VECTRA | vmware Carbon Black

Vectra AI and VMware Carbon Black: Enhancing endpoint and network defense

Key Challenges

While endpoint protection is a critical first line of defense, advanced attackers are increasingly using tactics that allow them to move quietly between endpoints or exploit devices where endpoint agents may not be deployed. In parallel, network-only monitoring may not provide the full host-level context needed for decisive action. This is why modern cybersecurity requires both endpoint and network visibility working together. The combination of endpoint insight from VMware Carbon Black Cloud and network-based behavioral analytics from Vectra AI ensures security teams can detect, investigate, and stop threats faster and more effectively.

Solution Overview

The Vectra AI and VMware Carbon Black Cloud integration empowers security teams by combining behavioral threat detection with endpoint context and enforcement.

1. Automated Detection: Vectra AI continuously monitors network traffic to reveal attacker behaviors that other tools miss.

2. Contextual Enrichment: Once a host session is flagged, Vectra polls Carbon Black Cloud EDR for host details such as machine ID, operating system, and isolation status.

3. Informed Response: Analysts can isolate suspicious endpoints using Carbon Black Cloud directly from the Vectra AI Platform UI.

4. Operational Efficiency: The integration minimizes manual investigation steps, streamlines workflows, and empowers faster, data-driven responses.

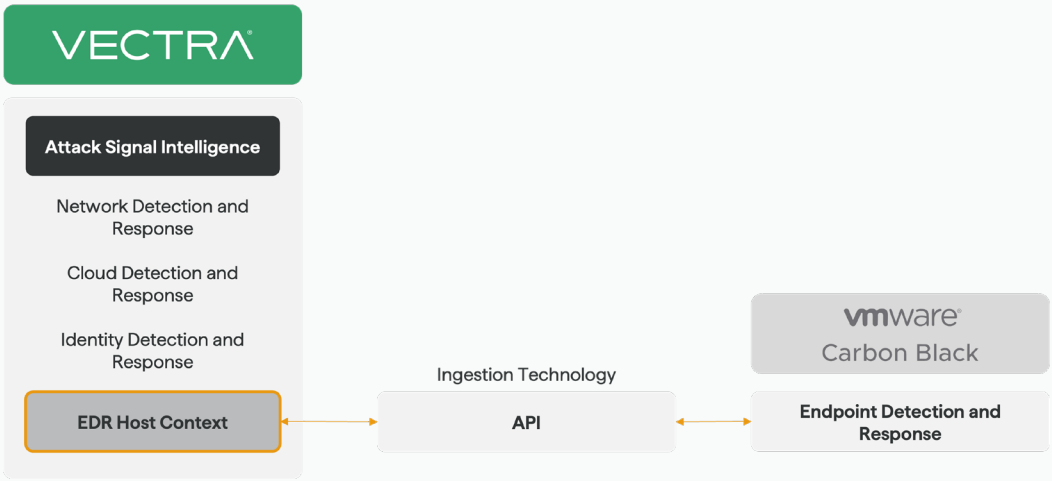
Solution Components:

- VMware Carbon Black Cloud EDR
- Vectra AI Platform

Key Benefits:

- **Faster Incident Response:** Vectra AI automatically detects attacker behaviors, while Carbon Black provides rich host context (machine ID, OS, isolation status) for deeper investigations.
- **Stronger Security Outcomes:** Security teams can quarantine compromised hosts directly through Carbon Black Cloud EDR, informed by Vectra's urgency and threat scoring.
- **Seamless Integration:** The integration enables efficient workflows within the Vectra AI Platform, reducing investigation time from hours to minutes.
- **Future-Ready Security:** Ongoing enhancements (such as support for advanced host search) ensure evolving coverage against modern threats.

How it Works



1. Detection: Vectra AI identifies suspicious activity in real time.
2. Enrichment: Host information is automatically pulled from Carbon Black Cloud EDR and enriches the Vectra detection(s).
3. Response: Security teams isolate compromised hosts, leveraging both behavioral analytics and endpoint lockdown capabilities.
4. Validation: Analysts confirm response actions within the Vectra AI Platform, with logs available for audit and compliance.

About Vectra AI

Vectra AI, Inc. is the cybersecurity AI company that protects modern networks from modern attacks. When modern cyber attackers bypass existing controls, evade detection and gain access to customers' data center, campus, remote work, identity, cloud, and IoT/OT environments, the Vectra AI Platform sees their every move, connects the dots in real-time, and stops them from becoming breaches. With 35 patents in AI security and the most vendor references in MITRE D3FEND, organizations worldwide rely on Vectra AI to see and stop attacks their other tools can't. For more information, visit www.vectra.ai.

About VMWare Carbon Black Cloud

VMware Carbon Black Cloud is a cloud-native endpoint and workload protection platform (EPP) that consolidates prevention, detection, and response into a single solution. With continuous monitoring, behavioral EDR, and simplified workflows, it helps organizations defend against advanced cyber threats while reducing the complexity of endpoint security.

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