Signal clarity is everything...

VECTRA

Identity Is the New Perimeter for Both Defenders and Attackers

98% Saw an increase in identities

The number of identities to protect is huge and growing, making the identity attack surface a huge target for attackers*

*IDSA The State of Identity and Security in 2023

90% Experienced an Identity Attack

Attackers are targeting identities in the first and later stages of their attacks.

*IDSA The State of Identity and Security in 2023

62%

don't have visibility into human or machine identities accessing sensitive data and assets*

*CyberArk Report 2023

A multi-million dollar ransomware attack can start with just a single compromised identity

Successful attacks involving identity come at a huge cost

okta
$2B
lost in market capitalization

CAESARS PALACE
$15M
ransom paid

MGM GRAND
up to **$8.5M** lost per day
even with no ransomware payment made

Attackers can bypass prevention, such as MFA, and endpoint protection. Here are examples of different situations when this happens:

Identity Compromise

1

Voice Phishing

- Uses Vishing (Voice Phishing) technique to ask IT helpdesk to reset MFA
- Authenticates to Azure AD account

2

MFA Bombing

- Steals employees' credential
- Initiates multiple MFA requests in the morning during work hour
- Employee approve one of the MFA requests

3

Authenticated endpoints

- Attackers abusing authenticated identities bypasses MFA
- No sign-on required for attacker to access connected data

4

Modern Phishing Kits

- Bypasses MFA automatically via token theft
- Generates convincing emails and landing pages enhanced with AI

5

SIM Swap

- Calls telecom provider pretending to be an employee
- Gets a target identity's SIM card and receives 2FA codes
- Access credentials

6

EDR bypass

- Endpoints don't monitor identities
- Active network attackers can execute a full attack without any payloads or suspicious endpoint interaction

7

Network and Cloud Pivoting

- Identities are synced across the cloud and network
- A compromise in one causes a compromise in the other

8

Insider Threat

- Rogue employee is bribed by attackers with financial incentives
- Rogue employee harvests data from Microsoft 365 apps for attackers

And there are numerous scenarios just like this. Luckily, Vectra AI can detect attacker behaviors even when prevention fails.

Learn more about how adversaries slip past preventative controls

Download the eBook