SentinelOne

SOLUTION BRIEF

Accelerate incident response with Singularity XDR 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 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 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.

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

Joint Solution

Mimecast and SentinelOne provide an integrated solution to stop threats, provide security insights and streamline response across the organization. Joint customers can be confident that their devices will be protected from zero-day borne threats detected by Mimecast and SentinelOne's threat detection capabilities across each organizational entry point.

Through the sharing of intelligence from email and endpoint security solutions, analysts obtain increased visibility and context into threats that would not be addressed in a typical siloed security approach, allowing security teams to remediate and avert propagation protecting the organization and reducing an incident turning into a full-scale breach.

mimecast

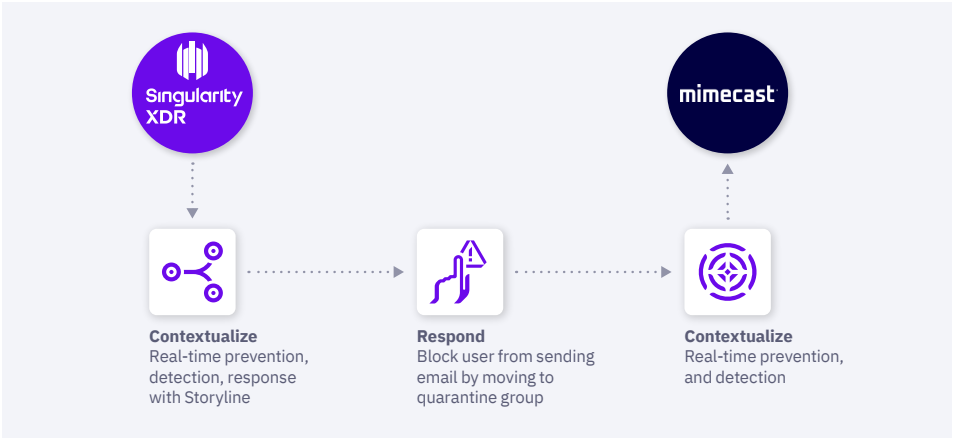
INTEGRATION BENEFITS

Prevent lateral email threat propagation

Accelerate Incident Response and contain threats faster by automatically quarantining affected users in Mimecast

Minimize delays with no context switches or multiple dashboards

Frictionless 1-click installation and configuration



01. SentinelOne identifies malware attempting to execute upon the endpoint, and an alert is generated.

02. The information relating to the 'logged in user' is sent to Mimecast, and the user is moved into a quarantine group to block email propagation.

03. Analyst kills and quarantines malware in SentinelOne.

SentinelOne Singularity XDR provides AI-powered prevention, detection, and response across user endpoints, cloud workloads, and IoT devices. When a threat is detected in SentinelOne, SentinelOne StorylineTM correlates detections and activity data across security layers, including email, endpoints, mobile, and cloud. Analysts can streamline response by automatically taking actions such as suspending email for a given user, blocking the user email, or quarantining them. Upon detection of the threat, SentinelOne can automatically suspend the last logged-in user's ability to send an email, helping secure a critical lateral movement path.

Conclusion

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 incident response with XDR automation.

Innovative. Trusted. Recognized.

Gartner

A Leader in the 2021 Magic Quadrant for Endpoint Protection Platforms

Highest Ranked in all Critical Capabilities Report Use Cases

MITRE ENGENUITY™

Record Breaking ATT&CK Evaluation

- No missed detections. 100% visibility
- Most Analytic Detections 2 years running
- Zero Delays. Zero Config Changes

Gartner peerinsights™ 4.9 ★★★★★

98% of Gartner Peer Insights™

Voice of the Customer Reviewers recommend SentinelOne

FedRAMP · AAA Certified · ISO 27001 CERTIFIED by schellman · VB 100 VIRUS virusbtn.com · AAA Certified · TEVORA PCI DSS Attestation HIPAA Attestation

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

Mimecast takes on cyber disruption for our customers; putting them first, and tackling their biggest security challenges together—email. Our mission is to protect organizations from malicious activity, human error and technology failure; and help lead towards building a more resilient world. Learn more about us at www.mimecast.com.

sentinelone.com

sales@sentinelone.com
+ 1 855 868 3733