# Lastline Defender for Cloud Email

## Unmatched Protection for Office 365 and Gmail

## Advanced Threats Bypass Cloud Email Security

Most cloud email security controls are only marginally effective in combating advanced threats such as account compromise, ransomware, phishing, and fileless malware. The native email protection in Office 365 Mail and Gmail can only block spam and some rudimentary attacks because they rely primarily on signatures. Even the add-on protection offered by Microsoft Advanced Threat Protection (ATP) cannot stop sophisticated threats from entering your users' inboxes.

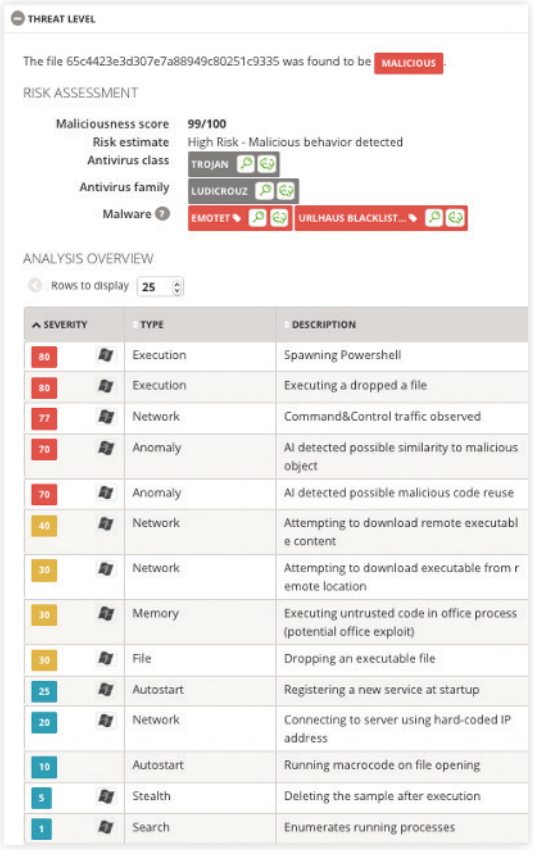
Attackers understand the limitations of email security and use a range of techniques to alter the signature of a file or URL including:

- Code permutation to alte critical elements of malicious code
- URL obfuscation techniques to prevent accurate parsing
- Code insertion or other constructs to change the file hash
- Code obfuscation techniques to hide malicious code in attachments

## Unique Cloud Email Protection

Lastline Defender™ for Cloud Email is a complementary layer of defense that works with Office 365 or Gmail. Lastline Defender blocks advanced email threats that other cloud email security technologies miss, without adding significant cost or complexity.

Lastline Defender for Cloud Email delivers a unique combination of the industry's highest-rated file analysis technology with supervised and unsupervised machine learning (ML). This gives you unsurpassed ability to stop evasive threats before they compromise your users.




### Industry-Leading File Analysis

#### Static and dynamic analysis

Lastline file analysis technology deconstructs every malicious behavior engineered into an object entering via mail, such as an attachment or download.

Lastline Defender for Cloud Email also uses file analysis to examine message headers and metadata, and analyze multiple parameters in any URL, including linked websites for malicious content

By performing comprehensive analysis on millions of real-world applications, documents, web pages, and emails, Lastline Defender continuously refines its detection technology which results in dramatically fewer false positives than other approaches.

## AI-Powered Detection

Lastline Defender for Cloud Email utilizes a unique ML algorithm to catch even the most advanced attacks. It analyzes over 300 indicators of compromise in each email for malicious activity by looking at a range of components, including:

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

## Additional Analysis to Detect Threats

Lastline Defender for Cloud Email analyzes historical emails to determine the prior trust relationship between the sender and receiver. It examines login and account activity to detect and block account takeovers. Lastline Defender for Cloud Email also correlates login events with past activity based on: geography, time of day, and account activity (such as sending a high volume of emails and sending emails with multiple recipients) for maximum protection.

# Catch the Threats Office 365, ATP and Gmail Miss

Lastline Defender for Cloud Email is engineered to catch threats Office 365, Office 365 with ATP, and Gmail miss.

| | Gmail | Office 365 Default | MSFT ATP | Lastline Defender for Email |
|---|---|---|---|---|
| **Advanced Malware Detection** | | | | |
| Antivirus Signatures | ▲ | ▲ | ▲ | ▲ |
| Virtual Sandboxing | | | ▲ | ▲ |
| Deep Content Inspection | | | | ▲ |
| Behaviroal Analutics | | | | ▲ |
| **Antii-Phishing Protection** | | | | |
| Domain Spoofing | | | ▲ | ▲ |
| Brand Impersonation | | | | ▲ |
| User Impersonation | | | | ▲ |
| **URL Protection** | | | | |
| Geography | | ▲ | ▲ | ▲ |
| Time of Day | | | ▲ | ▲ |
| Sending Phishing Emails | | | | ▲ |
| High Volume of Emails | | | | ▲ |
| Excessive | | | | ▲ |

*Lastline Defender for Cloud Email provides a complete security solution to protect your cloud email from malware, phishing schemes, and malicious URLs.*

## How It Works

Lastline Defender for Cloud Email scans inbound and internal emails, catching advanced threats that Microsoft or Gmail's default security or Microsoft ATP security fails to detect. Lastline Defender connects directly to the native API of your Office 365 or G Suite environment to analyze both real-time and historical information about every user, file, event, and policy.

## 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. This mode enables you to identify threats present in email without affecting the flow of messages.
- **Detect and Prevent Mode** provides an increased level of protection that scans email in your users' inbox, leveraging Office 365 or G Suite APIs. This mode adds an automated policy action to quarantine threats such as malware and phishing attacks.
- **Protect Mode** (inline blocking) provides the highest level of protection and scans emails prior to delivery to your users' inbox. Leveraging Office 365 or G Suite APIs and implementing email rules, Lastline Defender for Cloud Email can 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.

## Upgrade Your Cloud Email Protection Today

It takes only a few minutes to add Lastline Defender for Cloud Email protection to Office 365, Office 365 with ATP, and Gmail. Once you do, you'll be protecting your users from sophisticated threats attempting to disrupt your business. Lastline Defender for Cloud Email delivers the cybersecurity industry's highest fidelity insights into advanced threats targeting cloud email systems, enabling your security team to respond faster and more effectively.

**Lastline Corporate Headquarters**
1825 S. Grant Street, Suite 635
San Mateo, CA 94402

**Americas:** +1 (877) 671 3239
**www.lastline.com**
**info@lastline.com**