lastline™

SOLUTION GUIDE

Lastline Defender for Cloud Email:
AI-Powered Email Protection Eliminates Advanced Threats

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. While they can block spam and some rudimentary threats, Office 365 Mail and Gmail's native email protection cannot detect and block advanced threats such as ransomware, credential stealers, spear-phishing, business email compromise (BEC), and account takeover (ATO). In addition, protecting cloud email is more challenging than on-premises email because:

- Criminals need only figure out one vulnerability and they can launch the same attack against everyone using that platform
- It's easy to test by simply setting up their own Gmail or MS Office Mail account
- Once they compromise an email system, any email they send will appear to be an internal email, which typically is not scanned by email security solutions

Lastline Defender™ gives you the ability to augment your existing email security strategy with an additional layer of protection that detects the advanced threats other technologies miss, without adding significant cost or complexity.

Lastline® Delivers Unmatched Email Threat Visibility

Lastline Defender is a complementary layer of defense to enhance your cloud email security against advanced threats. It works with your existing Office 365 or Gmail system to protect your organization from sophisticated email threats.

Our AI learns from our comprehensive knowledge of malicious behaviors generated from our market-leading sandbox technology. This deterministic approach delivers fewer false positives than other products and fewer generic alerts that require additional investigation.

Lastline Defender delivers unmatched visibility and detection accuracy, enabling you to understand the objective of the attack, as well as respond faster to the threat before a data breach occurs. Your IR team can respond to alerts with certainty, eliminating the need to investigate generic alerts for potential false positives.

At the heart of Lastline Defender is Deep Content Inspection™, Lastline's market-leading sandbox technology. Deep Content Inspection imitates a complete operating system and hardware environment, delivering unmatched visibility into the malware, all programs and services it invokes, all operating system functions, and all kernel activity. It analyzes the actions of everything that occurs, including all CPU instructions, memory locations accessed, devices used, and network connections.

Why You Need Advanced Threat Protection

- Office 365 (even with Microsoft ATP) and Gmail can be easily fooled by advanced threats—especially evasive malware
- Traditional anti-phishing techniques are inadequate to prevent BEC
- Lack of internal email scanning misses ATO
- Only Lastline Email Defender-Cloud defeats
  - Malware
  - Phishing
  - BEC
  - ATO

"Next-generation" tools only have visibility down to the operating system level. They can inspect content and identify some potentially malicious code, but they can't interact with the malware like Lastline Defender can. This limited visibility means that they miss evasion techniques like encrypted strings that require CPU-level visibility to decrypt. As a result, they have significantly lower detection rates and much higher false positives, in addition to being easily identified and bypassed by malware employing evasion techniques.

These products can only monitor the interaction between an object and the operating system, which significantly limits their visibility into malicious behavior. This means they cannot see what is occurring within the malware itself, nor in other programs, operating system, or kernel functions used by the malware.

We engineered Lastline Defender to avoid being detected and bypassed like other "Next-Generation" tools. As a result of our unique approach, Lastline Defender delivers the visibility that other tools cannot.

Machine Learning to Defeat Phishing and Account Takeover Attacks

In order to catch the more advanced attacks, Lastline utilizes a unique machine learning algorithm that analyzes 300+ indicators in each email by looking at each email component:

- Headers
- Subject
- Body
- Links
- Content the links point to
- Zero fonts

The API integration also allows Lastline to analyze historical emails to determine the prior trust relations between the sender and receiver.

Even with these security measures, users may still lose their credentials. In order to provide a complete solution for phishing, Lastline analyzes login and account activity to detect and block account takeovers. This is done by correlating 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 emails with multiple recipients. By correlating these indicators through another machine learning filter, the algorithm is able to flag out compromised accounts while minimizing false alerts.

Lastline's anti-phishing algorithm combines traditional analysis capabilities with a proprietary machine learning algorithm that looks at all aspects of the email and is specifically trained to catch the things 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.

Prevent Business Email Compromise

Business Email Compromise (BEC) attacks often target cloud email systems like Office 365 and Gmail. They start with a spear-phishing attack or spoofed emails targeted at specific executives in order to commit fraud.

These attacks evade detection from email security controls that rely on content scanning or signature-matching. The emails do not contain links to any fraudulent sites or have malicious attachments, which normally trigger alerts.

Instead BEC attackers use publicly available data from social and business media sites to identify reporting relationships as well as names and titles of coworkers, upcoming travel, and so forth. They'll use this knowledge to create a realistic looking message from a trusted co-worker to initiate a fraudulent transaction, such as a wire transfer.

BLOCKING USER & DOMAIN IMPERSONATION

To block the user impersonation that initiates BEC attacks, Lastline Defender looks to see if a similar sender exists in the organization with a different email address. It also verifies the identity of the sender by cross referencing several fields in the email including the sender and the signature at the bottom of the email. It also detects when the sender is using a domain similar to the known domain but with a different source IP, different mail-flow path, and so forth.

Why Other Technologies Fail to Detect Advanced Threats

There are several reasons why advanced threats can bypass the default email security you have with Office 365 or Gmail. These services reply on technologies that are either outdated or easily detected and avoided:

Signature-based Detection

Threat actors can easily alter the signature of their code to avoid detection. Because security tools examine the internal components of an object to generate a signature, modifying even a single bit in any of the malware's components changes the object's signature. Some of the malware tools on the dark web enable payload-changing capabilities with a simple check box to foil signature-based systems. There are multiple transformation techniques used by malware authors, and applying any of them can alter a signature:

- Code permutation
- Register renaming
- Expanding and shrinking code
- Insertion of garbage code

Unfortunately, it can be several days or even weeks after a new malicious object appears in the wild before security vendors update their signatures. Until the new signature arrives, signature-based security controls will not detect the malware.

In fact, some vendors may never add signatures to their databases for many advanced malware threats. Malware that uses less sophisticated techniques and targets large numbers of victims has a much higher chance of having its signature added to a malware database. Advanced malware, on the other hand, uses sophisticated evasion techniques and often targets fewer victims. This narrower focus greatly reduces the odds that its signature will ever appear in a database of malicious objects.

Sandboxes and Other Virtual Environments Used by Next-Gen Tools

Security vendors embraced sandbox technology several years ago to overcome the failures of traditional signature-based technologies to detect advanced malware. Sandboxes simulate a network environment to fool the object into demonstrating malicious behavior, thus allowing the sandbox to identify and block the object before it can compromise systems or applications.

Because sandboxes use observed behaviors and not signatures to detect malware, they were very effective initially in detecting new strains of malware. However, today's advanced malware is engineered specifically to detect when it is running in almost every sandbox on the market. The malware avoids taking any malicious actions to evade detection while in the sandbox, allowing it to enter your network and initiate its malicious behavior.

The reason why advanced malware can bypass most sandboxes is that they typically utilize virtual machine (VM) environments like VMware, Xen, KVM, Parallels/Odin and VDI. In theory, the environment provided by the VM is self-contained, isolated, and indistinguishable from a "real" machine. Unfortunately, VM technologies insert artifacts, which allow advanced malware to discover that it is running in a virtual environment. These artifacts include additional operating system files and processes, supplementary CPU features, and other components necessary for the virtualization to work.

Advanced malware looks for these artifacts to detect the presence of a sandbox. For example, some of the techniques used by malware to recognize a VM environment include:

- Examining registry keys for values that are unique to virtual systems
- Detecting if VM tools are installed
- Checking for certain processes and services that are specific to VM environments

It is not only highly skilled hackers who can implement sophisticated evasion techniques like these. Today there are numerous toolkits available that allow novice cybercriminals to create malware that can detect the presence of a VM.

Blacklists and Header Inspection Inadequate

When it comes to defeating phishing, traditional email security checks of header data and URL filtering with blacklists only catch about 15% of phishing attacks at the time the email is received. Most phishing attacks that bypass the default security are true zero-day and come from senders appearing to be highly reputable.

Additionally, these checks and blacklists are ineffective in spotting account takeovers because they do not take into consideration historical email behavior of users. Other tools do not typically scan internal email, so critically important indicators of account takeover are not seen.

Improved Email Security without Complexity

We designed the Lastline architecture to give you the maximum protection you want while offering the deployment flexibility and low TCO you need. Our subscription model, with low user-based pricing, gives you superior protection while increasing the efficiency and productivity of your security resources.

Using Deep Content Inspection and machine learning technology, Lastline Email Defender-Cloud delivers what other current products cannot:

- Unmatched visibility for web, network traffic, and email traffic.
- Anti-phishing and URL protection
- Account takeover protection

Free 14-Day Trial of Lastline Defender

For more information please visit www.lastline.com or email sales@lastline.com

LASTLINE CORPORATE HEADQUARTERS
203 REDWOOD SHORES PARKWAY
SUITE 500
REDWOOD CITY, CA 94065

AMERICAS: +1 (877) 671 3239
EMEA: +44 (0) 207 749 5156
APAC: +65 6829 2207
WWW.LASTLINE.COM