PRODUCT BRIEF

IronDefense for Microsoft Azure

Advanced Network Detection and Response in the Cloud

Proactive mitigation of cyber threats

IronDefense

PRODUCT BENEFITS AT A GLANCE

Reduce impact of an attack

Leverages advanced behavioral analytics and AI/ML techniques built by elite cyber defenders to detect sophisticated threats in cloud, virtual, and on-premise networks.

Gain visibility across the threat landscape

Receives real-time collective threat intelligence, knowledge sharing, and collaboration with peers for faster threat detection.

Increased effectiveness of existing SOC resources

Integrates seamlessly with existing cyber defenses and SOC workflows to improve detection efficacy and reduce response time to minutes.

IronNet's IronDefense Network Detection and Response (NDR) solution is a highly scalable platform that leverages advanced behavioral analysis and integrated cyber hunt to detect cyber threats missed by traditional cybersecurity tools. Designed by national security experts and top intelligence data scientists, IronDefense delivers industry-leading detection and shares insights for existing and emerging cyber threats.

Meeting the challenge

As an advanced NDR platform, IronDefense improves visibility and detection across your enterprise cloud, virtual, and on-premise infrastructure. Our solution detects stealthy threats using advanced behavioral detection techniques. An Expert System automatically acquires contextual data and applies security playbooks to the triage and risk analysis of detected anomalies. IronDefense integrates with IronNet's IronDome Collective Defense solution to provide visibility into the threat landscape and facilitate peer-security operations center (SOC) insights that help prioritize threats based on risk to your business ecosystem, industry, or region. Best of all, IronDefense fits seamlessly within existing security infrastructure, enabling security teams to efficiently and effectively detect and respond to new threats using existing workflows and security tools.

For CISOs

IronDefense reduces detection gaps and enables security teams to prioritize resources to defend against real—not theoretical—cyber threats targeting your company, industry, or region.

For SOC analysts

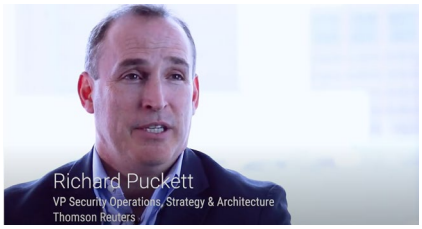
IronDefense identifies known and unknown threats while also automatically acquiring relevant contextual data and triage insights from peer cyber analysts. This allows analysts to make informed decisions quickly, reducing mean-time-to-response.

For threat hunters

IronDefense's hunt capabilities are built by hunters for hunters, enabling security teams to analyze and hunt across cloud, virtual, and on-premise network data in seconds and to pull full packet capture (PCAP) on any flow.

WHY WE CHOSE IRONDEFENSE

THOMSON REUTERS



"As we look to defend our estate as it integrates with various cloud environments, we were impressed by IronNet's capabilities, especially in side-by-side testing with other analytic and detection platforms in the market today."

- Richard Puckett, former VP Security Operations Strategy and Architecture for Thomson Reuters

ABOUT IRONNET

IronNet is a global cybersecurity leader that is revolutionizing how organizations secure their enterprises by delivering the first-ever Collective Defense solution 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.

Key IronNet capabilities for Azure

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.

Detect account takeover attempts

IronDefense's detections and indicators for suspicious logins work with Azure AD (Active Directory) audit and Office 365 logs to find attackers focused on compromising Microsoft accounts.

An automated system that gives SOC analysts Tier 3 assistance

IronDefense's Expert System vets, prioritizes, and rates alerts long before they reach analysts. The Expert System automates the acquisition of contextual data and applies security playbooks written by IronNet defensive subject matter experts. This automation empowers analysts to make faster and better triage decisions for anomalies detected in Azure.

Unparalleled detection across cloud, hybrid, and on-premise networks

IronDefense integrates with Azure, other public cloud providers, private clouds, and on-premises networks to deliver a singular view of your infrastructure. IronDefense scales from small enterprises to Fortune 100 companies and can monitor a single Azure deployment or all of your IT infrastructure.

Real-time visibility across cloud, multi-cloud, and business ecosystems

IronDefense works with our IronDome Collective Defense solution to deliver real-time visibility to threats targeting your supply chain, industry, or region.

Seamlessly integrates with existing security infrastructure

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. IronDefense then delivers effective detection and response in Azure without complex setup and within your existing security workflows.

Proven expertise for the Collective Defense of your organization

IronNet partners with all customers to deliver a personalized experience to help your security team plan, implement, integrate, and operate IronDefense. Our highly skilled industry experts with deep commercial, military, and intelligence experience will work with you every step of the way to deliver measurable improvements to detect network-based threats across your enterprise.

Experience IronDefense

Thinking about IronDefense advanced threat protection? Regardless of your industry or company size, the proof is within reach. A 30-day, remote IronDefense Proof-of-Value (PoV) will give your organization insights into how IronDefense can improve your cyber defenses.