

FedRAMP

Email Security – Cloud with AVAS protection meets the FedRAMP security requirements for cloud services operated by government and public education entities.

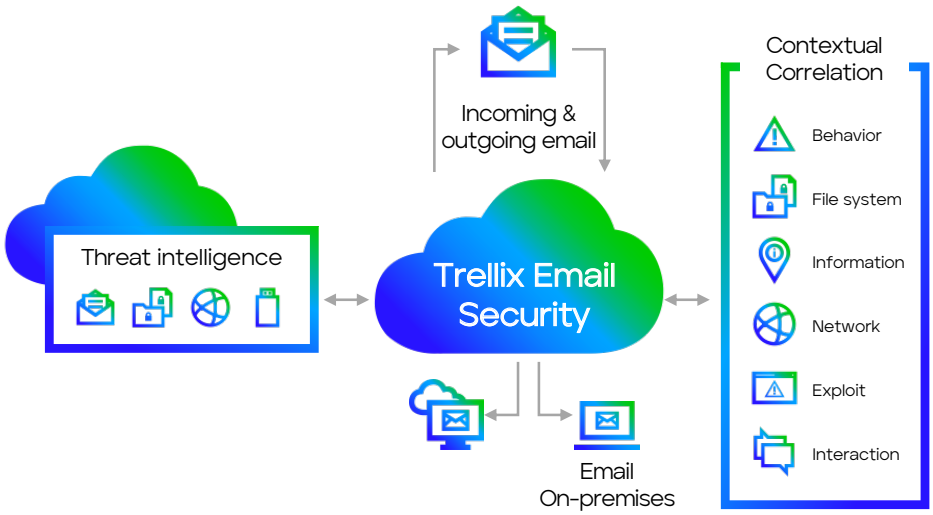
SOC 2 Type 2

Email Security – Cloud also complies with the American Institute of Certified Public Accountants (AICPA) Service Organization Controls (SOC 2) Type 2 Certification for Security and Confidentiality.

platforms, and enterprise applications, ensuring people can work together securely across the extended enterprise.

Trellix Intelligent Virtual Execution (IVX) offers:

- Dozens of out-of-the box integrations to popular applications such as slack, box, Salesforce, Microsoft Azure, and Google Workspace, ensuring quick time to value using a single solution.
- Automatic, unobtrusive file inspection so employees and partners can confidently collaborate without fear of unintentional compromise
- High-fidelity alerts ensure the SOC is notified only when malware detected
- Rich contextual information help defenders visualize how malware is acting within the virtual image, with evidence mapped to the MITRE ATT&CK framework



Learn more about Trelix Email Security – Cloud at https://www.trellix.com/en-us/platform/email-security.html

Trellix
6220 American Center Drive
San Jose, CA 95002
www.trellix.com

Visit Trellix.com to learn more.

About Trellix

Trellix is a global company redefining the future of cybersecurity. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix's security experts, along with an extensive partner ecosystem, accelerate technology innovation through machine learning and automation to empower over 40,000 business and government customers.