SOLUTION BRIEF

IronNet and Swimlane

Reduce the impact of cyber attacks through advanced threat detection and automated response

Why we work better **together**

SWIMLANE

SOLUTION BENEFITS AT A GLANCE

Visibility across the threat landscape

Receive real-time collective threat intelligence, contextual information on new threats, and higher order analysis of anomalies correlated across communities.

Increase effectiveness of existing SOC resources

Streamline and automate operations to eliminate alert fatigue with curated threat ranking, integrated security tools, and automation of manual tasks.

Reduce the impact of an attack

Lessen business repercussions and security risk by detecting threats earlier in the attack lifecycle and protecting against malicious activity before it invades the network.

Designed by national security analysts and top intelligence data scientists, IronNet provides network detection and response (NDR) at enterprise scale, and Collective Defense across communities of enteprise peers to identify advanced threats that are often missed by existing commercial cybersecurity solutions. Swimlane's security orchestration, automation and response (SOAR) platform eliminates alert backlogs and maximizes the incident response capabilities of over-burdened and understaffed security operation centers (SOC) by automating operational workflows and integrating security tools. The integration of IronDefense with Swimlane enables more advanced threat detection, higher accuracy prioritization, faster mitigation, and proactive protection. IronDefense uses advanced behavioral analytics and collective intelligence to find unknown threats, while weeding out false positives to avoid alert fatigue.

Business Challenge

Cyber defenses operate in silos where individual companies defend by themselves against a range of threats using traditional cybersecurity tools that often miss advanced and new malicious network traffic patterns. This inability to detect novel threats, new variations of existing threats, or detection coverage gaps against known threats increases the burden of an already overworked security operations team.

There is a better way to defend. By taking a behavioral detection approach and working together in real time with enterprise peers in a collective and collaborative approach, enterprises can gain defensive economies of scale that optimize their existing cybersecurity investments, reduce the impact of an attack, and gain visibility across their business ecosystems.

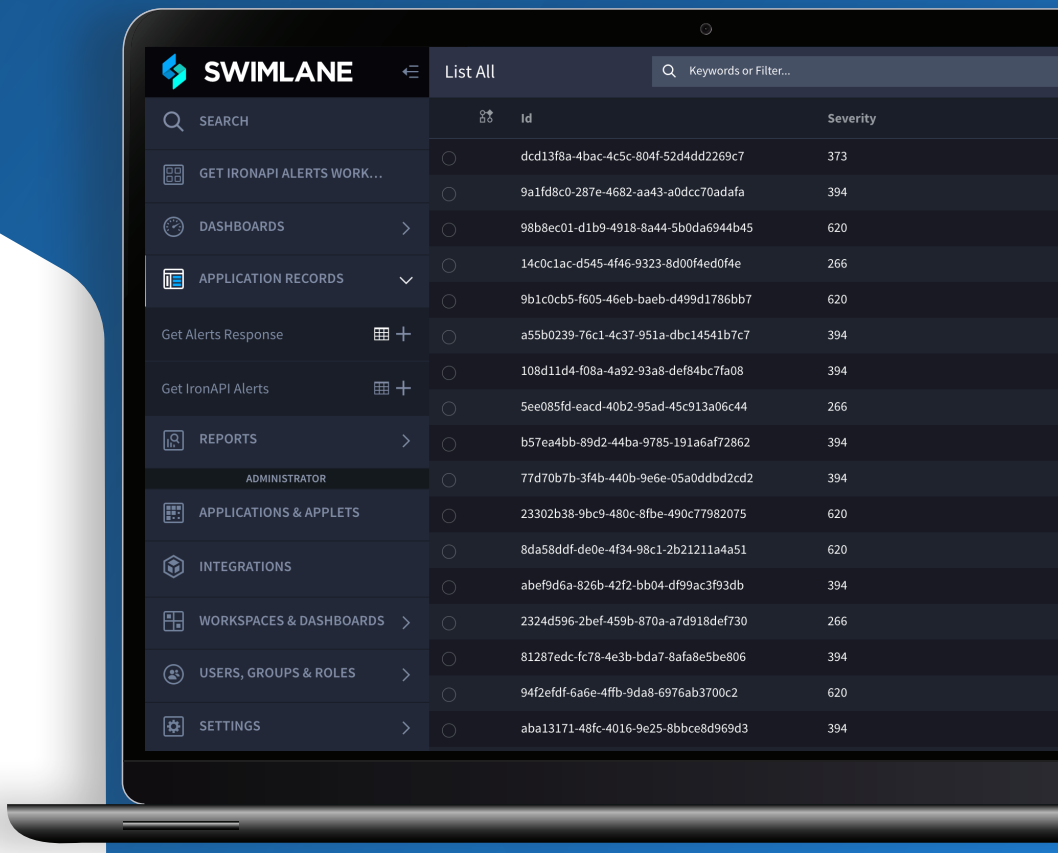
Solution Overview

IronNet's IronDefense NDR solution vets, qualifies, prioritizes, and rates alerts before they reach analysts. IronDefense automates many of the time-consuming discovery steps and indicates the severity of anomalous activity to enable analysts to make decisions about behavior in a shorter amount of time. Together with IronNet's IronDome Collective Defense solution, analysts have complete visibility into the threat landscape, delivering real-time collective threat intelligence insights from peer enterprise SOCs on the detection, investigation, triage, and response for each alert detected locally by IronDefense.

The IronDefense Plugin for Swimlane enables customers to seamlessly apply their threat response playbooks to events detected by IronDefense. This plugin enables security teams to manage alerts more efficiently by integrating teams, processes, and tools together through the automation of tasks and orchestration of workflows. With the IronDefense Plugin for Swimlane, users can swiftly and easily create custom visualizations to display any dataset in its most useful format. Data ingestion from IronDefense allows users to capitalize on Swimlane's ability to automate security actions through playbooks and rapidly triage IronDefense events and alerts in an automated, semi-automated, or manual fashion. The app allows users to capitalize on Swimlane's customizable dashboards, implementing unique workflows and case management components, and the ability to quickly build playbooks with unlimited automated actions. Users can also download, create, and share custom dashboards which track data and operating metrics tied to ongoing IronDefense events, alerts, and IronDome community activity.

ABOUT SWIMLANE

Swimlane is at the forefront of the growing market of SOAR solutions, delivering 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 needs, including prioritizing alerts, orchestrating tools, and automating the remediation of threats, improving performance across the entire organization.



The feedback loop of information sharing between Swimlane and IronDefense continuously improves collective threat intelligence, speeds remediation, and strengthens the cybersecurity stance.

ABOUT IRONNET

IronNet is a global cybersecurity leader that is revolutionizing how organizations secure their enterprises by delivering the first-ever collective defense platform operating at scale. Our solutions leverage our unique offensive and defensive cyber experience to deliver advanced behavioral analysis and collective intelligence to detect known and unknown threats.

How It Works

IronAPI enables IronDefense and Swimlane to interact, sending and receiving the data they need without a graphical user interface. IronAPI conforms to the REST (representational state transfer) web architecture which is designed to provide optimum performance, scalability, simplicity, and reliability.

When IronDefense data is ingested into Swimlane, it provides users the ability to take proactive measures on next-generation firewall (NGFW) and endpoint detection and response (EDR) tools to prevent further attacks. These measures include creating blacklists to alert on or block additional malicious activity and quarantining devices. Employing strategies like these permits IronDefense Swimlane plugin users to expand the utility of IronDefense and increase the ROI of other products integrated with Swimlane. This data ingest also helps drive analyst workflow automation, such as IT service management (ITSM) ticket creation. By leveraging the IronDefense Swimlane plugin, users can eliminate the manual and tedious process of creating tickets to initiate remediation efforts to allow SOC analysts to focus their attention on analyzing alerts.

The IronDefense Plugin for Swimlane also enables data upload and sharing. Users can share analyst assessments with IronDefense to enable Collective Defense via the IronDome platform. Events, alerts, and IronDome collective threat intelligence information are all available through the IronDefense Plugin for Swimlane, which means other participants in IronDome will be able to use the information to improve their security posture. Users can also update existing NGFW and EDR alert workbooks to submit observed malicious Indicators of Compromise (IoC) to IronDefense to look for correlations across the IronDome community. By sharing these discoveries with IronDome, IronDefense Swimlane plugin users are able to understand the trends of attackers by receiving information on whether the same malicious activity has been observed by other IronDome participants.