VECTRA AI

Customer Story | Financial Services

Fortune 500 Financial Services Company Goes Beyond the Basics to Secure Microsoft Environment with Vectra AI

This leading global investment organization focuses on long-term value creation across diverse industries. Operating within hybrid environments, including on-premises (data centers) and cloud, the company manages a complex digital footprint. With billions of assets under management, they face the mounting challenge of maintaining comprehensive visibility across their expanding attack surface.

Organization
Fortune 500 Global Investment Organization

Industry
Financial Services

The Challenge
Expanding infrastructure in Azure and adopting Copilot for M365 introduced new security challenges for this Fortune 500 company, making it harder to track and contain identity-based threats across a highly interconnected environment.

The Solution
By adopting Vectra AI, the company gained the visibility and detection capabilities needed to stop attacks that native tools missed, strengthening its security posture.

Security Transformation

Platform value at a glance: stopping two identity-based attacks within six months

As an early adopter of Vectra AI's sensors and detections for Microsoft 365 — paired with 24/7 monitoring through Vectra MDR — the investment organization has built a strong track record, stopping two identity-based attacks within just six months. In both cases, Vectra AI identified the threats early and prevented data breaches and operational disruptions.

	Attacker Behavior	Attack Attempt	Vectra AI's Defense
Incident 1	Deployed novel AiTM attack technique to target and compromise high-stake credentials and gain initial foothold.	Attempted access to confidential information. Valid credentials also neutralized information protection (AIP). Deployed persistence mechanisms.	Detections and early containment successfully kept data secure, ultimately evicting the attacker from the environment.
Incident 2	Compromised credentials were used in attempt to initiate BEC scheme against business partner.	Attacker leveraged access to initiate email thread to lure external business through a seemingly legitimate email.	Detections across multiple components in attack chain identified objective and enabled containment.

The Challenge

Addressing security gaps in a Microsoft-centric environment

When you're responsible for securing a Fortune 500 financial services company, having visibility across your Microsoft ecosystem isn't just a nice to have — it's essential.

For this company, building out its infrastructure in Azure added new security challenges to an already distributed environment spanning both on-premises and the cloud.

Each environment and component has its own intricacies, yet they are highly interconnected, making it essential to track threats across the entire ecosystem. Delivering on this need in a cost-efficient way would be impossible without a centralized, low-noise detection platform tuned for relevant attack paths.

"With cloud, one could argue that you know less about what to monitor for and defend against; it's a new paradigm," the CISO explained.

Attackers move fluidly across domains, making it difficult to connect behaviors and generate actionable alerts in real-time. With signals scattered across systems, defenders face fragmented data and increasingly sophisticated attack techniques, such as social engineering.

The adoption of Copilot for M365 raised particular concerns. If an attacker is able to assume the credentials of a user with Copilot provisioned, the functionality can accelerate their path to achieving their objective — both in lateral movement and in rounding up the crown jewels for exfiltration. To address this, the CISO advocated for an 'assume breach' approach to be applied to Copilot as well, ensuring such attacks could be detected and stopped.

"Microsoft is a critical piece of our IT ecosystem, but when it comes to security, we need to be better than basics. With Vectra AI, we get the integrated, aggregated threat signal we need to effectively defend our Microsoft environment, it also centralizes the analysis and correlation of those signals, saving us time and effort."

CISO
Fortune 500 Financial Services

The Solution

Beyond the basics: finding the attacks that Microsoft misses

The company needed advanced detection capabilities to identify threats that could bypass or evade Microsoft's native tools. Facing increasingly sophisticated attackers, the CISO leaned on their eight-year partnership with Vectra AI. By relying on the Vectra AI Platform, powered by Attack Signal Intelligence across their network, identity and cloud, it delivered the integrated visibility and protection their team was searching for.

"Microsoft is a critical piece of our IT ecosystem, but when it comes to security, we need to be better than basics," the CISO said. "With Vectra AI, we get the integrated, aggregated threat signal we need to effectively defend our Microsoft environment, it also centralizes the analysis and correlation of those signals, saving us time and effort."

With Vectra AI's unified approach, the company successfully stopped a phishing-as-a-service, Adversary-in-the-Middle (AiTM) attack targeting high-value assets that native tools missed. As AiTM attacks grow more common, slight shifts in attacker behavior often evade native tools. To counter this, the CISO tapped into Vectra's refined AI models to detect evolving tactics and automate the manual work of detection engineering.

The Vectra AI Platform also addresses key challenges in their Azure environment. "Vectra's coverage for Azure has been incredibly helpful. It allows me to track changes and additions made by the cloud team, ask about areas of concern like Key Vaults, and go beyond basic posture and add extended controls where it matters most," the CISO shared. "Vectra AI gives me easy access to logs in one centralized location, so I don't have to jump between interfaces to find the information I need. That saves a lot of time."

While native tools detect attacker behaviors in isolated surfaces, Vectra AI connects the dots across every stage of potential attacks and prioritizes urgent threats.

Putting detection to the test to stay ahead of attackers

To validate their detection capabilities, the company conducted security testing using the Microsoft 365 & Azure AD Attack Framework (MAAD-AF). This attack simulation emulated advanced attacker techniques, including living-off-the-land strategies commonly used by ransomware and APT groups. The results were striking: During the test, Vectra AI detected all nine simulated attacks, while Microsoft E5 did not identify any.

The security testing reinforced the need for an additional layer of defense beyond a Microsoft E5 license. With Vectra AI's ability to detect and correlate attacker behaviors across every stage of the kill chain, the team is now empowered to tackle threats that might otherwise slip through the cracks.

The Results

With Vectra AI in their toolkit, the financial services company saw notable results, including:

- **Reduced exposure** by identifying attacks that Microsoft missed, and gaining integrated visibility and a complete picture across networks, identities and clouds
- **Removed latency** by reducing manual detection engineering and tuning in Microsoft Sentinel
- **Maximized talent** through effective Managed Detection and Response (MDR)

"We can maintain good detection capability while, at the same time, not having to allocate a whole lot of resources," the CISO emphasized. "Vectra AI is a capable end-to-end detection and response platform and has been instrumental in how we build these capabilities as part of our security program. Vectra's success is my success."

"Vectra's coverage for Azure has been incredibly helpful. It allows me to track changes and additions made by the cloud team, ask about areas of concern like Key Vaults, go beyond basic posture, and add extended controls where it matters most."

CISO
Fortune 500 Financial Services

Read more customer stories

About Vectra AI

Vectra AI is the leader in AI-native security and observability. Vectra AI delivers organizations real-time visibility into their network, clear insight into which behaviors matter, and the ability to act before risk becomes impact. By connecting on-premises, multi-cloud, identity, SaaS, edge, and IoT/OT infrastructure, Vectra AI helps organizations reduce exposure, accelerate detection and response, and automate security operations with AI. With over a decade of AI and ML innovation, 39 patents and a Leader in the 2025 and 2026 Gartner Magic Quadrant for Network Detection and Response, Vectra AI empowers security teams to stay ahead of emerging AI powered attacks, increase operational efficiency, and prove resilient in an increasingly complex, AI-driven world. For more information, visit www.vectra.ai.

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