VECTRA
SECURITY THAT THINKS

WHITE PAPER

How to Improve ROI and Operational Efficiency for Cybersecurity

COST-EFFECTIVE
OPERATIONAL EFFICIENCY
CLOUD-NATIVE
ENTERPRISE

TABLE OF CONTENTS

Vectra® protects business by detecting and stopping cyberattacks.

As a leader in network detection and response (NDR), Vectra® AI protects your data, systems and infrastructure. Vectra AI enables your SOC team to quickly discover and respond to would-be attackers —before they act.

Vectra AI rapidly identifies suspicious behavior and activity on your extended network, whether on-premises or in the cloud. Vectra will find it, flag it, and alert security personnel so they can respond immediately.

Vectra AI is *Security that thinks*®. It uses artificial intelligence to improve detection and response over time, eliminating false positives so you can focus on real threats.

75-90% **Vectra customers report reductions in time spent on investigations by 75% to 90%, and successfully deferred analysis to IT generalists instead of escalating incidents to higher-paid experts.**

HIGHLIGHTS

- A lack of resources to effectively execute improvements and a shortage of staff and skills are the two biggest impediments facing incident response teams, according to the SANS Institute.
- The Cognito NDR platform uniquely automates security investigations that would normally require hours of manual effort from highly trained security analysts and data scientists.
- With the highest degree of certainty, the Cognito NDR platform discovers security events that would otherwise have gone unnoticed. This leads to a net increase in the number of events and precise and timely incident response.
- By correlating and scoring specific hosts under attack, security teams using the Cognito NDR platform can perform analysis in minutes and eliminate days and weeks of investigation, log reviews, and SIEM-based analysis.
- Automating threat hunting with the Cognito NDR platform ensures that all traffic is inspected, less time is spent on manual investigation and correlation, and all staff members are empowered to rapidly mitigate active threats.

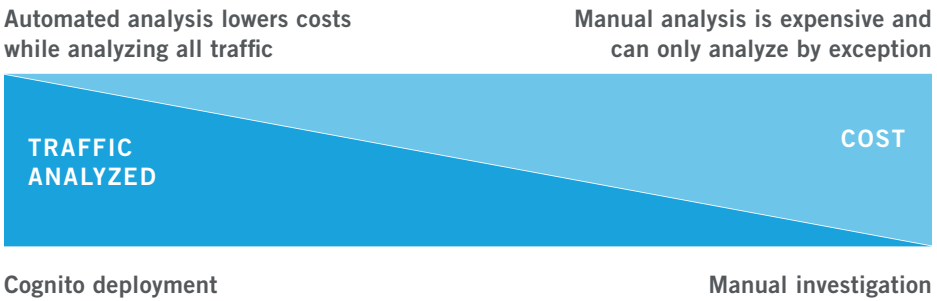
Introduction

IT security is an ongoing exercise in operational efficiency. Organizations have a limited set of resources to address an unlimited set of risks, threats and attackers. This asymmetry means that security products must always be evaluated in terms of security efficacy as well as their impact on the operational fitness of the organization. Does a solution drain on manpower and resources or does it make staff more productive and nimble across cloud, data center, IT, and IoT networks?

The need for efficiency is especially pronounced in the context of modern cyberattacks. Unlike commodity attacks, today's targeted threats are far more damaging and require more time and skill to detect and respond.

In the past, security could solely rely on signatures to automatically deflect thousands of attacks without much thought. But more sophisticated attacks thrive on their ability to evade signatures and other preventive controls. This, in addition to insider threats, has created a need for new security approaches and put a premium on staff with strong cybersecurity skills.

To meet this challenge organizations must be able to automate the detection and response to sophisticated attacks, while making security teams as efficient and productive as possible. The Cognito® Network Detection and Response from Vectra® meets both these demands, and this document focuses on the many ways the Cognito NDR platform helps security teams get the most out of limited staff, time and resources.



Areas of focus

Today, the process of detecting targeted threats in cloud, data center, IT, and IoT networks is manual and expensive. Cognito NDR platform is designed to automate the process and lower costs. The value of Cognito can be illustrated in three ways:

Skill One of the biggest challenges of modern security teams involves recruiting and retaining exceptional security and data science staff. Talent and experience in these fields are rare, yet are required in order to recognize the subtle indicators of attackers that successfully infiltrate cloud, data center, IT, and IoT networks.

Time The most important factor in detecting cyberattacks is time. Attacks must be detected in near real time before key assets are stolen or damaged. Unfortunately, these attacks are also the most time consuming to detect. They require a variety of skills and in-depth investigative know-how to determine the scope of an attack.

Costs Cyberattacks have direct costs that extend beyond time and staffing. Expensive incident response and forensic analysis services are often required after an attack. Cognito helps avoid the cost of third-party incident response and investigations entirely, while lowering dependence on manual log analysis.

A note on the scope of analysis

The scope of this document is limited to savings that Cognito delivers to security teams within an organization. It ***does not*** estimate the total financial impact of a network data breach. Consequently, potential fines, credit monitoring for affected customers, legal fees, brand damage and other costs associated with loss are not factored in.

While these costs are very real, the differences in organizations, the types of data they hold, and the wide range of hard and soft costs of a data breach make estimating the true cost of a breach notoriously difficult.

To meet this challenge organizations must be able to automate the detection and response to sophisticated attacks, while making security teams as efficient and productive as possible.

For example, leading industry research puts the cost of a breached data record anywhere from 58 cents over $201 per record depending on the unique factors of the organization and whose estimates you use. As such, this document does not attempt to identify the full financial benefit of the Cognito NDR platform, but instead focuses on savings for security and IT teams.

Vectra addresses the most critical skills shortages

As security evolves, organizations increasingly find themselves searching for highly specialized and rare sets of skills. Security and data science skills are at the top of the most-wanted lists, making the best in these areas limited and costly. The Cognito NDR platform automates menial tasks at scale, which reduces the overall need for dedicated specialists and makes all members of the existing security team more efficient, productive and focused on higher-level tasks.

The current skills gap

Information security has been the most commonly reported skills shortage for several years. A lack of resources to effectively execute improvements and a shortage of staff and skills are the two biggest impediments facing incident response teams, according to the SANS Institute. In addition to traditional security roles, data scientists are highly sought-after as security team members. This is due in part to increased reliance on data science for everything from getting more value out of SIEMs to building custom behavioral models to detect insider threats.

According to IDG's State of the CIO, data scientists and security staff topped the list of their skills shortage.

Unsurprisingly, the high demand for these rare skills has made cybersecurity analysts and data scientists some of the most highly paid positions in IT. A recent report from Glassdoor found that the average salary for a data scientist was $118,709 compared to $64,537 for a trained programmer.

The most qualified data scientists demand even higher salaries. An analysis by recruiting firm Burtch Works found that the median salary was $175,000 for top individual-contributor data scientists.

Of course, salary is just a portion of the fully loaded cost of an employee, which will be much higher. However, this comparison of salaries gives a view into the premium associated with security and data science talent.

The Vectra value: Using automation to close the skills gap

By automating threat detection through artificial intelligence (AI) and data science, the Cognito NDR platform identifies threats that would be impossible to find through manual investigation, while simultaneously lifting the time and resource burden from security teams.

The intelligence in the Cognito NDR platform is driven by a dedicated team of security researchers and data scientists who focus exclusively on the most advanced cybersecurity techniques and detection strategies.

Vectra researchers analyze millions of malware samples, attack tools and evasion techniques, as well as monitor metadata from participating Vectra customers worldwide to identify the latest trends and attack techniques. The sweeping, global scope of this opt-in data reveals trends that would not be obvious by simply analyzing data.

This global data set continually drives automated analysis in the Cognito NDR platform. Cognito uniquely automates security investigations that would normally require hours of manual effort from highly trained security analysts and data scientists.

As a result, the Cognito NDR platform enables organizations to directly address the most pressing skills shortages in IT security – cybersecurity analysis, incident response and data science. And unlike manual approaches that focus on small amounts of suspicious traffic, the Cognito NDR platform analyzes ***all*** traffic – across cloud, data center, IT, and IoT networks.

A simple analysis shows just how valuable this level of automation can be. The annual license for Cognito NDR platform software to monitor a 500-host network is $25,000 per year. While the actual throughput could vary, we will estimate this 500-host network to generate around 500 megabits per second of traffic.

Based on the previous example, a high-end security analyst and data scientist would cost about $300,000 a year and would only analyze a fraction of the total traffic. The image below is an update of the previous one with more precise metrics about the cost per analyzed gigabit.

Based on this ability to automate analysis, customers can manage security incidents faster and without the need to hire additional expert staff. Deferring hiring can have significant financial value.

YEARLY SAVINGS IN STAFFING COSTS	
New headcount deferred	1
Fully loaded cost for expert talent per hour (NSS Explanation)	$75
Yearly cost	**$156,000**

Time: The most expensive metric in breach detection

Time is the most important factor in the detection of hidden cyberattacks. To mitigate damage, attacks must be detected in near real time before key assets are stolen or damaged. The problem for security teams is that these attacks are the most time-consuming to detect.

Once an attacker bypasses prevention controls at the perimeter, the job of threat detection and response becomes a very manual and time-consuming process. Investigations require a variety of forensic analysis skills – malware analysis, forensic packet and log analysis – and the correlation of massive amounts of data from a wide range of sources. This set of tasks requires a broad and specialized set of skills and a significant amount of time.

Advanced threats have become quite adept at bypassing signatures, sandboxes and other security techniques deployed at the perimeter. Simple investigations into these events can last hours, and a full analysis of an Advanced Persistent Threat (APT) can take days or weeks.

The Cognito NDR platform automates the analysis phase and detects threats immediately. The analysis process integrates many disciplines, including an understanding of malware behavior, evasion techniques, user behavior analysis, and the ability to correlate threats to identify the presence and location of a targeted attack in cloud, data center, IT, and IoT networks.

This approach identifies threats that would otherwise be impossible to find and does so without human involvement. The Cognito NDR platform automatically prioritizes events, explains each phase of an attack, and provides quick access to the source metadata from packets to verify the detected threat.

Each detection maps to the MITRE ATT&CK framework for concise language in communicating attacks as well as prescriptive advice for next steps, enabling security teams to take immediate corrective action. This allows them to condense hours and days of manual effort into minutes and seconds, and take action before damage is done.

The costs of security investigations and incident response

This section offers a basic framework for estimating the cost of investigating security events and incident response. Because no two cases are exactly alike, a variety of industry standards and benchmarks were used to estimate costs. It is possible to edit certain metrics so that they more closely reflect the realities of your organization.

The effort and expense of security investigations can be divided into three phases:

1. **Daily security analysis and investigation** This may include inspection of events and alerts from security solutions, analysis of logs, host-based alerts, and analysis of newly identified or common threats. The end goal is to determine if there is a significant security event. This phase can be particularly time-consuming if the goal is to detect the presence of an APT.
2. **Internal incident response** This phase picks up when a serious security event is identified in the previous phase. It is often dependent on a Security Incident Response Team (SIRT). The SIRT can consist of dedicated personnel or be formed ad hoc from existing staff. This phase continues until the event is contained and remediated, which can last from minutes to months.
3. **External incident response** External incident response services are often contracted in the event of a successful breach. It typically occurs if an attack goes undetected by internal staff or was discovered late in the attack lifecycle.

Each of these areas entails examining similar metrics – namely the frequency of an event, the amount of time it takes for staff to work the event, and the cost of staff time.

Estimated Cost =
Number of events × Time-to-resolution × Staff value

While these factors are common to each phase, actual values will vary based on the phase of analysis. For instance, daily analyses may include a large number of brief investigations, while incident response may include an ongoing investigation over days, weeks or months. Calculations are shown separately for each phase to better account for these differences.

Calculating the cost of daily security analysis

The daily tasks of security investigation and analysis are handled differently by every organization. Whether done by a dedicated team of experts or ad hoc by security generalists, virtually all security products require an investment of time to extract actionable cybersecurity intelligence. The analysis should identify if there are security events that require further inspection and response.

Analyzing the time spent on daily security activities requires an estimate in the amount of time per day spent investigating and analyzing events. This can be performed by a variety of staff with different levels of experience and expertise.

Hourly staff rate These calculations use the default rate of $75 per hour to estimate the cost of a team member. This rate is used to estimate the fully loaded cost of an experienced security engineer to determine the total cost of ownership (TCO) of a security solution.

The table below provides a very simple estimate of investigation costs for a small enterprise, using modest assumptions.

STAFF COSTS OF DAILY ANALYSIS	
Percentage of day spent on investigations	20%
Number of staff involved in investigations	2
Average hours per year spent on investigation	832
Average hourly wage for staff	$75
Yearly cost	**$62,400**

The Vectra value

The Cognito NDR platform consolidates and automates the identification of active threats inside a cloud, data center, IT, and IoT networks. Detections can consolidate dozens to hundreds of underlying events and metadata samples to provide a final diagnosis.

Furthermore, each event is scored and prioritized based on its threat, certainty and phase of the attack lifecycle. This makes it easy for staff to distinguish adware botnets and other lower-priority threats from active targeted attacks that aim to steal corporate assets.

This automation offers two benefits – security teams can perform investigations in less time and non-expert staff can handle more investigations.

Vectra customers have reported reductions in time spent on investigations by 75% to 90%, and have successfully deferred analysis to IT generalists instead of escalating incidents to higher-paid experts. The analysis below takes a conservative 50% reduction to the time of analysis and reduces the average hourly wage from $75 to $55. Compared to the previous baseline, this leads to a savings of $39,520 and a 63.3% reduction in costs.

STAFF COSTS OF DAILY ANALYSIS WITH VECTRA	
Percentage of day spent on investigations	10%
Number of staff involved in investigations	2
Average hours per year spent on investigation	416
Average hourly wage for staff	$55
Yearly cost	$22,880
Yearly savings	**$39,520**

Calculating the costs of internal incident response

The incident response volume and process varies greatly, depending on the organization. The SANS Institute study of enterprise incident response was used to set reasonable baselines.

The study collected incident response data from over 250 companies and includes the frequency of events and overall time to containment. It also found that most organizations experienced security incidents, including some smaller companies with under 100 employees.

Number of incidents Most organizations reported between one and 25 incidents, with the most active environments reporting over 500. A conservative estimate with an average of 17 incidents per year, per organization was used, based on the SANS data.

Time to containment There was a wide variance in the time to containment. The most common response time was between six and eight hours, while the longest took more than six months. Only the most commonly reported categories were used to prevent the skewing of data, producing an average time to containment of 29 hours.

STAFF COSTS OF INTERNAL INCIDENT RESPONSE	
Number of events per year	17
Average time to containment in hours	29
Number of staff on SIRT team	3
Average hourly wage	$75
Yearly staff costs of SIRT	**$110,925**

The Vectra value

In addition to detecting hidden signs of a threat, the Cognito NDR platform correlates the multiple phases of an attack to specific hosts and workloads and identities/accounts that are under attack. The ability to condense massive amounts of data down to a few specific hosts, workloads, identities, and accounts is most critical to the rapid containment of a threat.

It is important to remember that most network intrusions remain undetected for an average of 56 days, according to the 2020 Mandiant M-Trends report. And according to the SANS Institute study, once a threat is detected, the time to containment can take days to months.

The Cognito NDR platform dramatically reduces both of these figures. The analysis by Vectra is limited to the direct comparison of incident response efforts to ensure a proper apples-to-apples comparison.

With the highest degree of certainty, Cognito NDR platform discovers security events that would otherwise have gone unnoticed. This leads to a net increase in the number of events and precise and timely incident response. While many of these events are managed automatically, Cognito NDR platform accounts for a doubling in the number of events detected.

The Cognito NDR platform also vastly reduces the amount of investigation needed to diagnose hosts, workloads, identities, and accounts that require remediation. By correlating and scoring specific hosts, workloads, identities, and accounts under attack, security teams using Cognito NDR platform can perform analysis in minutes and eliminate days and weeks of investigation, log reviews, and SIEM-based analysis.

Once again this data is based on real-world examples from Vectra customers who reduced their average time to containment to 30 minutes or less. The calculations below are conservative estimates to reduce the overall time to containment to three hours. ***These assumptions reduce the cost of incident response by $87,975, which maps to a savings of 79.3%.***

STAFF COSTS OF DAILY ANALYSIS WITH VECTRA	
Percentage of events per year	34
Average time to containment in hours	3
Number of staff on SIRT team	3
Average hourly wage	$75
Yearly staff costs of SIRT	$22,950
Yearly savings	**$87,975**

Calculating the costs of external incident response

To establish baselines for external incident response fees, we referenced publicly available contracts for incident response services and published reports. In these cases the hourly rates for services hovered close to $400 per hour, and the overall costs typically fell between $200,000 and $500,000.

Mandiant charged the state of South Carolina $386/hour, resulting in a total cost of $500,000.

COSTS OF EXTERNAL INCIDENT RESPONSE	
Hourly rate of outside incident-response staff	$400
Total billable hours	500
Cost of third-party incident response	**$200,000**

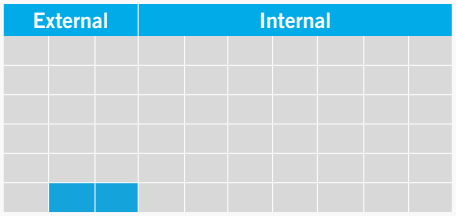
The Vectra value

While not every organization experiences such a charge in a given year, these numbers do represent real-world costs of external incident response in the case of a major undetected breach.

The core value of the Cognito NDR platform is to proactively detect advanced threats and stop network breaches before data is lost or damaged. To estimate values, Vectra chose the low end of the incident response service costs and amortized the risk over a four-year period. This equates to a savings of about $50,000 per year.

Manual approach

Traffic analyzed



Traffic is analyzed by exception
- Primarily focused on perimeter traffic
- Often triggered by suspicious or inconclusive signature or sandbox results
- Opportunistic

Active detection phase

Hours, days, weeks of investigation

×

High-paid, specialist talent ($75 - $100/hour)

Manual use of best talent
- Requires highly trained staff
- Mix of very rare skills (Malware, traffic, data science)
- Quickly saturated (does not scale)

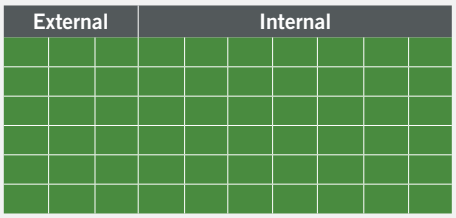
Post-mortem IR phase

- **Very expensive**
- **$400/hour**
- **$200,000 to $500,000**
- **Damage is done**

Penalty phase
- Very expensive
- Open-ended investigation
- No opportunity to mitigate

Vectra approach

Traffic analyzed



Full inspection of traffic
- All traffic analyzed for malicious actions
- N-S and E-W traffic
- Detects all phases of an attack
- Cloud logs

Active detection and response phase

Real-time detection (seconds)

↓

Prescribes next steps for general IT staff

Automated, actionable detections
- Investigations condensed to seconds
- Remediation performed automatically or by IT generalists

Post-mortem IR phase

- **Very expensive**
- **$400/hour**
- **$200,000 to $500,000**
- **Damage is done**

Penalty phase AVOIDED
- Threats proactively managed

Summing it up

This paper offers a basic approach for estimating the operational costs of security investigations and the savings that can be achieved by deploying the Cognito NDR platform in cloud, data center, IT, and IoT networks.

The Cognito NDR platform provides substantial yearly savings in the following key areas:

CATEGORY SAVINGS	
Security and data science headcount	$156,000
Time savings of daily security operations	$39,500
Time savings of incident response	$88,000
Avoidance of third-party incident response	$50,000
Total	**$333,500**

These savings naturally scale in larger organizations with larger security teams. Automating threat hunting with the Cognito NDR platform ensures that all traffic is inspected, less time is spent on manual investigation and correlation, and all staff members are empowered to rapidly mitigate active threats.

Conclusion

New types of threats naturally require new types of security. But most security products require a significant investment in human time and talent in order to deliver value. Organizations are often full of security products that were either never fully deployed or simply aren't used because the staff can't support them.

The Cognito NDR platform from Vectra is one of the few cost-effective solutions that finds threats that others can't while saving time, headcount, and money for security organizations.

By automating the time-consuming tasks required to investigate cyberthreats, the Cognito NDR platform is expressly designed to serve the needs of security teams and not the other way around. This lets organizations build an efficient security architecture – across cloud, data center, IT, and IoT networks – removes bottlenecks and empowers all members of the IT and security staff to detect and respond faster to hidden cyberthreats.

For more information about Cognito Detect and how to improve ROI, please contact a service representative at sales-inquiries@vectra.ai.

Email info@vectra.ai vectra.ai