Whitepaper

mimecast

Better Together: Security Integration in Healthcare is Urgent and Achievable

The Mimecast-Netskope-CrowdStrike Triple Play for Healthcare

Executive Summary

Few responsibilities are more important than healthcare cybersecurity, or more challenging. Lives are at stake — many lives — and attackers know that as well as you do. Cybercriminals know healthcare professionals are facing greater stress and more relentless demands than ever as they seek to deliver excellent care in a pandemic era. They know healthcare staff must navigate multiple complex systems, from networked IoT devices to legacy point-of-care systems to remote billing services, with extensive data sharing and vast attack surfaces, all of which make this a difficult world to secure. They know care providers view patients as a higher priority than passwords. They see growing reliance on traveling healthcare professionals who may be unfamiliar with key processes, and whose access is difficult to manage. And they know even the best healthcare IT and security teams are insufficiently resourced, leading to more mistakes and higher inadvertent insider risk.

Healthcare security leaders know all of this, too. The question is: What can they do about it?

To protect against new attacks at scale — and safeguard data in use, at rest and in motion — in radically cloud-centered environments where perimeters are quickly fading, healthcare providers need to leverage more intelligence, more automation and, above all, better integration. This white paper shows how to combine best-of-breed cybersecurity solutions from Mimecast, Netskope and CrowdStrike in an integration to address the healthcare industry's most urgent information security challenges.

You'll learn how our combined Triple Play solutions simplify integration of IT security infrastructure, enabling defense in depth to modernize security and simplify operations without impacting performance for healthcare organizations. The white paper reviews specific challenges the Triple Play can help you address, shows how integration can be established in minutes, and presents use cases that demonstrate how the Mimecast, Netskope and CrowdStrike Triple Play delivers superior layered protection to secure modern healthcare organizations and their patients.

mimecast CROWDSTRIKE netskope

Facing the Twin Challenges of Cyberattack and Data Loss

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

Cyberattacks have grown more ubiquitous and sophisticated as they exploit compromised access, human trust and errors, and distributed cloud environments. Protecting endpoints, workloads, identities and data from today's zero-day attacks and advanced polymorphic malware are a challenge to every security team and often can't be deterred. Malicious actors increasingly take advantage of widespread vulnerable entry points into cloud environments to evade legacy defenses, which often involve logging in to a healthcare provider's own cloud services via legitimate credentials they steal via email phishing.

Reducing dwell time has become more crucial than ever. Even in industries where lives aren't at stake, companies aim to detect attacks in less than one minute, investigate them in under 10 minutes and remediate them in an hour or less. In healthcare, speed of remediation is even more crucial. Healthcare cybersecurity professionals must worry about ransomware attacks that take life-saving systems offline, cancel critical appointments, disrupt entire facilities, require enormous ransom payments — and leave the institution's reputation in shambles.

But cyberattacks aren't a security team's only challenge. Concurrently, healthcare organizations must manage explosive growth in data, potentially spread across thousands of apps and services. As HIPAA and other compliance rules toughen, client and patient privacy expectations also rise.

Data loss protection becomes more mission-critical, too, as malicious actors continue to exploit vulnerabilities to achieve their goal of stealing any and all organizational and patient data.

Healthcare organizations need unprecedented control and visibility into data in use, at rest and in motion. At the same time, clinical and other employees each want to choose their own devices and connections in order to access cloud services from anywhere, in hybrid work/home environments, avoiding traditional tools like VPNs that can sometimes deliver a poor user experience.

Responding with More Intelligence, Automation and Integration

How can healthcare 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, with shadow IT representing up to 97% of app use? How can they manage increasingly complex infrastructures with fewer resources?

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*, both for repetitive tasks such as authorizing new devices, and for remediation, which can only be effective against modern attacks if it is triggered automatically and starts working instantly upon recognition of a threat.
- Above all, *more integration*, so all security systems can share access to all the timely threat intelligence that is available, and make it actionable.

Integration is held "above all" because fast, reliable integration between modern healthcare IT and security tools is essential for actionable intelligence and automation. Integrating best-of-breed technology within your existing security stack ensures that intelligent systems have the timely and enriched information to analyze adversary tradecraft and react effectively — 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 healthcare security teams manage their infrastructures as a unified whole. But, as healthcare organizations know better than most, for integration to work, it needs to be practical and easy to implement — so they can apply it fully without sacrificing performance, a common side effect of adding complexity to their infrastructures.

Overcoming Traditional Challenges to Security Integration

For security organizations in healthcare environments, 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 can't manage, or locking yourself into a legacy vendor solution?

To address these issues, in 2021 Mimecast 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. Since then, all three partners have been working continually to expand and deepen integration, so you can automate email removals, create playbooks that trigger automated remediation, get more value faster from wraparound managed services, and deliver better care without adding unnecessary friction to the caregiver's experience.

What's more, 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.

Today's Threat Environment

- 90+% of threats still manifest first via email
  - 319 billion emails sent per day[1]
  - 2,415 cloud apps used in an average enterprise, 97% of them shadow IT[2]
  - 20% of users move sensitive data between cloud apps, risking DLP violations[3]
- Over 90+% of business leaders are adopting a hybrid working model for knowledge workers[4]

---

1 Radicati Group, Email Statistics Report, 2021-2025, February 2021.
2 Netskope Cloud and Threat Report, January 2022
3 Ibid
4 *Harvard Business Review* (Gartner), "11 Trends that Will Shape Work in 2022 and Beyond," January 13, 2022.

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.

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 health organization or system. 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 CrowdStrike-Mimecast-Netskope 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.
- **The CrowdStrike Falcon Platform** (base license or above) to provide next-generation endpoint protection against a full spectrum of attacks, from commodity malware to the latest exploits.
- **Humio, a CrowdStrike company, provides log management and observability** to analyze and correlate Mimecast email security logs with other key sources, centralizing visibility, accelerating detection across the full kill chain, enabling more complete threat hunting to uncover unremediated threats buried in your network, and disrupting more attacks before they can spread.
- **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 Exchange for bi-directional automated threat intelligence sharing for partner integrations with client deployments.

Working together, all these platforms share both data and analytics. This has multiple benefits. Given 90+% of new attacks first manifest through email, CrowdStrike and Netskope platforms 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, 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.

By sharing enriched data between platforms, healthcare organizations can get more threat context faster within their environment to improve their security team's detection and response capabilities. Combining Mimecast's high-quality early alerts with CrowdStrike Falcon's enriched endpoint telemetry allows Falcon to search networks to see if attacks first discovered in email have appeared elsewhere, so complex threats can be detected, investigated and remediated far more rapidly. Similarly, Netskope Next Gen Secure Web Gateway can better protect data across the organization by leveraging the knowledge being generated by Mimecast's platform to better protect users and data by blocking malicious content attempting to be stored or shared internally within cloud platforms.

Exchanging threat data is important but insufficient: to improve control within your distributed environment, you need ways to act on new threat data automatically and in near real-time to stay ahead of modern adversaries before a potential breach. To that end, Netskope, Mimecast, and CrowdStrike work together to deliver automated and actionable intelligence with continuous feeds to enable your team to stop bad actors.

Netskope directs 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 enhanced detection and response capabilities intelligence enables from layered security, the Mimecast-Netskope-CrowdStrike Triple Play reduces human error and increases speed of detection. 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 legacy orchestration tools can typically achieve, you can gain comprehensive visibility, simplify the unification of tools, and reduce time to protection.

The Triple Play also creates a unified omnichannel solution to prevent data loss across the entire organization by providing in-depth visibility and control from endpoint to cloud. Seamlessly improve control over your dispersed 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, Mimecast, Netskope and CrowdStrike make it easier to automate complex facets of your security, allowing you to "set-and-forget" — empowering security teams to accomplish more with fewer resources and focus 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. This continual collaboration and addition of new unified capabilities, such as new email headers embedded by Netskope and acted upon by Mimecast to improve compliance and prevent data exfiltration. In recent months, the partners have added cross-platform automation to block future emails matching a threat, removing emails matching threat indicators, whether to lock down a device in CrowdStrike, restrict a user's activity in cloud services in Netskope, or assign them additional security awareness training, all based on their actions in email or elsewhere.

To speed up your capabilities and prevent operation friction, 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.

Triple Play Use Case #1: Preventing Cloud Attacks

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

For example, in one likely scenario, a clinician in your organization receives a fake link to information about new hospital processes associated with a newly-emerged variant of COVID. A link might take a user to a SharePoint site asking them to download a weaponized Microsoft Office file. It might connect to a Google Drive to pull additional malware content. The malware can then fetch a configuration file from Github to tell it what to do, then use Slack to establish command and control, and finally achieve its ultimate goal: exfiltrating data from the user's endpoint to a Dropbox account controlled by the criminal.

Mimecast would recognize and block this email attack if it is directed to the employee through the official healthcare organization email account it serves. But most users have multiple email accounts, including personal accounts which may be used for work. An attacker may send malicious URLs or files to those accounts given their heightened vulnerability and lack of protection. With the integrated Mimecast-Netskope-CloudStrike 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.

Netskope can now leverage Mimecast's newest zero-day information to alert CrowdStrike to immediately block, alert, coach or quarantine content associated with the attack. With this layered protection, you gain more context allowing your team to stop the attack before it succeeds, whether it originates through a personal email account, a USB device or another vector. Moreover, at-risk endpoints can now have their access to cloud activities and data reduced, further protecting the organization.

With Humio, a CrowdStrike company, you get a log management platform that can easily ingest Mimecast email logs and create live searches that trigger near-real-time alerts on email threats. Users can then configure automated actions through SOAR platforms in order to disrupt attacks in progress and contain them before they can spread and worsen. Drawing on email data delivered continually by Mimecast, together with other high-value data sources such as network, identity and endpoint logs, Humio accelerates discovery of where attackers have moved within your environment.

Mimecast's detections of bad URLs, IPs or domain names can uncover key evidence for nearly-immediate use in containment. Since Humio maintains access to all logs across the entire timeline of the attack, healthcare organizations can be more confident that the full extent of an attack has been uncovered, enabling more focused, targeted, and effective remediation. Healthcare organizations save money by recognizing which systems needn't be rebuilt, while improving confidence that they've fully rooted out the attacker's presence.

Integration in Minutes, Step by Step

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

Integrating with the CrowdStrike's Falcon Insight™ endpoint detection and response solution requires only a few easy steps: Create an Integration procedure in Mimecast's administrative console, specify CrowdStrike Falcon Threat Exchange, add the authentication keys CrowdStrike provides, and enable notifications, automated email removal and two-way communications. The entire process typically takes no more than five minutes. Integration with Netskope is established through Netskope's Cloud Exchange administrative console, and is equally quick and straightforward.

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

Today, many healthcare organizations rely more than ever on traveling temporary staff. This makes it more complex to manage access, increases the risk of error, and adds friction to the staff experience, leading doctors and nurses to evade controls in a hurry to care for their patients.

Adaptive policies, bannering, and real-time awareness training can help with a transitory workforce in healthcare on new systems.

For example, temporary staff may be required to log on through technology such as a terminal server or a traditional VPN, sometimes resulting in unacceptable performance, or they may decide it's easier to receive critical files through their personal Gmail accounts than via hospital email addresses.

In the understandable interest of safety, hospital security administrators may err on the side of blocking activities; clinicians and other staff respond by evading controls. Even permanently affiliated clinicians likely operate from their own offices, with their own at-risk networks, devices, software, and third-party links — often, without the support of cybersecurity professionals. Data can exit healthcare organizations via cloud services outside your control, also known as shadow IT.

All of this makes it easier to lose personal healthcare information (PHI) — risking human life, as well as compliance and the institution's reputation.

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 in both email text and attachments, scanning them as they leave the client'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, 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.

As Netskope-Mimecast-CrowdStrike integration expands, shared APIs will identify individuals who have clicked high-risk links or even failed internal phishing tests, and use that information to optimize response. For example, a small chunk of personal information might not be automatically blocked by the Mimecast email gateway because it appears legitimate, but Netskope can query Mimecast to determine if this data has been moving around the organization. Using this output to recognize a threat, Mimecast can directly block new emails containing the same data for fortified protection. Conversely, Mimecast may recognize a data loss risk and inform Netskope, triggering automated instructions to the CrowdStrike Falcon platform regarding managed endpoints or through CrowdStrike's Humio log management platform.

In short, when working together, the Triple Play solution offers layered protection, reducing 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 personal email accounts or other weak links.

Next Steps: Gaining Even More Value from Integration

As suggested in the Data Loss Prevention use case above, implementing these Triple Play technologies establishes a foundation for driving more value over time. For example, healthcare organizations can leverage Mimecast's rich APIs to integrate additional security capabilities such as 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 — fortunately, Mimecast's identification of new attacks is often hours ahead of other email-based data feeds. Therefore, extending Mimecast data and insights more widely can continually increase customers' value. This extension of data helps healthcare organizations and beyond prevent elusive zero-day attacks, recognize intrusions rapidly, hunt threats effectively and trigger automated SOAR incident response playbooks quickly — reducing dwell time. Mimecast's open API platform makes it easy to customize integration, 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 helps healthcare organizations:

- **Improve alignment between security and IT operations.** With Triple Play integrated data, SecOps and IT ops 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.

- **Accelerate the implementation of top-level security strategies.** With the Triple Play, organizations have the timely information needed to support dynamic decision making about the security posture of any device, application or user seeking access; and can move toward fully aligning identity with policy. For example, healthcare organizations can widen the use of cloud services, confident that they'll have the same or better visibility and data loss prevention capabilities than in their legacy on-premises VPN environment. The combination of Mimecast-Netskope-CrowdStrike enables healthcare security teams to move toward a fully zero-trust adaptive policy architecture, fortifying security and ensuring defense-in-depth.

For more details on Mimecast integrations with the CrowdStrike Falcon platform, visit:
store.CrowdStrike.com/apps/mimecast

For more details on Netskope integrations with the CrowdStrike Falcon platform, visit:
store.CrowdStrike.com/apps/netskope

For more details about integrating with CrowdStrike Falcon, visit:
community.mimecast.com/s/article/CrowdStrike-Falcon-Integration

For more details about integrating with Humio, visit:
library.humio.com/reference/integrations/mimecast/index.html

For more details about Netskope integration, Netskope community members can log in and visit :
support.netskope.com/hc/en-us

Learn More and Move Forward

The Mimecast-Netskope-CrowdStrike integrated Triple Play helps healthcare organizations automate to slash threat response times, improve security teams' efficiency, enable better threat hunting across the kill chain, and resist both malicious attacks and data loss in an environment where everyone – from clinicians to clerical staff to cybersecurity specialists -- faces unrelenting pressure.

Given each partner's best-of-breed leadership, many healthcare organizations already have one or more of these technology platforms in place. If so, they possess an exceptionally easy and rapid path to end-to-end security integration that builds on existing investments. If not, the Triple Play offers a proven, well-supported, and complete best-of-breed alternative for evolving long-term cybersecurity strategies in the face of fast-changing threats. With the Triple Play, healthcare organizations gain state-of-the-art layered protection to minimize risks stemming from legacy technology and provide defense-in-depth security to proactively protect the organization, employees, and patients.

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

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