

mimecast



netkope



CROWDSTRIKE

okta

White Paper

The Powerful Alliance of CrowdStrike, Mimecast, Netskope and Okta:

Flexibly Integrating Best-of-Breed Solutions and Adaptive Controls

Executive Summary

Security and IT organizations must protect against new attacks at scale — and safeguard data in use, at rest and in motion — in cloud-centered environments where perimeters have faded as quickly as distinctions between work and home. To do so, they need to leverage more intelligence, more automation, and better, more flexible integrations.

This white paper shows how CrowdStrike, Mimecast, Netskope and Okta have combined their best-of-breed cybersecurity and identity solutions to comprehensively address information security and data loss challenges, including the rising problem of insider risk. The white paper reviews specific challenges these best-in-class solutions address, shows how integrations can be established in minutes, and presents three use cases that demonstrate the value delivered.

Facing the Challenges of Cyberattacks, Data Loss and Insider Risk

Today, 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 focus on access compromise, human trust and weaknesses. So has the rise in using standard cloud resources to evade legacy defenses, often by logging into legitimate cloud services with legitimate credentials stolen via email phishing. Today's zero-day attacks and advanced polymorphic malware challenge even sophisticated defenses, and can't always be deterred. Further, relying on

conventional password policies often causes poor user experiences, leading users to adopt bad practices that increase risk. And so, an increasingly difficult problem is insider risk, whether it is created by deliberate action, or more often, by careless or overwhelmed, inadequately trained people.

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. Per the "1-10-60 Rule," which CrowdStrike introduced in 2018, 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 can cause far more damage and become even harder to expunge.

In addition to deterring and mitigating cyberattacks, 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 user identity, coupled with user behavior resulting in data in use, both at rest and in motion. At the same time, organizations must improve employee user experiences while managing devices and connections in a "work from anywhere" world — otherwise, they can end up with users who are frustrated enough to try working around the security controls already in place.

Merely layering on additional tools that don't work together isn't the solution: It adds friction while sensitive data may remain at risk. Organizations need to make sure their tools work together smoothly and well so that they can quickly propagate information and act upon all the insights available to them. They also need unified identity services to respond in ways that are more adaptive, fine-grained, timely, accurate, and effective. As they do this, they open new opportunities, including the ability to build a true Zero Trust environment.

Responding with More Intelligence, Streamlined Operations, Scalability and Flexibility

How can security and IT teams 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 97%¹ of app use? How can they manage increasingly complex infrastructures with fewer resources?

Security and IT teams can answer these questions by applying:

- *More intelligence*, via AI and machine learning technologies capable of recognizing and acting on threats more rapidly, adaptively, 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 timely threat intelligence and as the organization grows, it can reliably control access to all of its infrastructure and data via a centralized identity and access management system.

¹[Netskope Cloud and Threat Report, Netskope, July 2021](#)

Integration is held “above all” because fast, reliable integration is essential to leveraging intelligence and automation. It ensures that intelligent systems always have the timeliest information to analyze — especially for alerting on 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.

In particular, it has become increasingly clear that the entire security stack should share a unified identity provider. By integrating identity services in flexible and innovative ways, organizations can improve visibility and access control across their entire estate, helping them manage their infrastructures through a unified, contextually driven identity defense..

Overcoming Traditional Challenges of Security Integration

For security teams, 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?

In the past, integrating diverse security solutions into a cohesive framework posed significant difficulties, leading to gaps in protection and increased management complexity. For example, security operations leaders were forced to build bespoke integrations for incompatible products that could often lead to gaps in visibility and an inability to share threat information.

However, with this integrated approach, organizations can now seamlessly consolidate their security operations and address various security aspects efficiently. This collaborative synergy empowers organizations to tackle traditional challenges of security integration with unparalleled effectiveness, creating a fortified security ecosystem that shields against emerging threats and enhances overall cybersecurity posture.

² [Mimecast State of Email Security](#)

³ [Harvard Business Review \(Gartner\), “11 Trends that Will Shape Work in 2022 and Beyond,” January 13, 2022](#)

⁴ [Mimecast State of Email Security](#)

⁵ [Radicati Group, Email Statistics Report, 2022-2026, November 2022](#)

⁶ [Mimecast State of Email Security 2023](#)

⁷ [The State of Phishing 2022, SlashNext](#)

⁸ [CrowdStrike 2023 Global Threat Report](#)

⁹ [Netskope Cloud and Threat Report, Netskope, July 2021 and Beyond,” January 13, 2022](#)

¹⁰ [Netskope Cloud and Threat Report, Netskope: 2022 Year in Review](#)

¹¹ [Netskope Cloud and Threat Report, Netskope, July 2021](#)

¹² [CrowdStrike 2023 Threat Hunting Report](#)

Today’s Challenging Threat Environment

- 94% of companies think they need stronger protections than those that come with their Microsoft 365 and Google Workspace apps²
- Over 90+% of leaders are adopting a hybrid working model for knowledge workers³
- 75% of companies say collaboration tools pose significant new security risks⁴
- 333 billion emails sent per day⁵, and email volumes continue to rise in 80% of companies⁶
- Phishing attempts rose by 61% in 2022, to an estimated 255 million⁷
- Access broker services grew more popular: More than 2,500 advertisements for access broker services, which provide or sell illicitly acquired access to organizations, were identified in 2022. This marks a 112% increase from 2021.⁸
- Users upload an average of 20 company files/month to personal apps⁹
- 48% of all HTTP/HTTPS malware downloads originated from cloud apps¹⁰
- 97%+ of company apps are not IT managed, and 48% of unmanaged SaaS apps receive poor risk ratings¹¹
- The average breakout time for interactive eCrime intrusion activity declined from 84 minutes in 2022 to 79 minutes in 2023.¹²

Toward Better and Easier Security Integration

CrowdStrike, Mimecast, Netskope, and Okta embrace the importance of a robust partner ecosystem, united to provide organizations with comprehensive protection, data loss prevention, and identity services. By seamlessly integrating our best-of-breed solutions, we empower organizations to enhance visibility, minimize friction, and effectively address the ever-changing landscape of security challenges.

Our collaborative approach enables our security products to share critical data and inspection insights, harnessing the power of multiple detection technologies across your entire organization. This results in true layered security that surpasses the limitations of siloed security tools. With our integrated solution, evading one supplier's inspection infrastructure becomes significantly more challenging for attackers, preventing them from extending their intrusions and amplifying their impact.

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

- **Mimecast Email Security, Cloud Gateway** to block the most sophisticated attacks with an AI-powered, email gateway in the cloud; easily manage complex email environments; customize policies to meet your needs; and get essential added protection for Microsoft 365 or Google Workspace.
- **Okta Workforce Identity Cloud (WIC)** to protect your employees, contractors, and business partners with Identity-powered security. Empower agile workforces and high-performing IT teams.
- **CrowdStrike Falcon® Platform** to automatically predict and prevent threats in real time. Purpose-built in the cloud with a single lightweight-agent architecture, the CrowdStrike Falcon® platform protects the most critical areas of enterprise risk — endpoints and cloud workloads, identity and data.
- **Netskope Secure Service Edge (SSE)** 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; as well as Cloud Risk Exchange (CRE) to create a dashboard view of contributors to your company's overall risk score and trend, and trigger risk-reducing actions through business rules tuned to a normalized weighted score.

Compelling Value, Here and Now

Working together, all four platforms share 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 ingest real-time telemetry on zero-day attacks first identified by Mimecast's email scanners.

Since threat sharing is bilateral, Mimecast also leverages continuous streams of threat data from Netskope and CrowdStrike, improving the performance of Mimecast Email Security when faced with zero-day threats that don't first appear via email and may be cloud-enabled.

CrowdStrike delivers comprehensive threat telemetry to Mimecast. After undergoing triage, detections generated within CrowdStrike can be transmitted to Mimecast. Mimecast then incorporates this data into a block list to proactively block incoming threats that correspond to the indicators of compromise (IOCs). Furthermore, Mimecast can then initiate a scan of users' inboxes to identify and eliminate any latent threats that align with the IOCs, effectively removing malicious emails from circulation.

By incorporating integrated Okta identity services, organizations can apply a wide variety of authentication types, up to and including state-of-the-art phishing-resistant multi factor authentication (MFA) techniques. These include FIDO 2.0/WebAuthn support, PIV smart cards and passwordless authentication that minimizes end-user friction with phishing-resistant factors and adaptive policy checks. Control over all authentications and access to all resources can be applied automatically in a more granular and precise manner than ever before through Okta's single view.

Beyond IOC sharing, related email telemetry is ingested by the CrowdStrike Falcon platform to help with cross-domain detections and can reduce analysts' response times through alert prioritization and predetermined response actions. Additionally, response actions to block future threats matching sender and domain information can be shared with Mimecast.

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

Security 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.

With Okta's identity services integrated, a wide variety of identity-related actions can be triggered upon discovery of a potential compromise or increased risk. These can include: inform administrators, force password reset, force use of MFA, completely revoke access, or remove access only to Microsoft 365, a VPN, or other specific services. Changes can be applied not just to individuals, but to entire groups or subsets of the organization, based on dynamically changing risk assessments.





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

Together, CrowdStrike, Mimecast, Netskope and Okta are delivering 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. This eliminates duplication and enables comprehensive monitoring through a single model and dashboard with unified control.

Working together, these offerings make it easier to automate more facets of security in order to simplify operations — empowering your teams to accomplish more with fewer resources and refocus on higher-value tasks. The result is “defense-in-depth” that is deeper as well as wider, more adaptive, and easier to manage.

Perhaps best of all, integrating CrowdStrike, Mimecast, Netskope and Okta is remarkably easy. It's 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

	<p>Product of the Year, Overall Email Security CRN 2022</p> <p>Top Player, Secure Email Gateway The Radicati Group 2021</p>	<p>Market Leader, Email Security and Management Cyber Defense Global InfoSec Awards 2022</p> <p>Customers' Choice, Email Security (4/5/5.0) Gartner Peer Insights™ 2021</p>	<p>Leader, Email Security, Intelligent Email Protection, Secure Email Gateway G2 Crowd Spring 2021</p>	<p>Leader, Enterprise Information Archiving Gartner® Magic Quadrant™ 2022, 2021, 2016-2020[1]</p>
	<p>Leader, Security Service Edge (SSE) Gartner® Magic Quadrant™ 2023, 2022</p>	<p>Customers' Choice, Security Services Edge SSE Gartner Peer Insights 2022</p> <p>Customers' Choice, Secure Web Gateway, CASB Gartner Peer Insights 2021</p>	<p>Leader, Cloud Access Security Broker (CASB) Gartner® Magic Quadrant™ 2021, 2020, 2019, 2018, 2017</p>	<p>World's Best Cloud Companies Forbes 2022, 2021, 2020, 2019, 2018</p>
	<p>Leader, Access Management Gartner® Magic Quadrant™ 2022, 2021, 2020, 2019, 2018, 2017</p>	<p>Customers' Choice, Access Management Gartner Peer Insights 2022</p>	<p>Leader, Identity as a Service For Enterprise Forrester Enterprise Wave™ Q3 2021</p>	<p>Strong Performer, Customer Identity And Access Management Forrester Wave™ Q4 2022</p>
	<p>Leader (16 categories) G2 Fall 2022</p>	<p>Best Security Company SC Awards US 2022</p>	<p>Leader, Endpoint Protection Platforms Gartner® Magic Quadrant™ 2022</p>	<p>Global Leader, Innovation & Growth, Cyber Threat Intelligence Frost & Sullivan Frost Radar™ 2022</p>

Integration in Minutes, Step by Step

Bidirectional integration among these solutions is easy to establish and requires no scripting or programming.

Integration with Okta is established with a few clicks: in just a few minutes, you can define the scope of an automated or semi-automated policy, define a separate policy and/or group for each detected action, and raise authentication requirements. Within the Okta console, you can define powerful dynamic workflows without writing any code. Often, you can simply adapt a built-in policy to your needs — for example, changing the length of time users are restricted after they respond to a phishing email.

Integration with Netskope is established through Netskope's Cloud Threat Exchange administrative console, and is equally easy to implement.

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.

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

For more details about integrating with Okta, visit

<https://community.mimecast.com/s/article/Okta-Evidence-Based-Controls-integration>

For more details about integrating with CrowdStrike, visit

<https://community.mimecast.com/s/article/api-and-integrations-crowdstrike-falcon-integration>

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

<https://docs.netskope.com/en/mimecast-and-netskope-integration-solution-guide/>

Use Case #1: Insider Risk and Supply Chain Protection

If a user has been compromised (by whatever means), an attacker may attempt to infiltrate your company's supply chain by sending out malicious links from that user, who is assumed to be a trusted source. Mimecast inspects all outbound email traffic for malicious content, whether it takes the form of phishing links, zero-day attachments or sensitive data. Recognizing the malicious link in this outbound email, it prevents delivery — but that's only the beginning.

Mimecast sends detail on this contact back to CrowdStrike in the form of Indicators of Compromise (IOCs), allowing analysts to begin investigations and triage at the endpoint layer, tracking known executions of the IOCs historically and moving forward. Additionally, Mimecast contacts Okta, and the compromised user is moved into an Okta group: perhaps a group of "high-risk" users or a group of "users currently under investigation," or one of multiple groups triggering different levels of response. Okta immediately applies policies based on the user's group and the access they have.

Okta can perform a wide variety of out-of-the-box or customized tasks that precisely reflect the organization's needs. It might block users from accessing any resource whatsoever until an investigation of their previous action is concluded. And it can immediately terminate sessions in progress, even VPN sessions accessing non-cloud corporate systems or the user's corporate PC.

Okta might alert relevant security teams about the incident, via Slack or any other collaboration tool they use. This can be done either in conjunction with blocking access or (in some cases) while a team member evaluates what is happening to determine if it's truly a problem. Okta can also block user logins to specific resources such as Salesforce, Microsoft 365 or any AWS service. Or, based on the organization's preferences, it might upgrade the user's authentication requirements, perhaps by prompting for multi factor authentication.

Within Okta, it's easy to create dynamic workflows that can perform virtually any action across the integrated toolsets, including Netskope's Security Service Edge and CrowdStrike's Falcon platform for protecting endpoints. Such actions can be triggered without added coding or scripting, so even junior security operations professionals can accomplish more and SecOps teams can be more effective despite skills shortages. Workflows like these can also streamline resolving a problem and approving users' removal from a high-risk group so they can return to their ordinary activities, once remediations such as reimaging a desktop have been performed.



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.

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. Alternatively, Mimecast DLP identifies data patterns on its own, recognizes the outbound email as high-risk, and prevents delivery.

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 Okta-controlled identities and policies that Netskope is applying to its controls over all cloud services an organization may be using, for example from Dropbox to Salesforce.

Typically, Okta would immediately terminate sessions within applications and prevent re-authentication. However, as in the preceding case study, Okta's granular identity controls make it possible to flexibly apply a wide range of specific actions, either to individuals or to groups. These might include notifying a specific administrator, or providing a specific warning to a user. In our shared, integrated solution, these Okta identity controls can be triggered whether the first sign of a compromise comes from Mimecast's recognition of a phishing attack, Netskope's recognition of an inappropriate download of customer data, or CrowdStrike's recognition of malware or the turning off of a firewall at an endpoint.

Working together, the integrated 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.



Use Case #3: Preventing Attacks on Cloud Services and More

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 solution in place, Netskope's Security Service Edge 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 and Netskope Cloud Threat Exchange can 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.

Plus, with Okta identity integration, it's easy to configure a wide variety of options, including force password reset set, force reauthentication using MFA, disconnect from application, inform administrators, or log a helpdesk ticket. Since Okta provides unified identity services across the entire digital estate, the same groups, policies and dynamic workflows you apply to cloud services can be applied to important corporate resources outside the cloud, such as back-end accounts payable systems accessed remotely by managers via VPNs.

This evolution in threats has led to the need for a consolidated view of your attack surface, spanning email security, endpoint security, and identity protection. By sharing bi-directional threat intelligence, analysts now have a holistic perspective with data aligned to a common schema, removing the need to navigate between products with varying data structures. This, in turn, speeds up operational and response times.

Going beyond extended detection, these integrations provide enhanced response capabilities. Within the CrowdStrike console, analysts can proactively initiate remediation actions with Mimecast and Netskope. Revisiting the example outlined earlier, the suspicious email originally seen from the World Health Organization's domain is identified as a threat, analysts can block the domain or sender directly from the CrowdStrike console, saving valuable time. The same proactive approach extends to Netskope, allowing the adjustment of group policies and user privileges. Okta identity management data is ingested into CrowdStrike, driving automatic responses to specific conditions, such as forcing a user to reset their password when a critical XDR detection occurs.

Through these integrations among CrowdStrike, Mimecast, Netskope and Okta, IOCs can be exchanged in real-time to protect against multiple threat vectors, and represent a substantial step forward in terms of visibility and taking swift precise actions to safeguard the environment.

Next Steps: Gaining Even More Value from Integrations

With these integrated technologies in place, the four partners have established a foundation for driving more value over time:

• **Enhanced Security:** Each of these solutions specializes in a different aspect of security, providing comprehensive protection for your organization:

- CrowdStrike's advanced threat detection and response capabilities safeguard endpoints against sophisticated attacks.
- Mimecast ensures robust email security, protecting against phishing attempts and malware.
- Netskope offers granular visibility and control over cloud applications, mitigating risks associated with unauthorized access and data leaks.
- Okta centralizes identity and access management, enforcing strong authentication protocols and reducing the risk of unauthorized access to sensitive resources.

• **Streamlined Operations:** Integrating these solutions into your architecture simplifies management processes through unified insight and reduced manual effort. Obtain threat visibility and context across multiple entry points into the organization, while alerting analysts to high priority events contributing to effective decision-making. It can avoid downtime by protecting people earlier — leading to fewer trouble tickets, fewer interruptions and fewer employees forced offline due to security problems. Uncover the full kill-chain right through automated data collection and risk reducing actions, improving analysts' ability to respond at scale, all while reducing time to protection and integration costs through pre-built integrations.

• **Continued Innovation and Reduced Complexity:** As you leverage the benefits of this close partnership, ongoing investments ensure smooth integration and high levels of support for their integrated environments, continually adding new synergistic capabilities not previously available. For example, Mimecast, Netskope and Okta are working together on continuous auth, which will expand the types of first-party Okta and third-party signals that can be continuously assessed for risk and can trigger access changes to accelerate remediation.

Learn More and Move Forward

The integration of CrowdStrike, Mimecast, Netskope, and Okta presents a transformative opportunity for organizations to enhance their cybersecurity posture in today's cloud-centered and hybrid work environments. By leveraging the strengths of each partner's best-of-breed solutions, organizations can achieve significant improvements in threat response time and security team efficiency, leading to both time and cost savings. This integrated approach ensures robust protection against malicious attacks and data loss, safeguarding critical assets in the ever-evolving threat landscape.

Many organizations may already have one or more of these leading technology platforms deployed, making the path to comprehensive end-to-end security administration remarkably straightforward and rapid. Leveraging existing investments in these solutions incurs no additional cost while unlocking even greater value. Additionally, for those organizations reassessing their long-term cybersecurity strategy, the collective integration offers a well-supported and complete route to best-of-breed security. The synergy among these solutions allows organizations to maximize the benefits of their cybersecurity investments and ensure a robust and resilient security posture.

To learn more about your best path to best-of-breed integration, contact your Mimecast sales representative.

Email alliancepartner@mimecast.com or visit mimecast.com today.