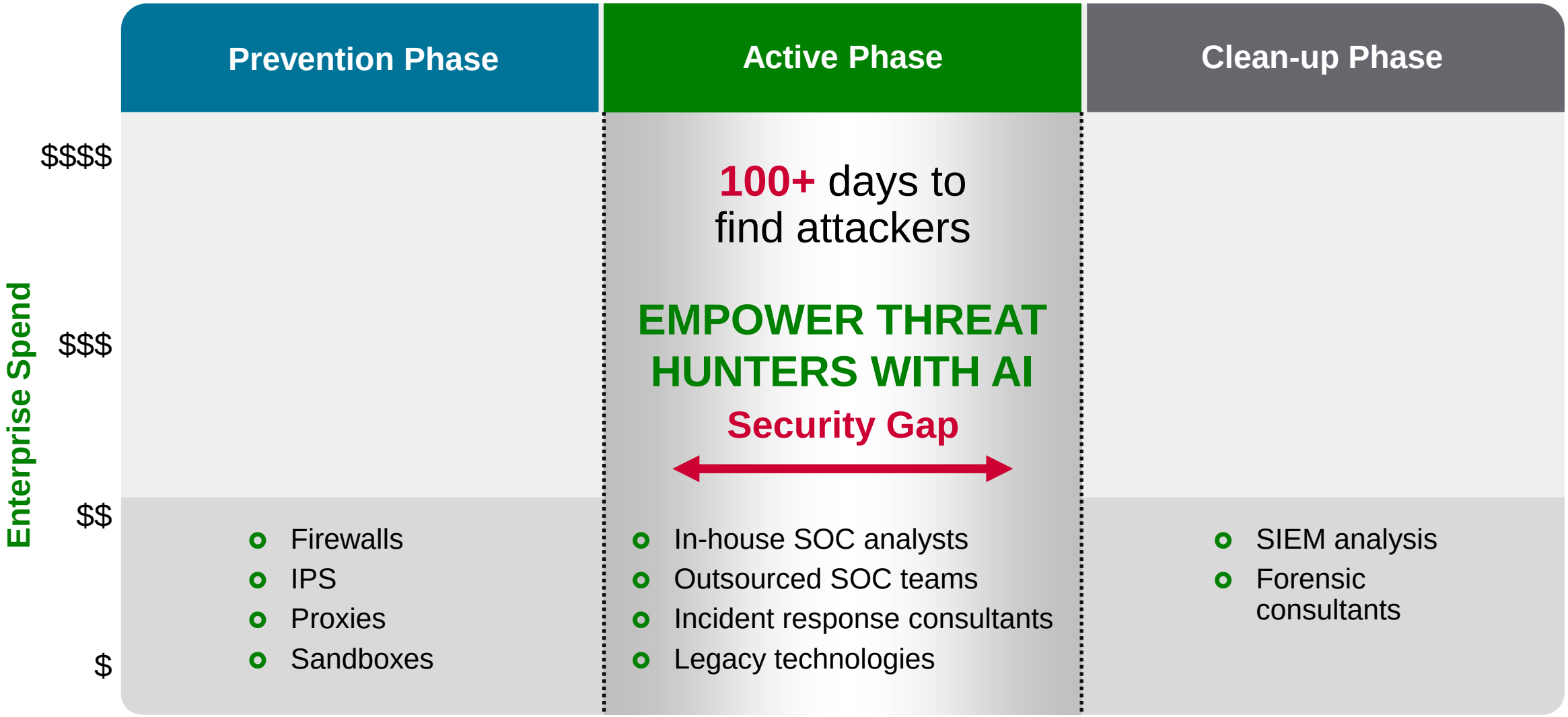
VECTRA®

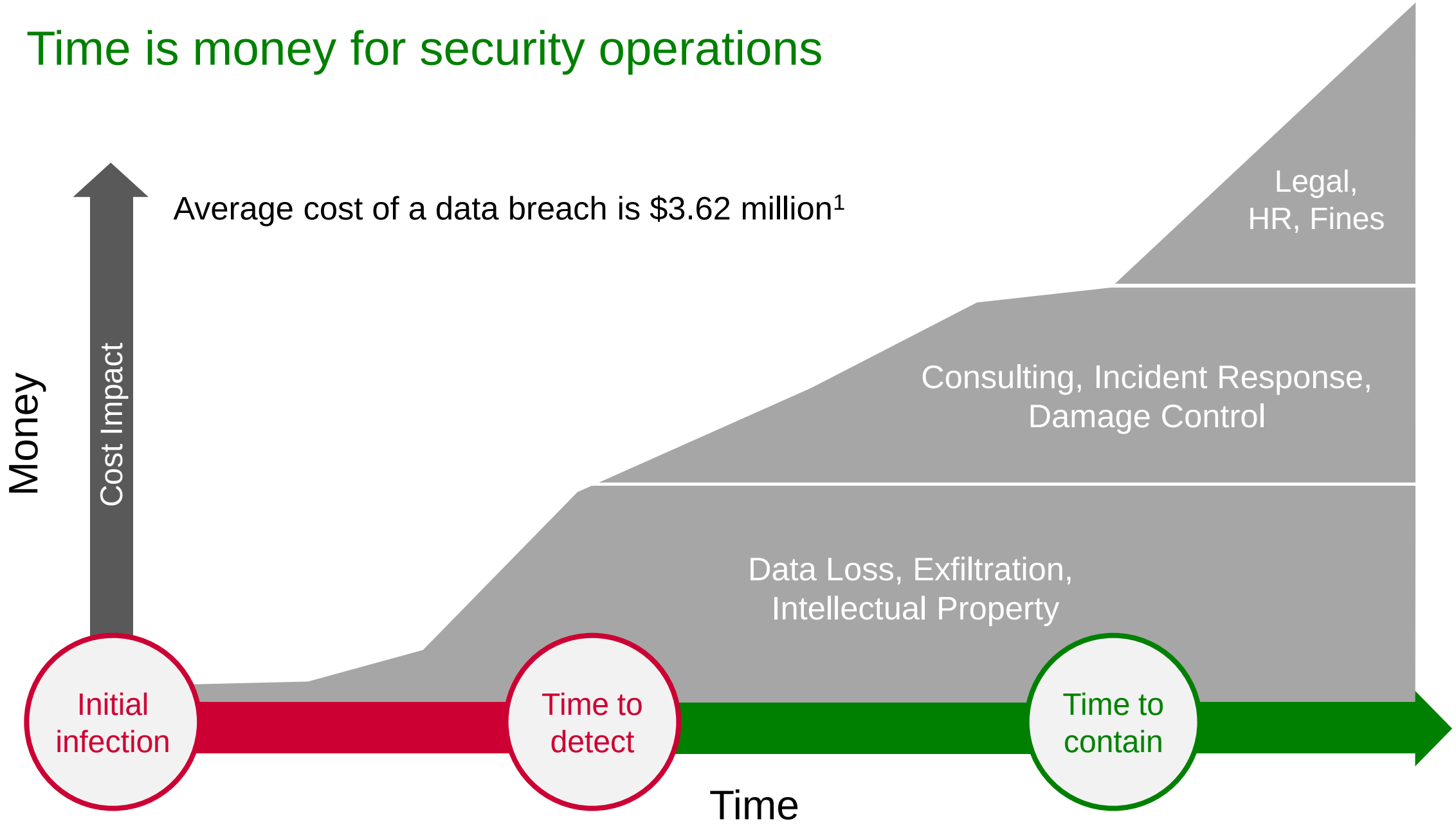
Security that thinks®

Empowering threat hunters with artificial intelligence

Enterprises are blind to attacks despite massive spend



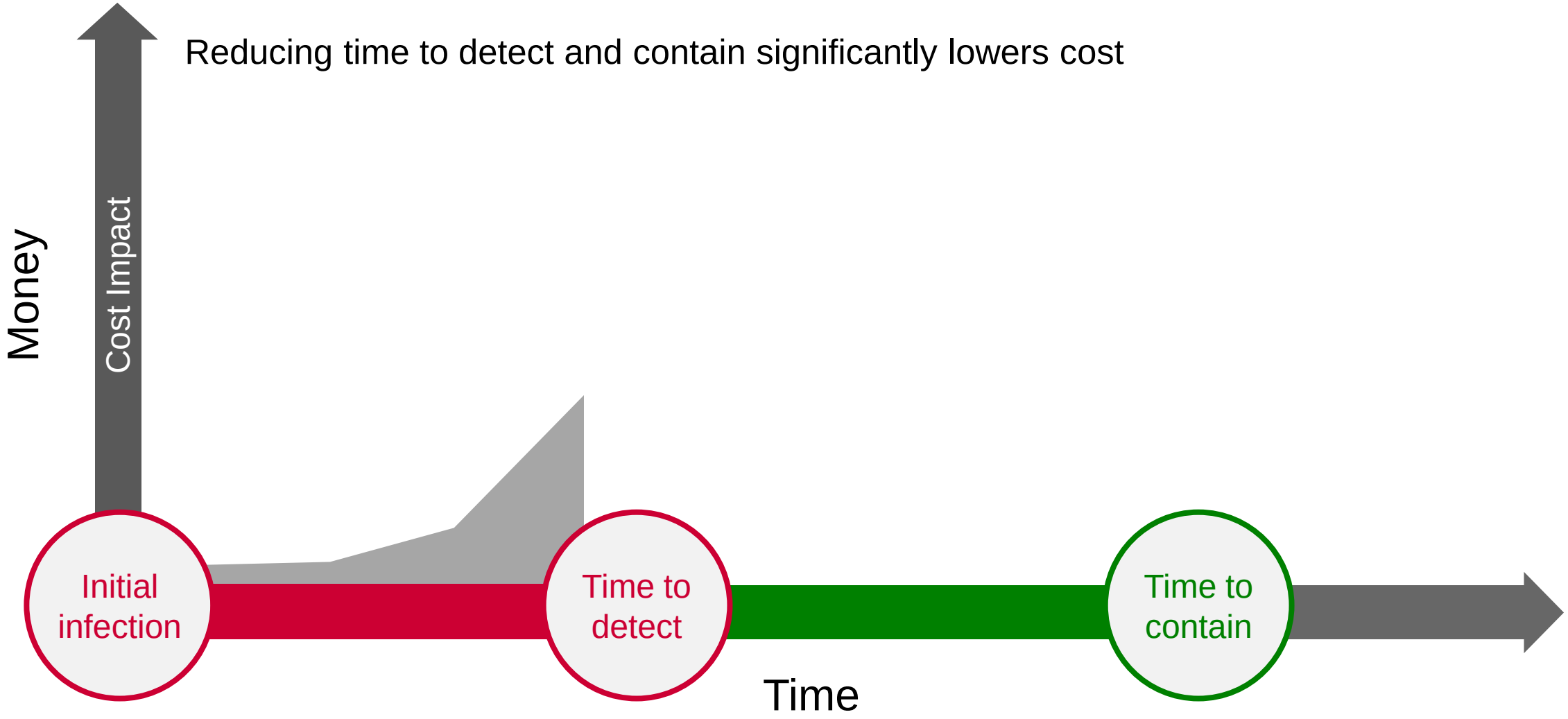
Time is money for security operations



[1] 2017 Ponemon Cost of Data Breach Study

Automating with AI delivers meaningful results

Reducing time to detect and contain significantly lowers cost



Trusted by industry leaders worldwide

Customers

HBO LATIN AMERICA GROUP
LIVE NATION
ticketmaster
Jackson HEALTH SYSTEM
TEXAS A&M UNIVERSITY
HydroOttawa
HomeServe
Microsoft
UNDER ARMOUR
KRONOS
Greenhill
NASDAQ
Pinterest
vetropack
UMass
Verifone
DAQRI
DZ BANK
coop
Tribune Media
Agilent Technologies
riverbed

Partners

vmware
CARBON BLACK ARM YOUR ENDPOINTS
CROWDSTRIKE
ixia
LogRhythm The Security Intelligence Company
Phantom
Radar
ArcSight
splunk>
Gigamon

Awards

CYBERSECURITY BREAKTHROUGH AWARD 2017
THE GOLDEN BRIDGE AWARDS GOLD BEST 2017 BUSINESS WORLD
InformationWeek TOP 125 VENDORS TO WATCH In partnership with InteropITX
CSO 50 AWARDS HONOREE 2017
SC 2017 awards finalist
THE CHANNEL CO. CRN SECURITY 100 2016
DARKReading Best of black hat Awards 2016 WINNER
Forbes HOTTEST CYBERSECURITY STARTUPS OF 2015
Gartner 2015 CoolVendor

Investors

khosla ventures
wipro
AME CLOUD VENTURES
JUNOS INNOVATION FUND
Gníomhaireacht Bainistíochta an Chisteáin Náisiúnta National Treasury Management Agency
Ciste Infheistíochta Straitéisí d'Éirinn Ireland Strategic Investment Fund
IA VENTURES
ACCEL PARTNERS
intel capital
ATLANTIC BRIDGE

Gartner Magic Quadrant for IDPS

Figure 1. Magic Quadrant for Intrusion Detection and Prevention Systems

Source: Gartner (January 2018)

Vectra is the only visionary in the Gartner 2018 Magic Quadrant for Intrusion Detection and Prevention Systems

Source: Gartner Magic Quadrant for Intrusion Detection and Prevention Systems
January, 2018
ID Number: G00324914

All statements in this report attributable to Gartner represent Vectra's interpretation of data, research opinion or viewpoints published as part of a syndicated subscription service by Gartner, Inc., and have not been reviewed by Gartner. Each Gartner publication speaks as of its original publication date (and not as of the date of this presentation. The opinions expressed in Gartner publications are not representations of fact, and are subject to change without notice.

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

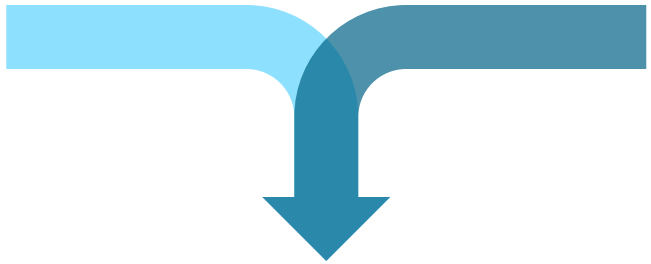
The most efficient way to hunt for threats

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

Cognito Detect: It's all about attacker behaviours

Security Research
Characterize fundamental attacker behaviors

Data Science
ML models to accurately detect behaviors



Attacker Behaviour models
High-fidelity, signatureless detection

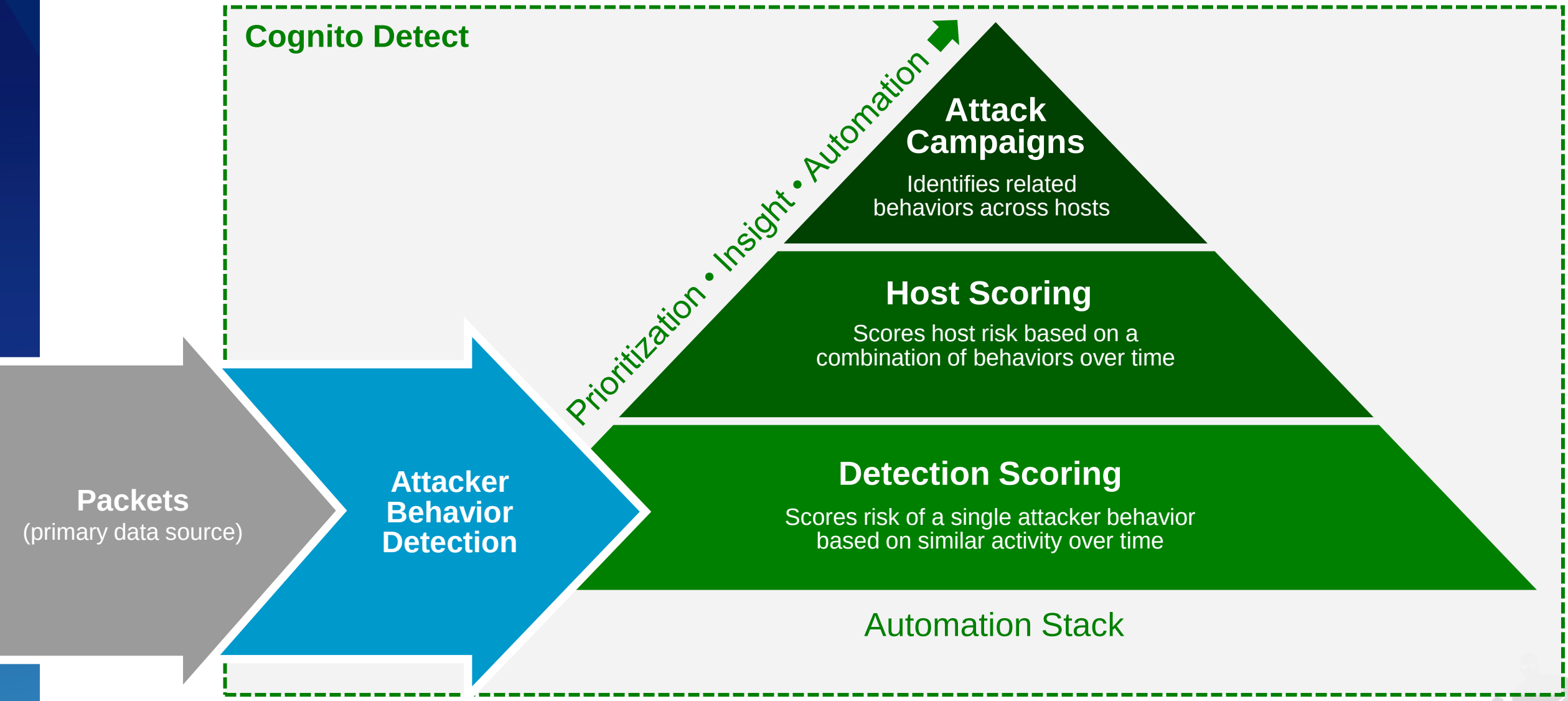
Command and Control	Reconnaissance	Lateral Movement	Exfiltration
Advanced C2: human control	Network sweeps and scans	Stolen accounts	Data movement
Botnet C2	Advanced: AD, RPC, shares	Exploits	Methods, e.g. tunnels
		Backdoors	

Detects Attacker Behaviours across the kill chain

Command and Control	Reconnaissance	Lateral Movement	Exfiltration
External Remote Access	Internal Darknet Scan	Suspicious Remote Exec	Data Smuggler
Hidden DNS Tunnel	Port Scan	Suspicious Remote Desktop	Smash and Grab
Hidden HTTP/S Tunnel	Port Sweep	Suspicious Admin	Hidden DNS Tunnel
Suspicious Relay	SMB Account Scan	Shell Knocker	Hidden HTTP/S Tunnel
Suspect Domain Activity	Kerberos Account Scan	Automated Replication	
Malware Update	File Share Enum	Brute-Force Attack	
Peer-to-Peer	Suspicious LDAP Query	SMB Brute-Force	
Pulling Instructions	RDP Recon	Kerberos Brute Force	
Suspicious HTTP	RPC Recon	Suspicious Kerberos Client	
Stealth HTTP Post		Suspicious Kerberos Account	
TOR Activity		Kerberos Server Activity	
Threat Intel Match		Ransomware File Activity	
		SQL Injection Activity	

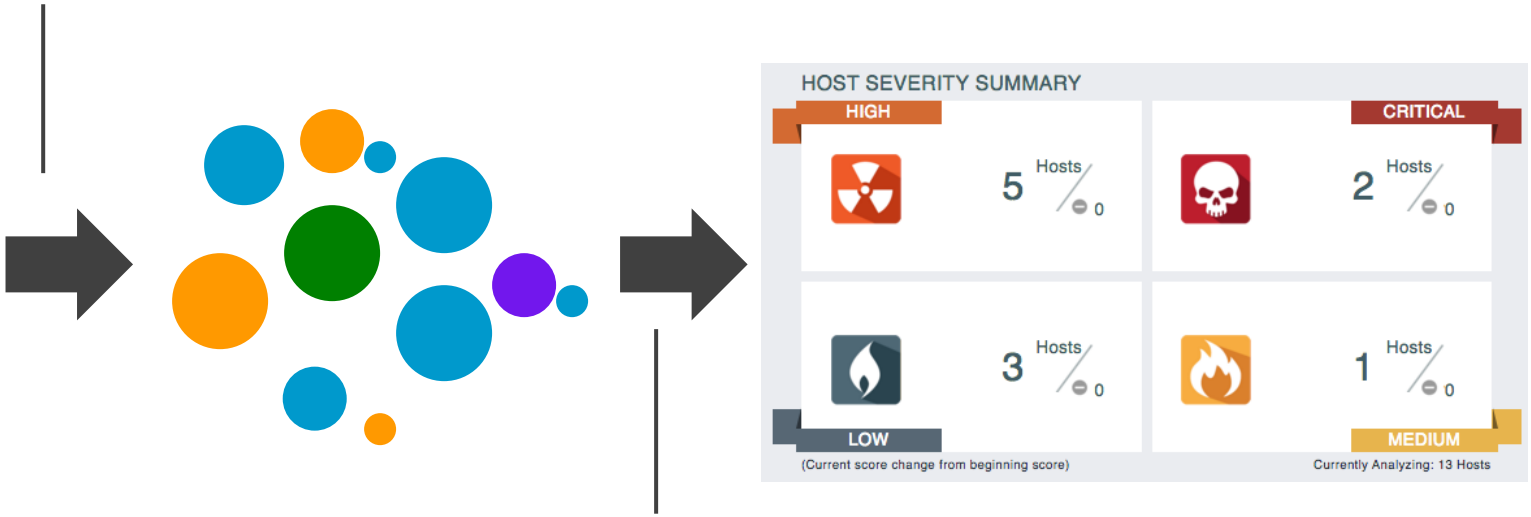
Botnet Monetization
Abnormal Web or Ad Activity
Cryptocurrency Mining
Brute-Force Attack
Outbound DoS
Outbound Port Sweep
Outbound Spam

Automated hunting for attacker behaviours….

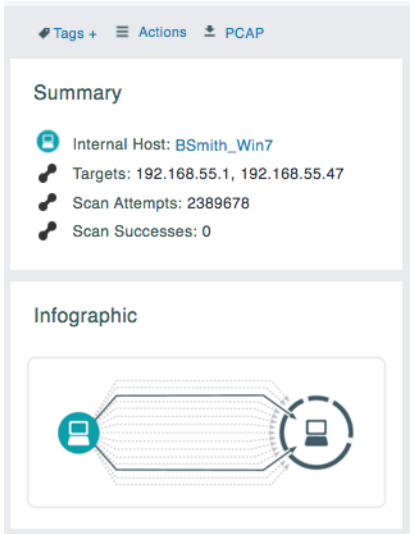


…to reduce the workload on security analysts…

Detect: 100s to 1,000s of network behaviors need to be condensed to a few detections



Report: Analysts need enough information to make a decision and recommendations for next steps



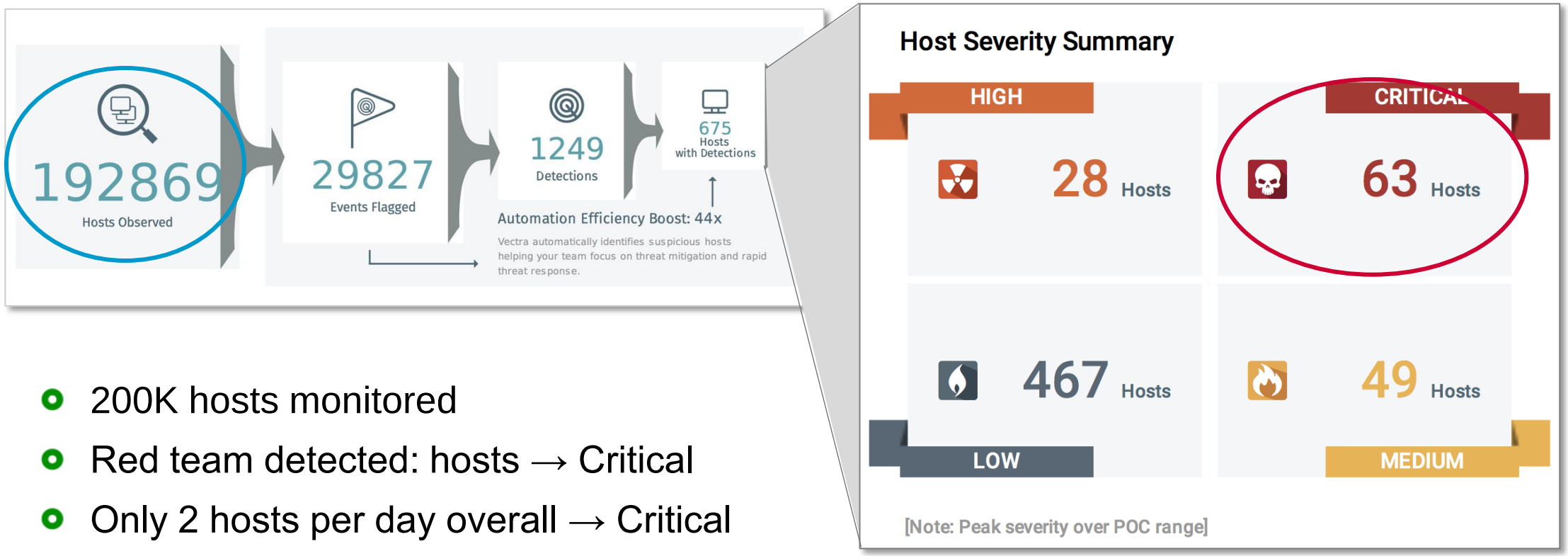
Triage: Detections need to be correlated to pinpoint physical hosts at the center of an attack

Respond: Vectra Cognito integrates with enforcement and incident response platforms

SOC
- SIEM
- Incident Response

- Firewall
- Endpoint
- NAC

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

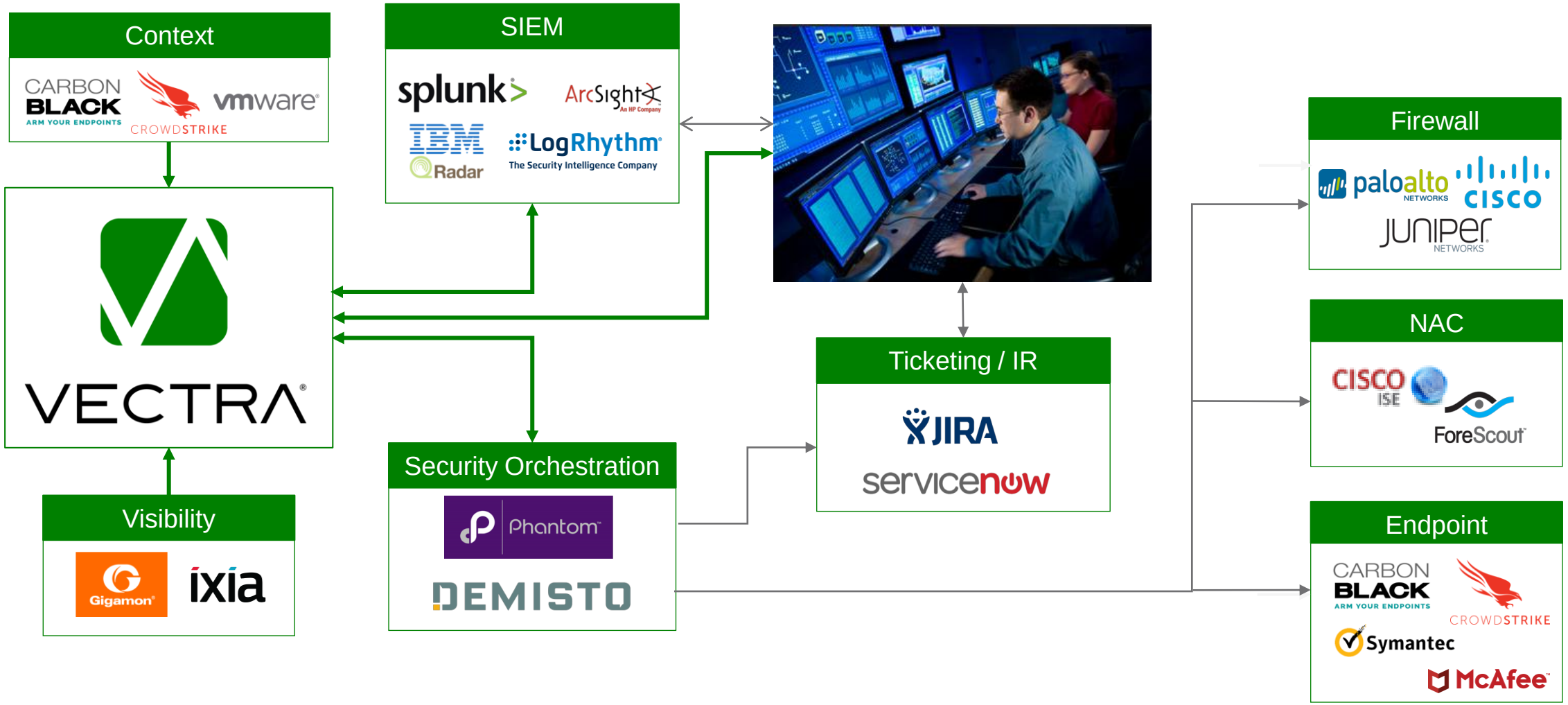


- 200K hosts monitored
- Red team detected: hosts → Critical
- Only 2 hosts per day overall → Critical

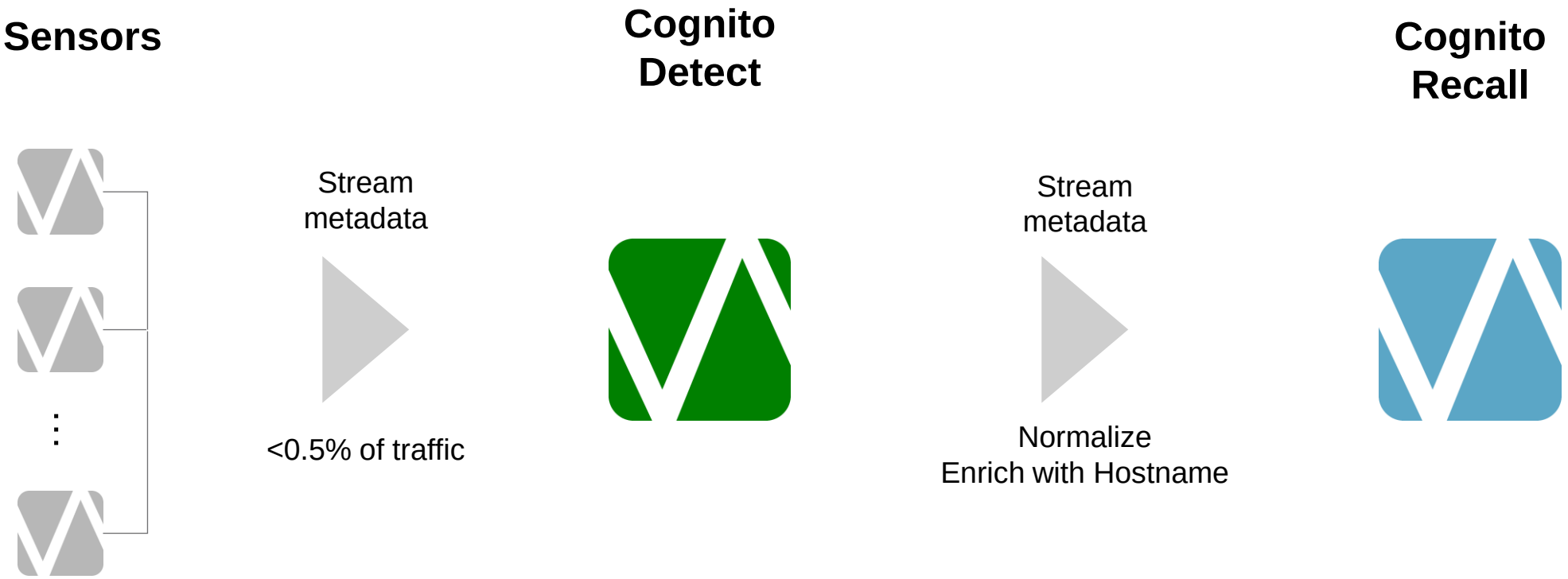
Cognito separates signal from noise

Improving efficiency through ecosystem

Streamline investigation | Automate response | Integrate with existing processes



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

- Extended metadata storage and search
- Limitless scale with Vectra Cloud

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


VECTRA®
Security that thinks®