Microsoft and Vectra — A Powerful Combination for Integrated Cybersecurity

Delivering integrated, best-of-breed cyber defense solutions powered by AI

In today's rapidly evolving digital landscape, organizations are facing an increasing number of sophisticated cyberthreats. To protect assets and data, organizations need a comprehensive and robust cybersecurity solution that can detect and respond to threats in real-time. However, right now, security teams struggle with the spiral of more — more attack surface, more sophisticated threats, more tools and more rules when the only "more" they really need is more threat signal efficacy and clarity. An integrated approach to simplify your cyber defense strategy that enables security teams to know what threats pose the most risk is critical to success.

The integration of Microsoft Defender, Defender for Cloud, Microsoft Sentinel and the Vectra platform harnessing Security AI-driven Attack Signal Intelligence™ delivers a comprehensive and robust cybersecurity solution that helps organizations protect their assets and data from today's advanced threats. By integrating these solutions, organizations can leverage the strengths of each, resulting in a more effective and efficient cybersecurity posture.

Key Security Challenges

- Increasing analyst workloads
- Growing cloud complexity, vulnerabilities and exploits
- Identifying and prioritizing real attacks
- More devices accessing cloud and on-premises networks
- Keeping pace with cloud-based attacks

Integrated security coverage where you need it most

Defending against modern cyber attackers comes down to arming defenders with the right attack surface **coverage**, signal **clarity** and intelligent **control**. Vectra and Microsoft accomplish this by integrating the following solutions:

Vectra Threat Detection and Response platform harnessing Security AI-driven Attack Signal Intelligence™ provides the hybrid cloud building blocks to future proof your cyber defense as your attack surface expands.

Attack surface coverage across 4 of the 5 attack surfaces: network (both on-premises and cloud-based), public cloud, SaaS, identity and endpoint detection and response (EDR) integrations for context, workflow and response.

- Vectra Network Detection and Response (NDR)
- Vectra Cloud Detection and Response (CDR) for AWS
- Vectra Cloud Detection and Response (CDR) for M365
- Vectra Identity Detection and Response (IDR) for Azure AD
- Vectra Recall to query, investigate, hunt for threats.
- Vectra Stream for security-enriched metadata lake
- Vectra Managed Detection and Response (MDR)

Signal Clarity with Vectra's Security AI-driven Attack Signal Intelligence™

Automate threat detection, triage and prioritization across the cyber kill chain from execution, persistence and reconnaissance to command and control, evasion, access, escalation, lateral movement and exfiltration.

Intelligent Control with AI-enabled operations

An intuitive user interface that puts answers at analysts' fingertips. Including automated workflows that reduce complexity and cost by automating manual tasks, while targeted response puts analysts in control with flexible response actions triggered automatically or manually.

Microsoft Defender and Defender for Cloud

Microsoft Defender and Defender for Cloud are two complementary cybersecurity solutions that provide organizations with comprehensive protection against cyberthreats. Microsoft Defender provides protection for devices and data, while Defender for Cloud provides protection for cloud-based workloads. By leveraging the strengths of both solutions, organizations can build a stronger and more secure digital landscape.

Microsoft Sentinel

Microsoft Sentinel is a cloud-native security information and event management (SIEM) solution provided by Microsoft. It provides organizations with real-time security insights and threat detection capabilities. With Microsoft Sentinel, organizations can monitor their security posture and respond to threats in real-time.

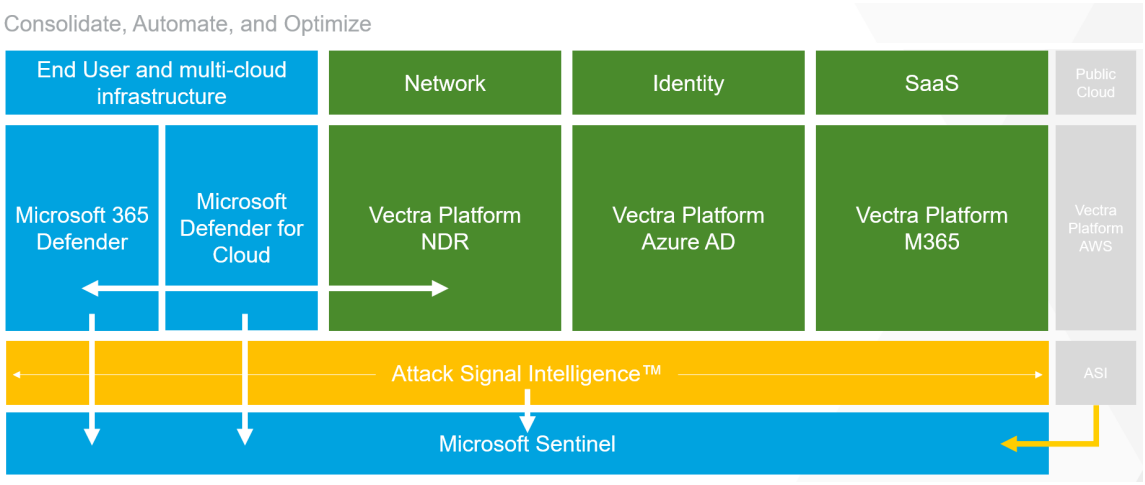
The solution integrates with various Microsoft security solutions, such as Microsoft Defender and Microsoft Azure, to provide

a comprehensive view of an organization's security posture. Microsoft Sentinel leverages the power of AI with Vectra's Attack Signal Intelligence to detect and respond to threats that evade traditional security solutions.

Microsoft Sentinel enables organizations to create custom security rules and alerts to help detect and respond to specific security incidents. The solution also provides organizations with detailed reports and dashboards that provide insights into their security posture, making it easier to identify areas for improvement.

An integration to extend coverage across your expanding attack surface

The Vectra platform integrates with Microsoft Defender and Microsoft Sentinel, empowering security teams to streamline cybersecurity detection, investigation, prioritization and response. Organizations that utilize these integrations deliver more effective, and efficient security operations and reduce the time to respond and resolve cybersecurity incidents.



What it means for your SOC

Vectra and Microsoft provide powerful, simple and integrated cybersecurity solutions to meet the needs of the modern SOC. Organizations are able to rapidly detect and respond to known and unknown threats with coverage across all attack surfaces, gaining unmatched threat signal clarity with control that enables human intelligence to take intelligent action — optimizing security investments and boosting SOC efficiency and effectiveness. Your security operations will be more resilient to attacks, experience more efficient processes and workflows while your analysts are able to turn the tables on attackers.

For more information...

- Visit our Partner Page
- Learn more about Microsoft Business Threat Protection
- Watch an overview video on Vectra and Microsoft Sentinel
- See an overview video on Vectra NDR and Microsoft Defender

About Vectra

Vectra® is the leader in hybrid cloud threat detection and response. 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