VECTRA
SECURITY THAT THINKS®

SOLUTION BRIEF

How Vectra secures your entire network

Identity is the key to the cloud

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

Vectra uniquely protects the entire network of hybrid, on-premise, and cloud connectivity with our learning behavioral models that understand both hosts and identities – tracking and stopping attackers earlier in the kill chain.

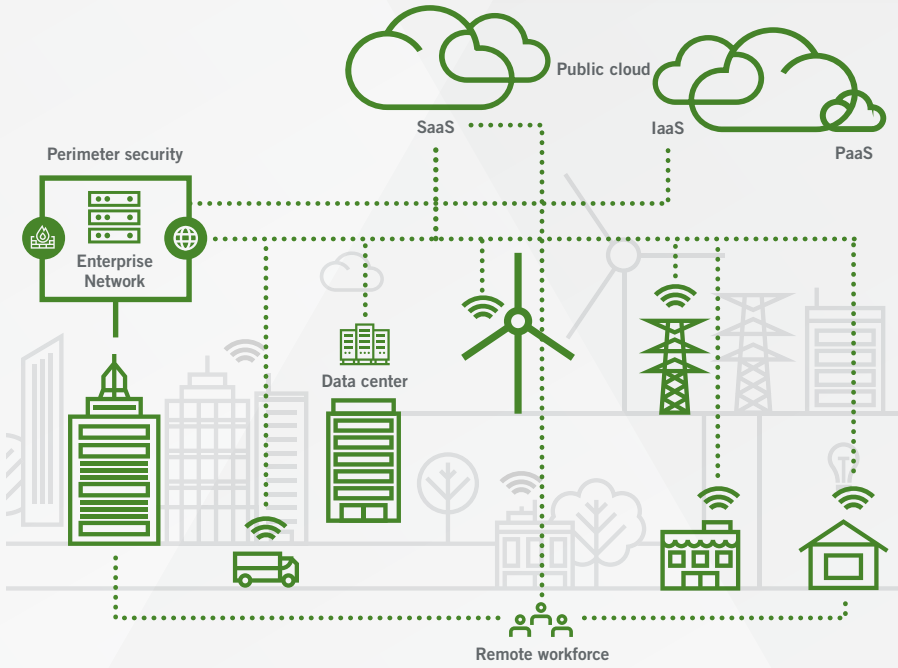
Securing data in cloud

As the location of data shifts from internal systems to cloud-based applications, organizations lose control of the data storage and visibility into how it is accessed.

The increasing number of remote workers combined with the number of IoT devices accessing corporate networks make both traditional network security solutions like IDPS, and endpoint solutions including EDR, blind to activity and data in the cloud.

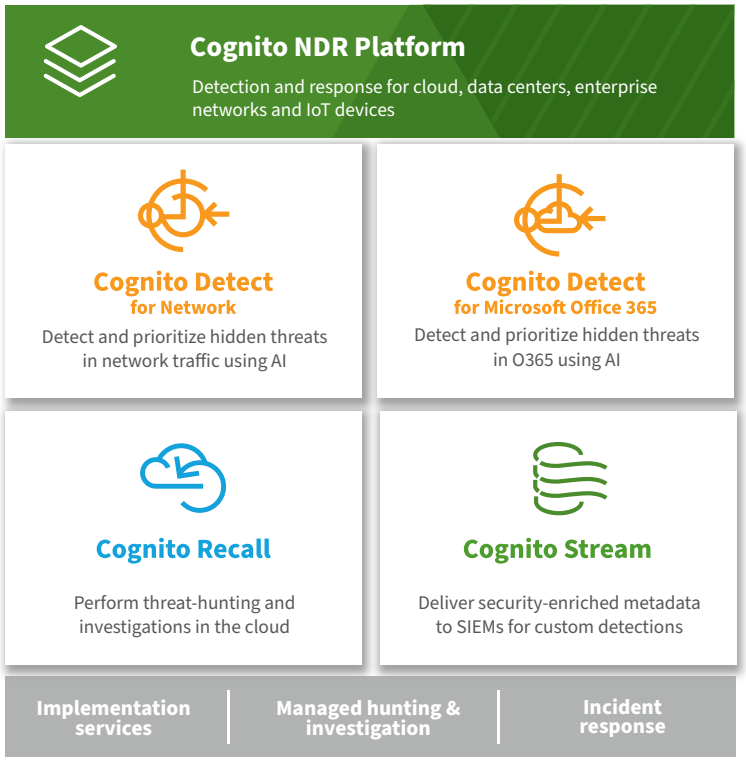
KEY BENEFITS

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



Trying to implement virtual firewalls to filter access is cumbersome to maintain, disruptive to your employees, and easily circumvented by attackers.

Vectra's network detection and response (NDR) platform seamlessly integrates with SaaS applications like Microsoft Office 365, IaaS providers including Amazon Web Services (AWS), and cloud virtualization platforms giving visibility into who is accessing them, regardless of how and where. Our patented ML threat detection models continually analyze how users are accessing, using, and configuring cloud services and account usage from Identity Providers (IdPs) including Microsoft Azure AD.



This unique vantage point allows us 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. Vectra ultimately reduces the risk associated with cloud migration.

Full hybrid cloud visibility

In on-premise environments, most security solutions are concerned with tracking assets using machine identities such as MAC or IP addresses. In the cloud those descriptors quickly become opaque or irrelevant. 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 important unique identifier seen in logs needed to be analyzed for security anomalies.

Vectra is the only solution that can detect threats across the entire network, tying together attacker activities and progression between cloud, hybrid, and on-prem environments.

Our solution enriches the opaque network metadata and cloud logs with usable information like host names, so you can keep track of hosts as their IPs change, in addition to users as they authenticate between workloads. Our patented machine learning (ML) models focusing on privileged access keep track of accounts and identities and how they normally behave, which translates to detection of account takeovers, privilege escalations, and credential abuse.

This allows us to give security professionals a complete view of attackers, and how attacks progress, regardless where it starts, moves and stops. The Vectra Cognito detection capabilities, combined with native integrations to disable accounts and isolate endpoints and workloads, allows us to stop any attacks in the enitre network before it leads to a breach of your data.

Monitor identities in cloud

Adversaries have switched from malware-based attacks that compromise endpoints to attacks that target user credentials, especially for cloud applications where your data is held directly.

These attacks 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 harder. 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 malicious intent by analyzing how hosts, accounts and workloads are being accessed.

For more information please contact a service representative at info@vectra.ai.

Vectra can detect malicious intent by analyzing how hosts, accounts and workloads are being accessed. By analyzing data from both identity provider (IdP) services and cloud applications, our custom ML models detects telltale attacker behaviors earlier in the kill chain than ever before. This gives security analysts a full picture of their entire network and allows them to monitor accounts for attacks and abuse, regardless if they are by external or internal actors.

Email info@vectra.ai vectra.ai