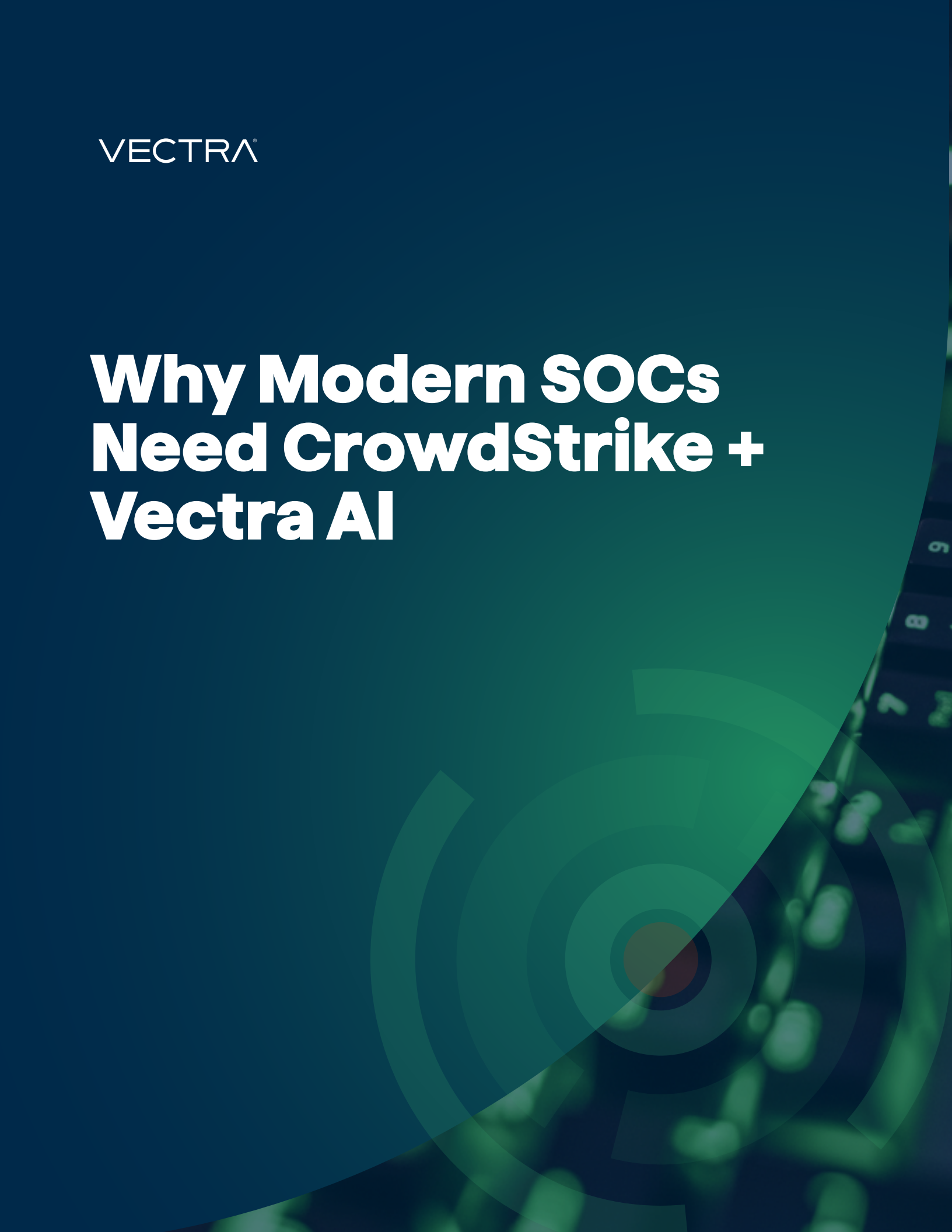
VECTRA

Why Modern SOCs Need CrowdStrike + Vectra AI



SECTION 1

The Modern Reality

Attackers Don't Stop at the Endpoint — and Neither Should Your Detection

EDR is foundational. But modern attackers exploit identity, cloud, SaaS, unmanaged devices, and encrypted network traffic — areas where endpoint visibility alone cannot provide full coverage. Modern attackers don't operate in silos, and they don't need an endpoint agent to move forward. With security teams responsible for hundreds of thousands of assets, placing an agent everywhere is impractical, and most EDR solutions remain vulnerable to common evasion techniques. The result is blind spots, alert fatigue, and missed threats across an ever-expanding attack surface.

SECTION 2

The 5 Reasons EDR is Not Enough

1 Agents Can't Be Everywhere

Up to 50% of devices may lack an EDR agent, and because EDR only monitors systems running an agent, unmanaged devices (e.g. IoT/OT assets, network gear, contractor systems) create significant blind spots that attackers knowingly exploit.

HOW VECTRA AI AND CROWDSTRIKE WORK TOGETHER

Vectra AI provides agentless network visibility across **on-prem data centers**, identity, cloud, and unmanaged assets — enriching CrowdStrike Falcon Insight XDR detections with full attack surface context.

2 EDR Is Being Bypassed, Evaded, or Disabled

Validated attacker behaviors, such as kernel driver abuse, agent tampering, and EDR hook removal tools, demonstrate that endpoint protection is not 100% foolproof.

HOW VECTRA AI AND CROWDSTRIKE WORK TOGETHER

When attackers bypass endpoint protection, Vectra's AI-driven network telemetry detects post-compromise behaviors — then automatically triggers CrowdStrike host isolation via integration.

> Vectra sees the behavior.

> CrowdStrike isolates the host.

3 Host-Centric Visibility Misses Lateral Movement & Identity Abuse

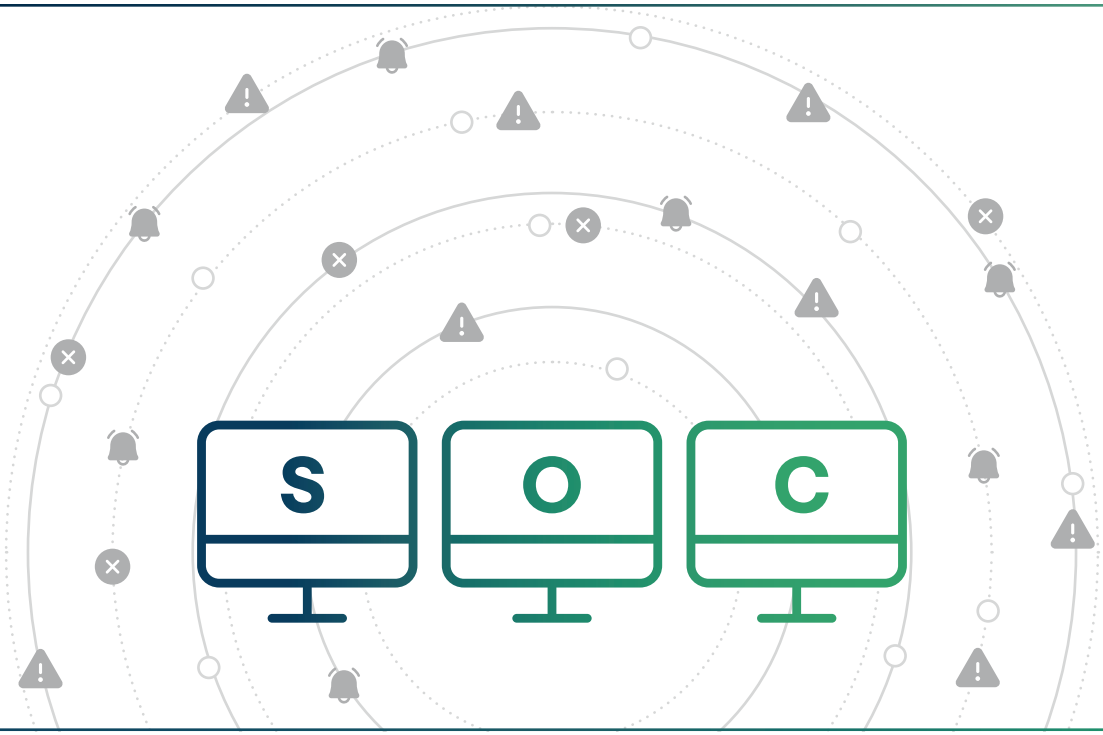
EDR has limited visibility into east-west lateral movement, encrypted SSL in C2, Kerberos abuse, and cloud pivoting. Because identities are highly portable, attackers can move across systems, shift to hosts without EDR, and assume other compromised accounts. For effective response and recovery, there needs to be comprehensive blast-radius visibility across all affected hosts and identities.

HOW VECTRA AI AND CROWDSTRIKE WORK TOGETHER

Vectra correlates network, identity, SaaS, and cloud signals using our patented AI, while CrowdStrike provides deep endpoint telemetry and response.

TOGETHER:

- Unified detections
- Correlated alerts
- Faster investigations inside Falcon Next-Gen SIEM



4 SOCs Are Drowning in Alert Noise

SOCs face roughly 3,800-4,000 alerts a day, yet fewer than 1% are truly actionable. More tools do not necessarily produce better signal.

HOW VECTRA AI AND CROWDSTRIKE WORK TOGETHER

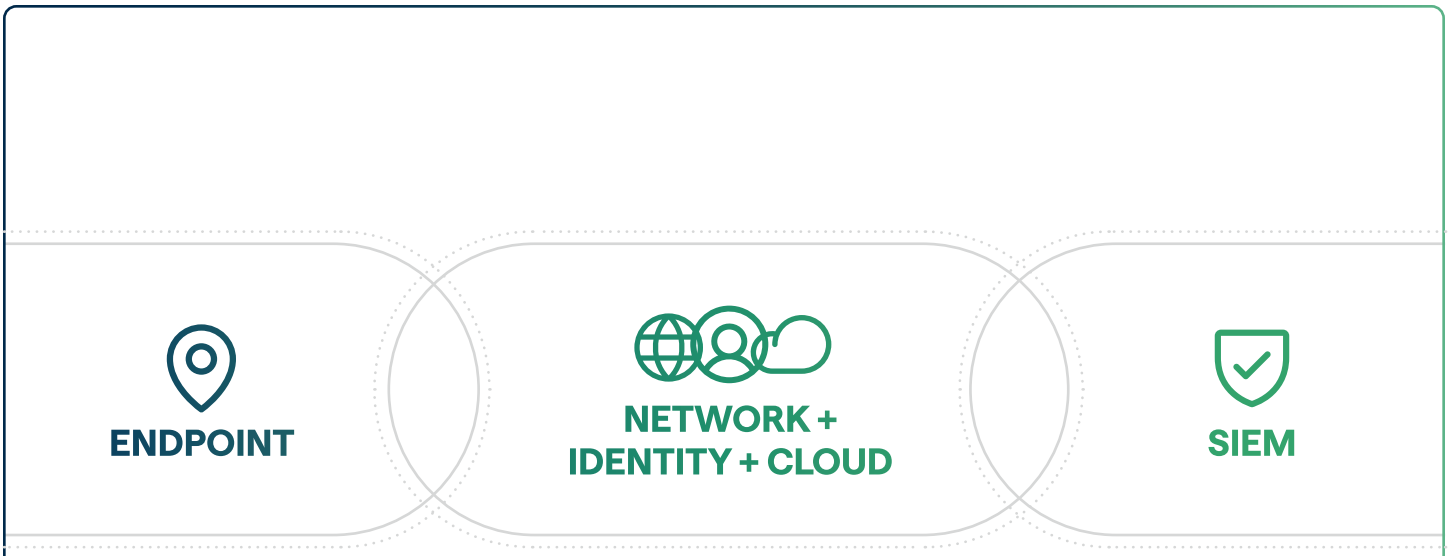
Vectra AI reduces noise by prioritizing real attacker behaviors using AI-driven signal.

CROWDSTRIKE FALCON NEXT-GEN SIEM:

- Correlates petabytes of data
- Enables lightning-fast queries
- Provides unified investigation workflows

RESULT:

> Fewer alerts
> Higher fidelity detections
> Faster MTTR



5 SOC Visibility Triad Requirements

Effective SOC visibility depends on logs (SIEM), endpoints (EDR), and network (NDR). If one is removed, attackers will exploit the resulting gap.

VECTRA + CROWDSTRIKE POSITIONING

PILLAR	SOLUTION
Endpoint	CrowdStrike Falcon Insight XDR
SIEM	CrowdStrike Falcon Next-Gen SIEM
Network + Identity + Cloud	Vectra AI Platform

Together, they form a complete, AI-powered XDR architecture.

SECTION 3

How the Partnership Works

Better Together: Unified Detection and Response

1. CrowdStrike detects suspicious endpoint behavior
2. Vectra correlates with network, identity, cloud signal
3. Falcon Next-Gen SIEM unifies investigation
4. Automated host isolation via CrowdStrike
5. SOC sees one prioritized entity view

SUPPORTED BY:

Bi-directional integration

Single pivot between platforms

Integrated Next-Gen SIEM ingestion of Vectra signal

SECTION 4

What This Means for Security Leaders

Coverage

Hybrid visibility across:

Endpoint | Network | Identity | Cloud | SaaS

Clarity

AI-driven threat correlation across attack vectors

Up to 80–99% alert noise reduction

Control

Automated identity, device, and traffic isolation

Unified investigation backed with AI-enhanced metadata

Seamless SIEM integration

SUMMARY

Modern Attack Resilience Requires More Than EDR

EDR is foundational.

But modern cyber resilience requires:

- NETWORK GROUND TRUTH
- IDENTITY VISIBILITY
- CLOUD TELEMETRY
- AI-DRIVEN CORRELATION
- AUTOMATED RESPONSE

The Combined Power of CrowdStrike Falcon Platform + Vectra AI.

One unified detection and response layer —

Seeing what happens on the endpoint and across everything connected to it.

About Vectra AI

Vectra AI is the cybersecurity AI leader in protecting modern networks from modern attacks. From on-premises data centers to multi-cloud, identity, SaaS, IoT/OT, edge, and AI infrastructure, the Vectra AI Platform empowers security teams with the modern network observability, signal, and actions needed to preemptively reduce attack exposure, proactively contain active attacks in progress, and automate security operations to prove resilience in an always-on, AI-powered world. As the leader in Network Detection and Response and with 35 patents in cybersecurity AI, modern enterprises across the world trust Vectra AI to protect their modern network from modern attacks.

For more information please contact us:
Email: info@vectra.ai | vectra.ai