SOLUTION BRIEF

IronDefense on Nutanix

Private Cloud Network Detection and Response with Nutanix for IronDefense

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

Whether due to regulatory compliance, reliability and performance needs, or legacy system support, private cloud infrastructure is here to stay. Although private clouds are known and accessed by fewer users and therefore seem more secure, they are in fact open to the same security risks as public clouds. Whether public or private, the bigger an enterprise is the larger a security target its cloud network becomes.

To help address these risks, IronNet has collaborated with Nutanix to expand IronDefense deployment hosting options to include private and hybrid cloud environments, where cybersecurity flexibility and portability is of key importance. IronDefense delivers high-performance NDR and Collective Defense capabilities as an on-premise Software-as-a-Service (SaaS) solution, using minimal data center space and power resources. The Kubernetes-based architecture easily enables deployment of new IronDefense instances or migration of existing instances onto any sufficient private cloud infrastructure.

Meeting the security challenge

The IronDefense private cloud NDR solution is built on industry-leading Nutanix hyperconverged infrastructure (Nutanix HCI) technology that allows IronDefense to be hosted locally as a cloud-first SaaS platform, improving visibility and threat detection across your enterprise cloud, virtual, and on-premise ecosystems. IronDefense detects stealthy threats using advanced behavioral detection techniques by automatically acquiring contextual data and applying security playbooks to the triage and risk analysis of detected anomalies.

IronDefense also integrates with IronNet's IronDome Collective Defense solution, hosted in a public cloud, to provide visibility into the broader threat landscape and facilitate peer-to-peer sharing of threat insights. This unique capability helps prioritize threats based on risk to the business ecosystem, industry, or region. Most importantly, IronDefense fits seamlessly within existing security infrastructure, enabling security teams to more efficiently and effectively detect and respond to new threats while using familiar 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 capability 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 pull full packet capture (PCAP) on any flow.

IronDefense Capabilities

- **Superior behavioral detection that catches known and unknown threats.** IronDefense uses 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.
- **An automated system that gives SOC analysts Tier 3 assistance.** IronDefense's Expert System vets, prioritizes, and rates alerts long before they reach analysts. It automates the acquisition of contextual data and applies security playbooks written by IronNet defensive subject matter experts that empower analysts to make faster and better triage decisions.
- **Real-time visibility across business ecosystems.** IronDefense works with our IronDome Collective Defense solution to deliver real-time visibility of threats targeting your supply chain, industry, or region.
- **Seamless integration with existing security infrastructure.** IronDefense integrates seamlessly with security information and event management (SIEM); security orchestration, automation, and response (SOAR); endpoint detection and response (EDR); firewalls; and other security infrastructure tools.
- **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.
- **Key industries.** Finance, Energy and Utilities, Critical Infrastructure, Public Sector, Healthcare.

Efficiency and Performance

Until now, bringing NDR to private cloud environments was a challenge due to large, complex infrastructure. Individual server appliances have limited space and lack the flexibility to scale with each enterprise. As Nutanix's first certified NDR provider, IronNet now brings the most sophisticated cybersecurity analytics to the private cloud. With Nutanix HCI, private cloud infrastructure and deployment are simplified.

IronDome Collective Defense

Public cloud hosted-Dome instances provide even stronger protection.

Collective Defense is a secure community in which organizations from a sector, supply chain, or country share threat data, anonymously and in real time, to provide all members an early warning system about potential incoming attacks.

Group Level Threat Detection
Peer Threat Correlation
Peer Analyst Insight Sharing
Weekly Insights Report
(Optional) Government Sharing by Group

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.

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