

SOLUTION BRIEF

Netskope and Mimecast

While collaboration tools are increasingly adopted and present new challenges for IT Security teams, traditional email communications cannot be overlooked and left unprotected. Industry experts agree that email is the most commonly used attack vector today. Netskope and Mimecast provide security solutions that can help.

KEY USE CASES

- **Prevent data exfiltration through email:** Stop sensitive content from being emailed outside of your organization, even between business and personal instances of email
- **Protect sensitive content shared in collaboration tools:** Control activities that attempt to move sensitive data between cloud apps like Microsoft Teams and SharePoint
- **Secure critical data in storage:** Detect and protect sensitive data stored in managed cloud applications like Microsoft OneDrive
- **Establish consistent policies:** Create and enforce consistent data protection policies across SaaS, IaaS, web, and email
- **Create in-depth threat defenses:** Deploy threat protection to detect and stop malware in storage apps, cloud phishing, and more
- **Maintain an up-to-date security posture:** Exchange threat intelligence between solutions to strengthen your security posture and streamline incident response

THE CHALLENGE

With the rapid adoption of cloud applications and services, sensitive data is increasingly at risk as it moves outside the enterprise perimeter and beyond the reach of traditional security tools. Continuous and consistent data protection policies are now required across IT-managed cloud applications, plus thousands of user- and business-led cloud services, email, and websites that allow uploading or posting of data. Despite having native security controls, today's cloud applications provide limited protection against data loss and exposure, putting your sensitive information at risk. You need an integrated, more comprehensive security solution with less complexity.

NETSKOPE WITH MIMECAST

Netskope and Mimecast partner to provide a joint solution that addresses modern cloud security challenges and secures your data regardless of user location, application, or device type. Netskope, the leading security cloud company, provides deep visibility and granular control of cloud applications and the web, as well as advanced data and threat protection.

Mimecast, the leading email security company, supplies comprehensive email security, data protection and threat intelligence that complements Netskope and empowers common customers with enhanced protection, shared threat intelligence, and integrated workflows to optimize their security posture and operations.

CAPABILITIES

COMPREHENSIVE EMAIL SECURITY WITH CLOUD DLP

Together Netskope and Mimecast provide an “omni-channel” data loss prevention (DLP) approach to detecting and protecting sensitive information across your evolving cloud environment.

Preventing data exfiltration via email is a fundamental capability, ensuring sensitive content is not sent outside the organization or shared with unauthorized users. With the ability to understand and decode the modern language of the cloud (i.e., APIs, JSON, Protobuf) via Netskope Cloud XD, specific details of users, actions, applications, instances, and more can be used to enforce policies. For example, identifying attempts at exfiltrating data between business and personal instances of email is possible (i.e., john-work@corporate.com → john-personal@gmail.com). This also applies to preventing data loss between managed and unmanaged cloud apps. DLP policies can prevent insider threats, such as users downloading sensitive data from an approved app like Microsoft OneDrive and then uploading it to an unmanaged, unapproved app like Dropbox. This advanced protection is paramount for collaboration apps like Slack and Microsoft Teams, ensuring that proprietary information is not shared using chats, screen captures, or web form posts. Whether you are communicating with business partners via email, using SaaS applications like Slack or IaaS services like Amazon S3 buckets, or accessing numerous websites, Netskope and Mimecast protect your critical data from unauthorized access and inadvertent exposure.

Spam and impersonation attacks surged to the top of the list of cyberattack vectors during the coronavirus pandemic.

Mimecast Threat Intelligence, 2020

ADVANCED THREAT PROTECTION (ATP) FOR EMAIL AND CLOUD APPS

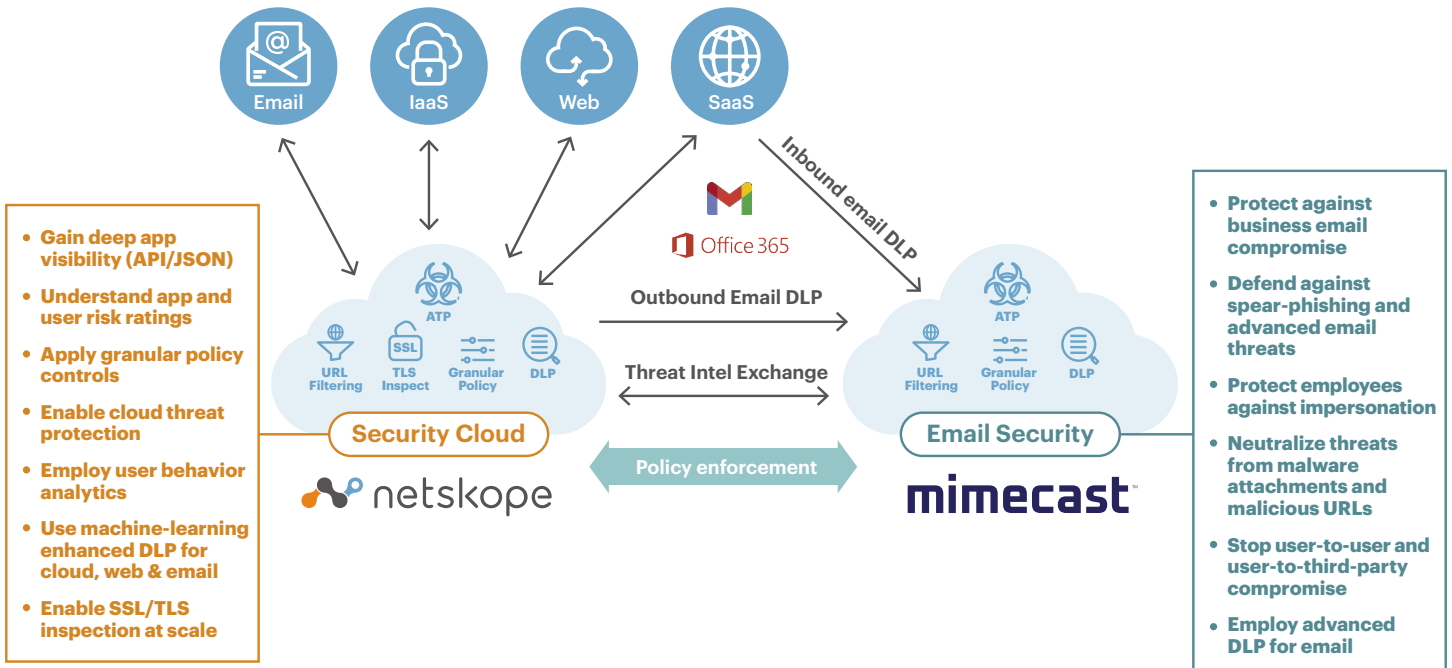
Preventing modern attacks like phishing and malware—whether delivered via email or the cloud—ensures that organizations have a solid security posture to stop inbound threats and their propagation internally. Email remains the number one attack vector in targeted and untargeted attacks, with cloud-delivered threats not far behind, as 70% of malware is now cloud delivered.* SecOps and Incident Response teams need a defense in-depth approach to battling these threats, and Netskope and Mimecast provide complementary solutions to resolve these challenges.

Mimecast protects organizations against business email compromise. This includes spear-phishing, file-less malware, and advanced malware attacks through a combination of static file analysis and sandboxing technologies. Malicious URLs are inspected and blocked via smart web defenses, and impersonation attacks are identified and stopped for targeted users.

Netskope protects organizations from attacks coming in via web and cloud applications with a combination of capabilities, including sandboxing, true file type analysis, URL filtering, and AI/ML-based threat analysis. Abnormal behaviors like bulk downloads and deletions are thwarted in real time via User and Entity Behavior Analytics (UEBA).

Granular policies can be applied to email, the web, and managed and unmanaged cloud apps to offer protection based on an organization’s unique needs. Instead of a broad “allow” or “block” approach, Netskope enables you to enforce granular user and account instance-aware policies to mitigate risk while maintaining productivity.

*Netskope Cloud and Threat Report, 2021



THREAT INTELLIGENCE SHARING STRENGTHENS SECURITY POSTURE

Modern security and risk challenges require multiple defenses with unique capabilities, combined with shared timely threat intelligence. With Netskope Cloud Threat Exchange (CTE), threat intelligence is shared in near real time, bilaterally between Netskope and Mimecast, as well as between Netskope and other security tools like Security Information and Event Management (SIEM) and Endpoint Protection Platform (EPP) solutions. Over 40 threat intel feeds are supported, plus the importing of Indicators of Compromise (IOCs), malicious URLs, and file hashes, to enhance threat defenses from both companies, ultimately benefiting joint customers.

Mimecast uses this threat intelligence to influence its prevention actions, such as stopping the latest cloud-based ransomware and impersonation attacks. Similarly, Netskope

70% of malware is now cloud delivered.

Netskope Cloud and Threat Report, 2021

garners threat intelligence from Mimecast to register, share, and stop threats from email. A CTE dashboard provides overall information on how frequently IOCs have been seen and from what systems, enabling joint customers to determine the scope of their attack surface.

The overall result enables optimized enforcement, reduced risk, and a boosted organizational security posture, ensuring that all users and devices, regardless of location, are protected with up-to-date threat intelligence.

DEFENSE IN-DEPTH: EMAIL, DATA, AND APPLICATION SECURITY

Combined, Netskope and Mimecast supply a powerful, extensible platform for securing email, cloud applications, and web access. Using granular visibility and contextual controls and data and threat protection across web, email, and cloud applications, the integrated solutions offer a modern defense in-depth design that benefits organizations of all sizes.

Providing uniform policy enforcement with “omni-channel” DLP simplifies management and operations significantly. With a 4-in-1 data protection solution (SaaS, IaaS, web, and email), and shared threat intelligence, SecOps teams have less to worry about and can focus on proactively enhancing their environment rather than constantly being reactive.

Lastly, Netskope NewEdge provides an optimized, high-performance global security cloud to enable advanced, real-time security functions like ATP and DLP for users anywhere, anytime. NewEdge eliminates costly backhauling and improves performance for remote offices and users going direct to net for their cloud applications. With its direct peering with Microsoft and Google in every data center worldwide, customers everywhere will have a positive, fast experience while using Netskope to access and protect their Exchange/O365 and Gmail services.

ABOUT MIMECAST

Mimecast (NASDAQ: MIME) 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 are the company that built an intentional and scalable design ideology that solves the number one cyber attack vector—email. 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. Learn more about us at www.mimecast.com.



The Netskope security cloud provides unrivaled visibility and real-time data and threat protection when accessing cloud services, websites, and private apps from anywhere, on any device. Only Netskope understands the cloud and takes a data-centric approach that empowers security teams with the right balance of protection and speed they need to secure their digital transformation journey. Reimagine your perimeter with Netskope.