VECTRA

SOLUTION BRIEF

# Protect Your OT with the Vectra Platform

**Digital transformation in business operations is driven by numerous technological initiatives including in OT (operational technology) environments. These innovations bring many changes that present new challenges.**

In an IT and OT world, attackers are bypassing prevention controls, infiltrating, compromising credentials, gaining privileged access, moving laterally and exfiltrating sensitive corporate data through means of credential phishing, breaching existing IT applications, committing supply chain attacks, amongst others — all undetected. Organizations don't know what they don't know.

**We call this the unknown.**

When it comes to OT attacks, infiltrating your OT environment is the first step. The unknown attack is the biggest risk to an organization's business critical data. The challenge for security teams boils down to how rapidly an attack is detected and prioritized, so it can be stopped before the attack can reach its final target and execute.

### Key challenges addressed:

- Always keeping your business operations intact
- Accurately identifying and prioritizing real attacks
- Single, unified view of both IT and OT environments
- Increasing SOC analyst workflow efficiency
- Growing IT & OT, cloud complexity, vulnerabilities and exploits

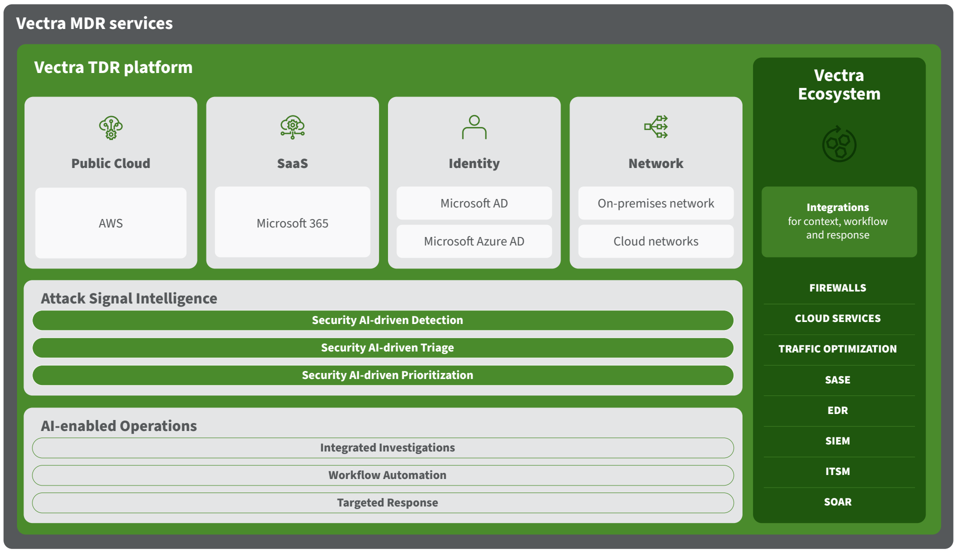
## Turn the tables on OT attackers

Our approach is simple. Defending against modern cyber attackers comes down to arming defenders with the right **coverage, clarity,** and **control**.

OT Attack Coverage for 2 and 3 layers of Purdue Model: Network (both on-premises and cloud-based), public cloud, SaaS and identity with integrations for endpoint detection and response (EDR) for context, workflow and response.

Vectra provides the building blocks to see and stop OT attacks no matter where adversaries choose to carry out their attack:

- Vectra Network Detection and Response (NDR)
- Vectra Recall to query, investigate and hunt for threats
- Vectra Stream for security-enriched metadata lake
- Vectra Managed Detection and Response (MDR)



**OT Signal Clarity with Security AI-driven Attack Signal Intelligence™:** automate threat detection, triage and prioritization across the cyber kill chain post compromise from execution, persistence and reconnaissance to command and control, evasion, access, escalation, lateral movement and exfiltration. Attack Signal Intelligence is your early warning system for OT attacks in progress.

**OT Control with AI-enabled operations:** an intuitive user interface that puts answers at analysts' fingertips. Automated workflows that reduce complexity and cost by automating manual tasks. And Targeted Response puts analysts in control with flexible response actions from locking down an account to isolating an endpoint to triggering SOAR playbooks.

## Key capabilities

### AI-driven Detection

Stop threats from becoming data breaches by harnessing Security AI to expose the complete narrative of an attack and cover over 90% MITRE ATT&CK.

### AI-driven Triage

Use ML to machine security analysts' intuition and automate alert triage, reducing alert noise by over 80%.

### AI-driven Prioritization

Harness Security AI to automate prioritization and escalate the data threats that matter most to the business.

### Integrated Investigations

Intuitive user interface puts answers at analysts' fingertips attributing threats to compromised accounts and users.

## What it means for your OT environment

With the Vectra Threat Detection and Response platform and services, your organization is more resilient to OT attacks:

- Up and running with actionable detections in days if not hours.
- Future-proof your defense as your IT and OT attack surface expands.
- Erase the fear from IT and OT high-risk threats going undetected and executing.

Your processes and workflows are more efficient:

- Complete visibility across your IT and OT in one single unified view.
- Automate analysts' manual tasks and time to investigate and respond.
- Optimize existing investments in your IT and OT.

Your security analysts are more effective:

- Reduce analyst burnout with accurate detection of malicious true positives.
- Increase analyst throughput by accelerating investigation and response.
- Build analyst expertise and skills hunting and defending against advanced attacks.

Vectra platform and services provide the intelligent signal that empowers security analysts to take intelligent action. The goal: empower SOC teams with the speed and scale to see and stop OT attacks from impacting your business.

Resources to Learn More

## About Vectra

Vectra® is the leader in Security AI-driven cyber threat detection and response for hybrid cloud. Vectra's patented Attack Signal Intelligence™ detects and prioritizes threats across public cloud, SaaS, identity, and networks in a single platform. Vectra's Attack Signal Intelligence goes beyond simple anomaly detection to analyze and understand attacker behavior. The resulting high-fidelity signal and deep context enables security operations teams to prioritize, investigate and respond to cyber-attacks in progress sooner and faster. Organizations worldwide rely on the Vectra platform and MDR services to stay ahead of modern cyber-attacks. Visit www.vectra.ai.

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