DATA SHEET

IronNet Collective Defense

Delivering Collective Defense through NDR

CORE FEATURES

- **Behavioral Analytics** utilizing Machine Learning (ML) and Artificial Intelligence (AI) techniques
- **End-to-end visibility** across hybrid and cloud environments
- **Packet-level investigations** with powerful hunt capabilities
- **Community triage and intelligence sharing** through the anonymized IronDome Collective Defense Platform
- **Overwatch threat hunting** services
- **Emerging Threat monitoring** and reporting

SOLUTION

Every cybersecurity organization needs a Network Detection and Response (NDR) solution for complete visibility and cyber defense. IronNet's Collective Defense solution provides NDR with the unique capability to anonymously share and correlate intelligence globally between communities of enterprises, organizations, and industries. Leveraging this collective intelligence, along with advanced behavioral analysis and emerging threat research, Collective Defense is able to detect activity missed by when implementing the CIS Defense In Depth strategy.

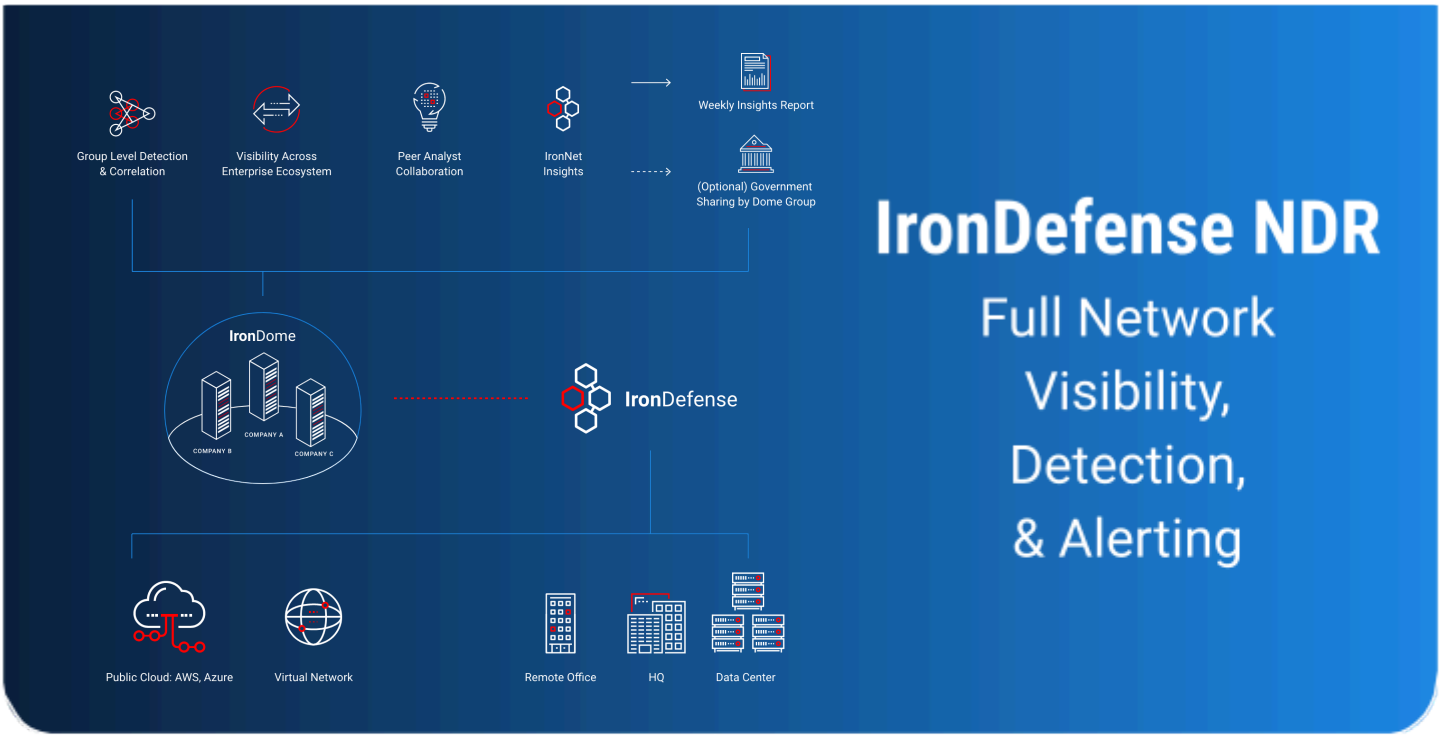
COLLECTIVE DEFENSE

From day one, at no additional cost, Collective Defense customers have access to the anonymized collective defense framework (IronDome). This enables alert correlation and indicator sharing between SOC's seamlessly. Reducing time to triage, this capability effectively acts as a 'SOC multiplier' as well as a growing threat intelligence repository.

How it works:

Collective Defense uses virtual/physical sensors within your enterprise to provide full network visibility, detection, and alerting through our Network Detection and Response (NDR) platform (IronDefense). Each deployment is connected to the Collective Defense Framework (IronDome) to enable anonymized intelligence and alert sharing. Multiple IronDome communities are established to categorize data by industry, such as government or healthcare. This results in the ability to identify benign, suspicious, or malicious activity faster by utilizing the triage of other SOC analysts within your community. For example, if an enterprise workstation at Customer A is infected with malware and is triaged and rated malicious, the same activity within Customer B would be marked malicious with analyst comments applied.

IronDefense ingests north-south traffic at your network perimeter and east-west traffic within your enterprise to provide full visibility across your network and full insights at the individual session level with its continuous PCAP capture capability. Iron Defense uses virtual/physical sensors and data collectors that can be deployed anywhere.



NETWORK VISIBILITY

Uncover hidden threats within your network through packet level investigations. While endpoint data and detections can be altered or stopped by an adversary, network traffic remains constant. Malware needs to communicate, which is why network detection is critical to completing a cybersecurity package. IronDefense targets the behavioral characteristics of these threats to identify both commodity malware and novel threats, enhancing the security posture of any organization.

RAPID RESPONSE

With one click, SOC analysts are able to pivot from an alert to the individual session(s) for immediate triage and analysis. With a hunt platform designed around investigations, session viewing and PCAP download can be handled within seconds. Custom and complex queries are also easy and intuitive for users to generate, providing a powerful hunt resource. In the event of an incident, IronNet Overwatch is a ready resource to assist in hunting and triage.

PROACTIVE DETECTION

IronDefense analytics use Machine Learning (ML), Artificial Intelligence (AI) techniques, and behavioral models to provide alerting and detections following the MITRE ATT&CK framework. This establishes a baseline of detection, which is further enhanced by Emerging Threat alerting through open-source Suricata rules and IronNet 'Threat Intelligence Rules (TIRs)'.

OVERWATCH SERVICES

IronNet Overwatch consists of Cyber Threat Intelligence (CTI) and Cyber Security Analysts that monitor all customer environments for emerging threats and critical alerts. Through threat research and threat hunting, IronNet Overwatch ensures all customers not only have additional eyes on their environments, but a technical resource to assist in triage and analysis.

Summary:

IronNet is a global cybersecurity leader that is revolutionizing how organizations secure their enterprise. Leveraging advanced behavioral analysis, evolving threat indicators, and anonymized collective intelligence customers can expect to instantly expand their capabilities, capacity, and coverage from day one. Collective Defense provides customers a unique capability to defend together within the IronDome collective defense framework.

➜**Want proactive C2 intelligence?** Learn more about IronRader and request a 14-day trial.
➜**Want to learn more about our anonymous collective intelligence?** Learn more about collective defense.