VECTRA

vmware®

Cognito enhances data center protection through VMware

Visibility into hidden cyber attacker behaviors throughout virtualized environments

CHALLENGE

Virtualization and cloud architectures present new cybersecurity challenges in the data center, including lack of visibility into virtualized environments.

Cyber attacks are often at a mature stage when they reach the data center, characterized by internal reconnaissance, lateral movement, command-and-control traffic, and the compromise of user and administrator credentials.

SOLUTION

Through its interoperability with the VMware vSphere hypervisor, vCenter management console and NSX Network Virtualization and Security Platform, the Cognito cybersecurity platform from Vectra addresses critical vulnerabilities at every layer of the virtualized data center and exposes cyber attacks against applications, data, virtualization layers and the underlying physical infrastructure.

BENEFITS

- Native visibility into vSphere, including traffic between virtual machines on the same server or different servers, regardless of physical or virtual switches.
- Exposes cyber attacks against data center applications, data, the physical infrastructure and virtualization layers.
- Displays data from the vCenter console, such as virtual machines spun up and down and the activity of critical workloads.
- Email notifications are sent to the relevant administrators about changes in the VMware environment that merit security consideration.
- VMware NSX micro-segmentation and adaptive security policy-enforcement capabilities improve mitigation response-times and reduce risk.

Virtualization and cloud architectures have transformed the data center, bringing significant gains in efficiency and agility.

However, the data center is a key target for cyber attackers, who often pivot quickly from the point of entry to the data center, where the lack of internal security controls and network visibility makes it easier for them to spy, spread and steal key assets.

For example, attackers may initially compromise an employee laptop via a phishing email or social engineering, then establish persistence within the network by spreading from the initial victim to other hosts or devices.

To control the ongoing threat, attackers will plant backdoors or hidden tunnels to communicate from inside the network, map out the internal network, identify valuable resources, and compromise devices and user credentials along the way.

The most coveted data center asset is administrator credentials, which enable attackers to access enterprise data. In addition, administrative protocols give attackers backdoor access into the data center without having to exploit an application vulnerability.

For example, using standard administrative tools such as SSH, telnet or RDP, attackers can easily blend in with normal admin traffic and use their position of trust to access or damage critical assets.

Advanced attackers, including nation-states, increasingly target physical servers, routers, switches, and even firewalls. Tools like Synful Knock have shown how attackers can burrow beneath the operating system to gain complete administrative control over a router and subsequently launch attacks against other systems and routers in the same network.

These tools represent rootkits that sit below the level of the operating system, making them extremely difficult to detect using traditional methods and quite dangerous. For instance, if attackers plant a backdoor below a server's OS and read the physical disk, they can see and potentially steal all the data on that disk.

Some 80% of data center traffic never leaves the data center, which makes it invisible to traditional security controls. Lack of visibility into the traffic between workloads is also a significant security blind spot.

In addition, when platforms are virtualized, visibility is lost to the physical network for virtual machine-to-virtual machine communication on the same physical hardware.

Consequently, any virtual data center cybersecurity solution must be interoperable with the virtualization platform to provide visibility into potential threats, and it must be able to retain context and visibility across the dynamic virtual environment as virtual machines and workloads spin-up. It is critical for security teams to see as much of this context as possible before the attack reaches the data center.

In addition, since advanced phases of attack often exploit allowed protocols and do not rely on malicious payloads, it is important that a cybersecurity solution use behavioral models to detect threats.

Similarly, data center security solutions must focus on detecting attackers who have already compromised the perimeter and moved on to more advanced attack phases, such as internal reconnaissance, lateral movement, and data exfiltration.

The Vectra and VMware solution

Vectra® offers the industry's first comprehensive approach to identifying cyber attacks that target data centers. Using artificial intelligence, the Cognito™ threat detection and response platform from Vectra exposes attacks against application, data and virtualization layers as well as the underlying physical infrastructure.

All network traffic is monitored by Cognito to reveal attackers who have gained a position of trust inside the network. Threat-detection models leverage data science, modern machine-learning techniques and behavioral analysis to identify the fundamental behaviors at the heart of every cyber attack.

Inside the data center, Cognito persistently monitors critical applications, data and the underlying physical infrastructure. As Cognito continuously learns normal behaviors, all traffic into, within and out of the data center network is tracked.

By learning the specific resources or workloads of the data center administrator, as well as what tools and protocols are typically used, Cognito recognizes abnormal behaviors and alerts security teams to potentially compromised or rogue administrators.

Likewise, Cognito will immediately generate a detection if previously-unused administrative protocols are used in the data center or are used in a manner that is new.

Cognito applies this methodology to the unique environment of the virtual data center with detection models that specifically focus on exfiltration, abuse of administrative protocols and privileges, as well signs of rootkits and backdoors implanted in the physical data center infrastructure.

The goal of Cognito is to identify attacks well before data is accessed. For example, it detects data exfiltration, including fast, high-volume exfiltrations as well as slow, low-volume approaches. Cognito also monitors and detects staged transfers in the network and identifies hidden tunnels within HTTP, HTTPS and DNS protocols.

Cognito natively interoperates with the virtualization platform and provides real-time visibility into the behavior of attackers in cloud data centers. Interoperability with the VMware vSphere hypervisor, vCenter management console and NSX Network Virtualization and Security Platform enhances Cognito by providing visibility into all traffic between VMware-based virtual machines, whether they're on the same server or different servers, and regardless of physical or virtual switches.

VMware vSphere

Vectra virtual sensors (vSensors) connect to any VMware vSwitch to give Cognito visibility into traffic between workloads on the same physical host and detect threats passing between workloads in the virtual environment.

The vSensors capture and distill metadata from the traffic and send it to the Cognito platform, which analyzes information from all sensors and generates threat detections based on current and historical data.

Through this interoperability, security administrators gain an always up-to-date view of the virtual environment, can easily verify coverage or identify any workloads that may not be covered, as well as monitor VMware hosts and identify any resource or configuration problems that could affect the health or security of the data center.

Interoperability with vSphere also allows Cognito to retain intelligence and persistently track and model workload behavior, even as a workload moves – a key trait for detecting malicious behaviors.

The interoperability with vSphere also enables Cognito to generate email notifications to the appropriate administrators (e.g., security administrators and VMware administrators) about changes in the virtual environment that merit security consideration.

For example, a newly deployed physical server may require the addition of a vSensor for monitoring or a virtual machine might be moved to a different host where there is no vSensor to provide security coverage.

VMware vCenter

With VMware vCenter interoperability, Cognito provides an always up-to-date view of the environment. For example, it visually displays the connections between all workloads and the type of traffic flowing between them.

In addition to providing a top-down overview of the virtual environment, Cognito can alert staff any time a virtual asset is not being monitored or suspicious activity is detected, prompting administrators to take action.

VMware NSX

By leveraging the VMware NSX micro-segmentation and adaptive security policy-enforcement capabilities, Cognito further improves security response times and reduces business risk. Specifically, Cognito will work with joint customers to provide increased visibility and automated threat mitigation orchestrated through Vectra Active Enforcement (VAE).

For example, when Cognito detects a threat that reaches a configurable threshold, VAE turns the detection into action by automatically adjusting NSX security policy to take an appropriate action, such as blocking malicious traffic, modifying the security policy, applying additional security services, initiating an anti-virus scan or quarantining the compromised host.

Together Cognito and VMware improve visibility into data center traffic, enabling faster threat detection and mitigation in order to minimize data loss and reduce business risk.

About Vectra

Vectra® is an artificial intelligence company that is transforming cybersecurity. Its Cognito™ platform is the fastest, most efficient way to detect and respond to cyberattacks, reducing security operations workload by 168X. Cognito performs real-time attack hunting by analyzing rich metadata from network traffic, relevant logs and cloud events to detect attacker behaviors within all cloud and data center workloads, and user and IoT devices. Cognito correlates threats, prioritizes hosts based on risk and provides rich context to empower response. Cognito integrates with endpoint, NAC, firewall security to automate containment, and provides a clear starting point for searches within SIEM and forensic tools.

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