SOLUTION BRIEF

IronNet and Splunk

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

Why we work better **together**

splunk>

SOLUTION BENEFITS AT A GLANCE

Gain 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.

Increased efficiency of SOC operations

Streamline processes and eliminate alert fatigue with prioritized threats, seamless integration, and automation of manual tasks.

Reduce impact of an attack

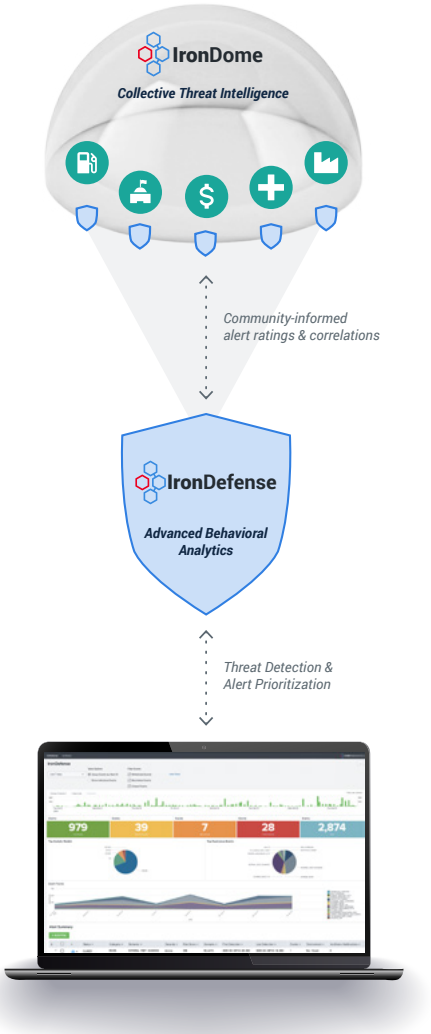
Lessen business repercussions and security risk by detecting threats earlier in the attack lifecycle through shared expert insights and proactive threat hunting.

Designed by national security analysts and top intelligence data scientists, IronNet's scalable Network Detection and Response (NDR) solution and Collective Defense platform provide visibility across communities of enterprises. This approach allows peers to identify advanced threats often missed by existing commercial cybersecurity solutions. Splunk's analytics-driven Security Operation Suite is a SIEM (security information and event management) platform that analyzes multiple data streams and enriches events with information from threat intelligence sources. In addition to analysis, Splunk performs real-time security monitoring, advanced threat detection, and forensics and incident management. Splunk helps enterprises improve visibility across multi-cloud environments and enables cross-collaboration to improve accuracy and response time.

The IronDefense App for Splunk strengthens your security stance by finding more unknown threats and providing better prioritization, faster mitigation, and proactive protection. IronDefense uses advanced behavioral analytics and collective intelligence to find unknown threats while weeding out false positives. When Splunk is used with IronDefense, users gain actionable insights, quickly identifying top threats and reducing total alert volume. Together with IronNet's IronDome Collective Defense solution, analysts have complete visibility into the threat landscape, delivering real-time, community-driven collective threat intelligence insights from peer enterprise security operations centers (SOC).

Meeting the challenge

Cyber defense teams are isolated, using conventional tools that often miss advanced or unknown threats. These gaps increase the burden of already overworked SOCs. There is a better way to defend. A collaborative, real-time, behavioral detection approach enables enterprises to optimize their existing cybersecurity investments, reduce the impact of an attack, and gain broader visibility across their business ecosystems.



The feedback loop of information sharing between Splunk and IronDefense continuously advances collective threat intelligence, improves operational efficiency, and strengthens the cybersecurity stance.

How it works

IronDefense works intuitively with Splunk so security teams can easily manage resulting alerts by integrating teams, processes, and tools together to triage and investigate suspicious network activity.

IronDefense vets, prioritizes, and rates alerts long before they reach analysts. By automating time-consuming discovery steps and indicating the severity of anomalous traffic, analysts can make decisions on activity faster.

The IronDefense App for Splunk allows customers to stream alert, event, and contextual data into their own Splunk instance, viewing anomalous network activity detected by IronDefense and enriched by IronDome. By compiling all shared event data into one alert and applying collective intelligence, IronDefense reduces the number of alerts an analyst is required to triage. For deeper investigation, including PCAP analysis, the user can easily pivot from the Splunk dashboard to IronNet's user interface with just one click.

Splunk users can leverage the IronDefense app to customize reports and dashboards, delivering powerful ways to illustrate incoming alert data. IronDefense events also include additional data that does not map to the Splunk Alert Common Information Model (CIM); this data is available for report generation within the Splunk interface through custom queries.

The IronDefense App for Splunk allows data upload and analyst feedback. Users can report their assessments of IronDefense discoveries to share their findings and continually improve the analytics and their accuracy. Viewing IronDome notifications in the Splunk App provides even greater insight into the threatscape, illustrating how the enterprise environment's alerts correlate to alerts from within their sector, thus enabling a faster, more proactive, collaborative approach to cybersecurity.

Download the app

The IronDefense App for Splunk is available for download in Splunkbase.

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.