mimecast™

paloalto® NETWORKS

White Paper

Mimecast and Palo Alto Networks: Easy Integration, Greater Resilience

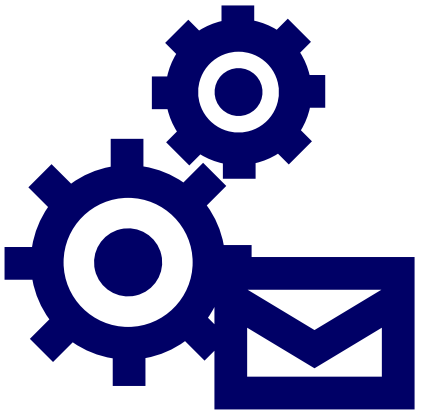
Integrating Best-of-Breed Solutions

Today, tactical threat response is essential but insufficient: Organizations need a strategic approach to improving cyber resilience and overall protection for the long term.

Native integration between Mimecast Targeted Threat Protection and Palo Alto Networks® Cortex Data Lake™, Cortex XSOAR™ and WildFire® technologies establishes a strong foundation for protecting entire organizations against fast-changing security challenges.

Our integrated technologies let organizations establish integrated, intelligent stores of up-to-date security information to support faster protection, detection and response. They help companies rapidly implement layered, optimized detection of email-borne attacks and accelerate response via automated playbooks and custom workflows that leverage both companies' combined threat intelligence.

This white paper explains how these best-in-breed technologies work together to help security teams achieve their goals by leveraging intelligence, automation and integration to get more out of existing security investments. It describes these native integrations and shows how they can be established in minutes — improving your security posture without adding headcount.



mimecast

Facing More Ubiquitous and Sophisticated Cyberattacks

Security organizations nowadays face increasingly ubiquitous and sophisticated attacks, often focusing on access compromise and "**layer 8**" (a.k.a. human) weaknesses, and enabled by the misuse of standard cloud services. Today's zero-day attacks and **advanced polymorphic malware** challenge even the best defenses, and can't always be deterred. Reducing dwell time has become more crucial than ever: Organizations need to detect attacks in less than a minute, investigate them in under ten minutes and remediate them in an hour or less. Otherwise, intruders gain a foothold, cause more damage and become even harder to expunge.

How can resource-constrained security and IT organizations improve overall protection and resilience even as their infrastructures grow more complex, while encompassing more remote working, BYOD and cloud services?

By applying:

- More *intelligence*, via AI and machine learning technologies capable of recognizing threats more rapidly and comprehensively than human analysts.
- More *automation*, offloading repetitive tasks, from isolating infected machines to filtering out false positives.
- Most importantly, more *integration*, so all security systems can share access to all the timely threat intelligence that is available.

The answer lies in integration, because fast, reliable integration is also essential to leveraging intelligence and automation. Integration provides intelligent systems the timeliest information to analyze — especially about zero-day attacks, which are typically attempted via email first, often hours before other vectors. It also enables automated processes to extend across the entire security infrastructure, helping security teams manage everything as a unified whole.

Today's threat environment

90+% of threats still manifest first via email*

225 billion emails sent per day

65% The IT sector saw a **65%** increase in ransomware incident response cases in 2020, largely due to COVID and remote work**

20% of users move sensitive data between cloud apps

37% of this activity risks DLP violations

20 Users upload an average of **20** company files/month to personal apps***

80+% of leaders will permit part-time remote work after COVID ends****

*Mimecast research
*Palo Alto Networks Unit 42 Ransomware Threat Report
***Netskope Cloud & Threat Report Data
**** Gartner, "Gartner Survey Reveals 82% of Company Leaders Plan to Allow Employees to Work Remotely Some of the Time," July 14, 2020

mimecast™

Overcoming Traditional Challenges to Security Integration

For security organizations, seamless integration has long been an important goal — but how can they integrate effectively without adding unnecessary complexity, or locking themselves into a single-vendor solution?

To address these issues, Mimecast from its inception has invested in the industry's most complete, fully documented library of open APIs and off-the-shelf third-party integrations. That combination provides wizard-based interoperability to any customer while empowering organizations that need more flexibility to customize their integration in new ways, based on their own requirements. Mimecast has partnered with Palo Alto Networks to offer a complete foundation for integrated security based on the two companies' best-of-breed technologies, from secure email gateways to SOAR, advanced malware analysis, next-generation firewalls and a unified, intelligent data store to serve them all.

Together, Mimecast and Palo Alto Networks offer end-to-end protection that far exceeds the capabilities of non-integrated solutions or those offered by a single supplier. Our security products leverage data and inspection insights gathered by each of them, offering true layered security that benefits from the diverse capabilities of multiple detection technologies.

The combined solution is a welcome contrast to single-vendor solutions that create a security monoculture, such as Microsoft 365 — where evading one supplier's inspection infrastructure could leave an attacker home free. Recent events, including Microsoft's patching of six zero-day bugs already being exploited in the wild and its inadvertent digital signing of a malicious rootkit, highlight Microsoft's attraction as a target and the need to complement its security technologies with independent best-in-class capabilities. Further exacerbating the security monoculture challenge is the limited ability Microsoft allows for sharing intelligence with non-Microsoft security products — so even when Microsoft 365 does recognize a threat, the rest of the organization's security infrastructure typically can't be made aware of it.

To help you protect, detect and respond, we bring together these well-proven, widely deployed offerings:

> **Mimecast's Secure Email Gateway with Targeted Threat Protection** to provide first-line defense against the full range of email-related attacks at all levels of sophistication, safeguarding use of any cloud or on-premises email platform. Mimecast defends against inbound spear-phishing, malware, spam and zero-day attacks by combining innovative cloud applications and policies with multiple detection engines and intelligence feeds; **Mimecast CyberGraph** leverages artificial intelligence to limit the effectiveness of social engineering attacks, including spear-phishing, with email tracker prevention and identity graph technology.

> **Palo Alto Networks WildFire** advanced cloud-based threat analysis and prevention service for addressing even the most evasive zero-day exploits and malware. WildFire's multi-technique approach combines cloud analysis, globally crowdsourced intelligence, innovative machine learning and an evasion-resistant custom hypervisor.

> **Palo Alto Networks Cortex Data Lake** to collect, integrate and normalize your enterprise's security data. Not just a generic data lake, Cortex helps a network administrator investigate and explore firewall data to protect against threats and attacks.

> **Palo Alto Networks Cortex XSOAR** to help transform security operations with scalable, automated workflows for a wide spectrum of security use cases. It orchestrates and automates incident response, accelerating incident investigations with rich threat intelligence data and automated playbooks.

mimecast

Working together, these platforms share both data and analytics. This has powerful benefits.

Since **90+% of new attacks first manifest through email**, Palo Alto Networks' cloud security services can now benefit from a continuous and near-instantaneous feed of new information on zero-day attacks first identified by Mimecast's email scanners. And since threat sharing is bilateral, Mimecast also leverages analyzed threat data from Palo Alto Networks' technologies, improving the performance of the Mimecast Secure Email Gateway when faced with zero-day threats that don't first appear via email or are cloud-enabled.

All these systems communicate virtually instantaneously, without human involvement or the need to continuously poll multiple feeds, determine whether new data exists, and then share it across the entire estate. This meaningfully reduces time to protection, and makes it easier to automate more facets of security as "set-and-forget" — so security teams can accomplish more with fewer resources and refocus on higher-value tasks. Leveraging Mimecast's high-quality early alerts alongside other data streams, it's easier to search networks for attacks that have recurred through non-email vectors.

Since all data is stored in the same intelligent Cortex Data Lake, and also leverages Palo Alto Networks' own extensive set of integrations, it becomes possible to apply advanced analytics to automate responses through all security systems across the enterprise, including Mimecast's.

They can now be investigated and remediated far more rapidly using Palo Alto Cortex XSOAR automated playbooks and custom workflows.

Through this close partnership, Mimecast and Palo Alto Networks have made — and continue to make — significant investments to ensure smooth integration and high levels of support for their integrated environments. Both are collaborating to add new synergistic capabilities not previously available.

mimecast

Use Case #1: Enhance Detection and Automate Remediation of New Email-Borne Attacks

Consider an advanced zero-day attack against multiple users simultaneously, starting as many do: through a phishing email. Defending against such attacks is critical but complex. It requires extremely fast detection and the ability to quickly find, root out and remediate the attack wherever it spreads.

By combining sandboxing and static file analysis from Mimecast's Targeted Threat Protection with cloud-based malware analysis capabilities of Palo Alto Networks' WildFire — and integrating data streams and analytics from both platforms — security organizations can recognize more attacks more quickly, thereby reducing risk. For example, if WildFire identifies a malicious threat, it automatically generates and distributes new preventions to Mimecast, minimizing the risk of infection from both known and unknown threats without any additional, manual action. The integration includes an automated remediation capability, which removes all instances of the malware detected to prevent them from spreading.

Palo Alto Networks' platforms may recognize that outbound firewall traffic shows signs of an endpoint responding to an external command-and-control bot. They can immediately instruct Mimecast to block the user from sending any other email because the account appears to have been compromised, or to scan outgoing as well as incoming email since many threat actors use compromised endpoints to spread.

Then, through Cortex XSOAR, Mimecast can be instructed to search for common indicators to identify other appearances of the same compromise across the organization's mailboxes, halting and remediating those as well.

Widespread attacks can trigger hundreds of alerts, generating alert fatigue and overwhelming analysts with repetitive and time-consuming tasks that limit their ability to identify root causes and end the attack. By integrating Mimecast with Cortex XSOAR, organizations enable the rapid and automated orchestration of a wide variety of repeatable actions during incident response, freeing analysts for higher-level tasks. Cortex XSOAR can interface with Mimecast's Secure Email Gateway to look up and decode URLs, search for relevant emails and attachments, remove emails from users' inboxes, or even make policy changes — e.g., blocking a malicious email address from sending data to the organization, or blocking known malicious URLs via email.

At the same time, two-way native integration means that Mimecast's analytical insights can be continually shared across the estate, informing playbooks that also trigger security actions by other systems, such as endpoints.

Integration in Minutes, Step by Step

Establishing an integration between Mimecast and Palo Alto Networks security systems requires no scripting or programming, no costly professional services engagement and no additional costs of any kind. That means you get return on value — fast.

To integrate Mimecast with Palo Alto Networks' Cortex Data Lake or WildFire, use the step-by-step Create an Integration wizard in Mimecast's administration console, specifying Palo Alto Networks, adding the authentication keys the company provides and enabling notifications and two-way communications. The entire process typically takes no more than five minutes. Integration with Palo Alto Networks' XSOAR is established through Palo Alto Networks' Panorama console and is equally straightforward with simple steps to incorporate into your existing playbooks.

Once integration is established, each system immediately begins to share data and analytics generated by the other(s). No further configuration is required, and the new information can be monitored from each system's administrative console.

Use Case #2: Improve Attack Investigations

When investigating new cyber threats, security teams need maximum visibility, attack context and forensic data in order to understand and assess risk and take appropriate action. Attack investigations also require analysts to pivot between suspicious indicators in order to gather critical evidence, and to capture and archive documentary evidence for after-action assessments and record-keeping. All this screen-switching can interrupt and distract analysts during an investigation, when time is of the essence.

Integrating Mimecast's Cloud Email Gateway with Palo Alto Networks' WildFire provides security teams with detailed context on who is being targeted, when, by what type of malware, and its intended actions. Forensic information about detected malware is always at hand in both systems.

When Mimecast's email gateway is linked to Cortex XSOAR, analysts can run enrichment playbooks to gain actionable information about new attacks by running Mimecast commands in the Cortex XSOAR War Room — performing all investigation and documentation tasks from a single pane of glass. Mimecast actions can be added to any existing or new playbook with Cortex XSOAR, either in advance or on the fly in response to an attack in progress.

At the same time, two-way native integration means that Mimecast's analytical insights can be continually shared across the estate, informing playbooks that also trigger security actions by other systems, such as endpoints.

mimecast™

A Fully Integrated Resilience Suite for Microsoft 365 Environments

After adopting Microsoft 365 productivity solutions, many organizations have layered on third-party security technologies to overcome critical gaps. Today, incorporating Mimecast and Palo Alto Networks technologies provides organizations the best of both worlds: smooth integration and reliable data sharing with Microsoft, combined with advanced tool sets that recognize and deter attacks which can't be prevented by any security monoculture, including Microsoft 365.

Layering on integrated Palo Alto Networks and Mimecast technologies offers more complete protection across the stack: from blocking zero-day email-based attacks, detecting unexpected behavior in endpoint traffic, to halting data leaks, to remediating via automated playbooks, to Mimecast Mailbox Continuity for uninterrupted access to live and archived email via Outlook or other email clients. Instead of point solutions, or living with one vendor's limitations, you get a fully integrated, best-in-breed resilience suite.

Learn Fast and Move Forward

Because the vast majority of cyberattacks — including zero-day attacks — manifest first in email, it should come as no surprise that Mimecast's identification of new attacks are often hours ahead of others'. Therefore, extending Mimecast threat intelligence and analytics insights more widely and automatically can meaningfully increase the speed of your organization's response. Integration with Palo Alto Networks technologies makes this exceptionally powerful.

Integrating Mimecast with Palo Alto Networks' WildFire enhances and accelerates threat detection and can automate remediation throughout the enterprise. Integrating Mimecast with Cortex Data Lake provides its advanced AI and machine learning a powerful new data source for understanding emerging attacks and evolving defenses. More gains can be made by further integrating Cortex XSOAR with Mimecast, our most popular SOAR integration by far. This enriches event views with more data, and supports even more comprehensive orchestration and automation of incident response workflows across all security areas (SecOps, NetSecOps, cloud) and products.

This translates into fewer successful zero-day attacks, more rapid recognition of intrusions, more effective threat hunting and shorter dwell time — all achieved more systematically and cost-effectively, even in cloud-based global business environments.

Given each partner's best-of-breed leadership, many organizations already have one or more of these widely deployed technology platforms in place. If so, they possess an exceptionally easy and rapid path to comprehensive end-to-end security administration that generates more value from the investments they have already made, at no additional cost.

But regardless of their existing infrastructure, many organizations continually reassess their long-term cybersecurity strategy as the threat environment rapidly evolves. Together, Mimecast and Palo Alto Networks offer a pathway for achieving stronger layered protection without added complexity or the risks of a security monoculture.

Learn more about this path to best-of-breed integration: contact your Mimecast sales representative, email **alliancepartner@mimecast.com** *or visit* **Palo Alto Networks** *today.*

mimecast™

Mimecast was born in 2003 with a focus on delivering relentless protection. Each day, we take on cyber disruption for our tens of thousands of customers around the globe; always putting them first, and never giving up on tackling their biggest security challenges together.

We continuously invest to thoughtfully integrate brand protection, security awareness training, web security, compliance and other essential capabilities. Mimecast is here to help protect large and small organizations from malicious activity, human error and technology failure; and to lead the movement toward building a more resilient world.