SOLUTION BRIEF

IronNet and Microsoft Azure Sentinel

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

Why we work better **together**

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.

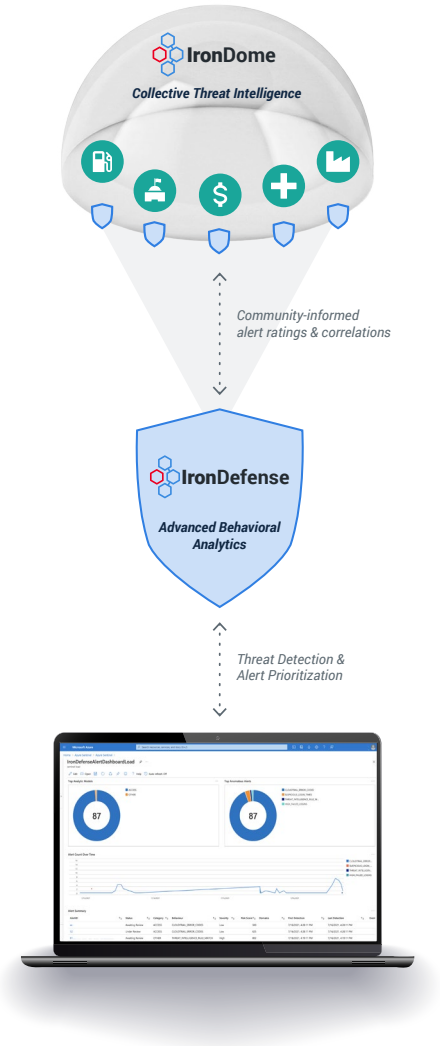
Reduce impact of an attack

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

Sentinel is a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution that collects data at cloud scale across all users devices, applications, and infrastructure, performing real-time security monitoring, advanced threat detection, and forensics and incident management.

+

IronDefense is IronNet's powerful NDR solution which uses Collective Defense to analyze a broader variety of data streams and enriches events with information from multiple threat intelligence sources, allowing customers to use Sentinel as a single pane of glass to display alerts, provide threat visibility, allow proactive hunting, and enable threat response more quickly.



The feedback loop of information sharing between Sentinel and IronDefense continuously advances collective threat intelligence, improves operational efficiency, 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

IronDefense works intuitively within Sentinel to help security teams easily manage resulting alerts by integrating teams, processes, and tools together to triage and investigate suspicious network activity with:

- **Superior Behavioral Detection:** IronDefense applies proven analytics based on machine learning (ML) and artificial intelligence (AI) techniques used in real-world defense against sophisticated cyber criminals and nation-state-level threat actors.
- **Automated Threat Intelligence for SOC Analysts:** IronDefense vets, prioritizes, and rates alerts long before they reach analysts, automating the acquisition of contextual data and applying security playbooks written by IronNet defensive subject matter experts. This system empowers analysts to make faster and better triage decisions.
- **Unparalleled Detection Across All Networks:** IronDefense integrates with public cloud providers such as Azure, private clouds, and hybrid and on-premises networks to deliver a singular view that scales with any infrastructure. Used with our IronDome Collective Defense solution, it delivers real-time visibility to threats targeting your network, supply chain, industry, or region.

Seamless integration with existing security infrastructure

Inputs

IronDefense ingests Azure NSG (network security group), Azure Active Directory, Office 365 network logs, and data from cloud sensors and correlates these sources of data with your SIEM (security information and event management), SOAR (security orchestration, automation, and response), EDR (endpoint detection and response), firewalls, and other security infrastructure tools.

Alerts

Alerts The IronDefense Integration for Sentinel enables customers to stream alert, event, and contextual data into their own Sentinel instance, viewing anomalous network activity detected by IronDefense and enriched by IronDome. PCAP investigation and customized dashboards are built to empower further analysis.

Collaboration

Collaboration The IronDefense Integration for Sentinel is bi-directional, allowing data uploads and analyst feedback to sync between the two interfaces. 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.

Learn More

Download the IronDefense Integration for Microsoft Azure Sentinel in the Azure Marketplace or contact IronNet for a demo.