

# Securing cloud IaaS, PaaS, and SaaS with Vectra AI

## Identity is the key to the cloud

Private and trusted networks are obsolete. Workloads have shifted from the data center to the public cloud. Network proliferation has created a new environment where identity is now the perimeter. This new perimeter cannot be protected by old network security focused on signatures and anomaly detection.

Vectra uniquely protects hybrid, on-premise, and cloud with learning behavioral models that understand hosts, services, applications, and identities – tracking and stopping attackers earlier in the kill chain.

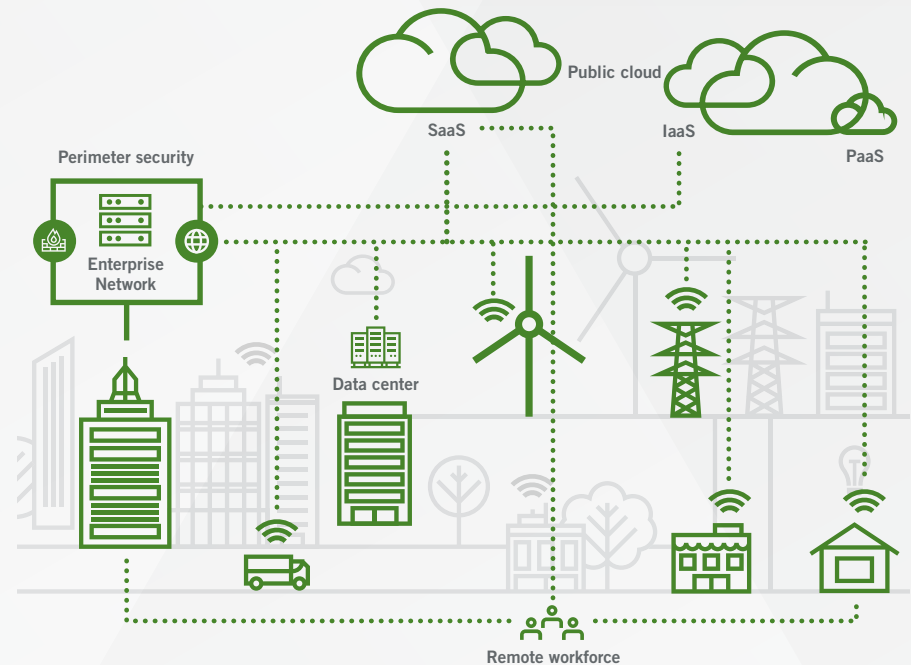
## Securing identity, users, and roles

Adversaries have switched from malware-based attacks that compromise endpoints to targeting user credentials in order to gain access to cloud applications and resources while avoiding detection.

Attacks using compromised user credentials are hard for security solutions like Cloud Access Security Brokers (CASB) and Web Application Firewalls (WAFs) to detect, as they look like legitimate user actions.

## KEY BENEFITS

1. Reduce the risk of a breach in cloud applications, infrastructure, and services
2. Track attacks as they pivot and progress between cloud, hybrid, and on-prem environments to identify apps, services, identities, and hosts involved
3. Monitor accounts, roles, and identities and how they are used in cloud environments



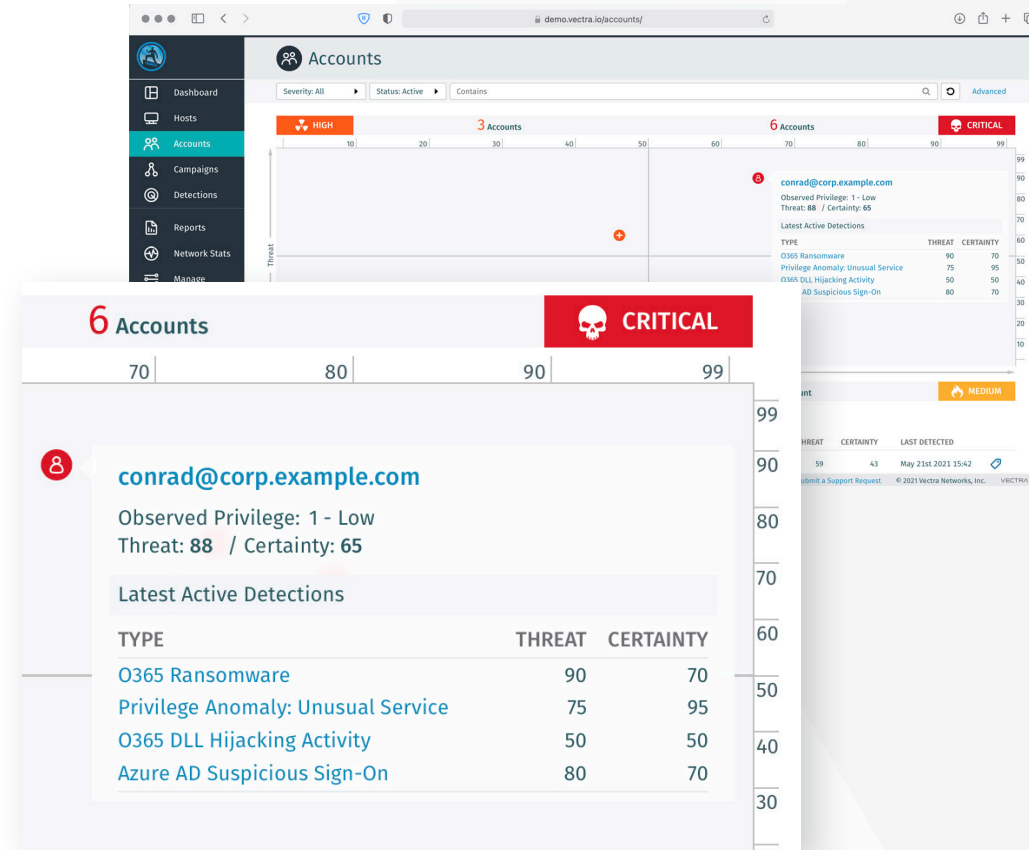
Attacks using compromised user credentials are hard for security solutions like Cloud Access Security Brokers (CASB) and Web Application Firewalls (WAFs) to detect, as they look like legitimate user actions. And if an external attacker is hard to detect, the threat posed by malicious insiders is even more challenging. Take for example an employee who has been granted access to a system and now wants to steal data or cause harm. How would you go about detecting and stopping this attack?

Vectra can detect this malicious intent by analyzing how hosts, accounts, roles, and workloads are being accessed and how they interact in your Microsoft 365 environment as well as any federated SaaS application using Azure AD. Analyzing data from both identity provider (IdP) services and cloud applications, custom ML models detect telltale attacker behaviors earlier in the kill chain than ever before. This gives security analysts a complete picture of their entire network and allows them to monitor accounts for compromise and insider threats.

## Securing cloud-native (SaaS) apps

As data shifts from internal systems to cloud-based applications, organizations lose control of the data storage and visibility into how it is accessed since they are no longer responsible for securing those components.

Trying to implement virtual firewalls or CASB solutions to filter access to SaaS and cloud-native applications is cumbersome to maintain, disruptive to your employees as it limits how and where they access the apps they need, and easily circumvented by attackers. Other cloud-native security solutions like cloud workload protection (CWPP) require agents to be deployed, and cloud security posture management (CSPM) requires constant tuning of the baseline, and both provide limited visibility into the expansive set of SaaS applications you use leaving you blind to attacks.



Analyzing data from both identity provider (IdP) services and cloud applications, custom ML models detect telltale attacker behaviors earlier in the kill chain than ever before.

Vectra seamlessly integrates with SaaS applications including Microsoft 365, SharePoint/OneDrive, Teams, and Exchange, as well as cloud Identity Providers, like Microsoft Azure AD, giving complete visibility into who is accessing them, regardless of how and from where. This unique vantage point allows Vectra to detect adversaries by the subtle yet distinct behaviors they manifest while attempting to steal or destroy your data, stopping them before they accomplish their goal.

## Threat Detection for IaaS & PaaS

Infrastructure as a service (IaaS) and platform as a service (PaaS) are ever changing, making them inherently impossible to secure. As a result, you cannot confidently deploy a cloud application in your IaaS or PaaS environment in a secure manner. In fact, through 2025, Gartner posits that 99% of cloud security failures will be the customers own fault (not the cloud provider).

By integrating with public cloud providers including Amazon Web Services (AWS), and private cloud virtualization platforms, and focusing on the control plane, Vectra detects attacks, regardless if they target the resources individually or the instance itself. By combining industry-best data science with security research to detect, prioritize, and stop attack campaigns, your security teams get only the critical security events that matter and detailed help with how to fix them, and DevOps can deploy applications with speed and confidence knowing their environment is protected.

## Full hybrid cloud visibility

Network security solutions are concerned with tracking assets using machine identities such as MAC or IP addresses. In the cloud, those descriptors are largely irrelevant or non-existent. IPs change frequently, workloads start and stop as demand changes, and MAC addresses aren't tied to hardware. The accounts, roles, and identities that access workloads become the unique identifier seen in logs.

The Vectra Threat Detection and Response Platform enriches both cloud logs and network metadata with usable information like hostnames, so you can keep track of hosts as their IPs change, in addition to users as they authenticate between cloud and on prem workloads. Patented machine learning (ML) models focusing on privileged access keep track of accounts, roles, and identities and how they normally behave, which translates to detection of account takeovers, privilege escalations, and credential abuse.

This allows Vectra to give security professionals a complete view of attackers, and how attacks progress, regardless of where it starts, moves, and stops. Vectra patented threat detection capabilities in conjunction with native integrations allows us to track all the roles and accounts used, lock down accounts, isolate endpoints and workloads, and stop attacks across the entire network before any damage can be done.






The screenshot displays the Vectra Threat Detection and Response Platform interface. The main view shows 'Account Information' for a 'Cloud Account' with the email '0365:conrad@corp.example.com'. The account was last detected on May 20th, 2021, at 20:24. Below this, a 'Network Account' section shows the email 'conrad@corp.example.com' with an observed privilege level of '1 - Low' and was last detected on May 20th, 2021, at 05:23. A 'Show Details' link is provided for the network account.

The background interface shows a 'Detections' table with the following data:


| Category | Type            | Account        | Threat | Certainty | First Seen          | Last Seen           |
|----------|-----------------|----------------|--------|-----------|---------------------|---------------------|
| Lateral  | 0365:Ranso...   | conrad@corp... | 90     | 70        | May 20th 2021 20:24 | May 20th 2021 20:24 |
| Lateral  | Privilege An... | conrad@corp... | 75     | 95        | May 20th 2021 05:23 | May 20th 2021 05:23 |
| Lateral  | 0365:DLI HL...  | conrad@corp... | 50     | 50        | May 19th 2021 21:37 | May 19th 2021 21:37 |
| C&C      | Azure AD Su...  | conrad@corp... | 80     | 70        | May 19th 2021 17:43 | May 19th 2021 17:43 |

## See for yourself

The Vectra Platform is a complete cloud-native security platform that tracks signs of attacker behavior across enterprise, hybrid, data center, IaaS, PaaS, and SaaS, all from a single point of control.

|                                                                                                                                                                                         |                                                                                                                                                                                                   |                                                                                                                                                                                       |                                                                                                                                                                           |                                                                                                                                                                                |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <br><b>Secure the Network</b><br>Network detection and response including data centers and IoT devices | <br><b>Secure SaaS Apps</b><br>Detect and prioritize hidden threats in Microsoft 365 and Azure AD federated apps | <br><b>Secure IaaS &amp; PaaS</b><br>Detect and investigate threats in AWS and apps running on AWS | <br><b>Hunt &amp; Investigate</b><br>Search for threats across your entire environment | <br><b>Enrich Data</b><br>Deliver security-enriched metadata to SIEMs for custom detections |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                         |          |                 |
|-------------------------|----------|-----------------|
| Implementation Services | Training | Managed Hunting |
|-------------------------|----------|-----------------|

 **Vectra Threat Detection and Response Platform** The only AI-driven threat detection and response platform that unifies Cloud, Data Centers, Enterprise Networks and IoT into a consolidated view

[Try Vectra free for 30 days](#)

[Test Drive Vectra Now](#)

For more information please contact us at [info@vectra.ai](mailto:info@vectra.ai).

Email [info@vectra.ai](mailto:info@vectra.ai) | [vectra.ai](https://www.vectra.ai)