IronNet's Ecosystem Integrations

Increase the efficiency of security teams with smarter, more effective workflows built through collective threat intelligence

The Splunk IronDefense Ecosystem Integration dashboard

ABOUT IRONNET

IronNet is a global cybersecurity leader that revolutionizes 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.

Why we work better **together**

IronDefense, IronNet's flagship Network Detection and Response (NDR) product, delivers scalable behavioral analytics and integrated hunt to a variety of public and private sector enterprises. Designed by national security analysts and top intelligence data scientists, IronDefense provides machine-speed detection at scale to identify advanced threats that are often missed by existing commercial cybersecurity solutions. IronNet's Collective Defense platform, IronDome, shares these behavior-based detections with communities of similar risk profiles to create a defensive fabric across companies, sectors, and nations.

To streamline the alert triage and incident response processes, IronDefense can integrate with a number of security products, including security information and event management (SIEM), security orchestration, automation, and response (SOAR), endpoint detection and response (EDR), and next-generation firewall (NGFW) tools. IronDefense also integrates with cloud platforms and traffic optimization products to further simplify the deployment process and strengthen your organization's security stance.

SIEM

IronNet integrates with several SIEM tools to retrieve logs, share detections, and retrieve analyst feedback. Communications are bidirectional.

- Splunk
- IBM QRadar
- Microsoft Azure Sentinel

SOAR

IronNet's SOAR integrations share detections, retrieve analyst feedback, and augment existing playbooks. Communications are bidirectional.

- Cortex XSOAR (formerly Demisto)
- Splunk Phantom
- Swimlane
- ServiceNow

EDR

IronNet integrates with EDR platforms to ingest endpoint event and entity context and initiate response to malicious activity. Communications are bidirectional.

- CrowdStrike

NGFW

IronNet integrates with NGFW products to dynamically block malicious activity and ingest logs for analysis.

- Palo Alto Networks

Cloud

IronNet's NDR solution IronDefense can be deployed using a variety of cloud hosts. By operating in the cloud, IronDefense provides sensor and log ingest for analysis to cover network and UEBA (user and entity behavior analytics) use cases.

- Amazon Web Services (AWS)
- Microsoft Azure
- Microsoft 365 (formerly Office 365)

Learn More

For more information about our solutions, visit our website.