SOLUTION BRIEF

IronNet

# IronNet and ServiceNow

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

Why we work better **together**

servicenow

### 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, protecting against malicious activity before it invades the network.

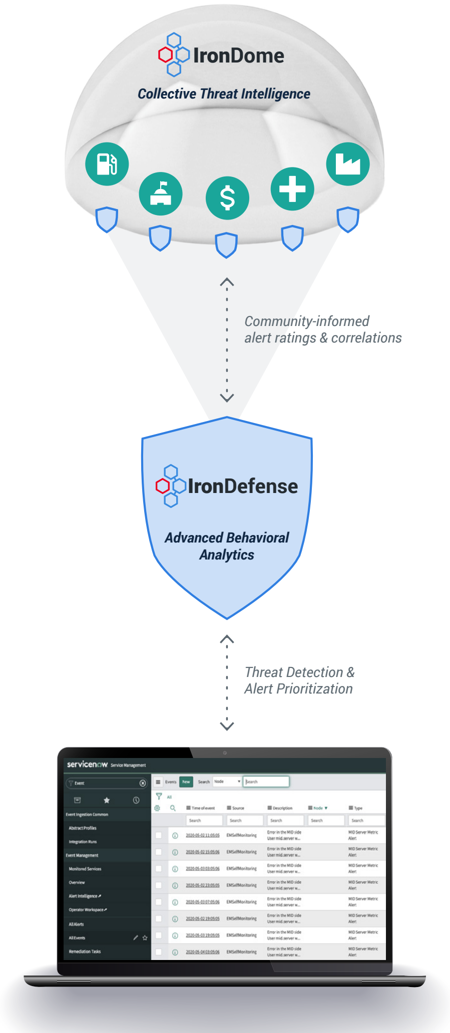
Designed by national security analysts and top intelligence data scientists, IronNet's scalable Network Detection and Response (NDR) solution, IronDefense, and Collective Defense platform, IronDome provide visibility across communities of enterprises This approach allows peers to identify advanced threats that are often missed by existing commercial cybersecurity solutions. IronDefense integrates with ServiceNow, a comprehensive IT service management platform (ITSM), to maximize IronDefense's incident response capabilities. By bringing together digital workflows on a single pane of glass, the IronDefense Integration for ServiceNow relieves overburdened and understaffed security operations centers (SOC). The integration 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. ServiceNow then automatically turns this threat intelligence into actionable response.

### Business challenge

Cyber defense teams operate in isolation against a range of threats. Individual companies defend using traditional cybersecurity tools that often miss advanced or unknown malicious network traffic patterns. These gaps increase the burden of already overworked SOC teams.

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 visibility across their business ecosystems.

# How it works


IronDome
Collective Threat Intelligence
Community-informed alert ratings & correlations
IronDefense
Advanced Behavioral Analytics
Threat Detection & Alert Prioritization
servicenow

ServiceNow and IronDefense work together to enhance the speed and efficiency of detection, triage, and response.

IronDefense strengthens existing cybersecurity platforms without slowing down operations. The IronDefense Integration for ServiceNow enables customers to create ServiceNow events during the IronDefense alert triage process and eliminates the manual process of creating ServiceNow events in IronDefense to track malicious and suspicious activity.

IronDefense vets, prioritizes, and rates alerts before they reach analysts. By automating time-consuming discovery steps and indicating the severity of anomalous activity, analysts can make faster decisions on activity. Together with IronNet's IronDome Collective Defense solution, analysts have complete visibility into the threat landscape, delivering real-time, community-driven threat intelligence insights from peer enterprise SOCs. With IronDome, analysts can share the detection, investigation, triage, and response for each alert detected locally by IronDefense.

The ServiceNow Configuration Management Database (CMDB) is configured to sync with IronDefense, which uses IP bindings to track entities. An analyst can use the corresponding IP lease dates to follow a device's evolution of IP addresses, providing full context of what happened at a given point in time. Analysts can use this information to triage an alert quickly and share it with ServiceNow to initiate further SOC investigation, ITSM ticket creation, and responsive measures. The CMDB integration also provides insight into why specific entities are vulnerable within the ServiceNow platform.

When IronDefense data is ingested into ServiceNow, it eliminates the manual process of creating ServiceNow events to track malicious and suspicious activity. This is crucial for accurate prioritization and efficiency in cases that require further investigation or remediation. The IronDefense Integration for ServiceNow enables customers to seamlessly turn collective threat intelligence into effective IT response.

## Download the integration

The IronDefense Integration for ServiceNow is available for download from the ServiceNow Store.

## 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.