SOLUTION BRIEF

Mimecast and Zscaler

Unified protection for sensitive data and business communications, combining Zscaler's Advanced Data Protection with Mimecast's Email Security platform.

Problem

Organizations embracing cloud services are discovering that traditional security approaches no longer suffice. As employees access resources from anywhere, the distinction between internal and external networks has vanished, protecting corporate assets is increasingly challenging as threats find new ways to exploit gaps in security coverage. The natural response to evolving security needs has led organizations down the path of tool accumulation, resulting in what can only be described as a tangled web of security solutions. This fragmented approach has created significant technical debt and operational complexity.

Alert fatigue has emerged as a critical concern for security teams dealing with an overwhelming volume of notifications from disparate security tools. This challenge is particularly acute given the rise of sophisticated multi-vector and multi-stage attacks, including advanced phishing campaigns, info stealers, and account ransomware. Security teams find themselves drowning in alerts while trying to piece together threat intelligence from disconnected systems, often missing critical signals amid the noise. Valuable time is spent in switching between tools and correlating information manually – time that could be better spent on strategic security initiatives and proactive threat hunting. The impact of these challenges extends beyond security effectiveness to affect business operations and risk management.

This understanding of current security challenges provides the foundation for developing more effective security strategies that address both immediate tactical needs and long-term strategic objectives. By acknowledging these pain points, organizations can better evaluate solutions that truly address the root causes of their security challenges rather than adding to the complexity.

Key Takeaways

- **Build layered defense**
  Share threat intelligence and enhance protection
- **Unified data protection**
  Consistent DLP policies across email and web channels
- **Simplify security operations**
  Reduce manual effort, tame complexity

$4.88 million global average cost of a data breach [1]

$10.5 trillion annually global cost of cybercrime [2]

85% of all social engineering attacks are attributed to phishing[3]

1. www.theconsultingreport.com/ibm-report-reveals-significant-rise-in-global-data-breach-costs-in-2024/ - :~:text=IBM%27s latest "Cost of,has surged to %244.88
2. www.forrester.com/predictions/#:~:text=With%20cybercrime%20expected%20to,while%20organizations%20pivot%20to
3. securityboulevard.com/2019/06/phishing-number-one-cause-of-data-breaches-lessons-from-verizon-dbir/

Protection Made Simple: The Mimecast and Zscaler Advantage

The integration between the Mimecast Human Risk Management platform and the Zscaler Zero Trust platform transforms how organizations protect their digital assets through a comprehensive, cloud-native solution. At its core, this solution operates through an extensive API framework that seamlessly connects security platforms and tools, creating a unified defense against modern cyber threats. The foundation begins with sophisticated threat sharing capabilities, where security intelligence flows bidirectionally between email and web security solutions. This continuous exchange ensures that when teams detect a threat in one channel, protection automatically extends across the entire security enterprise.

This integration eliminates security silos while maximizing the effectiveness of existing security investments. By creating a unified security fabric that spans email and web security, organizations achieve comprehensive protection without the complexity and overhead typically associated with managing multiple disparate solutions. This approach enhances security posture while providing the scalability and flexibility needed to address evolving cyber threats in today's dynamic business environment.

Today's digital workplace demands a sophisticated approach to protecting sensitive data. The integration delivers comprehensive data loss prevention by combining intelligent data discovery and protection capabilities across all channels. This unified approach ensures sensitive data remains protected whether it moves through or resides in web applications, cloud services, or email channels. This analysis extends beyond simple pattern matching to understand the context and sensitivity of the information being shared.

Through this unified approach, organizations implement consistent security policies across all communication channels while maintaining the agility needed to respond to emerging threats. The cloud-native architecture ensures efficient scaling of security operations while maintaining optimal performance, regardless of size or geographic distribution. This comprehensive strategy represents a fundamental shift from reactive, siloed defenses to a proactive, unified security posture built for modern business challenges.

Use Cases

Defenses with Threat Intel Sharing

Problem: A leading financial services organization struggled with sophisticated phishing attacks that bypassed traditional email security. Their security team managed 45 different security tools, creating significant blind spots between email and web security channels. Attackers exploited these gaps by launching coordinated attacks that began with phishing emails and led users to malicious websites.

Solution: By implementing the integrated Mimecast and Zscaler solution, the firm created a unified security fabric that enhances protection through real-time threat intelligence sharing between email and web security channels. Given that email serves as a primary mechanism to initiate breaches, Mimecast is at the forefront of receiving, analyzing, and identifying suspicious activity within email content. When Mimecast detects a suspicious email, it analyzes URLs embedded in the email and shares a list of these suspicious URLs with Zscaler. Zscaler then leverages this threat intelligence to enforce appropriate controls across the entire enterprise, proactively blocking access to associated malicious websites. This seamless integration strengthens the financial services organization’s ability to neutralize threats at both the email and web access layers, ensuring comprehensive security coverage.

Compliance Through Unified Data Protection

Problem: A large healthcare provider faced increasing challenges protecting sensitive patient data across email and web channels. Their existing fragmented security approach made it difficult to maintain consistent data protection policies, putting them at risk of compliance violations and data breaches. Manual coordination between security tools delayed threat response and strained IT resources.

Solution: To address these issues, Mimecast and Zscaler partner to deliver a unified data protection framework tailored for comprehensive protection of sensitive data across multiple channels. With this integration, emails received by Mimecast are automatically forwarded to Zscaler for advanced scanning and data classification. Zscaler's advanced file inspection capabilities identify where the content is sensitive or malicious and relay this decision back to Mimecast. Mimecast then enforces appropriate native email security policy actions. This integrated approach eliminates the operational silos of monitoring sensitive data loss across multiple channels within the healthcare provider's organization, ensuring compliance and reducing the risks associated with loss of confidential data.

Manufacturing Enterprise Streamlines Security Operations

Problem: A global manufacturer's security team spent excessive time switching between platforms to investigate and respond to threats. With operations across multiple time zones, their SOC analysts struggled to maintain consistent security controls and rapid incident response. The lack of integration between security tools created delays that attackers could exploit.

Solution: Implementing the Mimecast-Zscaler integration transformed their security operations through automated threat detection and response. The solution's cloud-native architecture enables consistent policy enforcement across all locations, while automated workflows reduce manual intervention.

About Mimecast

Mimecast is a leading AI-powered, API-enabled connected Human Risk Management platform, purpose-built to protect organizations from the spectrum of cyber threats. Integrating cutting-edge technology with human-centric pathways, our platform enhances visibility and provides strategic insight that enables decisive action and empowers businesses to protect their collaborative environments, safeguard their critical data and actively engage employees in reducing risk and enhancing productivity. More than 42,000 businesses worldwide trust Mimecast to help them keep ahead of the ever-evolving threat landscape. From insider risk to external threats, with Mimecast customers get more. More visibility. More insight. More agility. More security.