Solution Brief

mimecast | SentinelOne

Unify endpoint and email with SentinelOne and Mimecast

Integration Benefits

- Increase efficiency of incident triage and investigation.
- Expand visibility into endpoint and email activity.
- Reduce dwell time of insider threats with adaptive policy-based management.
- Reduce attack surface by integrating leading endpoint and email platforms.

Market Challenge

Organizations are continually facing a multitude of threats to corporate assets while the enterprise attack surface continues to expand. Email attacks remain a popular attack vector - according to Mimecast's 2021 State of Email Security, email threats have risen 64% over the course of the pandemic and 70% of the companies expect their business to be harmed by an email-borne attack.

Tactics change, increase in sophistication, new vulnerabilities are constantly being discovered and Security Operations Center (SOC) teams are stretched to the limit investigating and remediating each incident. SOC teams find themselves relying on limited data found during the investigation, accepting decisions will be made based on incomplete knowledge or drowning under the weight of information, but not having the sufficient time to act appropriately. Most of an analysts' time is spent on the collection, normalization, and prioritization of data, leaving little time to focus on solving the issue.

Security information sharing is not only useful for threat management but also for accurately determining IT risk, enabling secure business transformation, accelerating innovation, helping with continuous compliance, and minimizing friction for end users.

Organizations must find new ways to ensure they are protected while reducing complexity, minimizing risk, and decreasing the demand for an already over-taxed and under-skilled security team.

Joint Solution

Mimecast and SentinelOne provide an integrated solution to improve detection, stop threats, provide security insights, and streamline response across the organization. The integration helps with cross-domain detections, by leveraging identity, endpoint, application, email, and other tools to obtain a complete understanding of the threat landscape.

Email attack investigations usually require pivoting from one suspicious indicator to another to gather critical evidence, grabbing evidence and finalizing a resolution – manually running these commands traps analysts in a screen-switching cycle.

SentinelOne customers can ingest Mimecast logs along with your other cybersecurity tools to obtain a holistic understanding of the threat. Analysts can be confident they have the history of any incident and experience the flexibility of SentinelOne's dashboards to drill into events of interest with the ability to pivot through underlying data, enabling threat hunters to perform complex correlation searches across multiple data sources.

SentinelOne allows for instant response actions across distributed endpoints through native integrations designed for your security tools. This allows security teams to remediate and avert propagation, protecting the organization and reducing the chances that an incident will turn into a full-scale breach. By integrating Mimecast with SentinelOne, SecOps teams can standardize their incident response processes, accelerate the time it takes to detect and adaptive security measures for containing and remediating attack campaigns.

This equates to less time resolving and recovering from incidents, freeing up analysts to focus on other cybersecurity challenges and stay ahead of the next attack. Mimecast and SentinelOne enable organizations to defend against sophisticated attacks, integrate actionable intelligence into existing security solutions, and create a layered security defense across the digital estate.

With SentinelOne and Mimecast, joint customers can leverage cooperative defenses to protect enterprise devices and email. Together, security teams can rapidly respond to threats across endpoints and email for a holistic approach to threat triage, investigation, and incident response.

Key Use Cases

- **Operationalize Security Data for Threat Hunting and Investigation -** By ingesting logs from Mimecast into Singularity, customers can have additional email-borne threat visibility, threat hunting capabilities, dashboarding, and cross-telemetry alerting capabilities for their environments. By ingesting Mimecast logs into Singularity, customers will get better visibility into potential threats and take appropriate action to mitigate risks.

- **Accelerate Triage with Added Context -** Customers can accelerate incident triage and investigation by enriching threats in SentinelOne Singularity with contextually related emails or alerts from Mimecast. This integration allows customers to view contextually related emails or alerts in Mimecast in the XDR feed, enabling analysts to make decisions about the threat and take appropriate action quickly. For example, if a malicious file was executed on an endpoint, analysts using this integration can quickly investigate related emails or alerts from Mimecast.

- **Automate response across security layers, including email, endpoints, and cloud -** SentinelOne Singularity XDR provides advanced detection and response capabilities. With the ability to take automated or manual incident response actions in Mimecast, analysts can streamline their incident response process by taking rapid action to mitigate email and insider risk.

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.

About SentinelOne

More Capability. Less Complexity. SentinelOne is pioneering the future of cybersecurity with autonomous, distributed endpoint intelligence aimed at simplifying the security stack without forgoing enterprise capabilities. Our technology is designed to scale people with automation and frictionless threat resolution. Are you ready?