Trellix

DATA SHEET

Trellix® Email Security - Cloud

Adaptive protection that identifies, analyzes, and blocks email attacks

Highlights

- Offers comprehensive inbound and outbound email security
- Consolidates your email security stack with a comprehensive single vendor solution
- Supports custom YARA rules to enhance threat detection efficacy
- Enables Microsoft 365 Auto Remediate to remove emails that become malicious after delivery
- Integrates with any third-party email provider
- Provides in-depth knowledge about attacks and attackers from frontline investigations and observations of adversaries
- Meets the FedRAMP security requirements
- Natively integrates with Microsoft 365 and Google Workspace to provide seamless scanning of emails and instant protection against missed threats

Overview

To thrive, your organization needs a free flow of information. Email is a prime channel for most companies to connect with customers, suppliers, partners, and coworkers. Today there's a proactive way to keep email communications secure, so your company can focus on growing the business.

Most advanced threats arrive by email in the form of URLs linked to credential-phishing sites, fraudulent wire transfer requests, and weaponized file attachments. Email's highly targeted and customizable nature allows cybercriminals to successfully exploit it, making it the primary channel for cybercrime.

Trellix Email Security – Cloud reduces costs and increases employee productivity while minimizing the risk of costly breaches caused by advanced email attacks. This adaptive security tool continually learns about the threat landscape, absorbing an array of intelligence inputs to feed artificial intelligence/machine learning analytics that detect and counteract email threats before they can take hold.

Deployed in the cloud, Email Security – Cloud is a fully-featured secure email gateway that leads the industry in identifying, isolating, and immediately stopping URL, impersonation, and attachment-based attacks before they enter your environment. With features like auto remediation in Microsoft 365, emails that become retroactively malicious after delivery to a user's inbox can be extracted. Email Security – Cloud also scans outgoing email traffic for advanced threats, spam, and viruses.

Using a combination of intelligence-led context and detection plug-ins, Trellix unearths malicious URLs on a big data, scalable platform. Sender names and email addresses are checked for authenticity and content is examined for impersonation tactics to stop CEO fraud and

other malwareless attacks. The signatureless Trellix Multi-Vector Virtual Execution (MVX) engine analyzes email attachments and URLs against a comprehensive cross-matrix of operating systems, applications, and web browsers. Threats are identified with minimal noise, and false positives are nearly nonexistent.

Trellix collects extensive threat intelligence on adversaries through firsthand breach investigations and millions of sensors. Email Security – Cloud draws on this real evidence and contextual intelligence about attacks and bad actors to prioritize alerts and block threats in real time.

By integrating with additional Trellix extended detection and response (XDR) products, you can get broad visibility into multivector blended attacks and coordinate real-time protection.

Trellix Email Security – Cloud features

With personal information readily available online, a cybercriminal can use social engineering to trick almost any user into taking an action, clicking a URL, or opening an attachment.

Email Security – Cloud provides real-time detection and protection against credential harvesting, impersonation, and spear-phishing attacks that typically evade traditional email security services. Emails are analyzed and quarantined (blocked) if unknown and advanced threats are found 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 typosquatting URLs
- URLs embedded in emails, PDFs, and Microsoft Office documents
- OS, browser, and application vulnerabilities
- Malicious code embedded in spear-phishing emails

While ransomware attacks start with an email, a callback to a command-and-control server is required to encrypt the data. Email Security – Cloud identifies and stops these hard-to-detect multistage malware campaigns.

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

Superior threat detection

Trellix Email Security – Cloud helps mitigate the risk of breaches by identifying and isolating advanced, targeted, and other evasive attacks camouflaged as normal traffic, and analyzing and fingerprinting them for faster identification of future threats.

Advanced URL Defense and the MVX engine use cutting-edge machine learning and analytics to identify attacks that evade traditional signature and policy-based defenses.

An integral part of Advanced URL Defense, 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.

Another advance in URL detection is Skyfeed, a purpose-built, fully automated malware intelligence gathering system incorporated into Email Security – Cloud. Skyfeed collects social media accounts, blogs, forums, and threat feeds for false negative discovery. The multifaceted nature of Advanced URL Defense helps your organization stay safe from credential harvesting and spear-phishing attacks.

An email may start out as benign to get past security defenses and only become malicious after it's been delivered to a recipient's inbox. Email Security – Cloud retroactively analyzes and alerts you when an email becomes malicious post-delivery. Via the Microsoft 365 and Google Workspace APIs, Email Security – Cloud automatically extracts these emails from users' inboxes by creating an auto remediate policy.

The MVX engine detects zero-day, multiflow, and other evasive attacks by using dynamic, signatureless analysis in safe virtual environments. It stops the infection and compromise phases of an attack chain by identifying never-before-seen exploits and malware.

Enhanced AVAS protection

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

Email Security – Cloud also relies on dedicated detection engines to help guard against impersonation attacks, such as CEO fraud (often called business email compromise), which continue to significantly impact businesses financially. This is due in part to the lack of traditional threat indicators, such as malicious attachments or links, because the attacks are malware-free and rely on social engineering techniques. To combat these attacks and protect customers, Trellix has developed innovative algorithms, systems, and tools specializing in impersonation detection and defense.

"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

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 can accurately determine the age and maturity of a domain using in-house developed Newly Existing Domain (NED) and Newly Observed Domain (NOD) tools. It treats NEDs as suspicious and extensively inspects them for other attack indicators, such as typosquatting and sender display or username spoofing.

Instead of going through the process of buying and registering a domain, adversaries often change the display name or sender's username, so the email appears to come from a trusted source. Email Security – Cloud defends against this sender spoofing by determining each display name and username's authenticity using friendly name identification.

Outbound scanning

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.

Email Security Cloud also helps prevent data leaks and stop exfiltration of sensitive information over email with integrated Trellix DLP policy control. API-based integration with Trellix DLP extends enterprise class data security to email communications that is easy to deploy and enables email system administrators to monitor data events in real-time directly from the Email Security Cloud console.

Integration to improve alert handling efficiencies

Trellix Email Security – Cloud analyzes every email attachment and URL to accurately identify today's advanced attacks. Real-time updates from the entire Trellix security ecosystem combined with attribution of alerts to known threat actors provide context for prioritizing and acting on critical alerts and blocking advanced email attacks. Known, unknown, and non-malware-based threats are identified with minimal noise and false positives, so you can focus on real attacks. This helps reduce your operational expenses.

Rapid adaptation to the evolving threat landscape

Your organization can rely on Email Security – Cloud to continually adapt, providing a proactive defense against email-borne threats. Email Security – Cloud creates its own threat intelligence rather than relying on third-party feeds. In-house, email-specific threat intelligence (or Smart DNS), data collection capabilities, email security experts, and threat analysts provide the underlying infrastructure for enhanced antispam technologies and impersonation detection. Trellix uses deep intelligence about threats and attackers with adversarial, machine, and victim intelligence to:

- Deliver timely and broad threat visibility
- 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 and track their activities within your organization
- Retroactively identify spear-phishing attacks and prevent access to phishing sites by rewriting malicious URLs

Use the Trellix portal to view real-time alerts, create Smart Custom Rules, and generate reports. With Smart Custom Rules, you can make policies and rules based on multiple granular conditions.

Response workflow integration

Trellix Email Security – Cloud works with several other solutions to help automate alert response workflows.

Trellix Central Management System correlates alerts from both Email Security – Cloud and Trellix Network Security to get a broad view of an attack and set blocking rules to prevent the attack from spreading.

Helix works smoothly with Email Security – Cloud and is specifically designed to simplify, integrate, and automate security operations.

Easy deployment and cross-enterprise protection

Email Security – Cloud is fully cloud-based, and has no hardware or software to install. It's ideal when your organization is migrating its email infrastructure to the cloud and no longer needs to procure, install, and manage a physical infrastructure.

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.

Email Security – Cloud integrates seamlessly with cloud-based email systems, such as Microsoft Office 365 with Exchange Online Protection and Google Workspace.

To protect against malicious and fraudulent emails, simply route messages to Email Security – Cloud, which analyzes them for spam, known malware, and impersonation tactics first. It then uses the URL defense technology and signatureless detonation chamber MVX engine to analyze every attachment and URL for threats and stop advanced attacks in real time.

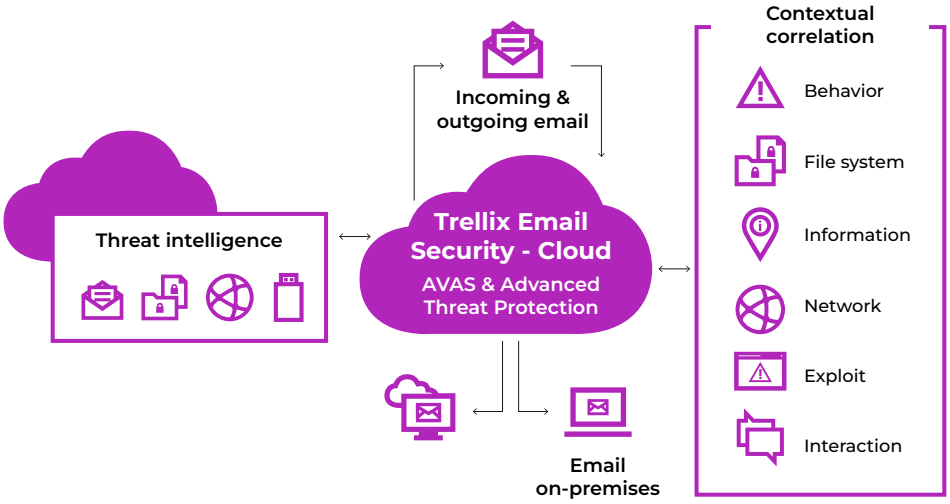
Additional capabilities

YARA-based rules enable customization

Email Security – Cloud enables analysts to use custom YARA rules to manage and enhance detection, stop the latest threats, and identify ongoing campaigns.

Active-protection or monitor-only mode

Email Security – Cloud can analyze emails and quarantine threats 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 MVX analysis.



Learn more about Trellix Email Security – Cloud at trellix.com.

Copyright © 2024 Musarubra US LLC