

Stop the Next Supply Chain Attack

Digital supply chains offer skilled attackers a means to unknown access to your enterprise through vulnerabilities and malicious code embedded deep in third-party software. Meanwhile, cybersecurity has relied on what is known for decades where threat detection and response methodologies have relied heavily on signatures, anomalies and rules to see and stop cyber attackers from infiltrating organizations and stealing data. This approach is broken.

As enterprises shift to hybrid and multi-cloud environments, embracing digital identities, digital supply chains, and ecosystems — security, risk and compliance leaders are faced with more.

- More attack surface to cover.
- More evasive and sophisticated attackers.
- More tools and more data sets to analyze.
- More signatures, anomalies, rules to maintain.
- More alert noise, triage, false positives.
- More analyst fatigue, burnout, turnover.

Despite more tools, data, signatures, policies, rules, alerts and people — the core problem remains the same:

“We don’t know where we are compromised – *right now.*”

Why attackers target your supply chain:

- Locate and exploit vulnerabilities
- Gain unguarded access to your business
- Infiltrate and progress laterally inside your systems
- Get unknown access and control of your data
- Steal valuable and critical data

Vectra erases unknown threats across your supply chain

Vectra Threat Detection and Response platform provides complete threat coverage and signal clarity that puts your defenders in control against emerging, evasive and sophisticated cyber attackers. The Vectra TDR platform empowers analysts with:

Attack Coverage

Erase unknown threats across 4 of 5 attack surfaces — public cloud, SaaS, identity and networks.

Signal Clarity

Harnesses Security AI-driven Attack Signal Intelligence™ to automatically detect, triage and prioritize unknown threats.

Intelligent Control

Arm human intelligence to hunt, investigate and respond to unknown threats.

Get ahead and stay ahead of modern attacks

The Vectra TDR platform harnesses Vectra’s Security AI-driven Attack Signal Intelligence™ — a risk-based approach to cyberattacks reducing manual tasks, alert noise and analyst burnout. Attack Signal Intelligence empowers security analysts with AI-driven detection, triage and prioritization to find and stop attackers actively exploiting supply chains way before patching is available, so your team can investigate and respond to public cloud, SaaS, identity and network attacks before they become breaches.

AI-Driven Detection

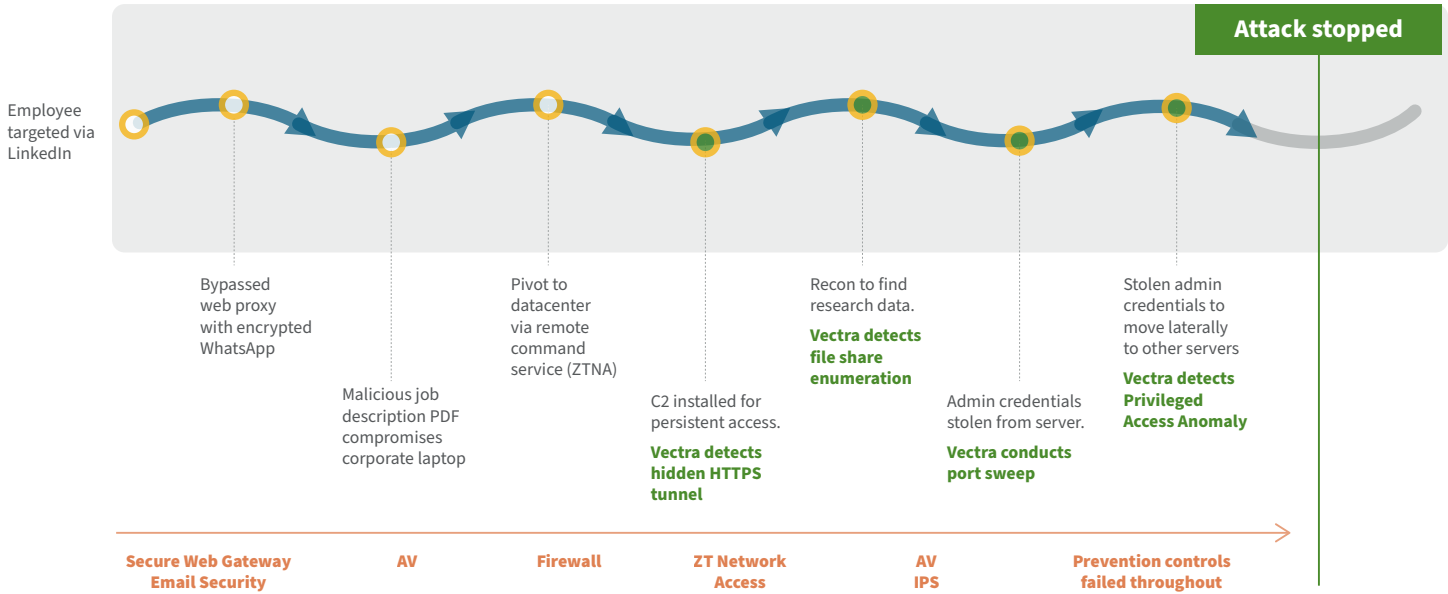
- Behavior-based models accurately detect attacker TTPs.
- Correlated detections of attacker TTPs across domains.
- Comprehensive visibility of the complete attack narrative.

AI-Driven Triage

- Continuous analysis of all active detections for commonalities.
- Intuitive by design to distinguish malicious vs. benign activity.
- Automated to expose the malicious and log the benign.

AI-Driven Prioritization

- Real-time threat analysis for severity and impact.
- Unified view of prioritized threats by severity and impact.
- Contextual alerting accelerates investigation and response.



Turn the tables on attackers targeting your supply chain with the Vectra platform

Your organization is more resilient to attacks

- Up and running with actionable detections in days if not hours.
- Future-proof your cyber defense as your attack surface expands.
- Reinforcements at the ready with Vectra MDR services (24x7x365 eyes-on-glass service to help you proactively detect, prioritize, investigate and stop attacks).

Your processes and workflows are more efficient

- Reduce SIEM costs and detection rule creation and maintenance.
- Automate analysts' manual tasks and time to investigate and respond.
- Optimize existing investments in EDR, SOAR and ITSM.

Your security analysts are more effective

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

Unlike other approaches that center on simple anomaly detection and require human tuning and maintenance, the Vectra platform exposes the complete narrative of an attack without human intervention, including those that target your supply chain. By harnessing Attack Signal Intelligence, security teams are empowered to erase the unknown, turn the tables on attackers and make the world a safer and fairer place.

[Learn more about the Vectra platform](#)

About Vectra

Vectra® is the leader in 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 enable 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 cyberattacks.