VECTRA
SECURITY THAT THINKS®

SOLUTION BRIEF

Securing Critical National Infrastructure with Network Detection and Response (NDR)

Public and private sector organizations – from government and military to banking, energy and transportation – have become increasingly digital-centric to seek economic savings, productivity gains and to create customer and citizen value.

This digital transformation is powered by a wealth of emerging technologies and approaches, including mobile, IoT, cloud, and pervasive high-speed internet connectivity. They all bring innovation and new operating capabilities, but also expand the cyberattack surface.

These vital services and infrastructure are components of Critical National Infrastructure (CNI). They are tantalizing targets for nation-state threat actors, hacktivists and terrorist organizations that seek to negatively impact day-to-day life.

> "I think it is a matter of when, not if, and we will be fortunate to come to the end of the decade without having to trigger a Category 1 attack."

Ciaran Martin
CEO, National Cyber Security Centre, United Kingdom[1]

62%

62% of detected incidents resulted in a breach of information, devices, or systems, according to a SANS institute incident response survey[3]

HIGHLIGHTS

- A common thread throughout is the need for continuous security visibility and network monitoring that enables the detection and response to signs of active threats. In many cases, the network infrastructure is specifically mandated as an inspection point.
- Slowing down attackers is only part of the challenge. It is vital to speed-up defenders too. CNI organizations must be able to quickly detect, understand, respond, and recover from the attackers that successfully penetrate their systems.
- An underlying limitation of threat signatures is that they search for known malicious payloads while anomaly detection only knows what is different instead of what is bad.
- Cognito Recall™ allows security analysts to perform in-depth investigations based on the actionable high-fidelity incidents identified by Cognito Detect™ while providing a workbench for proactive threat hunting activities.
- By using AI to automate threat detection and incident response, the Cognito NDR platform enables CNI organizations to condense days, weeks and months of security operations work into minutes, allowing security teams to take action to prevent data theft or damage.

CNI organizations must be ready and able to defend against a wide range of threats that attempt to steal from, disrupt, damage, or deny their operations. Well-resourced and motivated attackers are dangerously skilled and persistent. The result is an increase in the number of attempted attacks.

The underlying networks and information systems delivering these critical services and capabilities are now legislated, with the goal of reducing cyber risk and improving resiliency. The United States NIST framework and the European Union NIS directive identify key industries and sectors that are considered critical and define appropriate steps to secure services.

These initiatives have influenced country-specific guidance on how to secure CNI for organizations such as Germany's KRITIS, Switzerland's MELANI, and Australia's Critical Infrastructure Centre. A common thread is the need for continuous security visibility and network monitoring that enables the detection and response to the first signs of active threats. In many cases, the network infrastructure is specifically mandated as an inspection point.

Speed up defenders

- Threat and context awareness
- High-fidelity, low noise detections
- Achieve rapid, accurate understanding
- Effective response
- Confirmed recovering
- Learning and changes

Slow down attackers

- Attack surface minimization
- Perimeter protections
- Defensive controls
- Information management

Visibility and agility are the foundation of effective incident response

No defensive controls are perfect. A 2019 analysis identified threat actors hidden inside organizations and operating with impunity for a median of 56 days[2] before discovery. Such attacks can inflict significant damage through extended dwell times. In fact, 62% of detected incidents resulted in a breach of information, devices or systems, according to a SANS institute incident response survey[3].

Identifying potential threats and placing appropriate protective controls are rational first steps but it is important to recognize that persistent, motivated and skilled attackers will always find a way inside an organization's digital infrastructure.

"The biggest frustration to me is speed, speed, speed. I'm constantly asking the team what can we do to be faster and more agile?"

Adm. Michael Rogers,
director of the National Security Agency, commander of the U.S. Cyber Command and Chief of the Central Security Service (2014-2018)[4]

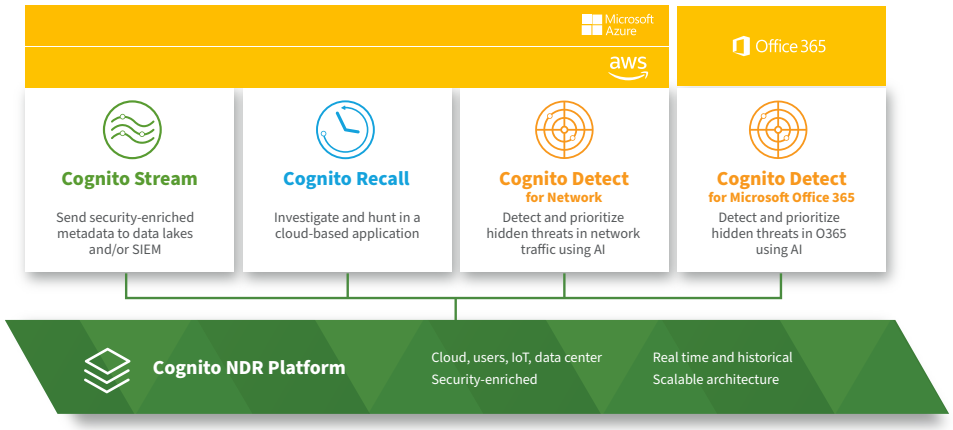
Slowing down attackers is only part of the challenge. It is vital to speed-up defenders, too. CNI organizations must quickly detect, understand, respond, and recover from attackers who get inside cloud, data center, IT, and IoT networks.

Every cloud service, data center, networked device, and user within the CNI organization forms part of an attack surface. Many component entities, such as IoT devices, also have little or no direct security controls or monitoring.

Cloud, data center, IT, and IoT networks provide vantage points across the infrastructure that advanced attackers will penetrate and spread. But the volume of data and ratio of the attacker signal-to-communication noise means that manual analysis and detection cannot provide the necessary scale, speed or efficiency.

The Cognito® Network Detection and Response (NDR) platform from Vectra® provides automated, high-fidelity detection alerts while suppressing the noise of inaccurate detections or benign alerts. It also collects metadata from all network traffic – cloud, data center, IT, and IoT – and enriches it with security insights and context.

This enables security teams to use a trail of forensic evidence for faster, more conclusive incident investigations and proactively hunt for threats.



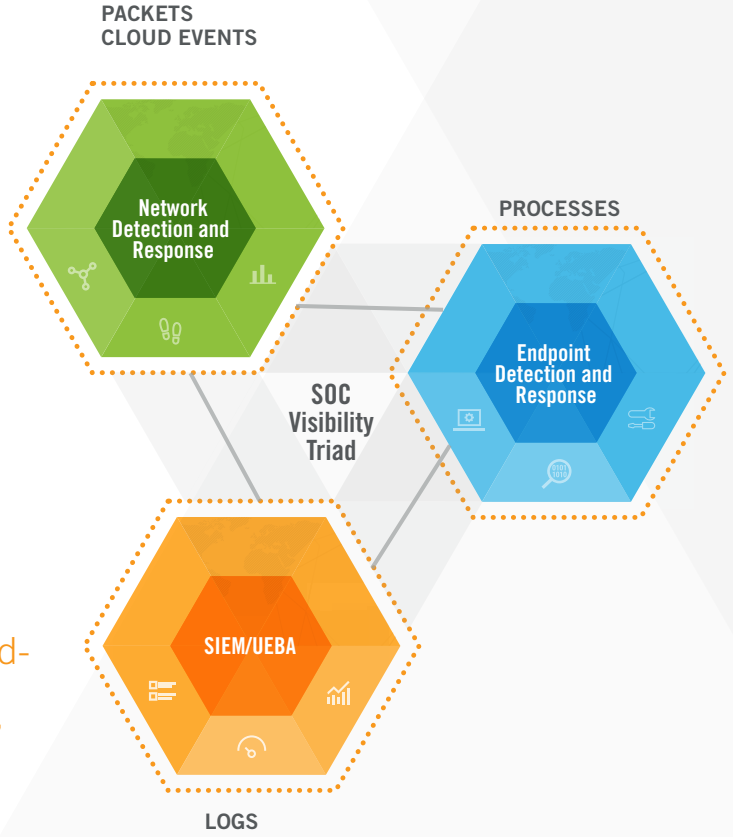
The Cognito NDR platform from Vectra

The Cognito NDR platform provides a complementary perspective to the insights delivered by endpoint detection and response (EDR) tools and detects attacker behaviors that are only visible in cloud, data center, IT, and IoT networks.

Security operations centers (SOCs) within CNI organizations can consolidate EDR and NDR threat detections into a SIEM, which acts the nexus of all security signals and security orchestration and response (SOAR).

This automation enables the crucial acceleration of many response tasks. Known as the SOC visibility triad, it significantly reduces the risk that an attacker can operate undetected inside an organization.

Vectra provides complimentary technical integration kits for leading EDR, SIEM and SOAR tools that simplify deployments, reduce risk and accelerate operational workflows.



"Vectra stands out for its ability to offer an unparalleled level of flexibility and agility to identify a variety of fundamental attack behaviors such as command-and-control communications, abuse of account credentials, data exfiltration, botnet monetization, and early indicators of ransomware activity."

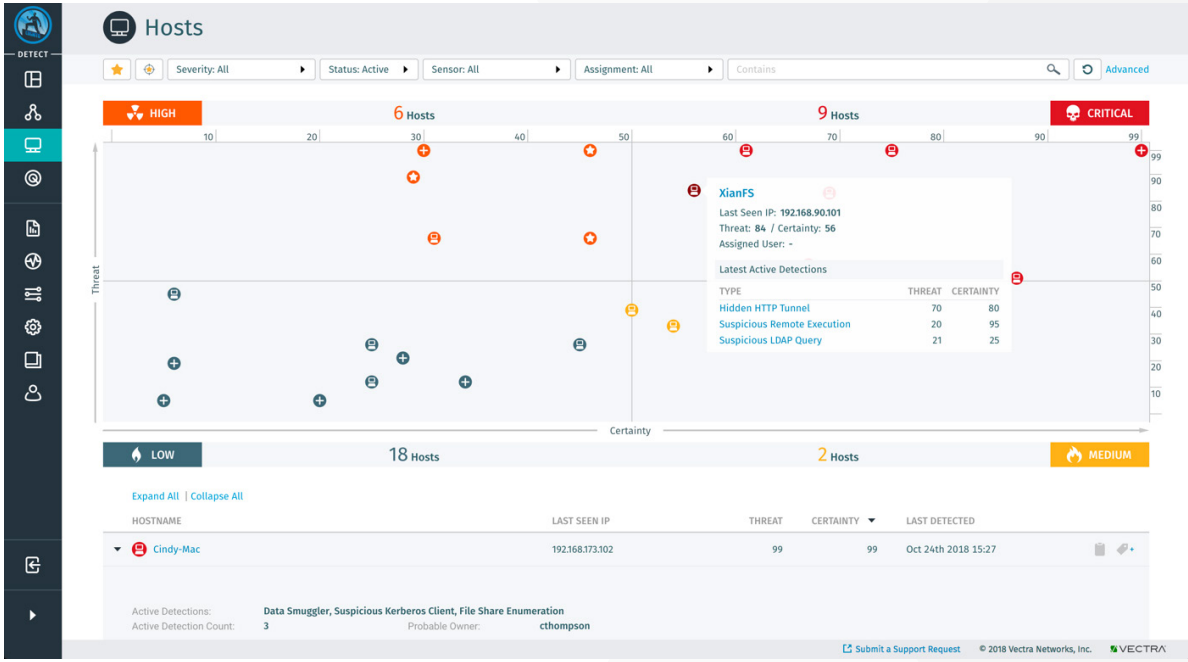
Vikrant Gandhi,
industry director at Frost & Sullivan

Detect attackers by their immutable behavior

Detecting today's advanced attacks has moved beyond the realm of traditional threat signatures and beyond exposing simple anomalous behaviors. An underlying limitation of signatures is that they search for known malicious payloads while anomaly detection only knows what is different instead of what is bad. It is easy for attackers to adapt and avoid these controls. Attackers will adopt normal user behaviors to avoid standing out from normal activity.

Detection approaches today focus on identifying the underlying malicious behaviors. This is conceptually akin to looking for malicious verbs as opposed to malicious nouns.

Attackers have a near-infinite supply of tools to help them spy, spread and steal inside the network. But they must perform the same tell-tale immutable behaviors.



Critical hosts prioritized by Threat Certainly Index in Cognito Detect

An underlying limitation of signatures is that they search for known malicious payloads while anomaly detection only knows what is different instead of what is bad.

Monitoring and recognizing these malicious behaviors can identify the signals that expose attackers who are active and spreading inside the CNI infrastructure.

Detecting attacker behaviors has long-term utility but is difficult to achieve without Vectra. By combining threat research, data science, advanced machine learning algorithms, and behavioral analysis, Cognito Detect overcomes these challenges.

Running on the Cognito NDR platform, Cognito Detect identifies the intent of network traffic and reveals malicious behaviors, independent of applications, even when traffic is encrypted. This approach reveals the key actions that attackers must perform to succeed, and it leaves them with nowhere to hide.

Cognito Detect applies algorithmic models directly to network traffic and cloud events to reveal underlying attack behaviors. It then automatically enriches that data with secondary sources, such as authentication logs and threat intelligence data. While these secondary sources are not required to detect an attacker, they provide context to accelerate the detection and response process for security analysts.

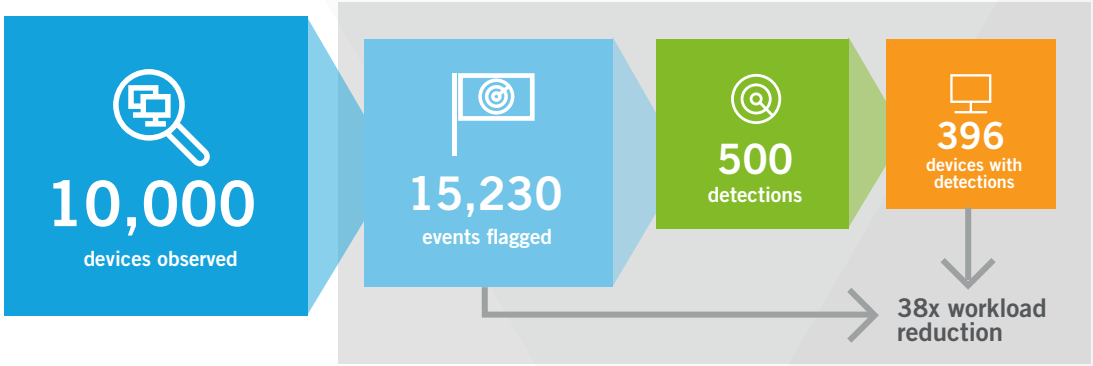
Detections are triaged, scored, prioritized, and shown in the Threat Certainty Index™ of the Cognito Detect dashboard. All detections are associated with a host and privileged identity accounts and correlated with other hosts and privileged accounts involved in the same attack campaign. A recent study of actual Cognito Detect deployments found a 38-times reduction in the Tier-1 security analyst's workload[5].

Incident investigations and threat hunting

Cognito Recall also runs on the Cognito NDR platform so that security analysts can perform in-depth investigations based on the actionable high-fidelity incidents identified by Cognito Detect. It's an indispensable investigative workbench for proactive threat hunting.

Cognito Recall provides visibility into network traffic by extracting security-enriched network metadata from all data packets. Unlimited amounts of metadata are then stored in the cloud for search, analysis and retroactive threat hunting.

Every IP-enabled device on the network is identified and tracked, and data can be stored for any length of time. Captured metadata includes all internal (east-west) traffic, internet-bound (north-south) traffic, virtual infrastructure traffic, and traffic and events in cloud computing environments.



REDUCTION IN WORKLOAD PER 10,000 DEVICES OBSERVED BY INDUSTRY

Industry	Events flagged	Detections	Devices with detections	Critical severity	High severity	Workload reduction
Education	12,666	617	650	11	34	19x
Energy	18,617	598	338	8	16	55x
F&I	19,510	511	361	8	20	54x
Government	9,328	249	268	6	12	35x
Healthcare	15,423	381	411	7	16	38x
Manufacturing	17,064	431	323	6	15	53x
Retail	9,437	421	283	7	24	33x
Services	14,679	430	365	12	20	40x
Tech	18,100	1,193	634	12	23	29x

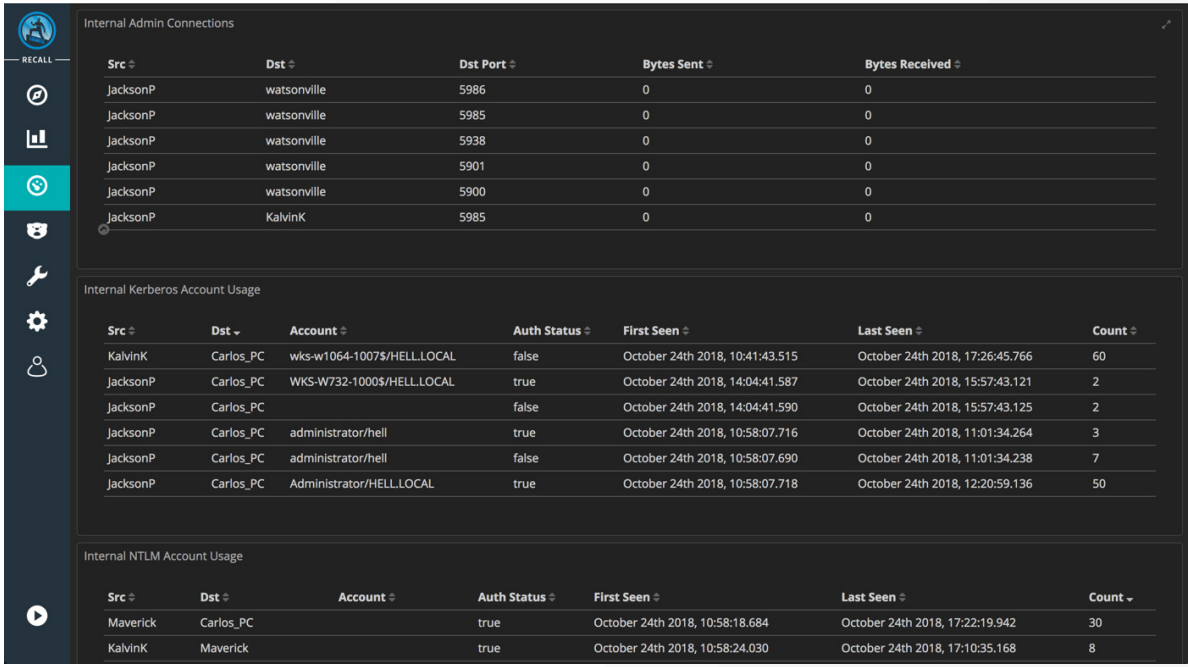
Cognito Detect reduces the workload for Tier-1 security analysts

This visibility extends to laptops, servers, printers, BYOD, and IoT devices as well as all operating systems and applications, including traffic between virtual workloads in the cloud and data centers – even SaaS applications. System authentication and SaaS logs provide context enrichment to network metadata analysis for accurate identification of systems and users.

With full metadata search capabilities and limitless data storage, Cognito Recall enables security analysts to determine whether indicators of compromise exist in metadata, including users, IP addresses and domains.

Cognito Recall also delivers in-depth information for more efficient threat hunting, such as PowerShell commands from a remote machine to a server or a specific type of connection from a remote site.

In some instances, anomalies could consist of any combination of these behaviors, such as unusual amounts of data sent to an uncommon IP address.



Enhanced account-based investigations in Cognito Recall

Leveraging the tight integration between Cognito Recall and Cognito Detect, analysts can create custom detection models and saved searches to tailor specific investigations and detection capabilities to their organizations.

Security analysts can easily follow the chain of related events from attacker detections found by Cognito Detect, third-party security products, and searchable, high-quality threat intelligence in historical network metadata.

When events or alerts are received from Cognito Detect or third-party security products, Cognito Recall ensures that security analysts have a full 360-degree view of all workload and device activity.

Leveraging the tight integration between Cognito Recall and Cognito Detect, analysts can create custom detection models and saved searches to tailor specific investigations and detection capabilities to their organizations.

With Cognito Recall, security analysts can investigate incidents with unprecedented efficiency using complete context about incidents, along with relevant details about associated devices, accounts, and network communications.

Another cornerstone of the Cognito NDR platform, Cognito Stream™ forwards security-enriched metadata to the CNI organization's own data lake or other tools for analysis and archiving. This gives security analysts instant access to the right data and the right context for faster incident investigations.

It extracts hundreds of metadata attributes collected from the cloud to the enterprise and presents the actionable security-enriched network metadata in a compact, easy-to-understand Zeek format.

Cognito Stream provides the details analysts need without NetFlow's problematic storage complexity and the overhead of continuous packet captures and recording. It sets up in less than 30 minutes, requires no performance tuning and no ongoing maintenance.

"Vectra has been an amazing tool for us in establishing a threat hunting initiative."

Security analyst, government organization, North America

By analyzing anonymized metadata shared from hundreds of Cognito NDR platform deployments, Vectra has identified attacker behavior insights that expose tactics that remain open to abuse.

Attacker behavior insights inside CNI organizations

Vectra has enabled hundreds of organizations around the globe to secure their Critical National Infrastructure. The benefits include reducing the risk of a breach, improving the efficiency of security operations, helping to ensure compliance, and extending cybersecurity to cloud operations.

By using AI to automate threat detection and incident response, the Cognito NDR platform enables CNI organizations to condense days, weeks and months of manual security investigations into minutes. This allows SOC teams to take immediate action to prevent damage and theft of their data.

By analyzing anonymized metadata shared from hundreds of Cognito NDR platform deployments, Vectra has identified attacker behavior insights that expose tactics that remain open to abuse. In many cases, these tactics cannot be completely blocked without materially damaging legitimate operations, so early and effective detection and response is essential.

Conclusion

With finite resources available to security teams, AI is increasingly important to the security of CNI. AI does not replace but instead augments people by providing them with security analysis, context, and deep insights at a speed and scale that is impossible for humans to achieve.

CNI security teams must adopt an assumed-compromised mindset and focus on early detection and response to advanced attackers. The AI-powered Cognito NDR platform from Vectra enables CNI SOC teams to identify and respond faster to hidden threats in cloud, data center, IT, and IoT networks.

For more information please visit www.vectra.ai/industries/cni

Email info@vectra.ai vectra.ai

1 The Guardian- Major cyber-attack on UK a matter of 'when, not if' – security chief, 2018
2 M-Trends 2020
3 SANS Institute SANS 2019 Incident Response (IR) Survey, 2020
4 The Hill - Our focus on Russian hacking obscures the real problem, 2017
5 Vectra – 2020 Attacker Behavior Industry Report