RAPID7 netskope mimecast

White Paper

The Rapid7-Mimecast-Netskope Triple Play:

A Better Way to Protect Data, Everywhere

Introduction:
A more complete and effective approach to data protection

Data protection is more important than ever. And it's harder, too. Organizations face relentless, explosive growth in the amount of data they must manage, and that data is now likely to be spread across dozens, hundreds or even thousands of apps and cloud services and potentially millions of diverse user devices. Meanwhile, compliance controls are growing ever more rigorous, customer expectations for data protection keep rising, and highly public data breaches are often significantly damaging reputations that were painstakingly built over decades.

In response, security organizations are seeking more coherent, comprehensive and automated ways to view activity, protect against data exfiltration, and act faster, earlier in the kill chain, to limit impact. It's not enough to invest in best-in-class security tools. Once you have them, those tools must be tightly integrated to protect data across the organization and throughout its lifecycle, and extend smoothly to apps and cloud services under your direct control as well as those used by employees which are outside your control. Those tools must also be operationalized by short-staffed teams in high-pressure environments. And as Gartner writes, effective security must combine "defined processes, well-informed and trained people, and effective technologies."[1]

1 Build a Successful Data Loss Prevention Program in 5 Steps, Gartner, February 2, 2022.

Protecting data with more intelligence, automation and integration

How can security organizations prevent data loss in highly complex environments, and with fewer resources? By applying:

- More intelligence, via machine learning technologies and more traditional analytics capable of recognizing and acting more rapidly and comprehensively than human analysts alone can, and by facilitating better decisions when humans are in the loop.
- More automation, from offloading repetitive manual tasks to accelerating and improving many facets of incident response and vulnerability management.
- More integration, so security systems can share access to all timely intelligence, and you can drive preventive, detective, investigations, and responses in concert across many security controls from multiple vendors, with all IT and security layers aligning and responding in concert.

In considering these three key tenets, note that simple, fast, and deep integration is essential to leveraging intelligence and automation. Integration ensures that intelligent systems always have the timeliest and most complete information to analyze and paths to respond. This is especially important in countering the latest attacks, such as fileless malware on private cloud resources, where greater visibility into the kill chain is essential to both detection and remediation.

Effective integration, for example, enables automated processes to extend from the email gateway and security service edge (SSE) to security information and event management/extended detection and response (SIEM/XDR) systems, and back. It helps security teams leverage their security controls as a unified whole, sharing and fully benefiting from rich logging (including apps and cloud services), metadata, indicators of compromise, malicious URLs, user activity, data movement, and advanced artificial intelligence/machine learning (AI/ML) analytics, including individualized user risk scoring, in near-real-time.

But how can organizations leverage integration effectively without adding complexity, or "locking in" to a single-vendor solution? At Mimecast, we have invested heavily in the industry's most complete, well-documented library of APIs and off-the-shelf third-party integrations. This approach to APIs has allowed Mimecast to take another step forward, enabling vendors like Netskope and Rapid7 to take advantage of this large library of APIs to create broadly capable integrations. As partners, Mimecast, Netskope, and Rapid7 can offer a strong foundation for integrated security and data loss prevention based on all three companies' best-of-breed technologies.

mimecast

Protecting data with more intelligence, automation and integration

- 90+% of threats still manifest first via email[2]
- 319 billion emails sent per day[3]
- 2,415 cloud apps used in an average enterprise
  - 97%+ of company apps are not IT managed, and 48% of unmanaged SaaS apps receive poor risk ratings[4]
- 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 cloud app instances[5]
- 50% of malware is now delivered via cloud apps[6]
- Over 90+% of leaders are adopting a hybrid working model for knowledge workers[7]

2. Mimecast research
3. Radicati Group, Email Statistics Report, 2021-2025, February 2021
4. Netskope Cloud and Threat Report, Netskope, July 2021
5. Netskope Cloud & Threat Report, Netskope, February 2021
6. Netskope Cloud and Threat Report, Netskope, April 2022
7. Harvard Business Review (Gartner), "11 Trends that Will Shape Work in 2022 and Beyond," January 13, 2022.

Meet the partners:
Mimecast, Netskope and Rapid7

Together, Mimecast, Netskope and Rapid7 offer end-to-end security and data loss prevention that far exceeds the capabilities of a single-supplier or of non-integrated solutions.

This collection of best-of-breed security products share data and analytical insights gathered by each, offering true layered security that helps companies link prevention, detection, investigation and response across tools and entire organizations. The combined solution is a welcome contrast to even the best single-vendor solutions, where evading one supplier's analytical infrastructure or not accomplishing timely detection to response can enable an attacker to run free for too long.

With the Mimecast-Netskope-Rapid7 "Triple Play," all three vendors complement each other. The result is greater protection, faster investigation and more focused remediation, whether issues are easily addressed (e.g., resetting a password on one user's laptop, blocking a bad domain associated with a high-risk inbound email), detecting data movement from company to personal app instances, or are more widespread and complex.

The Mimecast-Netskope-Rapid7 partnership brings together the following well-proven, widely deployed offerings:

Mimecast Email Security (Gateway) is award-winning email security that provides first-line defense against the attack vector that still represents 90% of new attacks: malicious email. It safeguards organizations against today's full range of email-related attacks at all levels of sophistication, including phishing, **business email compromise (BEC)**, spear-phishing, ransomware, malicious URLs and attachments, and more.

Rapid7 InsightIDR provides cloud-based SIEM/XDR capabilities to detect threats more rapidly, understand their true scope based on extensive relevant context, visibility, analytics, and respond more intelligently. In addition, **Rapid7 InsightConnect** multiplies your security team's impact with customizable workflows and integrations designed to operate consistently through a visual, workflow approach that integrates with Mimecast and Netskope through powerful plug-ins and multiple published workflows. Rapid7's SOAR, InsightConnect, spares security teams from mastering multiple APIs or creating and maintaining their own custom integrations. These two offerings are components of the **Rapid7 Insight Platform** that offers broad capabilities for assessing attack surfaces, vulnerability management, detecting suspicious behavior, and responding and remediating threats quickly with intelligent automation.

Netskope Intelligent Security Service Edge (SSE) unifies secure access service edge (SASE) networking and security services for cloud access security broker (CASB), secure web gateway (SWG) and zero trust network access (ZTNA) in a cloud-delivered single-pass architecture that ties security policies to identities. This protects users, applications and data even when employees use apps and cloud services outside IT control. Netskope also provides its **Cloud Threat Exchange (CTE)** for bi-directional automated threat intelligence sharing for partner integrations with customer security stack deployments. By integrating and sharing real-time telemetry on all major lanes of traffic — including web, managed and unmanaged/personal SaaS, IaaS offerings such as AWS S3 buckets, and public-facing custom apps — CTE increases visibility on rogue attacks. That includes the growing number of attacks that enter via email and contain links to compromised private SaaS services such as personal Google Drives and fake Microsoft login forms. In addition, Mimecast's scoring of each individual's awareness training participation and performance is now reflected in Netskope's Cloud Risk Exchange, contributing to its rich, accurate machine learning scoring of individual users. This can surface emerging insider or data exfiltration risks, such as signals that an employee may soon quit and take sensitive data.

The Triple Play creates a unified omnichannel solution for security and data loss challenges across the entire organization. It lets businesses improve control over their data via a single DLP engine that manages all enterprise data access, eliminating duplication and enabling comprehensive monitoring — all of which helps security organizations overcome traditional organizational and security control silos.

Robust two-way integration across all three platforms enables each to provide timely information that enriches their respective ability to both identify, and act on, risks. Working together, these offerings make it easier to automate more facets of security, helping security teams accomplish more with fewer resources. That way, security professionals can refocus on higher-value investigations and remediations, rather than a torrent of duplicative or undifferentiated alerts.

Mimecast, Netskope and Rapid7 have made — and continue to make — significant investments to ensure smooth integration and high levels of support for their respective systems. Mimecast and Netskope use Cloud Threat Exchange to automate threat intelligence sharing of new IOCs, while Rapid7 and Netskope use Cloud Log Shipper to export logs from Netskope to Rapid7 in near real-time. So, too, we are 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.

mimecast

Best-of-breed protection from recognized leaders

Tested and honored by customers and industry experts, over and over again.

Mimecast	**The Forrester Wave™: Enterprise Email Security** Forrester 2021	**Customers' Choice, Email Security (4/5/5.0)** Gartner Peer Insights 2021	**Leader, Email Security, Intelligent Email Protection, Secure Email Gateway** G2 Crowd Spring 2021	**Leader, Enterprise Information Archiving** Gartner® Magic Quadrant™ 2022, 2021, 2016-2020
Netskope	**Leader, Security Service Edge (SSE)** Gartner 2022	**Leader, Cloud Security Gateway** IDC Marketscape 2021	**World's Best Cloud Companies** Forbes 2020, 2019, 2018	**Cyber Security Award Data Protection - Enterprise** Fortress 2020
Rapid7	**Leader, MDR** IDC Marketscape 2021	**Leader, Magic Quadrant for SIEM** Gartner® 2021, 2020	**Strong Performer, Managed Detection & Response (MDR)** Forrester Wave 2021	**2022 Wizard Spider & Sandworm Participant** MITRE Engenuity ATT&CK® Evaluations

Use case #1:
Blocking malicious web resources

It's a common scenario: a web resource can be suspicious for any of a wide variety of reasons, and a security administrator needs to investigate whether the suspicion is warranted. If it is, the URL needs to be blocked across multiple systems as quickly as possible, lest users click the URL, visit the site, compromise their systems, and risk data exfiltration or ransomware. However, an incorrect blocking decision can inconvenience employees or even customers. And these "block/don't block" decisions often need to be made repeatedly, and then executed at scale, and enforced through web and email gateways, SSEs, and other systems.

Traditionally, these investigations are time-consuming and require multiple consoles and separate data sources, and multiple points of enforcement. Once a decision is reached, enforcing it may also require multiple manual actions. All this reflects the downside of today's rich but inadequately integrated security environments: investigations usually require pivoting from one suspicious indicator to another to gather critical evidence, grabbing and archiving evidence and finalizing a resolution. Running these investigations often traps analysts in a screen-switching cycle. The security team must learn, configure, monitor and use an increasing roster of tools, leading to endless cross-referencing, fact-checking, re-entering data and context-switching to accomplish even simple tasks.

Pre-built integrations developed for the Mimecast-Netskope-Rapid7 Triple Play radically simplify both investigation and response. For example, when triggered by a Rapid7 InsightIDR incident detection alert, Rapid7 InsightConnect can parse out the suspicious URL that drove the alert, gather extensive open-source or commercial intelligence data related to the URL and concisely present its findings to a human analyst in the preferred system, while requesting a simple decision to block or not. Once the analyst decides, pre-built integrations then instruct Mimecast's email gateway and/or Netskope's web gateway to take blocking policy update actions. Netskope Cloud Threat Exchange supports automated bi-directional threat intelligence sharing including file hashes and malicious URLs among triple play vendors for a seamless integration. The request for a decision can even be delivered via a Slack or Teams message, so the administrator can act even without opening a security console.

Explore this use case, along with a pre-built workflow.

Use case #2:
"Suspicious user" decisioning

In this case, Rapid7 InsightIDR generates an alert of suspicious user activity. A wide variety of user activities can contribute to triggering such an alert — for example, activity from an unexpected location; anomalous multiple file downloads or violations of mailbox forwarding rules that could suggest unauthorized attempts to exfiltrate data; or activities that diverge widely from a user's typical behavior.

Responding to this alert, Rapid7's InsightConnect goes to work, beginning by parsing the user's name and email from the alert details. The resources it can automatically draw upon for enrichment include Netskope's User Confidence Index (UCI), which uses machine learning models to score user risk. Based on this granular and dynamic assessment of the risk associated with this user and action, InsightConnect may suggest adaptive policy controls such as user quarantine or app activity limits, password resets, step-up authentication, real-time coaching that tells a user why an action is risky and guides them towards a safer alternative, or a request that the user justify the activity.

These suggestions would also reflect policy variables such as the sensitivity of a specific piece of data or a specific app. As in the first use case, the human analyst is presented with a policy choice — for example, do you want to force an Active Directory password reset or a step-up authentication? That choice draws on multiple sources of knowledge and insight and permits easy exploration of the context underlying the recommendation.

Explore this use case, along with a pre-built workflow.

Use case #3:
Malicious activity containment

Email remains the primary entry point into most organizations, and any attack which bypasses the inspection services can easily propagate across the user population through implicit trust of internal user emails. Working together, Rapid7, Netskope and Mimecast systems make it far easier to surface, prevent and mitigate the effect of malicious activity originated via email.

Rapid7 InsightIDR ingests logs from multiple sources and alerts the security team around a potential attack. Insight is provided related to the users, associated assets, and IoCs. Rapid7 InsightConnect, when triggered by a Rapid7 InsightIDR incident detection alert, can parse out the related user that drove the alert. The next step in the playbook is to search the associated logs from Mimecast for related emails containing viruses, and Netskope for identified DLP actions, all within the previous hour.

The results from the queries are then presented to an analyst in InsightIDR, where the analyst can make a final decision to quarantine the associated device by leveraging the Rapid7 agent, or take no action at all.

Working together, the Netskope-Mimecast-Rapid7 Triple Play makes it possible to improve the speed to response, which is based on contextual information thus improving analysts' decisions, and reducing overall risk.

Explore this use case, along with a pre-built workflow.

Next steps: Evolving integrations to increase value

With the Mimecast-Netskope-Rapid7 Triple Play in place, organizations have a foundation for driving even more value over time. They can leverage Mimecast's rich APIs to integrate additional security capabilities, making it easier to share data flows being generated by Mimecast, Netskope or Rapid7, and apply decisions made in tools such as Rapid7 InsightIDR and Rapid7 InsightConnect.

Ninety percent of attacks still manifest first in email, and Mimecast's identification of new attacks are often hours ahead of other data feeds. Therefore, extending Mimecast data and analytics more widely can continually increase their value. It helps organizations reduce risk, protect data across its lifecycle, recognize data loss and insider risks as soon as they emerge, and trigger automated responses more quickly. Put another way, it helps you accelerate your organization's prevention, detection, investigation and response.

Integrating Mimecast, Netskope and Rapid7 technologies also offers a platform for:

- **Improving alignment between security and IT operations.** With 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 earlier — leading to fewer trouble tickets, fewer interruptions and fewer employees interrupted 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 throughout the development lifecycle.

- **Accelerating the implementation of top-level security strategies.** For example, organizations can accelerate their cloud transition, confident that they'll have the same or better visibility, security, and data loss prevention capabilities that they had in legacy on-premises/VPN environments. They may be able to move more aggressively toward a fully zero-trust 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

As we've discussed, the integration of Mimecast, Rapid7 and Netskope can significantly improve organizations' ability to prevent data loss and improve their security organizations' efficiency through the entire data lifecycle and the entire kill chain.

Given each partner's industry-leading role, many organizations already have one or more of their widely deployed systems in place. If so, you possess an exceptionally easy and rapid path to comprehensive, end-to-end security administration as described in this paper.

Regardless of their existing infrastructure, many organizations are reconsidering their long-term strategy for security integration. Together, Mimecast, Rapid7 and Netskope offer a proven, well-supported and comprehensive route to integrations. By leveraging the capabilities of three exceptional providers, you can achieve stronger layered protection and avoid the added risks and complexity of a siloed, single-provider solution.

Learn more about the path to best-of-breed integration with **Mimecast**, **Netskope**, and **Rapid7**.

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.