DATA SHEET

Trellix Email Security – Cloud

Full Hygiene option

Overview

Email is the main entry point for most cyberattacks because it can be highly targeted and customized to increase the odds of exploitation. While the ability to detect malicious file attachments and URLs provides a solid base of protection from email threats, it doesn't offer comprehensive security. Sophisticated impersonation email attacks and spear-phishing campaigns require more robust detection capabilities to stay ahead of evolving threats.

Trellix Email Security – Cloud offers two protection options: Advanced Threat and Full Hygiene.

The **Advanced Threat** option leads the industry in identifying, isolating, and stopping URL and attachment-based attacks before they enter your organization's environment. It combines intelligence-led context and detection plug-ins to unearth malicious phishing URLs on a big data, scalable platform.

The **Full Hygiene** option can detect and stop not only advanced malicious files and URLs, but also the most highly targeted and sophisticated impersonation and business email compromise (BEC) attacks and spear-phishing campaigns.

Benefits of Full Hygiene

- Reduce the risk of business disruption, wire transfer fraud, loss of critical assets, and reputational damage that begins with an email threat
- Improve defense against impersonation attacks, spear-phishing, and ransomware
- Ensure confident, secure cloud email migration through seamless integration with trusted solutions such as Microsoft 365
- Increase security team productivity and focus on growth and profitability rather than responding to cyber incidents
- Maintain mandatory compliance and privacy laws applicable to your organization

Table 1. Comparison of Advanced Threat and Full Hygiene options

Feature	Advanced Threat*	Full Hygiene
Malicious file attachments scan	✓	✓
Malicious URL rewrite and scan	✓	✓
VX Engine (dynamic file and URL analysis)	✓	✓
Trellix Dynamic Threat Intelligence	✓	✓
Remediation on demand (automatic or manual for Microsoft 365)	✓	✓
Advanced reporting via Trellix Helix	✓	✓
Antispam and unwanted bulk email detection	—	✓
BEC protection (dynamic classification and machine learning)	—	✓
Outbound email scan	—	✓

*Trellix Email Security – Cloud with the Advanced Threat option can only be deployed behind a third-party secure email gateway (SEG).

At the core of both options is the Trellix Virtual Execution (VX) engine. VX analyzes emails using machine learning and analytics to identify attacks that evade traditional signature- and policy-based defenses. It identifies and blocks threats with minimal disruption, and false positives are nearly nonexistent.

Deployment options

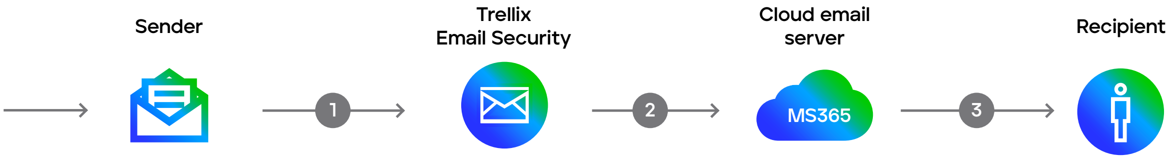


Figure 1. Trellix Email Security with Full Hygiene as the primary secure email gateway

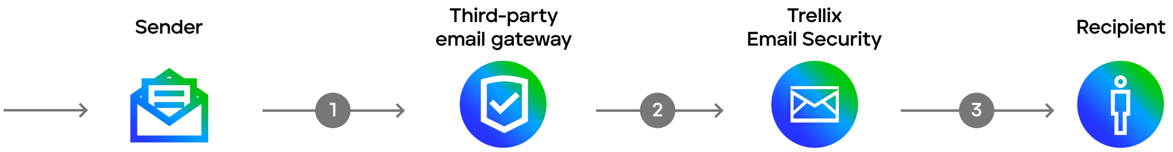
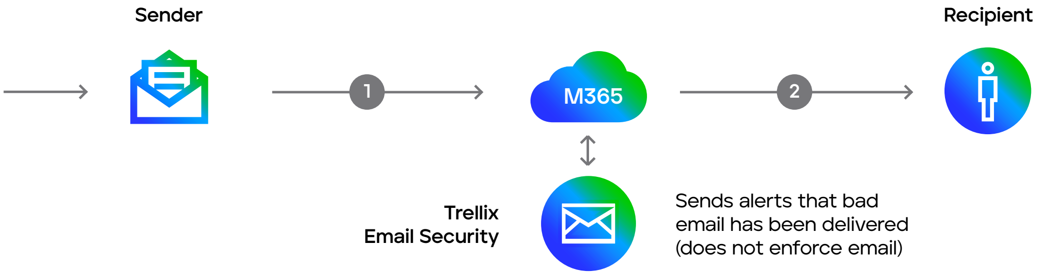


Figure 2. Trellix Email Security with Full Hygiene inline, second hop, positioned behind a third-party gateway with no mail flow enforcement



Sends alerts that bad email has been delivered (does not enforce email)

Figure 3. Trellix Email Security with Full Hygiene in BCC mode

SEG Requirements

- Advance threat detection
- Deep relationship analysis
- AV/AS filtering
- Impersonation detection

The ever-changing threat landscape requires your organization to understand your threat profile. You need to know which assets are at risk and focus on rapid threat detection and response to resolve incidents quickly. To remain mission-focused and minimize risk, your email security solution should detect and block the most advanced email threats the first time they're observed.

The Advanced Threat option for Email Security – Cloud provides dynamic detection and superior protection against advanced threats containing malicious attachments and URLs. With the Full Hygiene option, you gain comprehensive email protection to address everything from unwanted email to evolving threats, such as impersonation email attacks and spear-phishing.

To learn more about Trellix, visit trellix.com.

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

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.