proofpoint | SentinelOne

SOLUTION BRIEF

Proofpoint + SentinelOne

Caught in the inbox. Contained on the endpoint.



Turn Inbox Detections into Endpoint Protection

Email remains one of the most common ways attackers gain an initial foothold, but the attack doesn't end in the inbox. Once a malicious file reaches a device, adversaries move quickly to execute and spread. Security teams that rely on siloed email and endpoint tools miss the connection between those events, which gives attackers the time they need to do damage.

Since 2022, Proofpoint and SentinelOne have connected email threat detection to endpoint response. human-centric email threat intelligence from Proofpoint, combined with the autonomous SentinelOne Singularity XDR platform, means a file Proofpoint condemns is also detected and contained on your endpoints.

Share What the Inbox Learns with Your Endpoints

The global average cost of a data breach reached $4.99M in 2026.[1] Phishing and malware that slip into an inbox don't stay there, so catching a malicious file early, and containing it automatically if it lands on a device, can help reduce the risk of a costly compromise. Proofpoint Core Email Protection (TAP) identifies malicious attachments after delivery and shares those file indicators with SentinelOne.

Key Benefits

- Turn inbox verdicts into endpoint controls
- Contain condemned files automatically, without a manual handoff
- Detect the same file on any protected endpoint, even if it arrives by another route
- Add a layer of protection using licenses you already hold

Post-Delivery Detection	Endpoint Detection
Proofpoint Core Email Protection (TAP) TAP identifies a malicious email attachment after it has been delivered. It makes the condemned file's indicators available through the TAP API.	**SentinelOne Singularity XDR + STAR Rule** SentinelOne retrieves the file's indicators through the TAP API, using the Proofpoint module in the Singularity Marketplace. A Storyline Active Response (STAR) rule matches the file hashes and raises a threat if the file appears on any protected endpoint, even if it arrives by a route other than email.

Contain the File Without a Manual Handoff

A malicious file on a device doesn't wait for an analyst to copy its hash from one console into another. When SentinelOne finds a file Proofpoint has condemned, it responds automatically, based on the policies you already manage.

Policy-Driven Response	Custom Response Controls
Endpoint Group Policy When SentinelOne finds the file, the policy for that endpoint's group drives the response. SentinelOne can kill the process if the file has executed, quarantine the file, remediate, and roll back.	**Additional Controls** Teams can add the file hash to a watchlist or STAR rule, network-isolate the endpoint, or move it to a different policy group. This gives SOC teams more ways to contain a threat that has already reached a device.

1. IBM, *Cost of a Data Breach Report*, 2026.

©Proofpoint, Inc. 2026

Add a Second Control Without Adding a Platform

Joint customers get a second control on the same threat using the TAP and SentinelOne licenses they already hold, a TAP API credential, and the Proofpoint module in the Singularity Marketplace. There is no new platform to deploy or staff.

Indicators flow one way, from Proofpoint to SentinelOne, so what Proofpoint learns in the inbox becomes protection on the endpoint without extra analyst work.

Inbox verdicts become endpoint controls	Layered protection with licenses you already hold
A file Proofpoint condemns is detected on every protected device and contained according to your endpoint policy.	Joint customers add endpoint containment for email-borne threats without a new platform to deploy or staff.

Extend Your Email Defense to the Endpoint

Proofpoint's human-centric email threat detection and SentinelOne's autonomous endpoint protection each cover part of the path an attack takes. Connecting them means a file condemned in the inbox is also contained wherever it appears on the endpoint. Together, Proofpoint and SentinelOne help you close the gap between the inbox and the endpoint and respond to email-borne threats automatically.



Learn More

For more information, visit **proofpoint.com/us/partners/sentinelone**

proofpoint.

About Proofpoint, Inc. Proofpoint, Inc. is a global leader in human- and agent-centric cybersecurity, securing how people, data and AI agents connect across email, cloud and collaboration tools. Proofpoint is a trusted partner to over 80 of the Fortune 100, over 10,000 large enterprises, and millions of smaller organizations in stopping threats, preventing data loss, and building resilience across people and AI workflows. Proofpoint's collaboration and data security platform helps organizations of all sizes protect and empower their people while embracing AI securely and confidently. Learn more at **www.proofpoint.com**

Connect with Proofpoint: LinkedIn

Proofpoint is a registered trademark or tradename of Proofpoint, Inc. in the U.S. and/or other countries. All other trademarks contained herein are the property of their respective owners.