Eliminate the Advanced Email Threats that Evade Detection

Email attacks continue to succeed because threat actors keep developing new techniques that bypass both traditional and "next-generation" security controls, leaving your email systems at risk. Cloud email, such as Office 365 and Gmail, cannot stop advanced threats.

The native email protection in Office 365 Mail and Gmail cannot detect and block sophisticated threats such as ransomware, credential stealers, spear-phishing, business email compromise (BEC), and account takeover (ATO). They can only block spam and some rudimentary attacks, leaving your users unprotected.

AI-Powered Cloud Email Protection

Lastline Defender™ for Cloud Email is a complementary layer of defense that works with your existing Office 365 or Gmail system, augmenting those applications with Lastline's AI-Powered email protection. It blocks the advanced threats other technologies miss, without adding significant cost or complexity.

Lastline Defender for Cloud Email uses both structured and unstructured machine learning (ML) to detect mail-based advanced threats. Lastline's AI learns from our comprehensive knowledge of malicious behaviors generated from Deep Content Inspection, our market-leading malware analysis technology.

By performing comprehensive analysis on millions of real-world programs, documents, web pages, emails and files, Lastline's file analysis technology trains on more and better data. This training leads to better models and, in turn, a deterministic approach which delivers fewer false positives and fewer generic alerts than other approaches.

Lastline Defender for Cloud Email utilizes a unique ML algorithm to catch the most advanced attacks. It analyzes 300+ indicators in each email by looking at a range of components of the email:

- Headers
- Subject
- Body
- Link sites
- Linked files
- Fonts

Lastline Defender for Cloud Email analyzes historical emails to determine the prior trust relations between the sender and receiver. To provide a complete solution to prevent successful phishing attacks, it analyzes login and account activity to detect and block account takeovers. It correlates login events with past activity based on: Geography, Time of day, and other indicators and account activity (such as sending outgoing phishing emails, sending a high volume of emails, or sending emails with multiple recipients). By correlating these indicators through another ML filter, the algorithm flags compromised accounts while minimizing false positives.

Catch the Threats Office 365 and Gmail Miss

Lastline's anti-phishing algorithm combines traditional analysis capabilities with a proprietary ML algorithm that looks at all aspects of the email and is specifically trained to catch the threats Office 365 and Gmail miss. With the addition of account takeover prevention and advanced malware detection, Lastline provides a complete security solution to protect your organization from phishing schemes.
How It Works

Lastline Defender for Cloud Email scans inbound and internal emails, catching advanced threats after Microsoft or Gmail’s default security, or Microsoft ATP security fails to detect them. It connects directly to the native API of your Office 365 or G Suite environment. This provides both real time and historical information about every user, file, event and policy—not only of your users, but of everyone who has access.

Policy Automation

You have three choices for policy automation with Lastline Defender for Cloud Email:

- **Monitor-Only Mode** provides visibility into the cloud-hosted email leveraging Office 365 or G Suite’s publicly available API. Over 60 best-of-breed security technologies deliver scan results. This mode enables you to implement manual and automated query-based quarantines after delivery to the user mailbox.

- **Detect and Prevent Mode** provides an increased level of protection that scans email in your users’ inbox, leveraging the Office 365 or G Suite APIs. This mode adds an automated policy action to quarantine threats like malware and phishing attacks, based on the results of the best-of-breed security stack. This mode includes user notifications and release workflows.

- **Protect Mode** (inline blocking) provides the highest level of protection and scans emails prior to delivery to your users’ inbox. Leveraging the same Office 365 or G Suite APIs and implementing email rules, Lastline Defender for Cloud Email can scan email with a best-of-breed security stack to protect your end-users from malware, data leaks, phishing attacks and more. Scanning and quarantining takes place before email is delivered to your users’ inbox. This mode ensures the removal of threats before the user has access to the email.