proofpoint.

INTEGRATION BRIEF

Proofpoint and VMware Carbon Black Partnership

vmware®

Detect and respond to threats with a multilayered defense

Products

- Proofpoint Targeted Attack Protection
- Proofpoint Emerging Threats Intelligence Reputation List
- VMware Carbon Black Cloud

Key Benefits

- Detect and stop advanced email threats
- Achieve multilayered threat protection
- Secure organizational endpoints and data against sophisticated malware and malware-free attacks
- Enrich your own observational data with a global perspective on suspicious IP addresses and domains

More than 90% of attacks start with email.[1] And these threats are constantly evolving, which makes it next to impossible to keep pace with changes in the threat landscape. Proofpoint and VMware Carbon Black have partnered to give shared customers better threat intelligence as well as multilayered detection and response against these threats—from email to the endpoint.

Coming Together to Protect Against the No. 1 Threat Vector

Invariably, there will be threats that make it to users' endpoints. Keeping on top of daily changes in threats and making sure they can't cause harm to a device or spread to other endpoints becomes an increasingly difficult task.

Proofpoint Emerging Threats (ET) Intelligence Reputation List provides up-to-date threat intel feeds that identify new IPs and domains that are involved in suspicious and malicious activity. This reputation data can be fed to a watchlist in VMware Carbon Black Cloud, where it can be organized, filtered and alerted on. This increases overall threat awareness and reduces the number of threats your people see.

Proofpoint Targeted Attack Protection (TAP) provides an innovative approach to detect, analyze and block the more advanced threats that target your people. It offers unique visibility into these threats. And it provides additional intelligence to VMware Carbon Black Cloud to ensure you get best-of-breed multilayered protection.

VMware Carbon Black Cloud is a cloud-native platform. It combines the intelligent system hardening and behavioral prevention you need to keep emerging threats at bay. It consolidates multiple endpoint and workload security capabilities using one agent and a common console. And it helps organizations gain speed and efficiency.

This technical partnership provides our joint customers with the ability to protect their people and endpoints from an ever-changing threat landscape. It delivers additional security benefits and expanded visibility. And it does all of this at no additional cost.

1 Verizon. "2019 Data Breach Investigations Report (DBIR)." 2019.

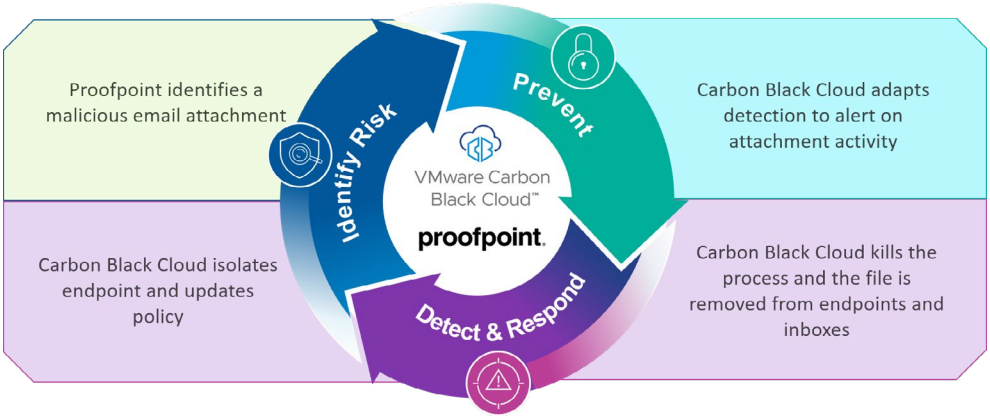

Figure 1. Together, Proofpoint and VMware Carbon Black Cloud protect against and respond to attacks that target corporate inboxes and endpoints.

How the Integrations Work

Actionable threat intelligence

For enhanced visibility into the most current threats, Proofpoint's ET Intelligence Reputation List shares up-to-date IP and domain reputation feeds with VMware Carbon Black Cloud Enterprise EDR. This data provides Carbon Black Cloud with deeper context for blocking more threats and improving your remediation capabilities.

Post-delivery protection and automated remediation

For multilayered post-delivery protection, TAP shares observed threat information with VMware Carbon Black Cloud. This offers you enhanced security to protect your people, both through email and the endpoint. When TAP sees that a malicious file has been delivered via email, it can alert Proofpoint Threat Response Auto-Pull (TRAP). There it quarantines the delivered messages. The message details are also shared with Carbon Black Cloud, which applies more security controls to the endpoint for multilayered protection.

The controls may include:

- Searching endpoints for the malicious file and purge if needed
- Adding the file hash to a Carbon Black Cloud Enterprise EDR watchlist feed
- Isolating the endpoint
- Moving the endpoint into a different policy
- Sending process and threat report information to a webhook to enable SOAR workflows

By leveraging these best-of-breed integrations, you can identify more threats, protect your users and automatically respond to potential threats to your endpoints. This means less risk and less time spent resolving and recovering from incidents.

LEARN MORE

For more information, visit **proofpoint.com**.