Whitepaper

mimecast

The Mimecast-Netskope-CrowdStrike Triple Play:

Integrating Best-of-Breed Solutions

Executive summary

Security and IT organizations must protect against new attacks at scale — and safeguard data in use, at rest and in motion — in radically cloud-centered environments where perimeters are fading as quickly as the distinctions between work and home. To do so, they need to leverage more intelligence, more automation and, above all, better integration.

This white paper shows how Mimecast, Netskope, and CrowdStrike have combined their separate best-of-breed cybersecurity solutions into a "Triple Play" to address IT's information security challenge. Our Triple Play makes it far easier to integrate IT security infrastructure for defense in depth and avoid the growing risks of implementing a security monoculture. The white paper reviews specific challenges the Triple Play is intended to address with best in class solutions, shows how integration can be established in minutes, and presents use cases that demonstrate the value delivered.

mimecast

CROWDSTRIKE

netskope

Facing the Twin Challenges of Cyberattack and Data Loss

Today, security organizations face increasingly urgent challenges that cannot be managed through traditional perimeter defenses and trust based on network location approaches.

Cyberattacks have grown more ubiquitous and sophisticated as they focus on access compromise, human trust and weaknesses, and use cloud enablement. Today's zero-day attacks and advanced polymorphic malware challenge even the most sophisticated defenses, and can't always be deterred. Malicious actors increasingly rely on standard cloud resources to support their attacks to evade legacy defenses, which often involve logging in to a business's own cloud services via legitimate credentials they steal via email phishing.

Reducing dwell time has become more crucial as the first stages of attack are the most critical for intruders to gain a foothold, achieve persistence and perform discovery. Organizations need to detect attacks in less than one minute, investigate them in under 10 minutes and remediate them in an hour or less. Otherwise, intruders gain a foothold, cause more damage and become even harder to expunge.

But cyberattacks aren't a security team's only challenge. Concurrently, organizations must manage explosive growth in data, potentially spread across thousands of apps and cloud services. As compliance rules and customer expectations increase, data loss protection becomes more business-critical than ever.

Organizations need unprecedented control and visibility into data in use, at rest and in motion. At the same time, organizations need to manage employee user experience while managing devices and connections in this work from anywhere landscape.

Responding with More Intelligence, Automation and Integration

How can security and IT organizations make access easier and cyberattacks harder — at the same time? How can they prevent data loss and enforce compliance as apps and cloud services sprawl beyond IT's control as shadow IT represents 97% of app use? How can they manage increasingly complex infrastructures with fewer resources?

Security and IT organizations can answer these questions by applying:

- More intelligence, via AI and machine learning technologies capable of recognizing and acting on threats more rapidly and comprehensively than human analysts.
- More automation, offloading more repetitive tasks, from authorizing devices to halting an attempt to email a spreadsheet containing Social Security numbers.
- Above all, more integration, so all security systems can share access to all the timely threat intelligence that is available.

Integration is held "above all" because fast, reliable integration is essential to leveraging intelligence and automation, too. It ensures that intelligent systems always have the timeliest information to analyze — especially about zero-day attacks which are typically attempted via email first, often hours before other vectors. Effective integration enables automated processes to extend from gateways to endpoints and ultimately SOAR/SIEM systems. It helps security teams manage their infrastructures as a unified whole.

Overcoming Traditional Challenges of Security Integration

For security organizations, seamless integration has long been the holy grail — but, as the metaphor suggests, those who seek it have faced serious obstacles. How do you integrate effectively without adding complexity you don't need, or locking yourself into a single-vendor solution — with the growing risk that an attacker can succeed by evading the security monoculture of a single defender?

To address these issues, Mimecast has already invested heavily in the industry's most complete, well-documented library of open APIs and off-the-shelf third-party integrations — a combination that gives wizard-based integration to all while empowering organizations that need more to flexibly customize integration in new ways, based on their own requirements. Now, Mimecast has partnered with Netskope and CrowdStrike to offer a complete foundation for integrated security based on best-of-breed technologies, from endpoint to email and web gateways, and from threat prevention to data loss prevention.

Toward Better & Easier Security Integration

Together, Mimecast, Netskope and CrowdStrike offer end-to-end protection and data loss prevention that far exceed the capabilities of non-integrated solutions, or those offered by a single supplier.

Our best-of-breed security products form a Triple Play that shares data and inspection insights gathered by each of them, offering true layered security that leverages multiple detection technologies together, across your entire organization. The combined solution is a welcome contrast to single-vendor solutions, where evading one supplier's inspection infrastructure could leave an attacker home free.

The Mimecast-Netskope-CrowdStrike Triple Play brings together the following well-proven, widely deployed offerings:

- **Mimecast Secure Email Gateway** (Perimeter Defense Plan or above) to provide first-line defense against the full range of email-related attacks at all levels of sophistication.
- **CrowdStrike Falcon Platform** (enterprise license or above) to provide next-generation endpoint and workload protection and visibility across the enterprise, preventing attacks on endpoints and workloads on or off the network.
- **Netskope Next Gen Secure Web Gateway** (Enterprise or Professional package) to unify SASE networking and security services in a cloud-delivered single-pass architecture that ties security policies to identities, protecting users, applications and data even when employees use apps and cloud services outside IT control. Netskope also provides its Cloud Threat Exchange (CTE) for bidirectional automated threat intelligence sharing for partner integrations with customer deployments.

Today's Threat Environment

- 90+% of threats still manifest first via email
  - 225 billion emails sent per day.
  - 2,415 cloud apps used in an average enterprise
  - 97% of them shadow IT
  - 20% of users move sensitive data between cloud apps
  - 37% of this activity risks DLP violations
  - Users upload an average of 20 company files/month to personal apps
- 80+% of leaders will permit part-time remote work after COVID ends[1]

[1]Gartner, "Gartner Survey Reveals 82% of Company Leaders Plan to Allow Employees to Work Remotely Some of the Time," July 14, 2020.

Working together, all three platforms share both data and analytics. This has multiple benefits. For example, since 90+% of new attacks first manifest through email, both CrowdStrike Falcon Platform and Netskope's Cloud Threat Exchange can now benefit from a continuous and near-instantaneous feed of new information on zero-day attacks first identified by Mimecast's email scanners. Since threat sharing is bilateral, Mimecast also leverages a non-stop stream of threat data from Netskope's Cloud Threat Exchange, improving the performance of the Mimecast Secure Email Gateway when faced with zero-day threats that don't first appear via email and may be cloud enabled.

Leveraging Mimecast's high-quality early alerts alongside other data streams, CrowdStrike Falcon, powered by their proprietary Threat Graph, provides complete real time visibility and insight into everything happening on the endpoint, empowering responders to understand threats immediately and act decisively.

Exchanging threat data is important but insufficient: to improve control, you need ways to act on new threat data automatically and virtually instantaneously. To that end, Netskope can now direct Mimecast's Email Gateway to block outbound email content recognized as sensitive or non-compliant, using the same identities and policies it applies elsewhere using the same DLP identities.

In addition to the benefit of true layered security that combines multiple detection technologies, the Mimecast-Netskope-CrowdStrike Triple Play reduces human error and increases speed. All three systems communicate virtually instantaneously, without human involvement or the need for orchestration tools to continuously poll multiple feeds, determine whether new data exists and then share it across the entire estate. By accelerating action beyond what orchestration tools can typically achieve, the partnership meaningfully reduces time to protection.

The Triple Play creates a unified omnichannel solution for data loss across the entire organization. You improve control over data via a single DLP engine that controls all enterprise data access, eliminating duplication and enabling comprehensive monitoring through a single model and dashboard.

Working together, these offerings make it easier to automate more facets of security as "set-and-forget" — empowering security teams to accomplish more with fewer resources and refocus on higher value tasks.

Through forming this close partnership, Mimecast, Netskope and CrowdStrike have made — and continue to make — significant investments to ensure smooth integration and high levels of support for these integrated environments. They're collaborating to add new synergistic capabilities not previously available, such as new email headers embedded by Netskope and acted upon by Mimecast to improve compliance and prevent data exfiltration.

Perhaps best of all, integrating Mimecast, Netskope and CrowdStrike is remarkably easy. It's typically wizard-driven, with no scripting, no programming, no costly professional services engagements, and no additional costs of any kind. That means you get return on value — fast.

Best-of-breed protection from recognized leaders — tested and honored by customers and industry experts, over and over again

Mimecast	**Leader** Forrester Wave Enterprise Email Security Q2 2021	**Best Email Security Service SE Labs** 2020	**Customer Choice, Email Security** Gartner Peer Insights 2021	******** **Secure Gateway** SC Media
Netskope	**Leader in CASB** Gartner Magic Quadrant 2020	**Customer Choice, CASB** Gartner Peer Insights 2021	**World's Best Cloud Companies** Forbes 2020, 2019, 2018	**Cyber Security Award** **Data Protection - Enterprise** Fortress 2020
CrowdStrike	**Leader in Endpoint Protection Platforms** Gartner Magic Quadrant 2021	**Leader** Forrester Wave Managed Detection and Response External Threat Intelligence Services Q1 2021	**4.9/5** Endpoint Protection Platforms	**AAA** SE Labs Endpoint Detection and Response

Triple Play Use Case #1: Preventing Cloud Attacks

The widespread adoption of cloud services means that organizations need to protect against attacks constructed using resources hosted on legitimate cloud services with legitimate URLs.

For example, imagine that an employee receives an email purporting to be from the World Health Organization, encouraging them to review important pandemic information by clicking a link. The link is to a SharePoint site which asks them to download a weaponized Excel file. It might connect to a Google Drive to pull additional malware content. The malware fetches a configuration file from Github to tell it what to do, then uses Slack to establish command and control, and finally achieves its ultimate goal: exfiltrating data from the user's endpoint to a Dropbox account controlled by the criminal.

Mimecast likely recognizes and blocks this email attack if it is directed to the employee through a business account it serves. But most users nowadays have multiple email accounts, including personal accounts they sometimes use for work purposes. An attacker may send to all those accounts. With the integrated Mimecast-Netskope-CrowdStrike Triple Play in place, Netskope's Next Gen Secure Web Gateway service can recognize an attack made through a personal email account or even another web service — often by drawing on a Mimecast hash created when the attack was first attempted via company email.

CrowdStrike can now leverage Mimecast's newest zero-day information to alert administrators and prevent the threat from executing on the managed endpoint devices. With this added protection, the attack can be halted before it succeeds, whether it originates through a personal email account, a USB device or another vector.

Integration in minutes, step by step.

Bidirectional Triple Play integration is easy to establish and requires no scripting or programming.

Integrating with CrowdStrike requires only a few easy steps: following the step-by-step Create an Integration procedure in Mimecast's administrative console, specifying CrowdStrike Falcon Threat Exchange, adding the authentication keys CrowdStrike provides, and enabling notifications and two-way communications. The entire process typically takes no more than 5 minutes. Integration with Netskope is established through Netskope's Cloud Threat Exchange administrative console, and is equally quick and straightforward.

For more details about integrating with CrowdStrike, visit

community.mimecast.com/s/article/Crowdstrike-Falcon-Integration

For more details about Netskope integration, Netskope community members can log in and visit

support.netskope.com/hc/en-us

Once completed, full bidirectional communication among all three systems works immediately, requires no further configuration, and can be monitored from each system's administrative console.

Triple Play Use Case #2: Omnichannel Data Loss Prevention

Organizations face a growing challenge to systematically prevent data loss when data can leave their network via any one of thousands of cloud services, many outside the IT team's control adopted as shadow IT. With minor changes, essentially the same straightforward integration process described in Use Case #1 helps manage this challenge.

Layering atop Mimecast's strong outbound email protections, Netskope Email DLP provides a view into the content of data — both email text and attachments, scanning them as they leave the customer's environment. If sensitive content is found, Netskope marks it in the email header for Mimecast to enforce protection policies based on a wide spectrum of potential orchestrated actions.

The standard response is a hard bounce: the email simply isn't delivered. But other actions are possible, including (for example) holding the email at the gateway. These decisions can now be driven by the same set of identities and policies that Netskope is applying DLP identities to its controls over all the cloud services an organization may be using, from Dropbox to Salesforce.

Working together, the Triple Play solution reduces the possibility of data loss whether inadvertent, negligent or malicious. It becomes more difficult for malware to find workarounds and successfully exfiltrate data by targeting the weak link of a personal email account.

Next Steps: Gaining Even More Value from Integration

With these integrated technologies in place, the Triple Play partners have established a foundation for driving more value over time.

For example, businesses can leverage Mimecast's rich APIs to integrate additional security capabilities such as SIEM or SOAR systems, enabling them to immediately leverage the data flows being generated by Mimecast, Netskope and CrowdStrike.

But remember, 90+% of new attacks still manifest themselves first in email — and in our experience, Mimecast's identification of new attacks are often hours ahead of other data feeds. Therefore, extending Mimecast data and knowledge more widely can continually increase their value. It helps organizations prevent more zero-day attacks, recognize intrusions more rapidly, hunt threats more effectively and trigger automated SOAR incident response playbooks more quickly. All of this reduces dwell time.

So, too, Mimecast's open API platform makes it easier to customize integration more extensively, and to extend up-to-date email security data to any firewall or remote office that hasn't yet been brought under the umbrella of Netskope's Next Gen Secure Web Gateway.

Integrating Mimecast, Netskope and CrowdStrike technologies also offers a foundation for:

- **Improving alignment between security and IT operations.** With Triple Play integrated data, SecOps and IT ops can gain greater visibility into each other's challenges. SecOps can provide better input and contribute more effectively to decision-making that helps IT operations improve uptime. It can avoid downtime by protecting people earlier — leading to fewer trouble tickets, fewer interruptions and fewer employees forced offline due to security problems. The same data flows and improved feedback may also help internal software professionals build more secure systems, supporting a DevSecOps approach that integrates security more deeply throughout the development lifecycle.
- **Accelerating the implementation of top-level security strategies.** For example, businesses can accelerate cloud transitions, confident that they'll have the same or better visibility and data loss prevention capabilities than in their legacy on-premises/VPN environment. Organizations may be able to move toward a fully zero-trust adaptive policy architecture. Because they have the timely information needed to support dynamic decision-making about the security posture of any device, application or user seeking access; and because they can fully align identity with policy.

Learn More and Move Forward

The integration of Mimecast, Netskope, and CrowdStrike creates a Triple Play that can help organizations significantly improve response time to threats, increase the security team's efficiency as measured in both time and cost, and improve protection against both malicious attacks and data loss in today's cloud-centered, hybrid office/home work 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 leverages even 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, Netskope, and CrowdStrike offer the first proven, well-supported and complete route to best-of-breed integration. By leveraging the partners' Triple Play capabilities, businesses can achieve stronger layered protection and avoid the added risks of the inherent security monoculture of a single-provider solution.

Learn more about this path to best-of-breed integration:

Contact your Mimecast sales representative. Email alliancepartner@mimecast.com or visit mimecast.com today.