

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.

The screenshot shows the 'Respond' dashboard interface. At the top, it says 'These entities are the highest priorities in your environment'. Below this, there are filter buttons for 'Status is Active' and '+Add Filter', and a 'Search' button. On the left, there is a 'Quick Filters' sidebar with categories: Groups, Assignments, Detections in, Detection Type, and Killchain. The main content area displays three entity cards, each with a red '100' urgency score indicator. Each card represents an Azure entity with a score of 100. The entities are:

- Entity 1:** Azure:81475151/key-vault-admin. Entity Importance: Medium, Attack Rating: 10/10. Determining Factor: Attack Rating. Attack Profile: Azure Threat Actor (Exfil, Lateral, Recon). Velocity: High. Last Seen: Aug 7th 2023 16:01.
- Entity 2:** Azure:81475151/azure-function-owner. Entity Importance: Medium, Attack Rating: 10/10. Determining Factor: Attack Rating. Attack Profile: Azure Threat Actor (Exfil, Lateral, Recon). Velocity: High. Last Seen: Aug 7th 2023 14:58.
- Entity 3:** Azure:81475151/azure-automation-account. Entity Importance: Medium, Attack Rating: 10/10. Determining Factor: Attack Rating. Attack Profile: Azure Threat Actor (Exfil, Lateral, Recon). Velocity: High. Last Seen: Aug 3rd 2023 22:14.

Entity based prioritization and attack scoring based on observed Azure events

Account: 8fd75812-ad6a-44dc-8164-c2256d38b110
Data Source: AngryAndroid azure-cp

Azure Suspect Public Storage Account Change ?

Exfiltration

←
→

Description

The settings for a storage account were changed to allow public access.

Summary

Account: 8fd75812-ad6a-44dc-8164-c2256d38b110
Target Storage Accounts: crucialdatahere
Application IDs: c44b4083-3bb0-49c1-b47d-974e53cb...
IPs When Detected: 136.226.64.191
Account Roles: contributor
Account Scopes: /subscriptions/689e1a87-e34a-49fe-...

Infographic

Attack Phase

Timeline (Events)

Sep 10 21:31 21:32 21:33 21:34 21:35 21:36 21:37 21:38 21:39 21:40 21:41

Recent Activity

Expand All | Collapse All

TARGET STORAGE ACCOUNT ?	SERVICE BACKED BY STORAGE ACCOUNT ?	APPLICATION ID ?	TIMESTAMP ▼
crucialdatahere	—	c44b4083-3bb0-49c1-b47d-974e53cbdf3c	Sep 10th 2024 21:35

Account 8fd75812-ad6a-44dc-8164-c2256d38b110 changed settings to crucialdatahere at 2024-09-10 21:35:22+00:00 allowing public access.

Resource ID ?	/SUBSCRIPTIONS/689E1A87-E34A-49FE-9F19-5CC0C09362F3/RESOURCEGROUPS/GSR-T3-AUT-TESTS/PROVIDERS/MICROSOFT.STORAGE/STORAGEACCOUNTS/CRUCIALDATAHERE	Account Scope ?	/subscriptions/689e1a87-e34a-49fe-9f19-5cc0c09362f3
Account Role ?	contributor	IP When Detected ?	136.226.64.191
		Subscription ?	689e1a87-e34a-49fe-9f19-5cc0c09362f3
		Tenant ID ?	67fbbd03-a48e-4b1e-b827-3b84e75550cc

Viewing 1-1 of 1

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

© 2024 Vectra AI, Inc. All rights reserved. Vectra, the Vectra AI logo, and Security that thinks are registered trademarks and the Vectra Threat Labs, and Threat Certainty Index. Other brand, product and service names are trademarks, registered trademarks or service marks of their respective holders. Version: 101724