VECTRA

Vectra AI Cloud Threat Detection and Response for Azure

Challenge: Modern attackers compromise identities to infiltrate your Azure PaaS environment

3 challenges customers like you face in securing an Azure environment.

- Identity compromise is the number one initial attack vector, the most expensive, and takes the longest to detect in a cloud data breach.
- Siloed visibility: Connecting the dots as attacks move laterally across Active Directory, MSFT Entra ID, M365, Azure IaaS and Azure PaaS is even harder.
- Siloed threat detection creates unmanageable alert volume for defenders.

Our Approach: We arm defenders with Azure coverage, clarity and control to outpace hybrid attackers

- **Coverage –** real-time detection of attackers across Azure PaaS instances
- **Clarity –** quickly identifying real attacks by correlating attacker behaviors in real-time
- **Control –** accelerating investigation and providing comprehensive response capabilities to stop Azure compromise in minutes and early in the attack progression

Why Vectra AI Cloud Threat Detection and Response for Azure

- **High-fidelity signal:** AI-driven detections prioritize the most urgent threats, while cloud attribution technology associates attacks across multiple surfaces with specific identities to streamline investigation
- **No more silos:** We secure your hybrid environment (Active Directory, Microsoft Entra ID, M365, Copilot for M365, Azure IaaS, and Azure PaaS) through a single pane of glass, enabling you to connect the dots during an attack.
- **Stop hybrid Azure identity abuse in real time:** detect, investigate, and stop suspicious Azure identity and control plane compromises with enhanced context for accelerated investigation and swift account lockdown

What makes Vectra AI Cloud Threat Detection and Response for Azure unique and superior

We automatically collect the right data and normalize it for streamlined and efficient use

Our real-time data ingestion engine automatically processes, standardizes and enriches Azure activity and resource logs, ensuring comprehensive monitoring of data within a single pane of glass.

We detect advanced attacker behaviors

Our high-fidelity alerts uncover real threats against Azure identities and important services such as Azure policies, Azure App Service and Azure automation accounts.

We connect the dots

Our cloud attribution technology for Azure attributes attacks across Azure IaaS, Active Directory, Microsoft Entra ID and Microsoft 365 (SaaS) with specific identities, offering unified visibility into hybrid attack surfaces in a single pane of glass and streamline investigation.

We prioritize urgent real attacks

Our AI-driven prioritization alerts SOC teams based on combining entity importance and attack profile to create an attack urgency score.

We identify Azure security gaps that can be exploited by attackers

Our Active Posture Dashboard identifies exposure points in the Azure environment, such as overly permissive identity access controls and public storage accounts that should not be publicly accessible.

We accelerate investigation

Our zero-query investigation provides context to the SOC, accelerating investigations by integrating enhanced logs and metadata across network, identity, cloud, and GenAI attack surfaces. (time to detect cloud breach vs speed of attacks).

We equip analysts to respond fast

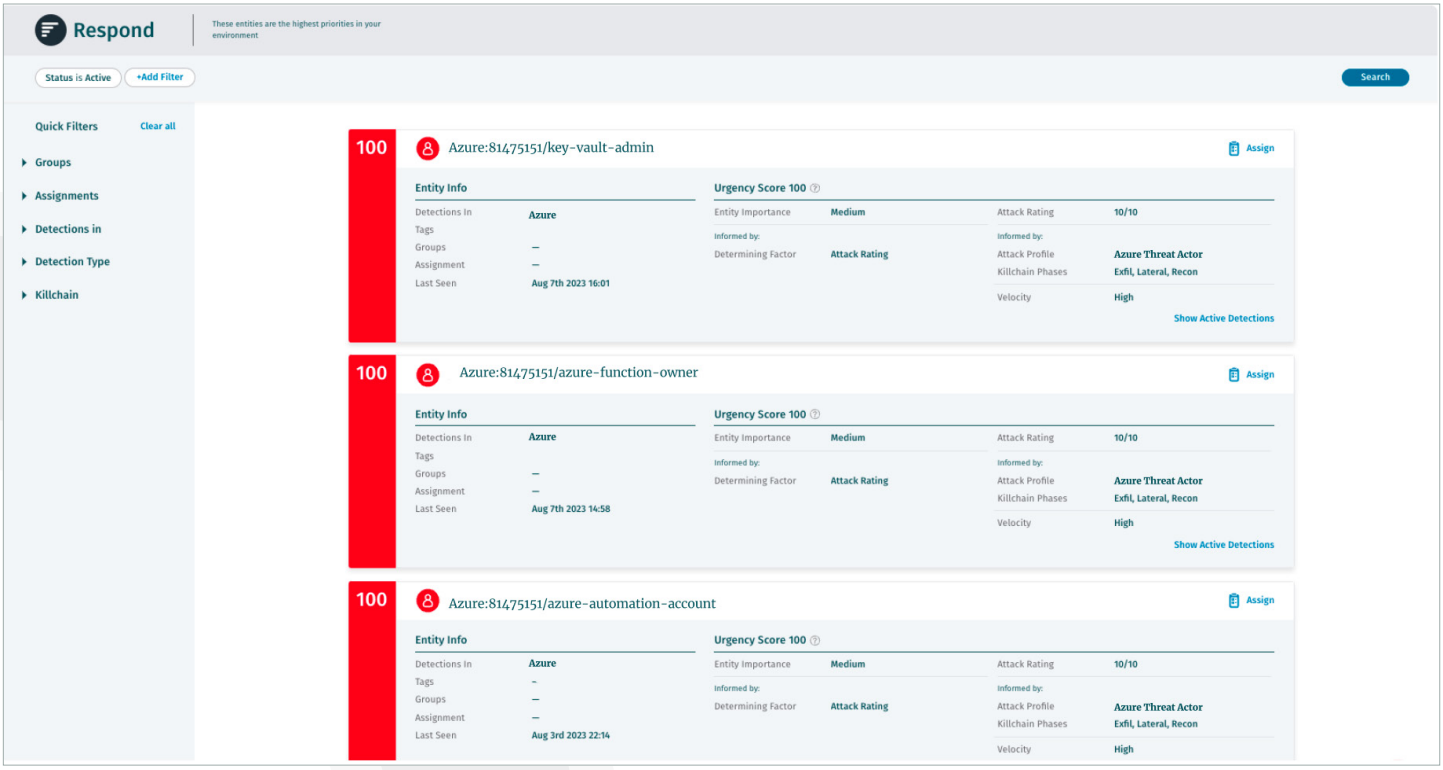
Our comprehensive response equips analysts with native, automated, and managed response actions to quickly stop Microsoft Entra ID accounts involved in an attack.

We can deploy in minutes

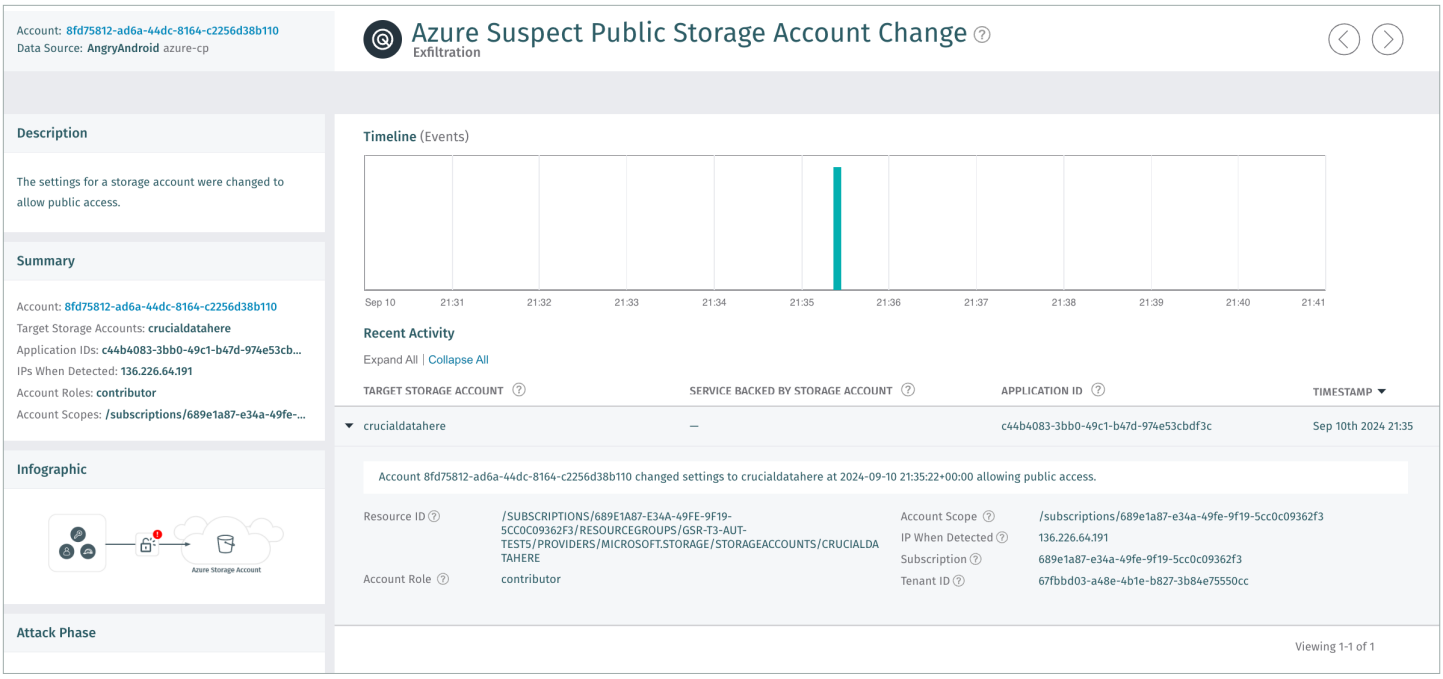
Our solution is agentless.

We are here to help

Our 24/7 MXDR hybrid attack experts augment your SOC by managing detection, investigation, and response for your hybrid and multi-cloud environments.



Entity based prioritization and attack scoring based on observed Azure events



Detection with high-fidelity alerts based on attacker tradecraft and attack tooling

Product Deployment/ Details

- Cloud Threat Detection and Response for Azure is delivered through Vectra AI Platform Respond UX
- Vectra ingests Azure activity logs and resource logs
- CDR for Azure Detections: https://support.vectra.ai/s/article/KB-VS-1822
- CDR for Azure Deployment Demo: https://vimeo.com/927271588/a8be207b73
- CDR for Azure Deployment Guide: https://support.vectra.ai/s/article/KB-VS-1715

Contact your Vectra AI account team to join the customer preview.

About Vectra AI

Vectra AI is the leader and pioneer in AI-driven Attack Signal Intelligence. Only Vectra AI natively delivers hybrid attack telemetry across public cloud, SaaS, identity, and networks in a single XDR platform. The Vectra AI Platform with Attack Signal Intelligence empowers security teams to rapidly prioritize, investigate and respond to the most advanced and urgent cyber-attacks to 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 MXDR services to move at the speed and scale of hybrid attackers. For more information, visit www.vectra.ai.

VECTRA

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