SentinelOne

SOLUTION BRIEF

Unify XDR and Email with SentinelOne and Mimecast

SentinelOne & Mimecast Joint Solution Brief

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 2022 State of Email Security report, 84% of U.S. organizations have reported phishing or ransomware attacks in the past 12 months and 72% said the number of email-based threats had risen1.

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. The majority 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

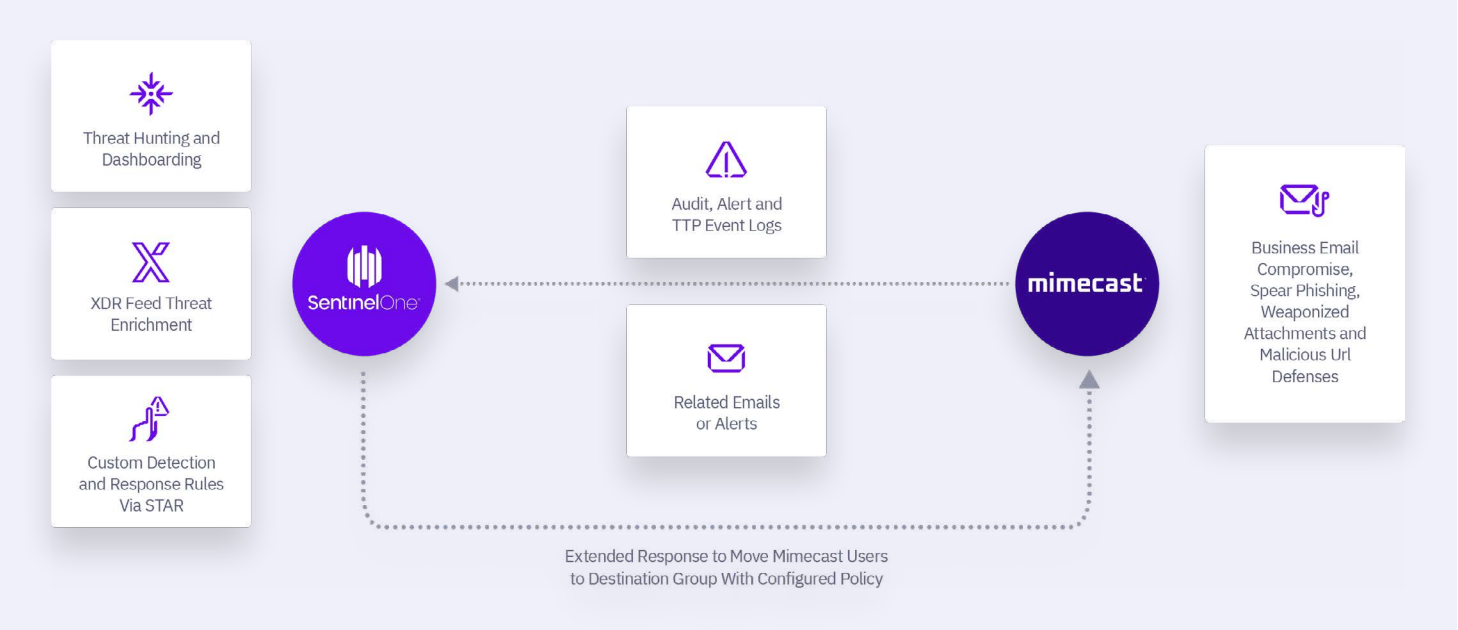
Mimecast and SentinelOne provide an integrated solution to improve detection, stop threats, provide security insights, and streamline response across the organization. The integration helps with cross-domain detections, by leveraging identity, endpoint, application, email, and other tools to obtain a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

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 XDR and email platforms



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 SentinelOn enable organizations to defend against sophisticated attacks, integrate actionable intelligence into existing security solutions, and create a layered security defense across the digital estate.

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.

The process involves collecting logs from Mimecast via API and forwarding them to Singularity for processing. Once the logs are ingested, customers can then create dashboards and saved searches within the platform to analyze the data and generate meaningful insights.

Logs ingested include:

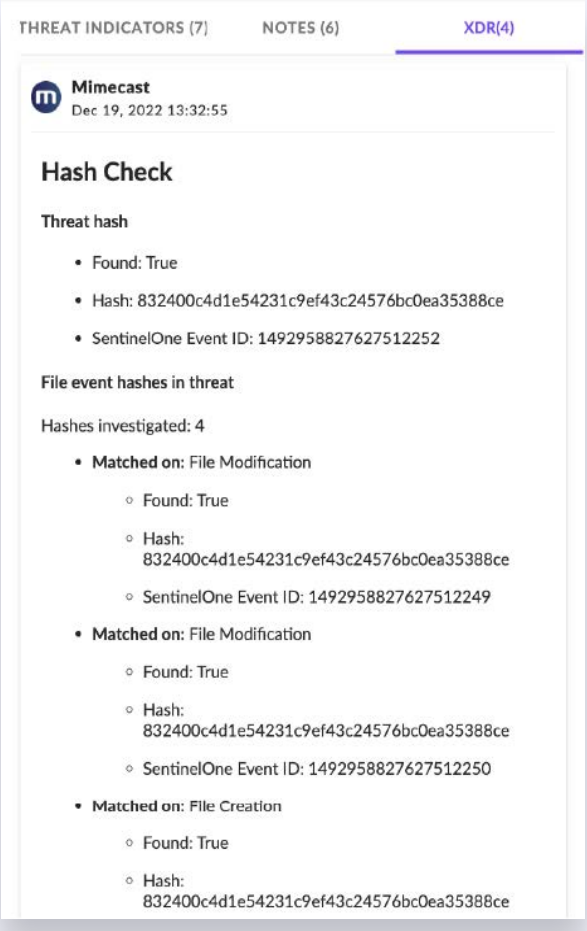
+ Audit eventsSIEM alerts/events
+ TTP attachment protection events
+ TTP impersonation protection events
+ TTP URL events

> “
>
> Data ingest is a major challenge for most vendors. To accommodate the volume, velocity, and variety of security data, XDR technologies must be anchored by a modern data pipeline that can collect and process security data at scale across hybrid IT.
>
> XDR technologies should also be able to provide automated machine-built context and correlation to provide the security team with automated insights across the enterprise security stack.
>
> **Dave Gruber**
>
> SR. ANALYST, ENTERPRISE STRATEGY GROUP

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.

The analysis capabilities of SentinelOne in conjunction with contextual emails or alerts from Mimecast equips customers with all of the necessary information they need to make an informed decision about how to handle a particular threat so they can take swift action. Added context helps minimize risk by ensuring any incidents are addressed quickly and efficiently.



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.

The automated incident response allows analysts to quickly take corrective action by suspending email for a given user, blocking the user's email, or quarantining them.

Gartner Peer Insights™

"Singularity is a reliable platform that gives each of its users the necessary protection to function without any problem and comfort.

★★★★★

IT SERVICE & PROCESS ENGINEER LEAD
IT

"With SentinelOne, our security, DevOps, and IT teams have one single source of truth to make data-driven decisions. We no longer have to stitch context across teams and use cases.

Kevin Vuong
CISO, COPART

Gartner Peer Insights™

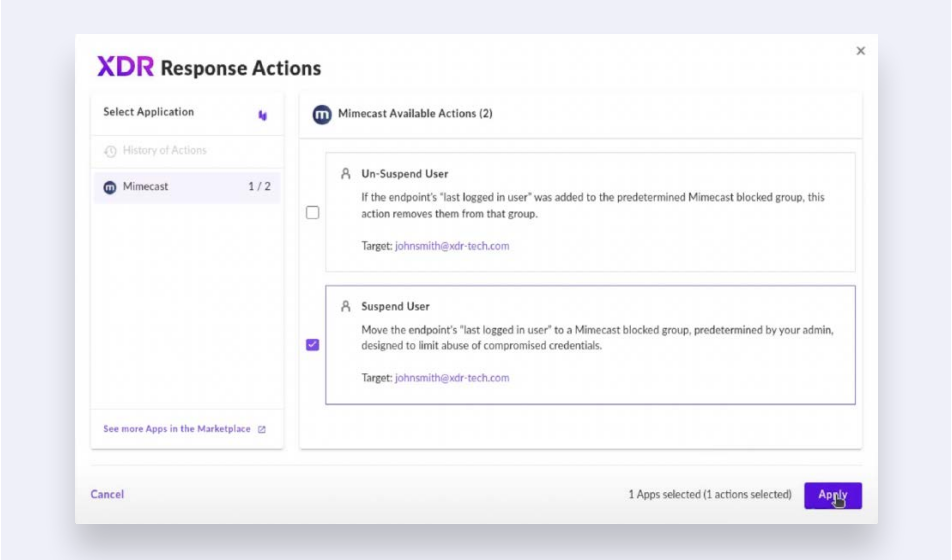
"Singularity is one of the most user-friendly platforms available. It's effective at detecting malicious behavior that traditional anti-virus software can't.

★★★★★

DIRECTOR
Energy and Utilities

Additionally, the platform provides alerting capabilities via Storyline Active Response (STAR) so customers can be notified and take an automated response, such as killing processes, quarantining malware or suspending a user if suspicious activity is detected in their environment. For example, upon detection of a threat, SentinelOne can automatically kill malware on the endpoint and suspend the last logged-in user's ability to send email, helping secure a critical lateral movement path and preventing further spread of an attack.

Manual incident responses are also possible through Mimecast integration, allowing security analysts to manually suspend or unsuspend a user based on analyst input (select manual response), analyst verdict (false positive) or threat status (marked as mitigated).



Conclusion/Summary

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.

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?

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.

sentinelone.com

sales@sentinelone.com
+ 1 855 868 3733