COMPANY OVERVIEW

IronNet

Redefining Cybersecurity

IronNet introduces the first automated, collaborative platform that reports correlated detections from advanced analytics and shares the anonymous metadata in real-time. This is Collective Defense.

> “The U.S. government and industry … must arrive at a new social contract of shared responsibility to secure the nation in cyberspace. This ‘collective defense’ in cyberspace requires that the public and private sectors work from a place of truly shared situational awareness and that each leverages its unique comparative advantages for the common defense.”
>
> *Cyberspace Solarium Commission Report, p. 96*

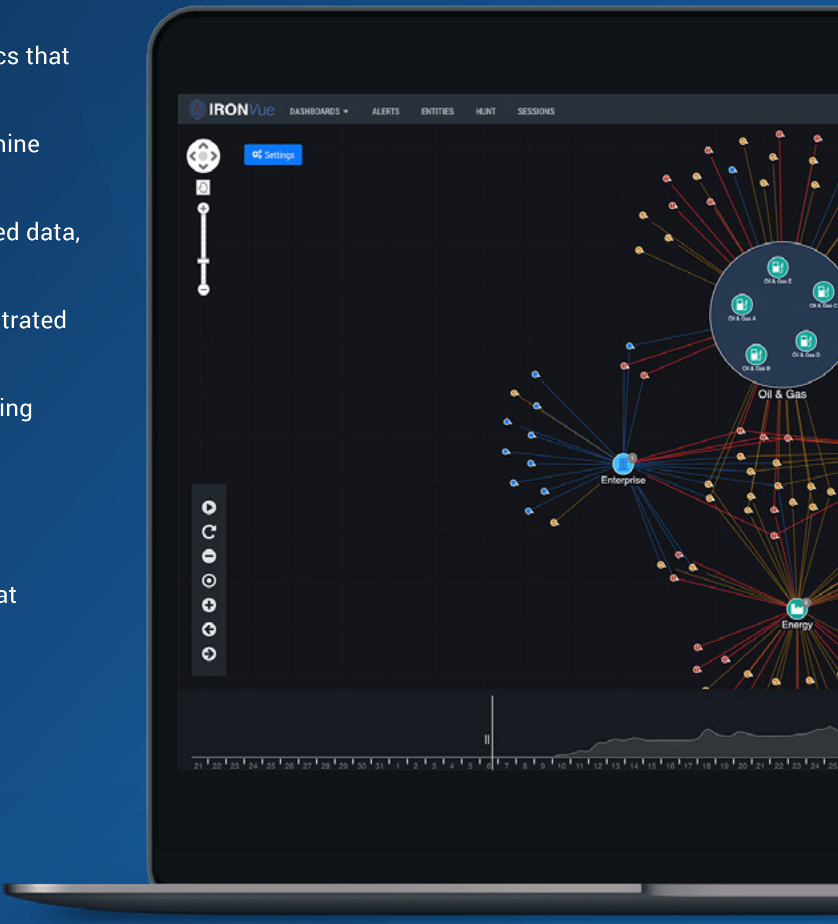
ABOUT IRONNET

Founded by General (Ret.) Keith Alexander, who served as Director of the NSA and Commander of USCYBERCOM, IronNet Cybersecurity provides a comprehensive defense-in-depth solution for identifying and mitigating advanced persistent threats (APT). Leveraging machine learning and deploying analytics designed by world-class data scientists, IronNet applies its tradecraft knowledge and experience to protect and defend critical infrastructure, industry sectors, and state and national governments.

The Cybersecurity Challenge		IronNet’s Solution
• Defending in silos against nation-state attacks does not work	▷	• Deliver a community-based platform that enables collaborative defense against shared threats in real-time
• Private sector and government must communicate and work together to protect the nation	▷	• Anonymously share correlated detections and analysts’ findings across the community
• Visibility into private sector networks to detect global threat campaigns	▷	• Detect campaigns and attacks before they impact your enterprise with visibility into shared threats
• Rapid malware and tool adjustments render signature-based detections ineffective	▷	• Deploy advanced behavioral analytics to detect threats most cybersecurity companies miss
• Detection is often too late, after a network has been compromised and data has been stolen	▷	• Provide early, actionable response through the Collective Defense infrastructure and SIEM/SOAR integrations
• The industry faces a shortage of trained cybersecurity analysts to identify and mitigate threats	▷	• Automate steps of an analyst’s workflow with tradecraft built into an Expert System

IronDefense

- Advanced network detection and response built upon analytics that learn typical network behavior and report deviations
- Applies computational rules from an Expert System to determine risk scoring
- Detects DNS Tunneling, enabling analysts to decode exfiltrated data, download packet capture (PCAP) files, and share findings
- Alerts at machine-speed when large amounts of data are exfiltrated from a network via the HTTP, HTTPS/TLS, and DNS protocols
- Identifies ransomware attacks and when users click on phishing attacks such as those that are skyrocketing in networks



IronDome

- First Collective Defense automated platform that shares threat detections from commercial data in real-time
- Not a threat intelligence feed like IT-ISAC (Information Technology - Information Sharing and Analysis Center)
- Shares correlated, anonymous metadata from IoCs at machine-speed
- Deployed from IronNet's Amazon Web Services (AWS) private cloud for security and reliability
- Analysts can share findings, comment, and rate alerts with the community through the Collective Defense Portal or a SIEM like Splunk or QRadar

IronDefense uses a growing set of behavioral-based analytics for world-class detections:

RECON

- External IP Scanning
- External Port Scanning
- Internal IP Scanning
- Internal Port Scanning

ACCESS

- Phishing HTTPS
- Credential Phishing
- PII Data Loss
- Lateral Movement Chains
- Suspicious File Download

C2

- DNS Tunneling
- Domain Generation Algorithm (DGA)
- Domain Analysis HTTP/TLS
- Periodic Beaconing HTTP
- Consistent Beaconing
- Encrypted Communications

ACTION

- Extreme Rates
- Extreme Rates TLS
- Unusual Day
- Denial of Service

OTHER

- Threat Intelligence Rule Match
- TLS Invalid Certificate Chain
- TOR Traffic
- Rare ASN

Experience Collective Defense

Join the IronNet community to experience first-hand the power of Collective Defense. IronNet offers a comprehensive Proof-of-Value (PoV) program to help assess the effectiveness of your organization's current cybersecurity solutions and determine how IronNet can close gaps with advanced behavioral analytics and Collective Defense.

Contact your IronNet sales representative today, or email info@IronNet.com to get started.