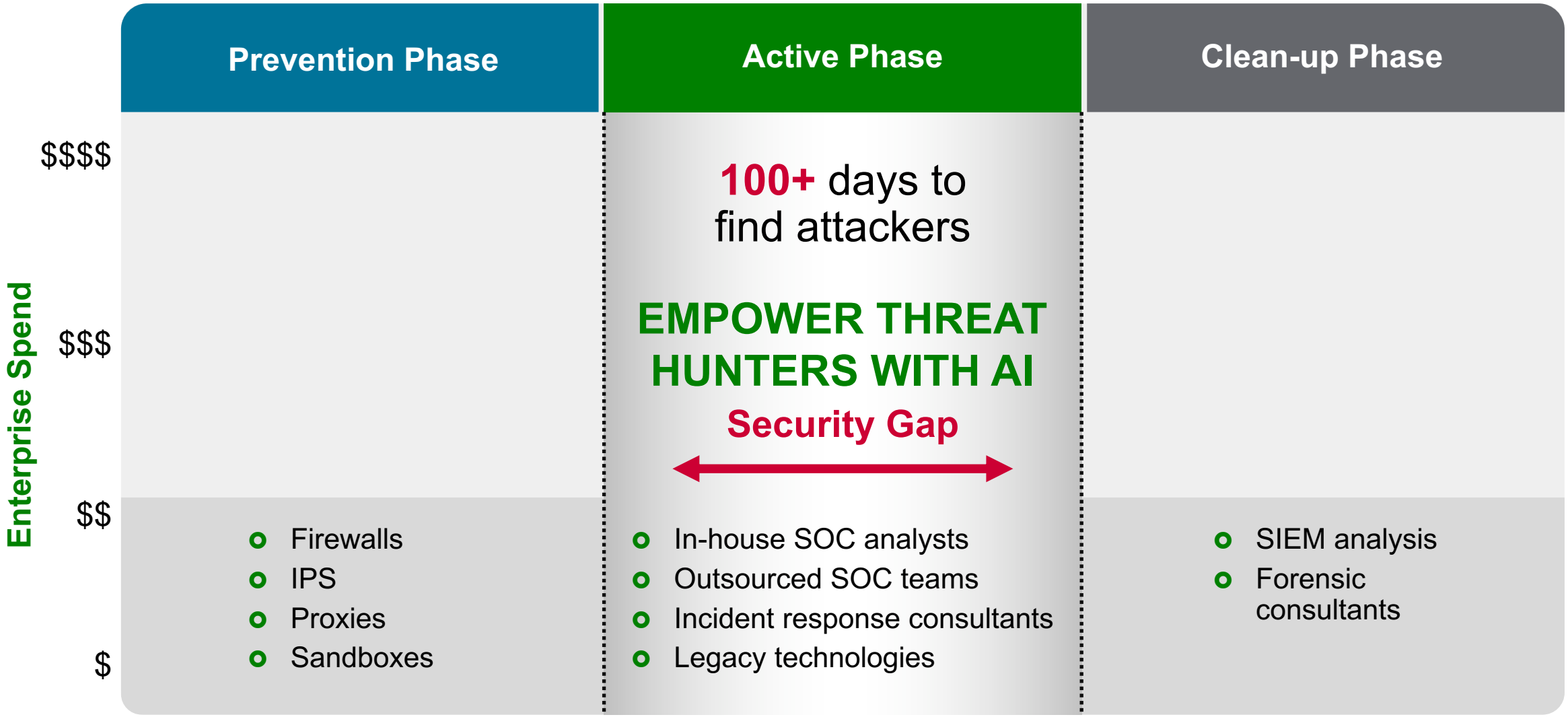
VECTRA®

Security that thinks®

Empowering threat hunters with artificial intelligence

Enterprises are blind to attacks despite massive spend



Source: M-Trends 2016

AI to empower threat hunters

Cognito Cyberthreat Detection and Hunting Platform

Detect

AI-powered automated threat detection

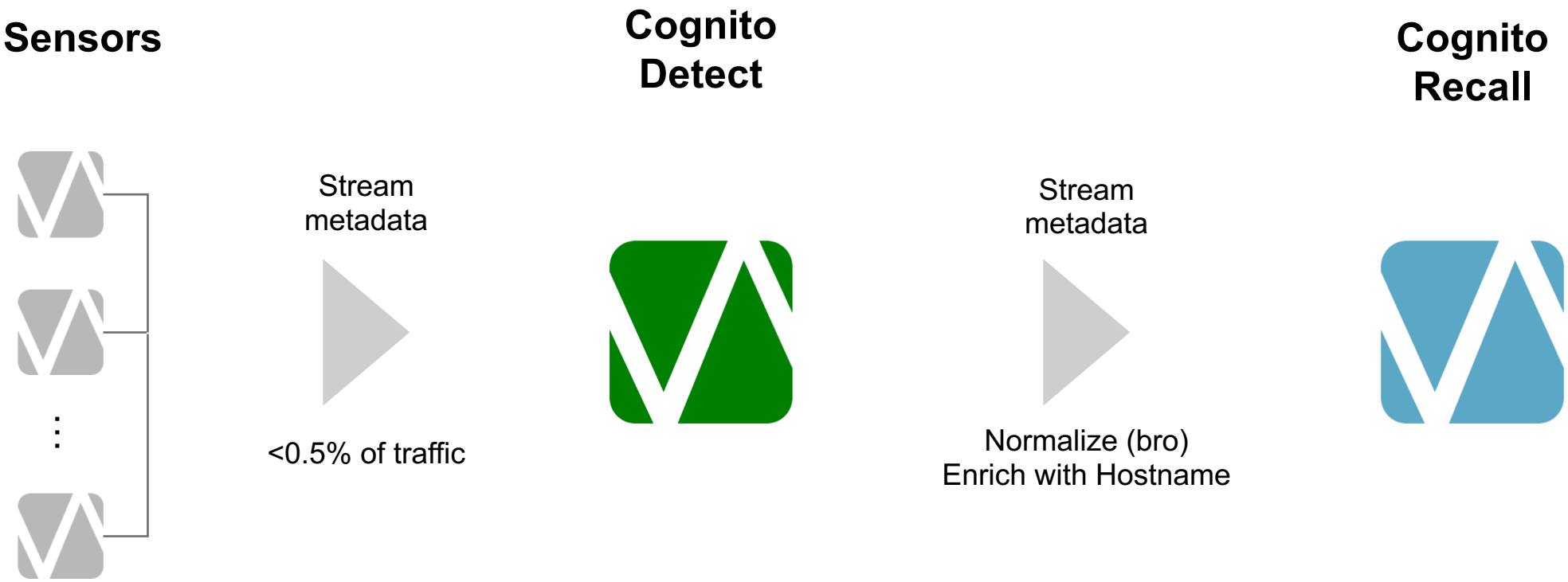
- Finds stealthy attackers in real-time
- Rich context to accelerate triage
- Custom IoC matching to augment AI
- Enterprise-wide coverage

Recall

The most efficient way to hunt for threats

- Eliminate the network visibility gap
- Intelligent investigation of activity by device
- Retrospective threat hunting
- Cloud-powered limitless scale

Architected for large enterprise scalability



- Passive deployment
- Extract metadata
- Packet rolling buffer
- Physical or virtual
- Up to 20Gbps

- Real-time detection
- Host scoring + Campaigns
- 6 months detection storage
- 500 sensors, 300K hosts, 50 Gbps in 1RU

- Full network metadata storage and search
- SaaS
- 2 weeks to unlimited

Cognito Detect – It's all about detecting attacker behaviors

Security Research
Characterize fundamental attacker behaviors

Data Science
ML models to accurately detect behaviors

Attacker Behavior models
High-fidelity, signatureless detection

10 Patents Awarded
20+ Patents Pending

Command and Control	Reconnaissance	Lateral Movement	Exfiltration
Advanced C2: human control	Network sweeps and scans	Stolen accounts	Data movement
Botnet C2	Advanced: AD, RPC, shares	Exploits	Methods, e.g. tunnels
		Backdoors	

Cognito Detections example across all phases of attack

Detect the behaviors that make botnets profitable

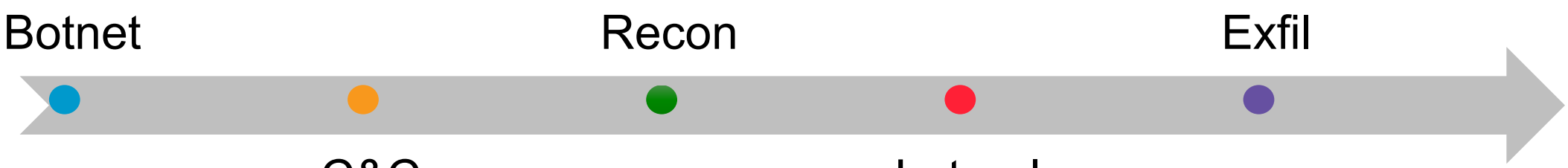
- Click-fraud, bitcoin mining, spam, DDoS, outbound scans, relay traffic

Detect attackers preparing to expand

- Vulnerability scans, low-and-slow network scans

Focus on your data and key assets

- Data smuggling, staged transfers, and slow-bleed exfiltration of data



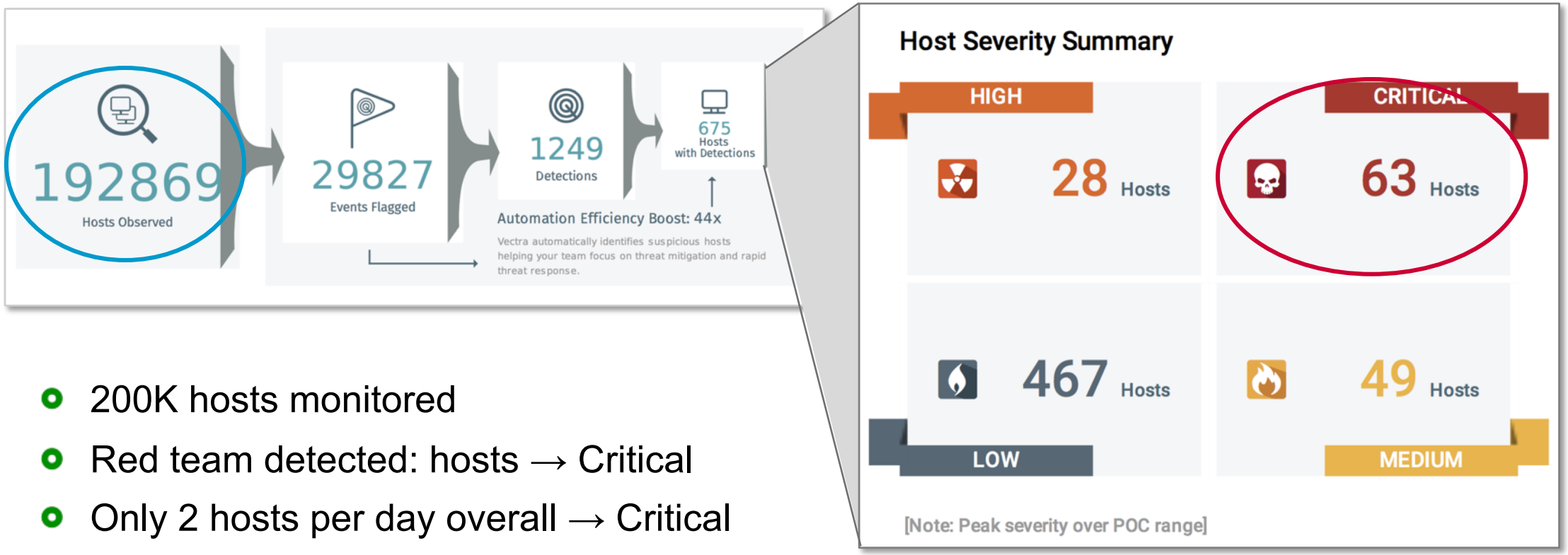
Find hidden communications that bypass firewalls and signatures

- Custom RATs, hidden tunnels, stealth posts, and anonymization tools

Find malware and human attackers as they spread through the network

- Spreading malware, compromised administrator credentials, and backdoors in the infrastructure

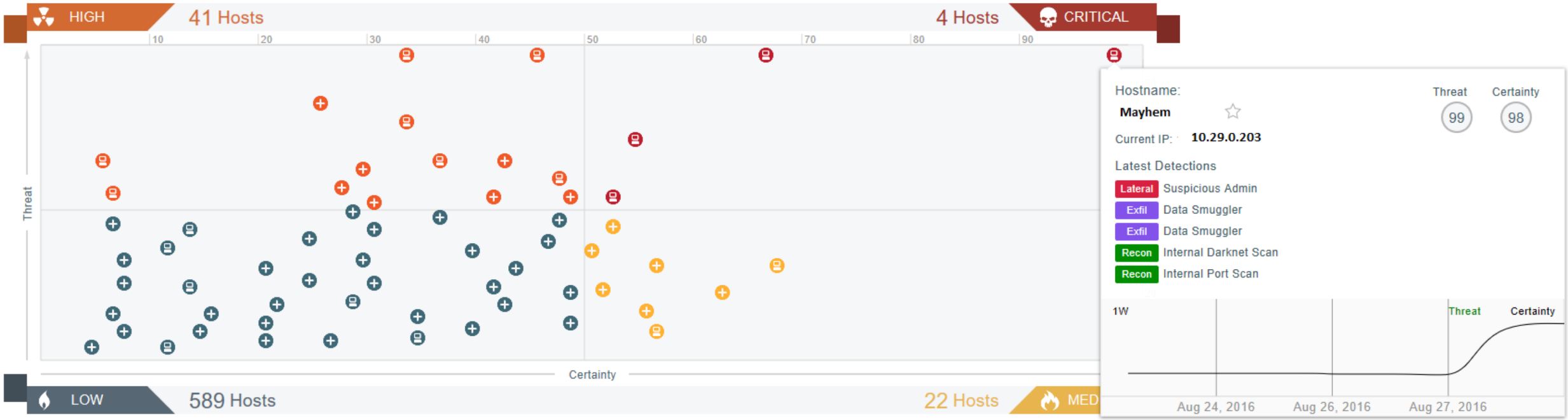
Cognito Detect: Low-noise, high-fidelity at scale: recent 30-day eval



- 200K hosts monitored
- Red team detected: hosts → Critical
- Only 2 hosts per day overall → Critical

Cognito separates signal from noise

Cognito Detect: User Interface



Cognito Recall: User Interface

- Empower threat hunters: complete record of historical network metadata
- Intelligent investigation of device activity – not just IP
- Cloud-powered limitless scale

Cognito Recall: Rich, enterprise-wide network visibility

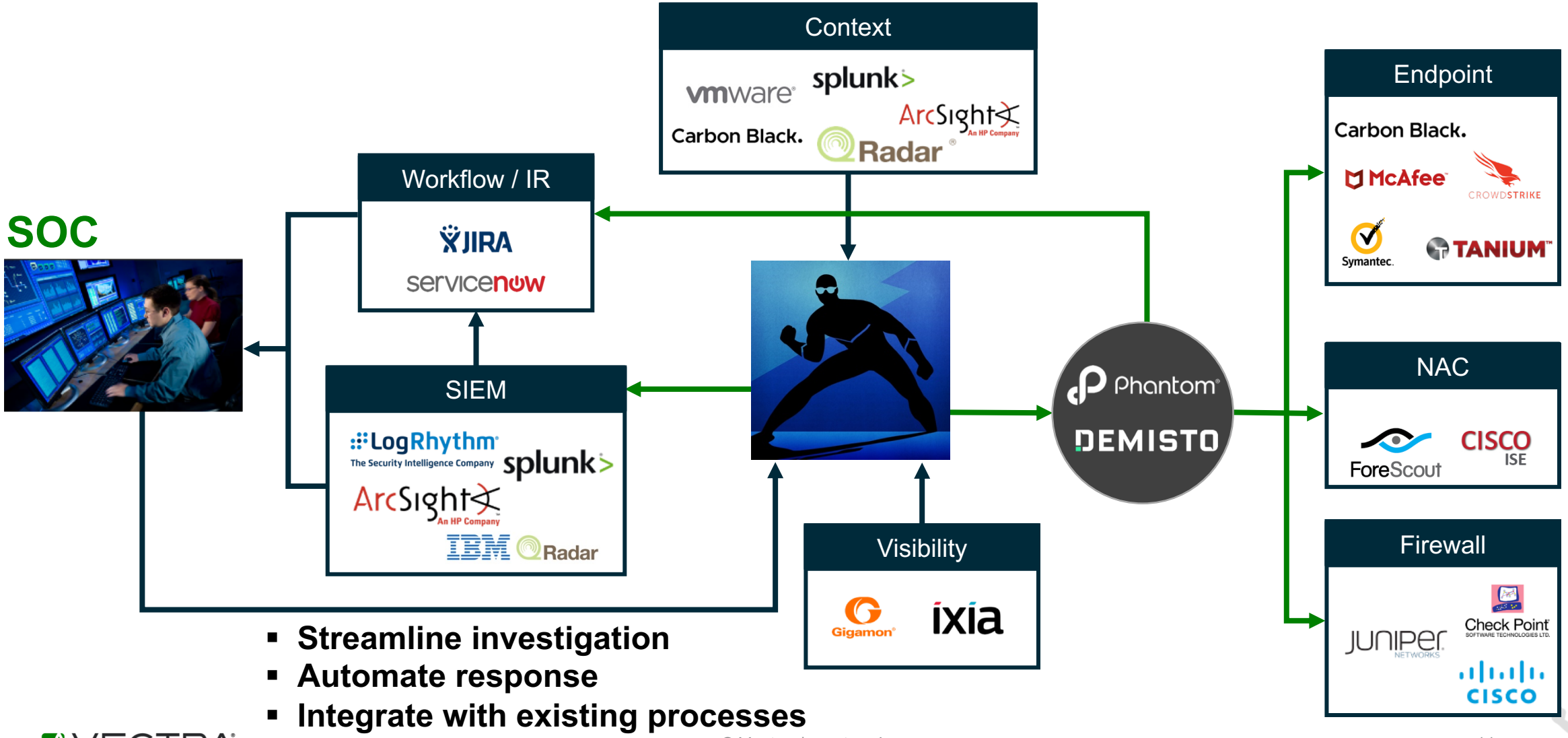
Supported network metadata formats

Bro Type	Description
conn	IP, TCP, UDP, connection details
dhcp	DHCP lease activity
dns	DNS query / response activity
http	HTTP request / reply details
kerberos	Kerberos authentication
ldap (not in Bro)	LDAP queries and responses
ssl	SSL handshakes
dce_rpc	Details on DCE/RPC messages
ntlm	NT Lan Manager - shows auth attempts over SMB, other protocols
rdp	Remote Desktop Protocol
smb_files	Details on SMB files
smb_mapping	SMB share mappings

Unique Cognito enrichment

Enrichment	Description
hostname	Based on HostID naming. Enables analyst to search metadata by host rather than manually correlating IP to host based on search timeframe.
directionality	Direction of the flow: in-to-in, in-to-out or out-to-in. Based on configuration of Cognito Detect for public vs private address space.

Cognito improves the speed and efficiency of incident response



- **Streamline investigation**
- **Automate response**
- **Integrate with existing processes**


VECTRA®
Security that thinks®