proofpoint.

SOLUTION BRIEF

Proofpoint + VMware Carbon Black

Post-delivery protection from inbox to endpoint.



Key Benefits

- Address a delivered malicious file on both the inbox and the endpoint without correlating by hand
- Quarantine messages with TRAP and share details with Carbon Black Cloud
- Apply endpoint controls such as search and purge, watchlist, isolation, or a policy change

Close the Gap Between Delivery and Response

A malicious file that gets past the inbox can still execute, spread, and persist on the endpoint. Teams that run email and endpoint tools separately spend time correlating what happened after delivery, and attackers use that time. Proofpoint and VMware Carbon Black Cloud (now Carbon Black Cloud under Broadcom) connect the two sides. When a malicious file is found after delivery, Proofpoint pulls the email and Carbon Black Cloud can contain the device, addressing the inbox and the endpoint in the same motion.

Find the File, Pull the Email, Share the Details

Proofpoint stops 369 million malware attacks every year.[1] Even so, a file that reaches a user can still cause harm on the device. Proofpoint Core Email Protection (TAP) detects malicious files after delivery, and the details are shared with Carbon Black Cloud.

[1] Proofpoint, By the Numbers, August 2026.

Post-Delivery Detection and Quarantine	Endpoint Controls
Proofpoint TAP and TRAP TAP detects malicious file attachments that have already been delivered to users and alerts TRAP, which quarantines the delivered messages. The message and threat details are then shared with VMware Carbon Black Cloud.	**VMware Carbon Black Cloud** Using the details Proofpoint shares, Carbon Black Cloud can search endpoints for the file and purge it, add the hash to an Enterprise EDR watchlist, isolate the endpoint, or move it into a different policy.

Extend Protection Beyond the Inbox

Proofpoint's email threat detection and Carbon Black Cloud's endpoint protection each cover part of the path a delivered file takes. Connecting them helps address that file on both the inbox and the endpoint. Teams that run SOAR can also send details to a webhook to build workflows. To see how the integration could fit your environment, including licensing and endpoint policies, talk to your Proofpoint representative.

Learn more: proofpoint.com/us/partners/vmware-carbon-black

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.

proofpoint.