Reduce Critical Infrastructure Risk with Integrated Signal for Your Hybrid Cloud

Reduce your exposure to critical infrastructure risk with integrated signal for your entire hybrid cloud infrastructure.

Critical infrastructure used to just be considered power plants, water supply and federal banking — Colonial Pipeline and JBS hacks changed that. These days, critical infrastructure encompasses virtually any industry or sector where disruption can create not only a temporary operation disruption, but a disruption that can directly impact our way of life. As the scale of critical infrastructure has expanded, and traditionally analog devices have become fully hybrid cloud capable, the attack surface against critical infrastructure has expanded dramatically. With more on the line, you need to be able to detect attacks against critical infrastructure early and reliably.

Key challenges to consider

- **Lack of attack coverage:** A critical infrastructure attack surface can be very large with attackers highly motivated for success. They may be financially incentivized ransomware operators or state sponsored actors motivated to wreak havoc on your critical infrastructure.
- **Multiple entry points:** Attackers can get in through traditional IT infrastructure, via supply chain compromise and through compromising third-party service technicians who are required to service equipment. These multiple angles significantly increase the chances of an attacker penetrating your organization.
- **Hybrid cloud operational complexity:** Most critical infrastructure relies on specialized hardware that does not run Endpoint Detection & Response (EDR), while leveraging protocols that may leave traditional solutions blind, and are harder to forensically analyze in comparison to traditional enterprise endpoints.
- **Tool sprawl:** Critical infrastructure can span many different cybersecurity solutions and implementations, making it hard to standardize on uniform endpoints — further diluting the possible attack signal from traditional detection technologies.

Key benefits of integrated hybrid attack signal:

- Zeros in on attacker behavior, analyzing in many dimensions to see real attacks in a sea of different.
- Maps attack progression by knowing what tactics and techniques attackers use to blend in and move laterally.
- Eliminate 90% of your attack surface blind spots, proactively identify 3x more threats.
- Cover >90% of hybrid cloud MITRE ATT&CK techniques.
- Reduce detection, investigation and response latency time from months to days.
- Provide a holistic view of attacks across all domains.

Key criteria to consider

Leverage technology that identifies attacker behaviors rather than specific patterns.

- Specific attacks may vary amongst critical infrastructure components. An integrated attack signal can identify the specific behaviors attackers use that appear as normal user activity.

Collect network metadata to identify transactions on the network that can be useful when powering investigations.

- Flow logs, HTTP, HTTPS, DNS and other protocol-specific logs can be helpful to understand exactly what operations a system performed to increase the speed of resolution.

Many critical infrastructure attacks start in the IT side of the house.

- Integrated attack coverage across the entire hybrid surface is critical for end-to-end protection to ensure that attacks cannot jump between different segments or surfaces.

Keys to success:

Coverage: Utilize a TDIR solution (such as the Vectra AI Platform), that unifies and consolidates attack telemetry across the entire hybrid cloud attack surface including identity, public cloud, SaaS and data center networks. In simplest terms, you can't reduce your risk, if you can't see what is happening across your entire hybrid cloud environment.

Clarity: Integrated, real-time AI-driven attack signal to automate threat detection, triage and prioritization across your hybrid cloud domains. Shift from event-centric threat detection to entity-centric attack signal. Entity-centric attack signal provides higher-fidelity alerts on hosts and accounts under attack, removing the need to triage hundreds if not thousands of threat events per day. By leveraging a TDIR solution such as the Vectra AI Platform, your SOC team can truly differentiate between benign and malicious true positives, saving countless resources and time while also reducing analyst burnout.

Control: Arm your SOC analysts by removing as much deployment complexity upfront to prevent further investigation and response latency in analyst workflows and put all of the context and controls they need at their fingertips. In addition, leverage co-managed services to add more reinforcements to your SOC team when talent resources are scarce or have limited access to the expertise needed for threat hunting.

Critical infrastructure is an attractive attacker target that needs to be protected by technology that can reliably detect attackers regardless of the techniques they employ — providing the clearest signal possible so SOC teams can quickly take action.

The Vectra AI platform delivers the most trusted integrated signal powering Open Extended Detection and Response (XDR) by providing hybrid attack surface coverage across public cloud, identity, SaaS, and data center networks through real-time Attack Signal Intelligence. The Vectra AI Platform prioritizes entities under attack with integrated, automated, and co-managed response that stops attacks executing and ultimately reduces the overall risk to your critical infrastructure.

Learn more about the Vectra AI Platform

See the Vectra AI Platform in action

Explore the Vectra AI Platform

Schedule a personal demo of the Vectra AI Platform

About Vectra AI

Vectra AI is the pioneer of AI-driven threat detection and response for hybrid and multi-cloud enterprises. The Vectra AI Platform delivers integrated signal across public cloud, SaaS, identity, and data center networks in a single Open XDR platform. The Vectra AI Platform with patented Attack Signal Intelligence empowers security teams to rapidly prioritize, investigate and respond to the most advanced and urgent cyber-attacks in their hybrid environment. Vectra AI has 35 patents in AI-driven threat detection and is the most referenced vendor by MITRE D3FEND. Organizations worldwide rely on the Vectra AI Platform and MDR services to move at the speed and scale of hybrid attackers. For more information, visit www.vectra.ai.

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