SWIMLANE

Solution Brief

Swimlane and VMware Carbon Black

Together, Closing the Gap on Cyber Exposure

Solution at a Glance

- Greater visibility across endpoints
- Faster investigation and evaluation
- Automated workflows and incident response

vmware Carbon Black

Why we work together

Carbon Black has been a leader in endpoint security for years. More than 6,000 organizations around the globe rely on the Carbon Black Cloud to understand and reduce cyber risk from endpoints. Leveraging Carbon Black and the Swimlane security orchestration, automation and response (SOAR) solution together enables security teams to enhance their automated remediation workflows through integrated endpoint intelligence and actions, including the ability to block a hash, kill a process or isolate a host from the network.

Challenge

Organizations of all sizes have embraced digital transformation to create new business models and ecosystems. To enable this transformation, companies are adding more and more endpoints to their networks. While these endpoints open up a whole new world of opportunities, the elastic attack surface creates a massive gap in an organization's ability to truly understand threats on the network perimeter. Every organization needs visibility into possible security risks, along with the ability to prioritize risks and investigate incidents easily and rapidly. Integrated tools with a unified view help security operations center (SOC) analysts accurately evaluate and take appropriate action on notable events as they happen.

Benefits of Integration

- Centralize and correlate insights gleaned from endpoints, third-party technologies and other data sources in the environment.
- Connect with and use data ingested from endpoints, implement workflows and automate triage.
- Take automated or manual action on endpoints from within Swimlane, including the ability to change a device's policy.

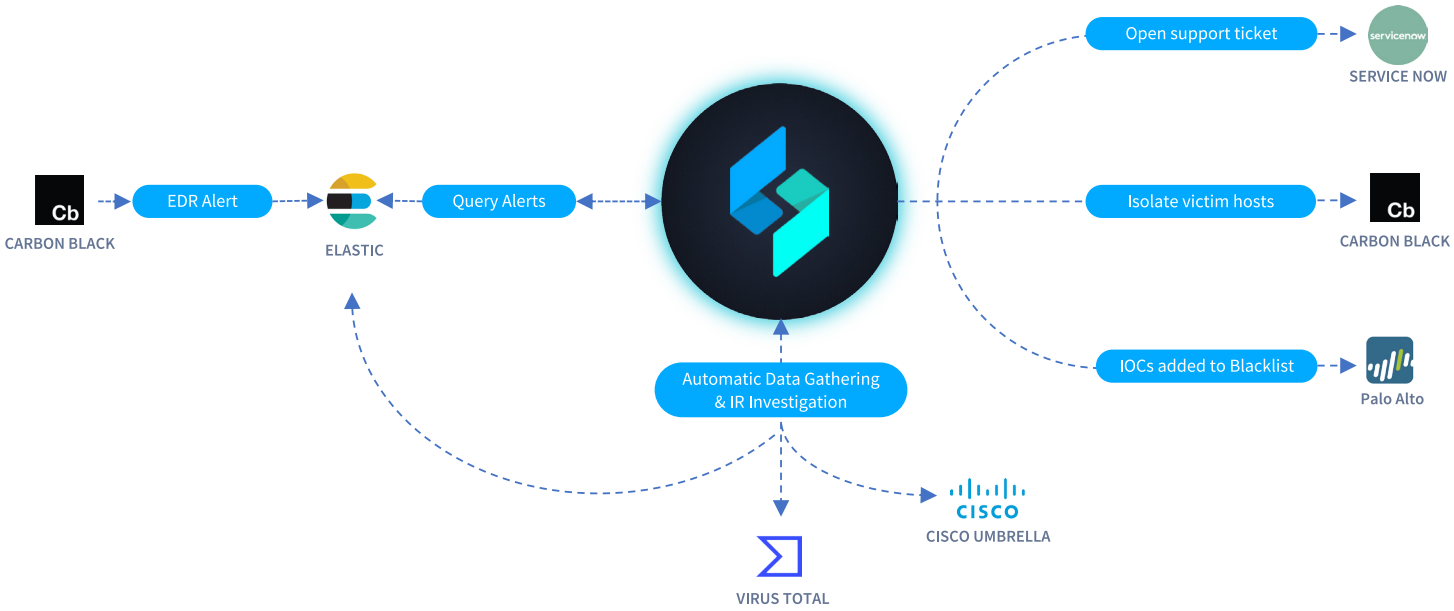
Solution Overview

Integrating Carbon Black with Swimlane allows customers to investigate, evaluate and take action on notable events easily and rapidly right from within the Swimlane case record.

How it works

- Swimlane connects to Carbon Black's cloud-based and on-premises products via API.
- Scheduled queries pull in all relevant alerts, events, devices and user details for centralized investigation and triage.
- Details from endpoints are used as thresholds or conditions to trigger automated workflows.

Carbon Black Products: CB Defense (NGAV), CB ThreatHunter (EDR), CB Protection (App Control), and CB Response (on-prem EDR)



Better Together

About Carbon Black

VMware Carbon Black is a leader in cloud-native endpoint protection with more than 6,000 global customers, including approximately one third of the Fortune 100.

About Swimlane

Swimlane is the leading independent SOAR solution created by analysts for analysts. It delivers scalable security solutions to organizations struggling with alert fatigue and analyst burnout.