SOLUTION BRIEF

IronDefense for AWS

Advanced Network Detection and Response in the Cloud

Proactive mitigation of cyber threats

SOLUTION BENEFITS AT A GLANCE

Reduced impact of an attack

Leverage advanced behavioral analytics and artificial intelligence capabilities built by elite cyber defenders to detect sophisticated threats in cloud, virtual, and on-premise networks.

Improved visibility across the threat landscape

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

Increased effectiveness of existing SOC resources

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

Designed by national security analysts and top intelligence data scientists, IronNet's Collective Defense platform is a highly scalable solution that leverages advanced behavioral analysis and integrated cyber hunt to deliver industry-leading detection, context, and insights about existing and emerging cyber threats. IronNet delivers superior behavioral detection through the use of proven analytics that leverage machine learning (ML) and artificial intelligence (AI) techniques, formulated through real-world defense against sophisticated cyber criminals and nation-state-level threat actors.

Meeting the challenge

IronNet enables enterprises to detect stealthy threats targeting your AWS, hybrid-cloud, and on-premise infrastructure. IronDefense applies advanced behavioral detection techniques to AWS VPC Traffic Mirroring, CloudTrail logs, VPC logs, and other data sources to improve visibility across AWS environments and detects threats often missed by traditional cybersecurity tools. IronDefense's integration with IronNet's IronDome Collective Defense delivers real-time visibility and insights into your threat landscape that improve your security team's ability to detect, triage, and respond to threats targeting your enterprise. Best of all, IronDefense fits seamlessly with 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 (MTTR).

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.

Key Benefits for AWS

- **Unparalleled detection across cloud, hybrid, and on-premise networks:** IronDefense works with AWS, other public-cloud providers, private clouds, and on-premise networks to deliver a singular view of your entire network. It is highly scalable and can monitor a single AWS deployment or all of your IT infrastructure.
- **Security and protection of AWS cloud deployments:** IronDefense's industry-leading NDR capability is available for AWS cloud deployments across a wide range of environments and services. Customers can natively replicate Amazon VPC traffic from more than a dozen AWS instance types to IronDefense without any third-party packet forwarding agents. IronDefense automatically analyzes data from cloud, on-premise, and hybrid deployments, enabling better detection and mitigation of more advanced cyber threats.
- **Advanced cyber threat hunting in AWS environments:** With Amazon VPC traffic mirroring, IronDefense customers have the ability to use advanced cyber hunt capabilities across enterprise network flow and employ PCAP analysis to investigate incidents, including in-depth event-defined queries.
- **Industry-wide visibility across peer AWS cloud environments with IronDome:** Threats and anomalies detected by IronDefense are automatically and anonymously shared with other industry peers or supply chain partners in real time through the IronDome Collective Defense platform. This allows IronDome members to identify new threat trends at the sector level, as well as specific new and novel threats in each customer environment. IronNet's innovative Collective Defense capability also enables analysts to collaborate in real time with their colleagues across the community to take immediate action to stop an active threat.
- **Fully automated system that gives SOC analysts Tier 3 assistance:** IronDefense 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, reducing the number of false positives and empowering analysts to make faster, better triage decisions on detected anomalies.
- **Seamless integration with existing security infrastructure:** IronDefense ingests AWS VPC Flow, DNS, CloudTrail, Office 365, cloud sensor, and network logs. IronDefense then correlates these sources of data with your SIEM (security information and event management)/SOAR (security orchestration, automation, and response), threat intelligence, endpoint, or other security infrastructure to deliver effective detection and response in AWS without complex setup and within your existing security workflow.

IronNet Services available on AWS Marketplace

IronNet partners with all customers to deliver a personalized experience to help your security team plan, implement, integrate, and operate IronDefense in AWS. 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.

- **Red Teaming:** With real-world experience in nation-state-level cyber operations, the IronNet Red Team emulates advanced adversarial tactics, testing for specific vulnerabilities that pose a critical risk to your enterprise. After their operation is complete, the Red Team works with your SOC defenders to remediate findings, recommend changes, and validate new controls.
- **Threat Hunting:** IronNet's experienced threat hunters track down the most elusive attackers on our customers' networks, guiding the eradication of live threat actors and reinforcing your security team through education and acceleration of their hunt tactics.
- **Security Advisory Services:** Our team of expert security consultants evaluate your current capabilities and develop a roadmap for program transformation prioritized on threat vectors impacting your industry and threat profile. IronNet's strength and experience acts as a force multiplier for your SOC, crafting a strategy that speeds your organization to a higher level of security.

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.

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.