VECTRA
SECURITY THAT THINKS.®

COMPLIANCE BRIEF

How Cognito addresses CIS Critical Security Controls (CSC) 7.1

The Cognito® threat detection and response platform from Vectra® continuously monitors and analyzes all network traffic to detect cyber attacks in progress as criminals attempt to steal enterprise data or cause harm to the organization.

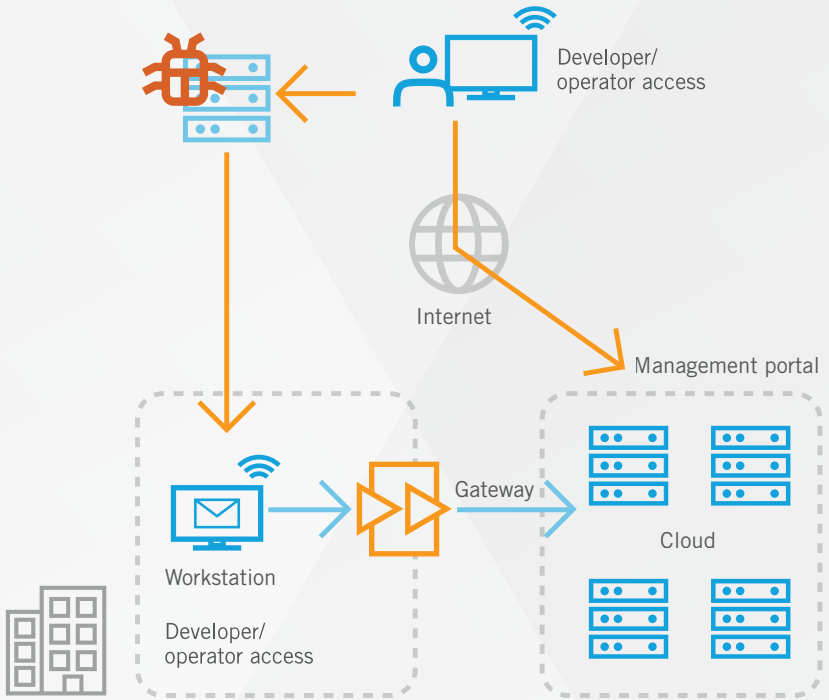
By using data science, machine learning and behavioral traffic analysis, Cognito reveals the hidden, fundamental attack behaviors that cyber criminals must perform in order to succeed.

The intelligence in Cognito learns normal network traffic patterns and host behaviors, which makes malicious attack behaviors stand out – even in encrypted traffic.

Always-learning threat detection models pinpoint attackers automatically and in real time over hours, days and weeks, correlates their malicious behaviors with hosts that are under attack, and anticipates their next move.

The Critical Security Controls (CSCs) developed through federal and community efforts, coordinated by the SANS Institute and maintained by the Center for Internet Security (CIS), are designed to mitigate modern attack profiles.

"Realistically, only by adopting basic cyber hygiene will enterprises meaningfully reduce their cyber-risk profile." **Jane Holl Lute**
board member and former CEO at CIS



Cognito will detect cyber thieves as they patiently make their way to assets in the network, persistently track the hosts involved in an attack, and recognize when a specific host or user account is abnormally accessing servers or data.

"Realistically, only by adopting basic cyber hygiene will enterprises meaningfully reduce their cyber-risk profile," said Jane Holl Lute, board member and former CEO at CIS.

"Innovations such as machine learning that incorporate behavioral analytics from Vectra automate a number of the Critical Security Controls and will enable wider-spread adoption of these best practices to really change the game in cybersecurity," she added.

Cyber attacks are a fact of life. It has become routine to hear about massive data breaches in the news. That's because organizations have multiple vulnerability points:

- Physical access
- Employees
- Devices
- Network and wireless access routers
- Online presence
- Shared connections with vendors and partners

With Cognito monitoring all network traffic 24x7, organizations can protect their assets, while achieving CIS Critical Security Controls across physical and virtual networks, as well as their individual hosts.

Cognito provides real-time insight into advanced persistent threats (APTs). This insight is fully automated with clear, intuitive reports that enable organizations to create a compliance audit trail as they take immediate, decisive action to stop attacks and mitigate their impact.

Achieving CIS Critical Security Controls with autonomous detection

Cognito continuously monitors all network traffic. Deployed inside the network perimeter, Cognito monitors internal (east-west) and Internet-bound (north-south) traffic to identify malicious attack behaviors that put in-scope assets at risk.

Cognito uses the network to gain high-fidelity visibility into the actions of all devices – from cloud and data center workloads to user and IoT device – leaving attackers with nowhere to hide.

Cognito also detects attack behaviors in all phases of the attack kill chain – command and control (C&C), internal reconnaissance, lateral movement, ransomware activity, data exfiltration, and botnet monetization behaviors – across all applications, operating systems and devices.

For example, Cognito will detect cyber thieves as they patiently make their way to assets in the network, persistently track the hosts involved in an attack, and recognize when a specific host or user account is abnormally accessing servers or data.

In addition, Cognito tracks the internal Kerberos infrastructure to understand normal usage behaviors and detect when a trusted user's credentials are compromised by an attacker, including the misuse of administrative credentials.

Cognito also provides multiple early-warning opportunities to detect ransomware, other malware variants and malicious activity that precede an attack on any network device, including devices that may not be able to run antivirus software.

This includes the ability to detect malware on mobile and IoT devices and servers that use any operating system. Cognito learns the traffic patterns and behaviors that are typical to a network, while remembering and correlating anomalous behaviors it has previously seen.

Protect enterprise data with Security that thinks®

It's time for security to get smarter. Attackers are already in your network, looking for an opportunity to steal high-value data. Cognito does the hard work by recognizing cyber threats amid the normal chatter in your network and anticipating the next move of attackers in real time so they can be stopped.

HOW COGNITO ADDRESSES CIS CRITICAL SECURITY CONTROLS 7.1		
	Control description	**Cognito**
Critical Security Control 1: Inventory of authorized and unauthorized devices		
1.2	Utilize a passive discovery tool to identify devices connected to the organization's network and automatically update the organization's hardware asset inventory.	**Host ID –** A host identification engine receives network traffic from a network and uses one or more artifact extractors to extract artifact data items that can identify a host. The artifact data items are stored in a host signature database. Network addresses to which the hosts correspond are stored in a network address database. A mapping table is implemented to match the data in the signature database and network database to generate durable host identification data that can accurately track hosts as they use different identification data and/or move between hosts.
1.3	Use Dynamic Host Configuration Protocol (DHCP) logging on all DHCP servers or IP address management tools to update the organization's hardware asset inventory.	DHCP requests and responses contribute to the data used to calculate the Vectra Host ID.
Critical Security Control 4: Continuous vulnerability assessment and remediation		
4.1	Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.	Vectra Cognito's Privilege Access Analytics identifies high risk and malicious use of privileged accounts, hosts, and services through direct observation and doesn't require access audit logs or prior knowledge of granted privileges.
4.5	Use multifactor authentication and encrypted channels for all administrative account access.	Vectra Cognito platform supports Multifactor Authentication of user and administrator accounts via 3rd party AAA services.
4.9	Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.	Vectra Cognito will detect brute force credential misuse attempts.

HOW COGNITO ADDRESSES CIS CRITICAL SECURITY CONTROLS 7.1		
	Control description	**Cognito**
Critical Security Control 6: Maintenance, monitoring, and analysis of audit logs		
6.1	Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.	Vectra Cognito supports NTP.
6.2	Ensure that local logging has been enabled on all systems and networking devices.	Vectra Cognito supports audit logging.
6.3	Enable system logging to include detailed information such as a event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.	Vectra Cognito supports event logging.
6.5	Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.	Vectra Cognito can forward detection alerts as SYSLOG/CEF event to a central log management or SIEM tool.
6.6	Deploy a SIEM (Security Information and Event Management) or log analytic tools for log aggregation and consolidation from multiple machines and for log correlation and analysis. Using the SIEM tool, system administrators and security personnel should devise profiles of common events from given systems so that they can tune detection to focus on unusual activity, avoid false positives, more rapidly identify anomalies, and prevent overwhelming analysts with insignificant alerts.	Vectra Cognito natively performs threat detection security analysis , scores and prioritizes detections correlated to hosts and accounts independent of a SEIM tool. Vectra Cognito can forward detection alerts such as SYSLOG/CEF to SIEM tools. A number of additional capabilities are available through in-SIEM apps, widgets, and API integrations. All of the security metadata streams analyzed by Vectra Cognito can also be forwarded to a SIEM.
6.7	On a regular basis, review logs to identify anomalies or abnormal events.	Vectra Cognito automatically identifies, scores, and alerts you to suspicious anomalies associated to known attacker behaviors.
6.8	On a regular basis, tune your SIEM system to better identify actionable events and decrease event noise.	Vectra Cognito Triage filters are used to suppress benign detections to increase salient alerts and decrease unwanted signal noise. Vectra Cognito AI algorithms do not require manual tuning or adaptation and are frequently updated for performance and new detection capabilities.

HOW COGNITO ADDRESSES CIS CRITICAL SECURITY CONTROLS 7.1		
	Control description	**Cognito**
Critical Security Control 7: Email and web browser protections		
7.6	Log all URL requests from each of the organization's systems, whether on-site or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.	Vectra Cognito monitors all Internet Ingress/Egress (N/S) traffic, including domain and destination IP address. Vectra Cognito detects known threat actor external infrastructure through the Vectra Threat Intel Feed or customer supplied STIX Threat intelligence feed. Malicious activity from command and control or data exfiltration behaviors is detected, scored, and sent as an alert.
Critical Security Control 8: Malware defenses		
8.7	Enable Domain Name System (DNS) query logging to detect hostname lookups for known malicious domains.	Vectra Cognito monitors all Internet Ingress/Egress (N/S) traffic including domain and destination IP address. Vectra Cognito detects known threat actor external infrastructure through the Vectra Threat Intel Feed customer supplied STIX Threat intelligence feed. Malicious activity from command and control or data exfiltration behaviors is detected, scored, and alerted. Observed DNS history is available and archived as part of the security metadata used by Cognito Stream and Cognito Recall.
8.8	Enable command-line audit logging for command shells, such as Microsoft PowerShell and Bash.	Vectra Cognito detects the suspicious use of Remote Execution and PowerShell.
Critical Security Control 9: Limitation and control of network ports		
9.1	Associate active ports, services, and protocols to the hardware assets in the asset inventory.	The historical use of active ports, services, and protocol by observed hosts can be identified using Vectra Cognito Recall or external analysis from tools fed data from Cogito Stream.
9.2	Ensure that only network ports, protocols, and services listening on a system with validated business needs are running on each system.	The use of forbidden ports can be identified using Vectra Cognito Recall or external analysis from tools fed data from Cogito Stream.
9.3	Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on the system.	The use of forbidden ports can be identified using Vectra Cognito Recall or external analysis from tools fed data from Cogito Stream.

HOW COGNITO ADDRESSES CIS CRITICAL SECURITY CONTROLS 7.1		
	Control description	**Cognito**
Critical Security Control 10: Data recovery capabilities		
10.1	Ensure that all system data is automatically backed up on a regular basis.	Vectra Cognito supports automated user-defined back-ups.
Critical Security Control 11: Secure configuration for network devices, such as firewalls, routers, and switches		
11.1	Maintain documented security configuration standards for all authorized network devices.	Vectra comes with documented security standards and default configurations.
11.4	Install the latest stable version of any security-related updates on all network devices.	
11.5	Manage all network devices using multifactor authentication and encrypted sessions.	Vectra Cognito supports multifactor authentication via a number of authentication services and standards.
11.7	Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.	Vectra Cognito supports an out-of-band management interface.
Critical Security Control 12: Boundary defense		
12.2	Perform regular scans from outside each trusted network boundary to detect any unauthorized connections which are accessible across the boundary.	Vectra Cognito monitors all observed traffic and creates security and connection metadata. This metadata is automatically detected, scored, and alerted about any suspicious or attacker behaviors. That same metadata is available and archived as part of the security metadata used by Cognito Stream and Cognito Recall for historical investigations.
12.3	Deny communications with known malicious or unused Internet IP addresses and limit access only to trusted and necessary IP address ranges at each of the organization's network boundaries.	Vectra Cognito can take blocking actions of identified host or services via API integrations with existing security controls such as NAC and Firewalls, or via direct integrations with Active Directory accounts and popular EDR tools.

HOW COGNITO ADDRESSES CIS CRITICAL SECURITY CONTROLS 7.1		
	Control description	**Cognito**
	Critical Security Control 12: Boundary defense	
12.4	Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.	Vectra Cognito supports custom models and searches to identify unauthorized TCP, UDP ports, or application traffic. Automated or analyst initiated blocking actions of identified host or services can be made via API integrations with existing security controls such as NAC and Firewalls, or via built-in integrations with Active Directory accounts and popular EDR tools.
12.5	Configure monitoring systems to record network packets passing through the boundary at each of the organization's network boundaries.	Vectra Cognito generates security and connection metadata from observed network traffic. Where the behaviour is identified and packets are still cached, a PCAP is saved and associated with the detection. All metadata is made available for archiving and investigations.
12.6	Deploy network-based Intrusion Detection Systems (IDS) sensors to look for unusual attack mechanisms and detect compromise of these systems at each of the organization's network boundaries.	Vectra Cognito generates security and connection metadata from observed network traffic. Where the behavior is identified and packets are still cached, a PCAP is saved and associated with the detection. All metadata is made available for archiving and investigations.
12.7	Deploy network-based Intrusion Detection Systems (IDS) to block malicious network traffic at each of the organization's network boundaries.	Vectra Cognito can take blocking actions of identified host or services via API integrations with existing security controls such as NAC and Firewalls, or via direct integrations with Active Directory accounts and popular EDR tools.
12.8	Enable the collection of NetFlow wand logging data on all network boundary devices.	Vectra Cognito generates security and connection metadata from observed network traffic. This metadata has far higher fidelity and utility than flow-based, sampled data sets such as NetFlow.
12.10	Decrypt all encrypted network traffic at the boundary proxy prior to analyzing the content. However, the organization may use whitelists of allowed sites that can be accessed through the proxy without decrypting the traffic.	Vectra Cognito uses TLS fingerprinting and AI powered metadata analysis to detect malicious behaviors within encrypted communications without decryption required.
12.12	Scan all enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices.	Vectra Cognito tracks Kerberos logs and enables monitoring of device/account authentication during login action.

HOW COGNITO ADDRESSES CIS CRITICAL SECURITY CONTROLS 7.1

Critical Security Control 13: Data protection		
13.3	Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.	Vectra Cognito can take blocking actions of identified host or services via API integrations with existing security controls such as NAC and Firewalls, or via direct integrations with Active Directory accounts and popular EDR tools.
13.5	Monitor all traffic leaving the organization and detect any unauthorized uses of encryption.	Vectra Cognito uses TLS fingerprinting and AI powered metadata analysis to detect malicious behaviors within encrypted communications without decryption required.
13.6	Utilize approved cryptographic mechanisms to protect enterprise data stored on all mobile devices.	Vectra Cognito can be used to analyze PKI certificates used in overserved historical communications to identify malicious and out of policy cryptography.
Critical Security Control 14: Controlled access based on the need to know		
14.3	Disable all workstation-to-workforce communication to limit an attacker's ability to move laterally and compromise neighboring systems through technologies such as Private VLANs or micro-segmentation.	Vectra Cognito automatically identifies, scores, and alerts on observed lateral movement attacker behaviors.
14.4	Encrypt all sensitive information in transit.	Vectra Cognito uses TLS fingerprinting an AI powered metadata analysis to detect malicious behaviors within encrypted communications without needing to decrypt, which provides protection without impacting privacy.

HOW COGNITO ADDRESSES CIS CRITICAL SECURITY CONTROLS 7.1		
	Control description	**Cognito**
Critical Security Control 16: Account monitoring and control		
16.6	Maintain an inventory of all accounts organized by authentication system.	Vectra Cognito's Privilege Access Analytics identifies high risk and malicious use of privileged accounts, hosts, and service through direct observation and doesn't require access audit logs or prior knowledge of granted privileges.
16.12	Monitor attempts to access deactivated accounts through audit logging.	Vectra Cognito's Privilege Access Analytics identifies high risk and malicious use of privileged accounts, hosts, and services through direct observation and doesn't require access audit logs or prior knowledge of granted privileges.
16.13	Alert when users deviate from normal login behavior, such as time-of-day, workstation location, and duration.	Vectra Cognito's Privilege Access Analytics identifies high risk and malicious use of privileged accounts, hosts, and services through direct observation and doesn't require access audit logs or prior knowledge of granted privileges.
Critical Security Control 19: Incident response (IR) and Management		
19.2	Assign job titles and duties for handling computer and network incidents to specific individuals, and ensure tracking and documentation throughout the incident through resolution.	Vectra Cognito supports role-based access and workflow capabilities to enable analyst collaboration and assignment of detections.
19.6	Publish information for all workforce members, regarding reporting computer anomalies and incidents, to the incident handling team. Such information should be included in routine employee awareness activities.	Vectra Cognito includes a custom reporting tool to generate incident response and threat detection reports on schedule and on demand.
19.8	Create incident scoring and prioritization schema based on known or potential impact to your organization. Utilize score to define frequency of status updates and escalation procedures.	Vectra Cognito uses a Risk Certainty Index score for observed attacker behaviors, associated hosts, and accounts. This enables the prioritization of the most salient threat detections.

HOW COGNITO ADDRESSES CIS CRITICAL SECURITY CONTROLS 7.1		
	Control description	**Cognito**
Critical Security Control 20: Penetration tests and red team exercises		
20.7	Wherever possible, ensure that Red Team results are documented using open, machine-readable standards (e.g. SCAP). Devise a scoring method for determining the results of Red Team exercises so that results can be compared over time.	Vectra Cognito will provide real-time detection of a Red Team test's replication of attacker post-intrusion behaviors. Full historical metadata will be available for historical analysis and reporting.
20.8	Any user or system account used to perform penetration testing should be controlled and monitored to make sure they are only being used for legitimate purposes, and are removed or restored to normal function after testing is over.	Vectra Cognito's Privilege Access Analytics identifies high risk and malicious use of privileged accounts, hosts, and services through direct observation and doesn't require access audit logs or prior knowledge of granted privileges.

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

Email info@vectra.ai vectra.ai