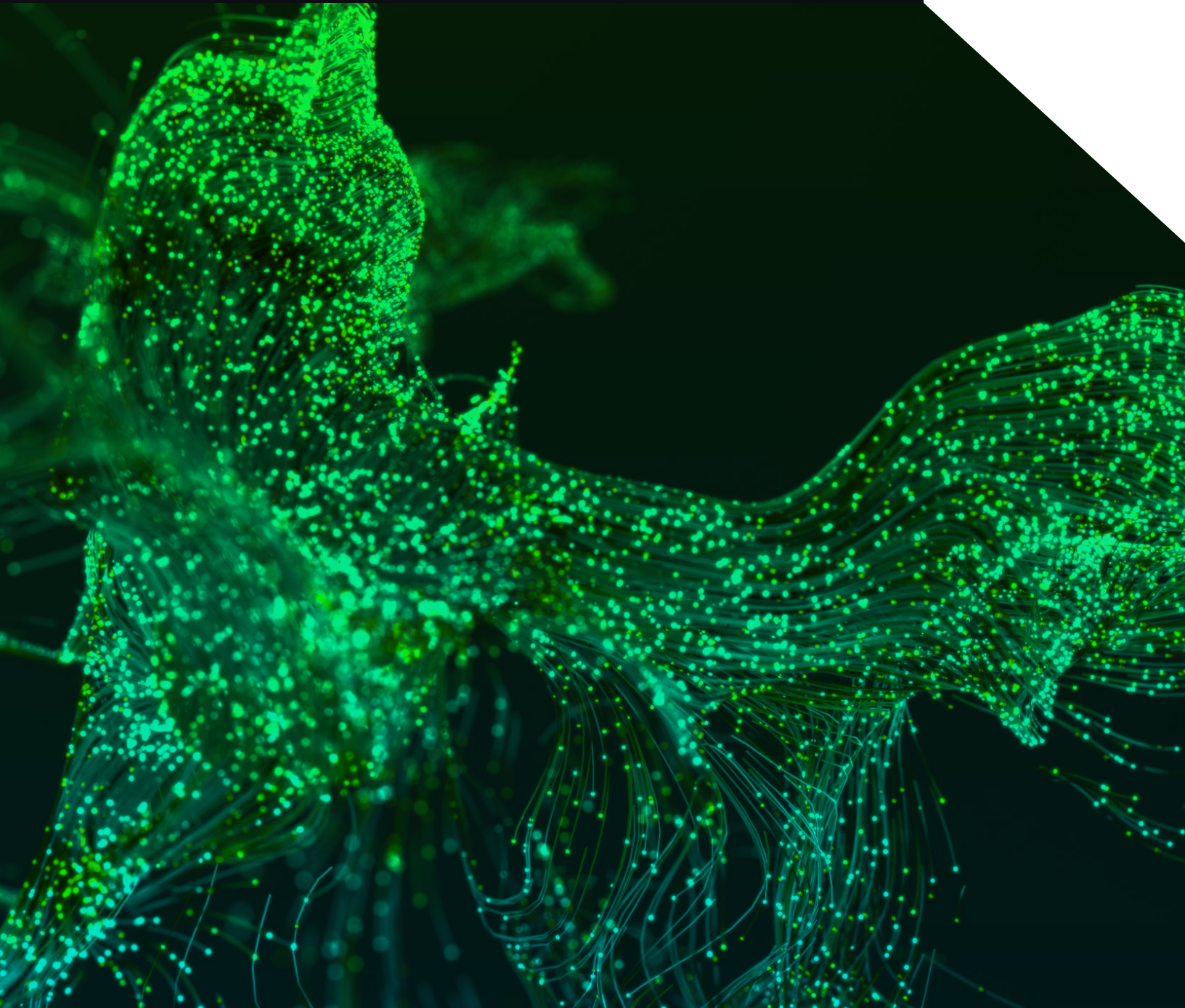



BlackBerry Cylance and Swimlane Partner To Optimize Enterprise Security Operations

Providing Faster Response Times and Accuracy To Alerts and Investigations

SOLUTION BRIEF





Swimlane allows automated responses to quickly update devices and policies through the BlackBerry Cylance API.

Introduction

BlackBerry Cylance and Swimlane increase security operations center (SOC) effectiveness by automating tasks, preventing threats, and improving alert accuracy and incident response time.

Value Statement

The partnership of BlackBerry Cylance and Swimlane allows organizations to apply true prevention and fast response to cyber attacks. BlackBerry Cylance's solution provides customers with the controls to automate significant portions of the security stack workflow. Leveraging AI and automation to perform advanced threat identification and analysis gives IT staff time to focus on other critical business needs.

Automated responses using endpoint intelligence provided by CylancePROTECT® to stop known, unknown, and zero-day malware is just the beginning. With Swimlane customizable orchestration, each customer gets what is needed to support their workflows, ultimately decreasing incident response times, increasing overall security, and improving ROI on security operations.

Use Cases

Lower Mean Time To Respond (MTTR) To Alerts

- **Challenge:** Sorting through, prioritizing, and investigating thousands of alerts can overwhelm SOC analysts. Manual threat research and correlation takes a significant amount of time and is prone to human error.
- **Solution:** Using BlackBerry® Cylance® prevention-first technology and the Swimlane Orchestration and Automated Response Platform helps enterprises respond more efficiently to modern threats. The joint solution reduces noise in the security stack while automating data retrieval, correlation, and response actions for alert-based workflows.
- **Additional Benefit:** Predictive threat prevention and automated responses handle a significant workload, giving SOC analysts more time to perform other critical

tasks for the organization. It also leads to fewer endpoint infections and alerts, meaning less time is spent on remediation and machine re-imaging.

DATA Enrichment/Incident Response

- **Challenge:** SOC analysts spend considerable time collecting, correlating, and analyzing alert information.
- **Solution:** Utilizing a CylancePROTECT threat event as a trigger, Swimlane can capture the full ecosystem environmental meta-data related to an incident. This complete data snapshot (including BlackBerry Cylance data gathered through APIs) helps analysts respond quickly and with increased accuracy.
- **Additional Benefits:** Swimlane allows automated responses to quickly update devices and policies through the BlackBerry Cylance API.

API-Driven Features	Runtime
Data Enrichment	Threat information containing multiple levels of detail is communicated from CylancePROTECT to the Swimlane dashboard. Swimlane can call the BlackBerry Cylance APIs to gather threat, device, policy, and other information to update its dashboard. Swimlane can also perform data enrichment on the rest of the environment and provide more information on alerts or workflows.
Environmental Check/Update	Using Swimlane, users can query devices via the BlackBerry Cylance API for the current status of device data, threat details, users, alerts, etc.
Malware Analysis	When CylancePROTECT detects and quarantines a malicious file, Swimlane calls the BlackBerry Cylance API to update its dashboard with the threat information. Swimlane can download the quarantined malware and send it to another security device, such as a sand box, for further analysis. Swimlane then updates the results to its dashboard.
Blacklisting	Given a file hash, Swimlane can update the BlackBerry Cylance blacklist. The hash can come from a CylancePROTECT detection or somewhere else in the environment (FW, CERT list, etc.).
Malware Hunting	Swimlane can search BlackBerry Cylance endpoints to see where a specific file hash has been encountered. The file hash can come from a BlackBerry Cylance detection or another device, CERT list, etc.
Policy/Zone Orchestration	Following an alert, Swimlane can update/alter BlackBerry Cylance policies and device groupings without leaving the Phantom interface.



Swimlane Dashboard for Security Alerts, Active Incident Workflow, and Ecosystem Status.

About Swimlane

Swimlane is a leader in security orchestration, automation, and response (SOAR). By automating time-intensive, manual processes and operational workflows, and delivering powerful, consolidated analytics, real-time dashboards, and reporting from across your security infrastructure, Swimlane maximizes the incident response capabilities of over-burdened and understaffed security operations.

Swimlane was founded to deliver scalable, innovative, and flexible security solutions to organizations struggling with alert fatigue, vendor proliferation, and chronic staffing shortages. Swimlane is at the forefront of the growing market for security automation and orchestration solutions that automate and organize security processes in repeatable ways to get the most out of available resources and accelerate incident response. Swimlane offers a broad array of features aimed at helping organizations to address both simple and complex security activities, from prioritizing alerts to remediating threats and improving performance across the entire operation.

Swimlane is headquartered in Denver, Colorado with operations throughout North America and Europe.



About BlackBerry Cylance

BlackBerry Cylance develops artificial intelligence to deliver prevention-first, predictive security products and smart, simple, secure solutions that change how organizations approach endpoint security. BlackBerry Cylance provides full-spectrum predictive threat prevention and visibility across the enterprise to combat the most notorious and advanced cybersecurity attacks, fortifying endpoints to promote security hygiene in the security operations center, throughout global networks, and even on employees' home networks. With AI-based malware prevention, threat hunting, automated detection and response, and expert security services, BlackBerry Cylance protects the endpoint without increasing staff workload or costs.



+1-844-CYLANCE
sales@cylance.com
www.cylance.com

