VECTRA®

How the Cognito platform increases visibility and security of zero trust

Introduction

The initial point of contact during a cyberattack is rarely the intended target. Attackers usually gain access to networks from a less secure workstation or IoT asset and work their way from there by gaining access to higher privileged hosts and accounts.

In fact, the recent ransomware variant RobbinHood that infected the cities of Greenville, N.C and Baltimore leveraged privileged accounts. The APT group Thrip did the same to further attacks against defense, telecom and satellite sectors.

Zero trust

This is why the concept of zero trust has grown significantly in the last couple of years. A zero-trust architecture fundamentally considers all entities in a network to be hostile and does not allow any access to resources until both the account and host have been individually authenticated and authorized to use that specific resource. This ensures that even if a host is compromised, further lateral movement is blocked within the network.

The gaps with access-only approaches

However, this approach to zero trust commonly seen in Privileged Access Management and Identity Access Management solutions still relies on single point in time-security gating decisions that use a predefined list of privileged identities. There are several issues with this approach being the sole implementation.

One issue involves simple configuration errors. This is especially common in cloud environments due to the differentiated skillset required to manage the complexity of constantly changing cloud resources as opposed to traditional on-prem counterparts.

Another issue is that once granted, access can easily be manipulated by attackers who use methods like credential abuse and privilege escalation. Both of these methods are especially hard for security practitioners to detect. They seldom have any visibility into the credentials being used on the network versus credentials assigned by Identity Providers (IdPs).

Continuous visibility and assessment of privilege

Closing this gap requires extending the preliminary method of authentication and authorization by continuously monitoring what accounts and identities are being used to access the network.

According to Gartner, “security and risk management leaders need to embrace a strategic approach where security is adaptive, everywhere, all the time. Gartner calls this strategic approach “continuous adaptive risk and trust assessment,” or CARTA and “with a CARTA strategic approach, we must architect for digital business environments where risk and trust are dynamic and need to be assessed continuously after the initial assessment is performed.”

"Once allowed into our systems and data," Gartner continues, "these entities – users, application processes, machines and so on – will interact with our systems and data, and all of these interactions must be monitored and assessed for risk and trust as they happen." *

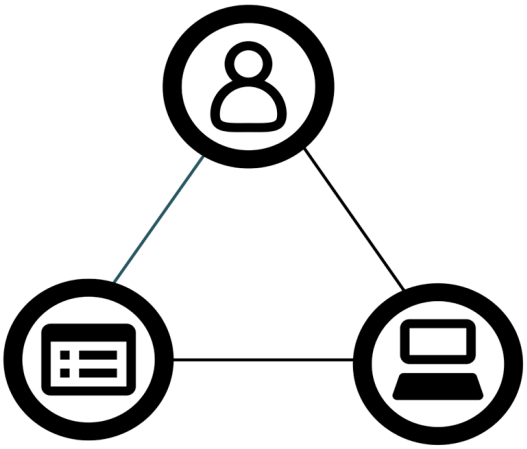
With monitoring, it is possible to observe if behaviors deviate from expectations in a risky way, and surface this to security practitioners to determine if access to the capabilities should be adapted or removed entirely.

Monitoring what interactions are actually occurring on the network – rather than looking at application logs or assigned permissions – exposes the immutable truth of what goes on inside a specific environment.

The Vectra approach

The three entities that need to be observed to gain full visibility into privilege on the network are:

- The hosts that are accessing workloads
- The servers that contain the workloads
- The user or service accounts being leveraged.



Monitoring the interactions of users, hosts and services is vital to understanding anomalies

The Cognito® platform from Vectra® continuously monitors the behaviors of users, hosts and services, and applies supervised and unsupervised AI models to score these behaviors for threat, certainty and prioritization of risk.

As a result, Cognito delivers a continuous real-time assessment of privilege. This empowers security teams with the right information to anticipate what assets will be targeted by attackers, and to rapidly take action against the malicious use of privilege across cloud and hybrid environments.

Flexible AI models

At the heart of Cognito are detection models that identify subtle indications of environment-knowledgeable attacks, all while only surfacing real events and eliminating noise.

The supervised AI models used by the Cognito platform allow for very quick detections even from day one without any deployment delays. Cognito currently leverages more than 90% of the MITRE ATT&CK framework, and Vectra is constantly including more with every software release.

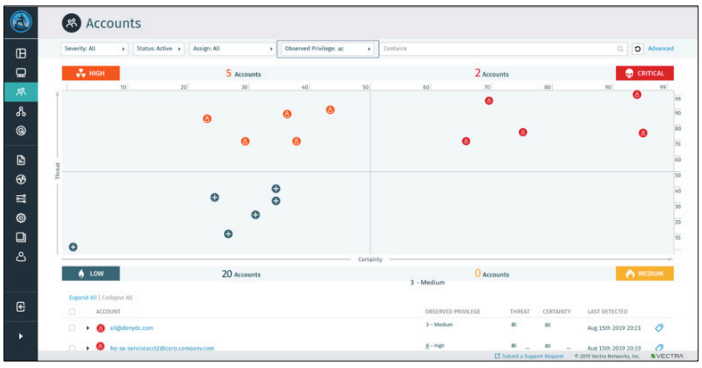
Privileged Access Analytics

A fundamental part of the engine that enables threat scoring is called Privileged Access Analytics (PAA). Rather than relying on the granted privilege of an entity or being agnostic to privilege, PAA focuses on how entities are actually utilizing their privileges within the network. This is known as observed privilege.

This viewpoint is similar to how attackers observe or infer the interactions between entities. In order to succeed, it is imperative that defenders think in a similar fashion as their adversaries.

PAA starts by grouping observed identities into groups based on similarity. This grouping is the baseline for incurring what constitutes as normal and abnormal access patterns. Cognito then applies further models to detect common access attacks.

An account, like a domain admin for example, may have the rights to access any system within the entire network. However, it is probably not accustomed to doing that, and therefore its observed privilege might be lower than that of a service account that is used to deploying software updates onto thousands of systems on the network.



Cognito Detect identifies and prioritizes all accounts that indicate anomalous behaviors

* Gartner, "Seven Imperatives to Adopt a CARTA Strategic Approach," Neil MacDonald, 10 April 2018

PAA is integrated across the entire Cognito platform, as well as through APIs. In Cognito Detect™, security professionals can find PAA under the Accounts Tab. This page surfaces all accounts in which Cognito has detected anomalies. The accounts are scored the same way Cognito scores hosts, on two axis for certainty and risk.

This is a very powerful way to give insight into what privileged identities exist on a network at any given time. Clicking on an account gives further context to an identity showcasing the observed privilege level fully enriched with Active Directory context, as well as the individual detections associated with that account for further investigation.

Cognito Stream™ features the same scalable security-enriched identity metadata in a Zeek-compatible format to feed custom detection and response tools

Conclusion

With Cognito from Vectra, security analysts now have the tools needed to identity and prioritize observed privilege across all of their networks.

VECTRA®
Security that thinks®

Email info@vectra.ai **Phone** +1 408-326-2020
vectra.ai