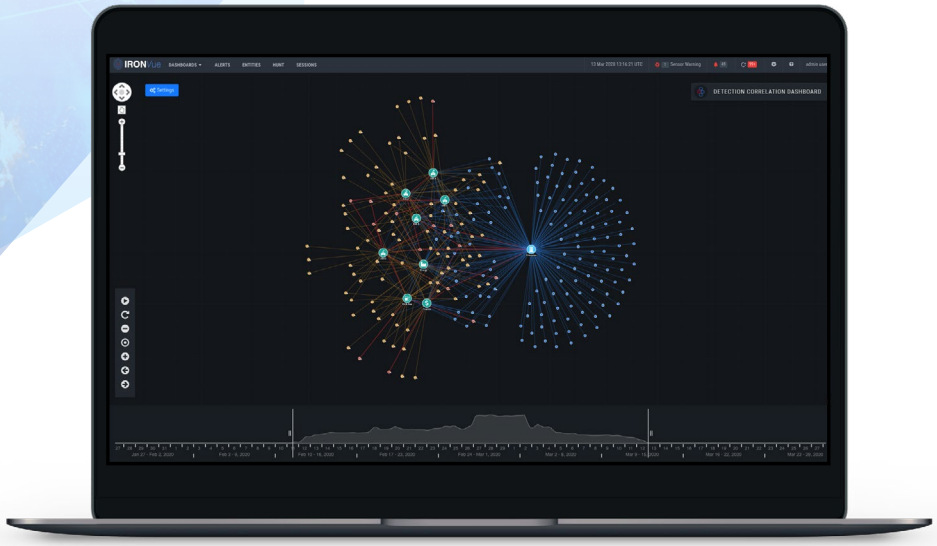
PRODUCT BRIEF

IronDefense Network Sensors

Network traffic analysis and response for the detection of advanced threats



Product Overview

The IronDefense network sensors (IronSensors) process network metadata and full packet-capture (PCAP) on enterprise physical, cloud, and virtual traffic, enabling security teams to gain real-time threat detection of known and unknown threats at scale.

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 Benefits

Superior behavioral detection

IronSensors, used with IronDefense, deliver proven analytics, machine learning (ML), and artificial intelligence (AI) techniques used in real-world defense against sophisticated nation-state-level threat actors.

Unparalleled scalability

IronDefense scales from small organizations to Fortune 100 companies to deliver unmatched detection of threats at enterprises of all sizes. Customers can deploy any number of cloud, virtual, or on-premise hardware IronSensors to fit their needs.

Real-time visibility across your threat landscape

Metadata captured by the IronSensors and analyzed by IronDefense is anonymously shared with an enterprise's IronDome Collective Defense community to provide real-time visibility of threats targeting your supply chain, industry, or region.

Unparalleled expertise

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.

Specifications

Virtual

Sensor Model	VIS-ESX-1
Role	Sensor and PCAP Storage
Virtual Environments	VMware ESX 6.x
Network Packet Capture Rate	Up to 1 Gbps
Mode of Operations	TAP/SPAN
vCPU	6
Clock Rate per Core	Minimum 2.5 Ghz
RAM	24 GB
Storage	10 TB
Virtual Network Interfaces Storage	3 (MGMT, TAP, Future)
FedRAMP Ready	Optional
Proxy	HTTP/SOCKS5

Cloud

Sensor Model	VIS-AWS-1
Role	Sensor and PCAP Storage
Cloud Provider	Amazon Web Services (AWS)
Network Packet Capture Rate	Up to 1 Gbps
Mode of Operations	AWS Traffic Mirroring
Required Instance Type	r5ad.xlarge
Storage	S3

Physical

Sensor Model	IS-0500	IS-1510	IS-3500	IS-4500
Role	Sensor + PCAP	Sensor + PCAP	Sensor Only	PCAP Only
Network Packet Capture Rate	Up to 1 Gbps	Up to 5 Gbps	Up to 10 Gbps	N/A
Rack Unit Size (Per Server)	1U	2U	2U	5U
Mode of Operations	TAP/SPAN	TAP/SPAN	TAP/SPAN	N/A
Network Ports	2x1 GbE, RJ45	4x1 GbE, 2x25 GbE SFP28 Transceivers: 1x1-10GbE SFP+ 1x10-25 GbE SFP28	4x1 GbE, 2x25 GbE SFP28 Transceivers: 1x10-25 GbE SFP28	4x1 GbE
Storage Configuration	RAID 5	RAID 5	RAID 6	RAID 6
Storage Capacity	4x12 TB Self- Encrypting, FIPS 140-2 compliant HDD	12x12 TB Self-Encrypting, FIPS 140-2 compliant HDD	2x1.2 TB Self- Encrypting, FIPS 140-2 compliant HDD	42x12 TB Self-Encrypting, FIPS 140-2 compliant HDD
Power Supply	Dual, Hot plug, Redundant (1+1), 350W	Dual, Hot plug, Redundant (1+1), 1100W	Dual, Hot plug, Redundant (1+1), 1100W	Dual, Hot plug, Redundant (1+1), 2200W
Trusted Platform Module (TPM)	v2.0, FIPS 140-2, CC Certified	v2.0, FIPS 140-2, CC Certified	v1.2v2, FIPS 140-2, CC Certified	N/A
Proxy	HTTP/SOCKS5	HTTP/SOCKS5	HTTP/SOCKS5	N/A