

# Advanced Threat Protection for Cloud-Based Email

## Executive Summary

Email has been and continues to be the go-to delivery channel for cyber criminals looking to wage their attacks. If your organization is leveraging cloud-based email, these channels need to be secured. This use case reveals why organizations continue to be susceptible to email-based attacks, and it shows how Cyphort's Adaptive Detection Fabric enables customers to establish strong defenses against these attacks.

## The Continued Dependence and Dangers Associated with Email

While many aspects of the IT landscape have gone through fundamental paradigm shifts in recent years, one essential reality has remained: Email continues to be one of the dominant mechanisms for personal and business communications. Another not so pleasant truth has also remained stubbornly evident: Email continues to be the preferred method of cyber attackers looking to deliver malware and wage advanced attacks. According to Verizon's 2016 Data Breach Report, two of the top three malware vectors are associated with email: Emails with malicious attachments ranked number one, and emails with links to malicious webpages was positioned third.<sup>1</sup>

Organizations aren't going to get rid of email anytime soon. However, the way email is managed and supported is changing. While cloud-based email services for consumers have been the dominant reality for more than two decades, now businesses are increasingly moving to adopt public cloud email services, such as those offered by Microsoft, Google, and other vendors. In fact, according to a recent Gartner report, in the first nine months of 2016, public companies' adoption of cloud-based email services grew 23 percent.<sup>2</sup>

## Customer Problem

Email remains a common attack vector for a simple reason: it works.

While organizations continue to invest in in-line detection and prevention platforms to block malicious web content, they remain vulnerable to email-based attacks. Why? Organizations typically employ in-line security tools for on-premises email, which rely on static, rules-based approaches. However, as the sophistication of attacks grows, advanced malware exhibits constantly evolving attributes that enable it to evade any kind of static signatures or rule-based approaches. In the past, for example, when malicious emails were found that were sent from a particular domain, a rule could be applied so that the domain could be blacklisted or blocked by an anti-virus platform. Today, however, attacks are too dynamic for static, rules-based approaches like URL blacklists to offer any real protections.

---

*According to Verizon's 2016 Data Breach Report, two of the top three malware vectors are associated with email: Emails with malicious attachments ranked number one, and emails with links to malicious web pages was positioned third.<sup>1</sup>*

---

<sup>1</sup> Verizon, "2016 Data Breach Investigations Report," page 46, [www.verizonenterprise.com/resources/reports/rp\\_DBIR\\_2016\\_Report\\_en\\_xg.pdf](http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf)

<sup>2</sup> Gartner, "Survey Analysis: Microsoft Grows Its Share of Public Cloud Email Among Public Companies Faster Than Google," Nikos Drakos, Jeffrey Mann, November 8, 2016, ID: G00298500

This challenge doesn't go away when organizations shift to cloud-based email. Cloud-based email solutions don't offer consistent safeguards against advanced threats contained within emails. Some cloud-based in-line detection tools may even exacerbate security and compliance risks by forcing organizations to transfer data to untrusted network segments.

Further, security teams lack solutions that correlate intelligence across multiple threat vectors, such as endpoints, Web, and email. While some email security solutions can do some inspection of email attachments and URLs and identify malware, they will lack the correlation needed to identify threats that may already be traversing the network or coming through web traffic as a result of a malicious link. For example, while an email security solution may identify a malicious link in an email, it won't provide visibility into whether other users have also visited the compromised URL.

Compounding matters is the performance-sensitive nature of email transmissions which pose a challenge to in-line security tools. They must make a decision quickly (and potentially miss critical threats), or they must introduce significant latency to perform a deeper threat inspection (thus compromising the user experience and user productivity).

To eliminate these challenges, organizations embracing cloud-based email need an effective solution that can quickly detect and quarantine the growing number of advanced threats delivered through email channels.

## The Solution: The Cyphort Adaptive Detection Fabric

Cyphort delivers advanced detection that enables your organization to address your critical exposure to all email-borne threats—whether you're managing email on-premises, leveraging cloud-based email services, or any combination thereof. With Cyphort's Adaptive Detection Fabric (ADF), you can establish strong safeguards and address a critical gap in your security defenses. The ADF is an innovative, distributed software security layer that leverages machine learning and behavioral analysis technologies of its SmartCore analytics engine to detect advanced threats that bypass traditional in-line web and email security tools. Not just new variations of existing threats—but entirely new families of malware. ADF offers the ability to safeguard against email-based attacks. ADF can extract emails as they're received, and inspect both email file attachments and embedded URLs. ADF then performs sophisticated analysis to find threats that traditional defense technologies miss.

### Advantages

ADF equips your organization with many unmatched advantages:

- ▶ **Detection and quarantine.** ADF detects malicious attachments and URL links and can automatically quarantine all malicious emails in near real-time.

- ▶ **High scalability.** ADF delivers robust scalability, with a capacity to process up to 2.4 million emails a day.
- ▶ **Flexible implementation.** ADF integrates easily with any existing cloud-based email deployment, including Microsoft Office 365 or Google Gmail, without having to change any network or email infrastructure, including routing and mail exchanger (MX) records.
- ▶ **Rich intelligence correlation.** ADF gives your team a single management console for viewing and tracking threats, including those coming through email and web traffic, as well as threats traversing your network laterally. Through syslog or its API-based integration, ADF can provide detailed threat intelligence to SIEM systems in a custom, tailored format. As a result, you can automate a range of tasks, such as the correlation of an infected endpoint IP address with the name of the registered user to expedite notification and mitigation.

### Benefits

When you leverage ADF, your organization can realize the following benefits:

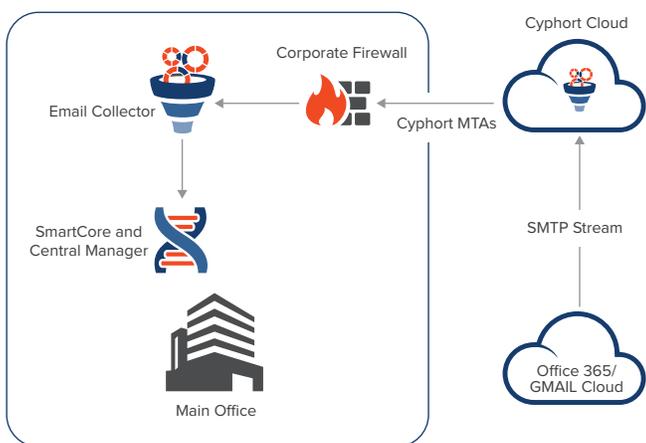
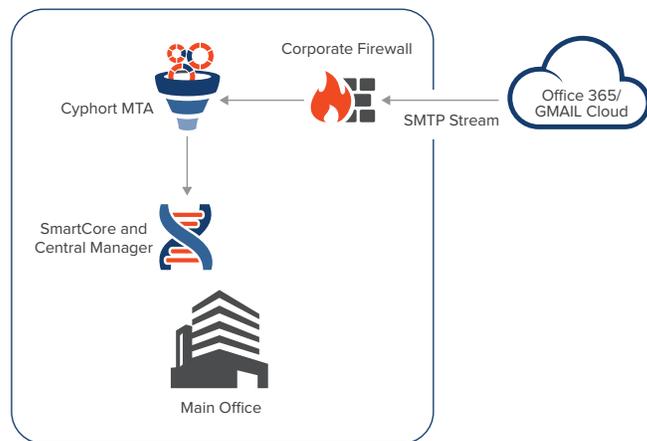
- ▶ **Maintain user productivity.** ADF enables your organization to address critical security requirements while ensuring an optimal user experience. ADF offers an optimized implementation that maximizes performance and throughput so that employees inside the network can continue to manage email correspondence without additional latency.
- ▶ **Establish comprehensive, advanced protection.** ADF guards against advanced malware, including new malware variants and entirely new malware families. With its capabilities for automated quarantining, ADF can ensure the damage from any malware is kept to a minimum. With ADF, you can protect users anytime they're checking and reading their email—no matter which device they use or which network they're on.
- ▶ **Ensure compliance.** With ADF, you can ensure your compliance obligations are being met. ADF allows you to maintain control of your data at all times to ensure data does not leak to networks segments outside of your organizations control. As a result, ADF enables you to avoid the security risks posed by cloud-based in-line detection tools.

### Deployment Options

ADF implementations feature the SmartCore engine and Cyphort Message Transfer Agents (MTAs), which are used to capture and forward files and URLs to the SmartCore engine. ADF supports flexible implementation options, so your organization can implement the solution in a manner that's well-suited to your objectives. The following sections detail the deployment alternatives.

### On-Premises Collection of Cloud-based Email

In this configuration, user emails are transferred from Office 365 or Gmail and sent to an on-premises Cyphort MTA for processing. The Cyphort MTA extracts the email attachments and URLs and sends them to SmartCore for multi-stage analysis. With Cyphort’s auto-mitigation, malicious emails are automatically and immediately quarantined.



### Cloud Collection of Cloud-based Email

In this scenario, user emails are transferred from Office 365 or Gmail and sent to a Cyphort MTA that’s hosted in the Cyphort cloud. The Cyphort MTA extracts email attachments and URLs and sends them to SmartCore for multi-stage analysis. With Cyphort Auto-Mitigation, malicious emails are automatically and immediately quarantined.

## Conclusion

With the advanced email threat protection capabilities of the Adaptive Detection Fabric, your organization can deploy cloud-based email solutions and feel confident that ADF will help minimize the security risks associated with this attack vector, while ensuring employees maintain high productivity with email messages. For an introduction to all of the components and features of the ADF, be sure to download the [product data sheet](#).

## About Cyphort

Cyphort, Inc. is a network security company providing mid- and large-size enterprise customers with the innovative Adaptive Detection Fabric, a scalable software solution designed to integrate with existing security tools to discover and contain the advanced threats that bypass the first line of security defense in an organization. Based in Santa Clara, California, the company was founded in 2011 and distributes its software through direct sales and channel partners across North America and international markets. Learn more at [www.cyphort.com](http://www.cyphort.com).