Solution Brief

Mimecast and Rapid7 InsightIDR

Security insights for proactive detection

Attackers target and leverage an organization's weakest security link - its people. By sending fraudulent messages designed to trick a person into revealing sensitive information (also known as phishing), executing business email compromise (BEC) attacks, impersonating brands, etc. - email is huge vulnerability teams need to secure.

By integrating **Mimecast** with **Rapid7**, organizations can analyze and investigate reported phishing attempts in minutes - stopping attacks before malicious actors can gain momentum in the network. Security teams can save time by accelerating the onboarding process, leveraging an intuitive dashboard to cut cyber attack detection time, and full visibility into the kill chain for proactive response.

Key Benefits:

- Earlier detection and containment of attacks, with rapid response to phishing and business email compromise tactics.
- Rapid7's InsightIDR, analytics and threat intelligence enrichment, detects threats within Mimecast events.
- Increase protection, reduce resource utilization, and improve analysis and knowledge of threats through built-in dashboards and Mimecast regional threat intelligence.
- Correlation across Mimecast events, alongside user, cloud, endpoint, and network data and detections from InsightIDR to quickly identify high-risk individuals and devices that may create future security breaches.

The Security Dilemma: Email Provides an Open Door to Attackers

Email is critical to business. With more people working remotely than ever before, employees depend on email almost exclusively to interact and collaborate with colleagues, suppliers, and customers. However, it is also an open door for threats.

Attacker tactics continue to change and become more sophisticated, and all the while new vulnerabilities are constantly being discovered. As these and other email-based attacks continue to surge, with countless ways attackers can break in, protecting email continues to be among the biggest challenges security teams face.

That said, securing email is one of the most important steps you can take to safeguard your organization from business disruption, data loss, and financial damage.

Email is an incredibly rich source of telemetry and threat intelligence – but this can often get lost in the noise of an enterprise security operation. Traditional rules-based detection requires fine-tuning and focuses primarily on known threats. Today's Security Information and Event Management (SIEM) tools must shift focus to visual, context-rich entities with email data, which allows Security Operations Center (SOC) teams to view their largest threat alongside other perimeter defense and security tools.

Integrated Solution

Mimecast and **Rapid7** provide an integrated solution to improve detection, stop threats and provide security insights gathered across the organization. Mimecast's Secure Email Gateway is often the first system to detect new threats through its multi-layered inspection capabilities. By integrating Mimecast with Rapid7 InsightIDR, security teams can leverage advanced threat detection, enhanced investigation, and faster response to increasing their overall level of protection through proactive actions that identify at-risk users and devices. Together, the platforms share high-fidelity indicators to help analysts quickly and accurately identify the root cause of an attack and remediate the threat. This helps security teams ward against initial infection and lateral spread that can lead to downtime, ransom demands, lost data, and stolen passwords.

InsightIDR, Rapid7's cloud-native SIEM and XDR, correlate millions of daily events in your environment directly to the users and assets behind them highlighting risks across your organization and prioritizing where to search to spot anomalous activity or threats in the cloud easily.

InsightIDR can ingest Mimecast logs, along with other log sources, to obtain complete visibility across environments and supports a robust library of third-party integrations to supplement its out-of-the-box endpoint, network, and user coverage. InsightIDR is built for dynamic, ever-changing environments to keep a step ahead of even the slickest attackers.

Mimecast + Rapid7 InsightIDR: Customer Use Cases

Threat correlation	Identify initial attack deployment methodology, characteristics, and subsequent access attempts without the need for manual effort or multiple toolsets.
Advanced threat detection	Improve your organization's security posture and detect threats by augmenting email perimeter defense with user and entity behavior analytics.
Lateral movement detection	Detect and follow attackers even as they switch IP addresses, devices, or credentials.
Alert prioritization	Increase efficiency and effectiveness by prioritizing the most pressing threats.
Threat intelligence	Understand how your organization has been targeted and what attacks have been blocked for better protection at the email perimeter, inside the network, and beyond its perimeter.

About Mimecast
For organizations concerned about cyber risk and struggling to attract and retain sufficient cybersecurity expertise and budget, Mimecast delivers a comprehensive, integrated solution that protects the No. 1 cybersecurity attack vector: email.

Mimecast also reduces the time, cost, and complexity of achieving more complete cybersecurity, compliance, and resilience through additional modules, all while connecting seamlessly with other security and technology investments to provide a coherent security architecture.

Learn more at **www.mimecast.com**

About Rapid7
Rapid7 (Nasdaq: RPD) is advancing security with visibility, analytics, and automation delivered through our Insight Platform. Our solutions simplify the complex, allowing security teams to work more effectively with IT and development to reduce vulnerabilities, monitor for malicious behavior, investigate, and shut down attacks, and automate routine tasks.

Over 10,000 customers rely on Rapid7 technology, services, and research to improve security outcomes and securely advance their organizations.

Learn more at **www.rapid7.com**