SWIMLANE

Solution Brief

Swimlane and Lastline

Streamline security operations with unmatched malware detection and response automation.

Joint Solution Benefits

Comprehensive malware detection and behavioral analysis. Identify and remediate adverse effects quickly with full visibility into the scope of an attack.

Optimized security operations. Streamline security operations and eliminate alert fatigue with integrated security tools and the automation of manual tasks.

Reduced MTTR. Reduce security risk with incident response automation.

The challenge for security operations

Traditional security operations centers (SOCs) rely on inefficient manual incident response processes with disconnected security technologies and are often outclassed by sophisticated malware designed to obfuscate its presence. Advanced threats like this stay hidden in the midst of constantly-growing alert backlogs for an extended period of time because analysts cannot keep pace with them. To remain effective in the ever-evolving threat landscape, security teams need to be empowered to detect and remediate complex alerts quickly, mitigating harm done to the organization.

The Lastline-Swimlane integration merges advanced threat detection with SOAR to stop sophisticated attacks.

Lastline is a threat detection and network security solution that specializes in identifying and analyzing sophisticated attacks using a market-leading sandbox technology capable of capturing malicious behavior missed by other tools. Swimlane is a security orchestration, automation and response (SOAR) platform that eliminates alert backlogs and maximizes the incident response capabilities of over-burdened and understaffed SOCs by automating operational workflows and integrating security tools.

The Lastline-Swimlane integration provides superior protection against sophisticated attacks and reduces mean time to resolution (MTTR). Lastline maps out malware actions, allowing security teams to understand the full scope of the attack in an organization's environment. Swimlane reduces incident resolution times by integrating with other security tools to automate time-consuming, manual response processes.

How it works

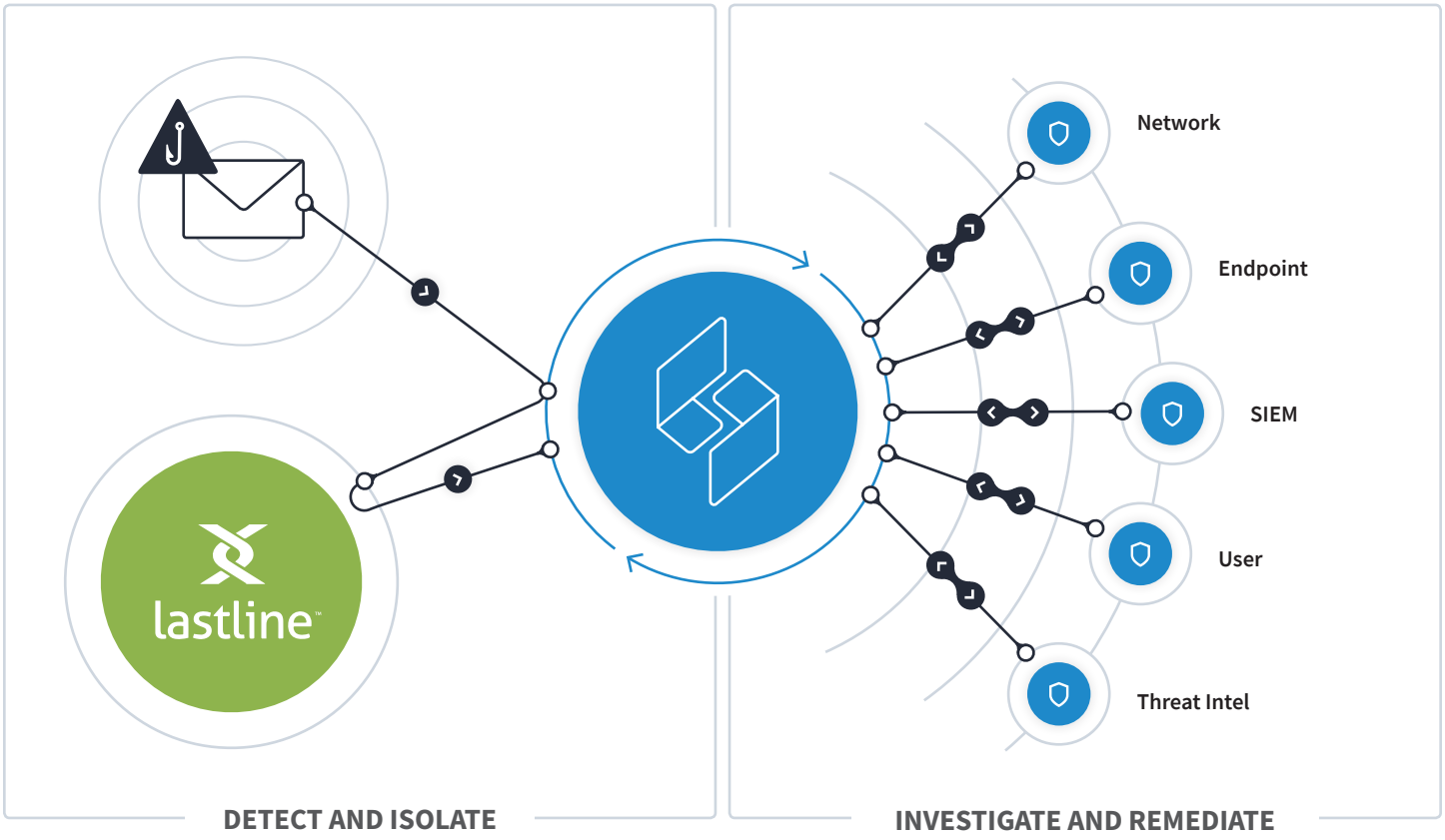
Lastline provides malware detection and analysis with its Deep Content Inspection™ sandbox environment designed to provide complete visibility into malware behavior by hiding threat analysis algorithms inside the hardware. Swimlane uses the information from Lastline's malware analysis to drive the logic inside automated incident response workflows, as well as threat intelligence to enrich incident records and enhance forensic activities.

Swimlane leverages its API-first architecture to establish a bidirectional connection with the entire security technology stack and acts as middleware to centralize information and response processes. The Lastline-Swimlane integration equips analysts with comprehensive incident information and empowers them to respond to advanced threats within minutes.

Neutralizing a sophisticated phishing attack

Problem:

Bad actors use phishing emails with evasive malware capable of altering its behavior to avoid detection, taking advantage of overwhelmed security teams with low threat detection capabilities. Attackers have days, if not weeks, to exploit the breach and



compromise sensitive data before an analyst gets to the phishing alert. Even after the alert is triaged, perpetrators can leverage remaining backdoors created by evasive malware missed during the investigation process to continue their attack.

Solution:

Detect and isolate. Swimlane integrates with email systems and monitors phishing inboxes to parse submitted emails and extract indicators of compromise (IoCs) instantly. Lastline imports discovered IoCs via an API and submits them to its Deep Content Inspection™ environment to analyze all capabilities of the evasive malware. Unlike other sandbox environments, Deep Content Inspection ™ operates at the CPU level and can simulate an entire host—including the CPU, system memory and other devices—to avoid detection by the malware.

When malware is detected, Swimlane pulls detailed information about the malicious activity from Lastline. This automatically triggers response workflows that send API calls to other security tools to initiate appropriate actions. Swimlane can notify users, search and delete emails from the servers, isolate hosts, update blocklists and much more at machine speeds, locking-out the attacker in seconds.

Investigate and remediate. Swimlane can then create a new case record and populate predefined fields in the case record with Lastline's analysis information. Case records guide the incident response process and can be fully tailored to an organization's phishing playbook or complex workflows. Analysts can define all aspects of the layout of a case record, add buttons to initiate additional lookups or response actions, and hide or show entire sections based on the workflow progression. Armed with Lastline insights, analysts can fully investigate and remediate an incident within a single case view in Swimlane.

About Swimlane

Swimlane is at the forefront of the growing market of security automation, orchestration and response (SOAR) solutions and was founded to deliver scalable and flexible security solutions to organizations struggling with alert fatigue, vendor proliferation and chronic staffing shortages. Swimlane's solution helps organizations address all security operations (SecOps) needs, including prioritizing alerts, orchestrating tools and automating the remediation of threats—improving performance across the entire organization. Swimlane is headquartered in Denver, Colorado with operations throughout North America and Europe.

For more information, visit www.swimlane.com.

About Lastline

Enterprise security professionals use Lastline to defend their organizations against advanced malware-based attacks that result in damaging and costly data breaches. Our solutions deliver the visibility, context and integration security teams need to rapidly detect and respond to network breaches. Guided by a dynamic blueprint of the breach unfolding within their organization, our customers achieve exceptional enterprise security using fewer resources and at a low total cost of ownership. Lastline solutions are sold directly, through an extensive channel of global partners, and are integrated into the solutions of leading security technology vendors worldwide. Lastline is privately held with headquarters in Silicon Valley.

To learn more, visit www.lastline.com