Solution Brief

mimecast

Mimecast and Exabeam

From detection to security insights.

Key Benefits

- Earlier detection and containment of attacks, with rapid response to phishing and business email compromise tactics.
- Exabeam 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, cloud, endpoint, and network data to quickly identify high-risk individuals and devices that may create future security breaches.

Cyberattacks are rooted in compromised credentials, most of which stem from emails. Through phishing, business email compromise (BEC) attacks, brand impersonation, and more, attackers use an organization's weakest security link — its people. As a result, email is one of the top three most common attack vectors for security teams to secure.

By integrating Exabeam and Mimecast, organizations gain search and correlation capabilities connecting email security to all other security log types to detect, investigate, and respond to cyberattacks. Using market-leading behavior analytics, data insight models, and extensive threat hunting capabilities, security teams can cut cyberattack detection times and uncover the entire kill chain by finding threats and other potentially malicious activity missed by other tools.

The Security Dilemma: Email Provides an Open Door to Attackers

From sharing proprietary information to sending financial details, email is how critical business gets done. With more people working remotely than ever, employees largely depend on email to interact and collaborate with colleagues, suppliers, and customers.

As these and other email-based attacks continue to surge, with countless ways attackers can break in, protecting email is among the most significant challenges security teams face. From business email compromise and spear-phishing to weaponized attachments and malicious URLs, attackers have many ways to get into an organization. In addition, their tactics continue to change and become more sophisticated while new vulnerabilities are constantly discovered. That said, securing email is one of the essentialsteps 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 enterprise security operations focusing on perimeter security devices. Security Information and Event Management (SIEM) tools must provide a central source of collating and correlating data from every part of the security stack to combine weak signals into meaningful attack timelines. This requires a shift in focus to visual, context-rich entities that show email security incursions, allowing SOC teams to view their largest threat vector alongside other perimeter defense and security tools.

Once an attack is initially contained, security teams must focus on uncovering all the events in an attack commonly found in the MITRE ATT&CK framework — a task that calls for the meticulous yet expeditious analysis of current and historical logs alike. Thorough investigations enable targeted remediation for affected systems and credentials to avoid significant operational impacts through mass system rebuilds. Legacy SIEM technologies have important limitations with the amount of data that can be ingested and retained, with slow historic search speed and high cost of ownership and operation. Because of high data retention costs, SIEMs often choose not to retain email security logs, creating organizational blind spots and increasing cyber and operational risks that worsen as data volumes increase. In turn, security teams become further constrained in their ability to manage risk, prevent data breaches, and avoid sky-high costs.

exabeam™

Exabeam and Mimecast - An Integrated Solution

Exabeam and Mimecast provide an integrated solution to improve detection, stop threats, and provide security insights across the organization. Mimecast's Secure Email Gateway is often the first system to detect new threats through its multi-layered inspection capabilities. Mimecast with Exabeam allows security teams to quickly detect, investigate, and respond to cyber threats that typically involve at-risk users and devices. This enables security teams to prevent initial infection and mitigate lateral spread that can lead to downtime, ransom demands, data loss, and stolen passwords.

The Exabeam integration with Mimecast equips security teams to better mitigate email and credential-based attacks across all IT environments. When combining Mimecast log data with Exabeam Security Analytics, customers can baseline normal activity for all users and entities. This integration allows security teams to visualize all notable events within a contextualized, automated Smart Timeline(™). The timeline provides the complete history of an incident and highlights the risk associated with each event. This powerful visualization and context streamlines investigations, eliminating hundreds of analyst queries.

Exabeam + Mimecast: Bringing insight to email security

Mimecast Email Security surrounds your communications with continuous protection to block the most sophisticated threats. By integrating Mimecast with Exabeam, you can leverage advanced threat detection, investigation, and response to increase your overall level of protection, increase your ability to identify email-based attacks, and take proactive action to identify specific individuals or devices that may become targets.

Together, Exabeam and Mimecast share high-fidelity indicators to help analysts quickly and accurately identify the root cause of an attack and remediate the threat. This enables you to protect your organization against initial infection and lateral spread that can lead to downtime, ransom demands, lost data, and stolen passwords.

Mimecast + Exabeam: Customer Use Cases

- **Detect and contain** attacks earlier with rapid response to phishing and business email compromise tactics
- **Enrich threat detection** involving Mimecast events with Exabeam analytics and threat intelligence
- **Increase** protection, reduce resource utilization, and improve analysis and knowledge of threats through built-in dashboards and Mimecast regional threat intelligence
- **Quickly identify** high-risk individuals and devices that may create future security breaches with correlation across Mimecast events, cloud, endpoint, and network security data

About Mimecast

Since 2003, Mimecast has stopped bad things from happening to good organizations by enabling them to work protected. We empower more than 40,000 customers to help mitigate risk and manage complexities across a threat landscape driven by malicious cyberattacks, human error, and technology fallibility. Our advanced solutions provide the proactive threat detection, brand protection, awareness training, and data retention capabilities that evolving workplaces need today. Mimecast solutions are designed to transform email and collaboration security into the eyes and ears of organizations worldwide

Learn more at **http://www,mimecast.com**

About Exabeam

Exabeam is a global cybersecurity leader that created the New-Scale SIEM™ for advancing security operations. Built for security people by security people, we reduce business risk and elevate human performance. The powerful combination of our cloud-scale security log management, behavioral analytics, and automated investigation experience gives security operations an unprecedented advantage over adversaries including insider threats, nation states, and other cyber criminals. We Detect the Undetectable™ by understanding normal behavior, even as normal keeps changing – giving security operations teams a holistic view of incidents for faster, more complete response.

Learn more at **http://www.exabeam.com**