VECTRA
SECURITY THAT THINKS.

DATA SHEET

The trade-offs between automatic and manual cyberthreat enforcement

Enforcement, as it relates to cyberattacks, are responses to attacker actions to bring an enterprise back in line with its stated security policy. Common examples of enforcement are blocking traffic to a specific IP, quarantining a device by restricting network access, reformatting a machine, or locking down account access.

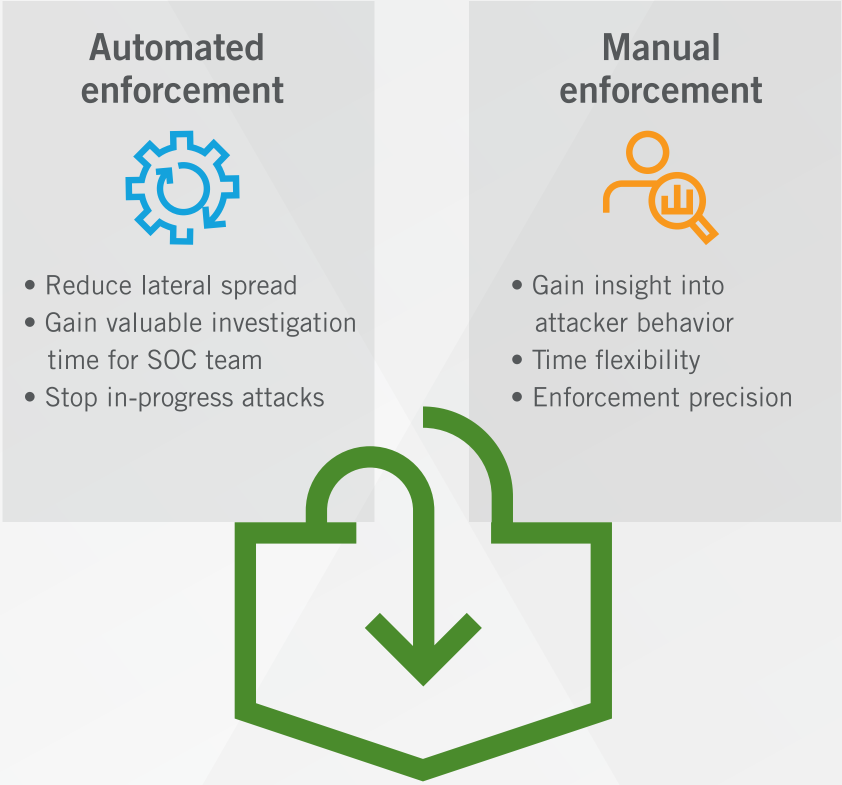
One of the most important considerations about enforcement options must be its effectiveness. After all, responding to cyberattacks is often a cat-and-mouse game. Every action from the security team will result in a reaction from the attackers. This means that even if the attacker is kicked out of the network, they will attempt to regain entry. Security teams must be prepared for changes in attacker tactics, attack escalations, and new victim targets.

In addition, attackers always have instantaneous feedback on their actions. They know if they are successful and can quickly retry if they are not. The defending team is not so lucky and will have no feedback on attackers' progress.

Benefits to host-based enforcement

For immediate and precise enforcement, analysts typically go directly to the source of an attack and lockdown the endpoint being used. This limits the attack's blast radius and gives the SOC more time to investigate and stop the attack.

However, this approach typically requires that the endpoint has some sort of agent or control software installed, which is not always the case. When possible enforcement on hosts should be combined with account-based enforcment as well.



Automated enforcement

- Reduce lateral spread
- Gain valuable investigation time for SOC team
- Stop in-progress attacks

Manual enforcement

- Gain insight into attacker behavior
- Time flexibility
- Enforcement precision

Vectra Lockdown enforcement

- Enable automatic and manual enforcement
- Uses a combination of score thresholds to pinpoint and lockdown specific accounts, hosts and cloud workloads

Benefits to account-based enforcement

It's been widely established by now that most modern cyberattacks target users instead of infrastructure or devices. Instead of using complicated exploits, many attackers get into the organization by stealing credentials through phishing or account takeover and logging in as a "legitimate" user.

This, combined with the growing standard of using cloud resources, means security teams should take a page out of the attacker playbook and consider enforcing based on users instead of the network or devices. Or in other words, use account-based enforcement.

In fact, account-based enforcement holds several advantages over network or machine-based enforcement options.

First, account-based enforcement creates a single enforcement point. In cases where attackers have compromised accounts, reformatting laptops isn't helpful when attackers can pivot to another device. Thus, account-based enforcement can be effective in cloud or hybrid environments where organizations don't own the service or infrastructure. It also limits lateral movement from attackers posing as employees with compromised accounts.

Account-based enforcement is also surgical and precise. Enforcement only affects the compromised user's account. No changes need to be made to the network. No blacklists need to be updated.

Finally, depending on the organizational structure, account-based enforcement can mean greater shared responsibility with IT. For enterprises where IT owns the user accounts, security teams can work with their IT counterparts to share the workload of managing user accounts and restoring access post-attack.

Enforcement types

Enforcement typically falls into two modes of operation: automatic and manual.

Automatic enforcements are actions triggered without human intervention, often after meeting a set of criteria, such as a predefined risk threshold and asset or account privilege. Manual enforcements require security staff to take the action.

There are compelling reasons to do either automatic or manual enforcement, or even a combination of both. Below, we'll cover some considerations for both types.

Considerations for automatic enforcement

Security teams often balk at the thought of automatic enforcement, but there are legitimate use cases where it can be helpful.

Automatic enforcement can be useful to reduce lateral spread and give resource-stretched security teams more time to investigate incidents. It is also useful as a temporary tool, especially for organizations without around-the-clock security staff for immediate investigations.

If an incident is already under investigation, automatic enforcement can help incident responders apply consistent security policies to multiple victims. Alternatively, if the incident is a known attack with established best-practices, security teams can use automatic enforcement to quickly follow approved remediation steps. An example is a known ransomware attack with prescribed recovery procedures. Of course, this scenario requires a high-confidence diagnosis to confirm it's a known attack or attacker.

Automatic enforcement actions can stop an attacker from progressing to the next phase in the kill chain. In this case, enforcement is surgically applied to a specific attacker activity and account, reducing additional risk.

In short, when applied judiciously, automatic enforcement can help prevent a bad situation from getting worse and buy more time for security investigations.

Considerations for manual enforcement

Manual enforcement requires a human to make the final decision and trigger action. This begs the question, if access to the same alerts, information, and forensics is available, why wait for a human to “press the button”?

In most cases, timing is the key difference.

There are advantages to not responding to active cyberattacks immediately. And while automatic enforcement can also be configured to trigger after a specified time, manual enforcement allows unrestricted time flexibility.

One key consideration for using manual enforcement is to let attacks play out to gain more information. Often, security teams can gather additional data by allowing the attacker to think they’re undiscovered.

In fact, certain information is only available after observing attacker behavior for longer periods of time. What other tools and tactics do they use? What data are they after, and where are they exfiltrating it? Researching an attack requires time and some amount of “free reign” within the network for the attacker.

Remember also that attackers will change their tactics if action is taken or taken too soon. This requires action to be taken thoughtfully. Manual enforcement allows security teams the flexibility to make decisions dynamically based on the attacker’s actions. By accruing more datapoints and correlating forensics, teams can also enforce with more confidence and accuracy.

Finally, manual enforcement lets security teams act with more surgical precision. Instead of applying the same action in all similar cases, teams can selectively trigger action for specific users, minimizing user impact. For example, instead of a mass password reset, maybe only employees within a certain geographic location need new credentials.

Requirements for worry-free enforcement

Regardless of whether you use automatic enforcement, manual enforcement or a combination of both, certain factors must be in place to ensure enforcement does not create more problems than it solves. Keeping in mind that attackers change tactics based on enforcement actions, effective enforcement ultimately needs to remove attackers from the organization and keep them out. Here are the key criteria for a worry-free enforcement solution.

Confidence is key

To confidently enforce, you must be confident the security information you’re basing decisions on is accurate. This means detection must rely on a high-fidelity system that aggregates data points for accuracy. Details like knowing the type of threat, risk level and certainty are crucial to making accurate enforce decisions.

Being able to correlate information from other security tools, like firewalls and SIEMs, also increases confidence and accuracy.

Enforce all necessary areas

Most enterprises have data both in the cloud, on their own premises, or hosted on partner infrastructure. Enterprise security stacks also encompass a wide variety of technologies like end point detection tools, network access controls, and firewalls. Consider enforcement solutions with a centralized account system that can enforce appropriate action across the entire enterprise infrastructure: on-premises, in hybrid environments, and across multiple technologies.

A solution that protects and enforces partner or contractor accounts also prevents those accounts from becoming attack targets.

Make it easy

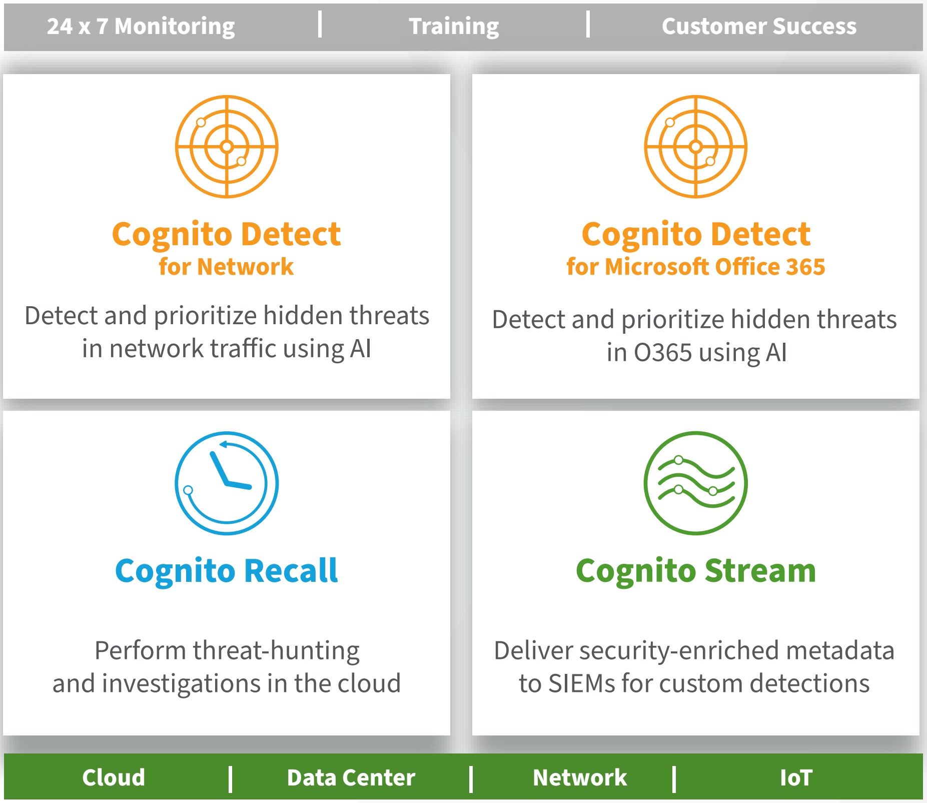
The type of enforcement action also matters. Choose enforcement actions that allow for accurate and reliable impact like account-based enforcement. Unlike network-based enforcement like blacklisting or TCP resets, account-based enforcement is effective, precise, and does not create unnecessary work for other departments.

Introducing Vectra lockdown enforcement

Lockdown lets security practitioners enable automatic and manual enforcement directly from the Cognito® Network Detection and Response (NDR) platform from Vectra®. It uses a combination of privilege score, account threat score, and account certainty score thresholds to lock down specific accounts, hosts and cloud workloads. Security admins can configure these thresholds, as well as how long the lockdown should last.

As always, other enforcement options are available through Vectra integrations with security orchestration and response (SOAR) partners.

The Cognito NDR platform is the fastest, most efficient way to detect and respond to cyberattacks, ensuring attackers are kicked out and stay out of enterprise environments.



24 x 7 Monitoring | Training | Customer Success

Cognito Detect
for Network
Detect and prioritize hidden threats in network traffic using AI

Cognito Detect
for Microsoft Office 365
Detect and prioritize hidden threats in O365 using AI

Cognito Recall
Perform threat-hunting and investigations in the cloud

Cognito Stream
Deliver security-enriched metadata to SIEMs for custom detections

Cloud | Data Center | Network | IoT

For more information please contact a service representative at sales-inquiries@vectra.ai.

Email info@vectra.ai vectra.ai

Version: **093020**