IDC ANALYZE THE FUTURE

The Business Value of Cognito Network Detection and Response from Vectra

RESEARCH BY:

Christopher Kissel
Research Director
Security & Trust Products, IDC

Matthew Marden
Research Director
Business Value Strategy Practice, IDC

December 2020 | IDC Doc. #US47016020

Navigating this White Paper

Click on titles or page numbers to navigate to each section.

BUSINESS VALUE HIGHLIGHTS

Click on highlights below to navigate to related content within this white paper.

>4.5:1 ratio
of quantified benefits to investment costs

5 months
to payback

63% lower
risk of major security event

Almost 3x more
threats proactively identified

85% more
efficient in identifying actual threats

57% fewer
impactful security breaches

>2x higher
productivity, impacted security operations team members

Executive Summary

In 2020, digital transformation was forced upon the majority of the world's businesses as COVID-19 caused an exodus from an on-premises workforce to a remote worker reality. In IT/SecOps, that means new VPNs, a stronger emphasis on identity access management and data security, and a different mechanism for users to access applications.

What does not change is the way the adversary conducts business. The enterprise network now stretches horizontally and visibility over a wider attack surface becomes difficult. Regardless of location, whether on premises or in the cloud, the network is becoming especially complex. Increasingly, the network includes direct access to SaaS applications in addition to company-owned applications in the datacenter and cloud—at the same time, VPNs and ingress/egress points require attention. Meanwhile, the security operations center team is receiving inputs from multiple security point products (each generating multiple and/or false alerts) or is trying to investigate unusual activities in the network (new domains accessed, strange port activity, or bottlenecks that may or may not be benign security issues).

Vectra has considered how network and cloud metadata can be curated and enriched to bring greater visibility into the heterogeneous network, monitor hosts and accounts to detect the subtle but immutable behaviors of active attackers, and apply supervised, unsupervised, and deep learning to network and cloud activity to lead security operations center analysts to conduct investigations based upon probabilistic outcomes of threat and certainty.

IDC spoke with organizations with enterprise-level operations across disparate locations and industry sectors about their use of the Cognito platform from Vectra to secure their IT environments. These Vectra customers reported benefiting from substantial improvements in their security capabilities through artificial intelligence (AI)-driven threat detection, prioritization, and response, which enable them to greatly reduce business risk.

For these organizations, enhanced security capabilities and reduced risk create value that IDC calculates will save $2.62 million per organization ($108,700 per 1,000 users of IT services) in the following ways:

- **Identifying, prioritizing, and addressing security threats** more proactively, effectively, and efficiently
- **Minimizing business risk** by reducing the frequency, duration, and impact of security breaches and unplanned outages
- **Empowering IT security teams** to work more efficiently and effectively and to handle increasingly large and complex networking and data environments while freeing up time and resources to focus on other security- and business-related projects
- **Reducing security-related and IT costs** by retiring certain security solutions, consolidating on the Cognito platform from Vectra, and enabling use of cloud solutions

Situation Overview

The proper cybersecurity posture does vary depending upon the type of business that the software/hardware is designed to protect, but unfortunately the biggest flaws in cybersecurity are nearly universal:

- A shortage of cybersecurity analysts creates a chasm in coverage and churn among analysts as companies compete for talent.
- Best-in-breed point products are effective at finding known threats or simple anomalies, but often without context or prioritization. Alerts without context are all but meaningless.
- The sudden digital transformation caused by COVID-19 changes networking in a fundamental way. The workforce becomes remote and gathering and unifying telemetry, never easy, is harder still.

Ultimately though, sensitive data (personally identifiable information, intellectual property, etc.) has its own gravity, the cloud has an edge, network layers contain flow data and file types, and devices have unique properties — all important to understand and protect. However, data, cloud, flow data and files, and devices all require visibility, and this can be achieved from the vantage point of the network, which connects them all. When understood properly, the network reveals which hosts and accounts are most vulnerable, and even after much obfuscation, analytics applied to the network can isolate the signal from the noise to determine whether there is an attacker — and attack vector — and what to do about it.

When understood properly, the network reveals which hosts and accounts are most vulnerable, and even after much obfuscation, analytics applied to the network can isolate the signal from the noise to determine whether there is an attacker — and attack vector — and what to do about it.

Overview of Cognito Platform from Vectra

Vectra uses sensor-driven technology that extracts relevant metadata from traffic or relevant logs from the cloud, including SaaS and IaaS, datacenter hypervisors, enterprise environments, and IoT devices. Vectra offers Cognito, which is its network detection and response platform, and Cognito Detect for Office 365. These capabilities are critical as endpoint detection and response (EDR) platforms are dependent upon compatible devices, security information and event management (SIEM) is unwieldy, and many security point products designed for a flatter architecture are kludgey when taking in flow data from public cloud environments.

Cognito uses a combination of supervised and unsupervised learning. Cognito uses a combination of over 40 supervised detection models (e.g., random forests, long short-term memory [LSTM] deep learning models) to detect attacker behaviors that are consistent in any enterprise environment. Unsupervised learning deploys 11 different machine learning algorithms that help determine peer groups, statistical baselines for end-user network behavior, and models designed to look specifically for activities germane to what an attacker might do. Deep learning and neural networking add decision tree, random forests, K-means clustering, and other metrics that could be described as a way to unify supervised/unsupervised learning and to account for relational elements in the network even through changing conditions such as network bursts, power outages, and end users leaving and entering the network. The depth of analytics is not confined to the network layer; another 20-plus learning models assess Office 365 and Azure Active Directory for anomalies.

Ultimately though, Vectra provides visibility for security analysts, prioritizes alerts, presents the information for an optimal investigation, and then, indirectly or directly through integrations, initiates the proper response. Security tools are thought to do this in theory; we found Vectra was strong in practice.

Vectra provides visibility for security analysts, prioritizes alerts, presents the information for an optimal investigation, and then, indirectly or directly through integrations, initiates the proper response. Security tools are thought to do this in theory; we found Vectra was strong in practice.

The Business Value of Vectra

Study Demographics

IDC interviewed individuals at nine organizations with significant knowledge about the impact of Cognito from Vectra on the effectiveness of their security operations and efforts. As shown in Table 1 (next page), these were organizations characterized by enterprise-level operations in terms of number of employees (>24,000 employees on average) and annual revenue (>$19 billion). Most interviewed Vectra customers have either an international presence in multiple markets or a substantial regional presence, which generates the business need to ensure robust security across disparate operations. Interviewed organizations provided perspectives on the impact of using Cognito from varied industry verticals, namely, financial services (2), retail (2), education, entertainment, software, technology, and transportation.

TABLE 1

Firmographics of Interviewed Vectra Customers

	Average	Median
Number of employees	24,128	5,500
Number of IT staff	1,031	250
Number of business applications	151	125
Number of terabytes (TB)	1.07 million	2,000
Revenue per year	$19.19 billion	$5.0 billion
Countries	United States (7), Germany, and United Kingdom	
Industries	Education, entertainment, financial services (2), retail (2), software, technology, and transportation	

Source: IDC, 2020 | n = 9

Choice and Use of Cognito from Vectra

Study participants described various reasons for choosing to deploy the Cognito platform from Vectra. Overall, purchase decisions related back to the recognition that the participants were missing critical capabilities in terms of identifying and addressing actual security threats to their business operations. For the most part, interviewed Vectra customers deployed the Cognito platform as an additive solution to their security environments that already included various other vendor solutions as well as technologies such as next-generation firewalls. All interviewed organizations reported using Cognito Detect from Vectra, with about half using Cognito Stream and Cognito Recall.

Interviewed organizations cited the power and efficiency of Cognito's AI- and data science-driven ability to identify, prioritize, and address security threats as driving their decisions to deploy the platform. They realized that increasing numbers of potential threats and data meant that they needed new functionality to identify actual threats; their existing approaches were no longer effective in terms of either minimizing risk or allowing their security teams to work efficiently.

Interviewed organizations cited the power and efficiency of Cognito's AI- and data science-driven ability to identify, prioritize, and address security threats as driving their decisions to deploy the platform.

Interviewed organizations spoke in specifics about their reasons for choosing Cognito from Vectra:

→ **Best in breed, depth of analysis:**
"We had a need for best-in-breed technologies within the space that we were looking for coverage …. We chose Vectra because of the depth of the analysis and the data science behind the algorithms. Rather than being just signature based, they were more holistic."

- **Most functional in detection, effective for regulatory compliance:**
  "Vectra was the best solution in terms of detection of anomalies, as well as for compliance with all data protection and privacy regulations. Vectra was also easier to integrate with other security solutions and didn't stress our other protocols."

- **Outperformed competitor in POC:**
  "We did a vendor RFP with multiple vendors and went with Vectra …. They performed the best when we did a bake off. In terms of security performance, they were far superior to the other [vendor POC finalist]."

Table 2 provides details about study participants' use of the Cognito platform from Vectra. As shown, they are using it to secure and provide threat identification and response capabilities across significant IT and business environments, including an average of 403 sites and branches and 664 physical servers running more than 5,700 virtual machines. The criticality of Cognito to these organizations is reflected in an average cost per hour of a serious security breach or unplanned outage of $884,000 in lost revenue and productivity as well as remediation costs, not to mention potential reputational and regulatory damage that is less easily quantified.

TABLE 2

Interviewed Organizations' Use of Cognito from Vectra

	Average	Median
Number of business applications	140	120
Number of sites/branches	403	50
Number of user devices	8,663	5,175
Number of other endpoints	9,389	5,000
Number of physical servers	664	400
Number of virtual machines	5,725	5,500
Potential cost per hour of serious security breach/unplanned downtime	$884,000	$300,000

Source: IDC, 2020 | n = 9

Quantifying the Business Value of Vectra

Interviewed organizations reported that they have substantially improved their ability to identify, prioritize, and respond to actual security threats with Cognito from Vectra. As a result, they have reduced costs and business risk associated with security breaches and unplanned downtime.

Meanwhile, their security teams benefit from automation and AI-driven functionality to work more efficiently and effectively. For study participants, these benefits link back to the much enhanced functionality that Cognito from Vectra enables in terms of recognizing and addressing threats.

Interviewed organizations spoke to the impact of Vectra on their security and business operations:

- **Speed to investigate alerts:**
  "The speed to investigate on alerts is absolutely a key benefit with Vectra. That was quite problematic for us; it took two hours to figure out what an alert meant and how to get to the bottom of it. We've brought that down to minutes with Vectra. The quicker we react, the less the damage to the corporation. Anybody that asks me, I will say that is one of the key reasons why I would choose Vectra."

- **Improved ability to identify network intrusions:**
  "With Vectra, we have been able to detect pretty much any type of intrusion into our network, including the stuff that we actually pay for—that is, stress testing our network security. We're detecting everything with Vectra—100%. Before using Vectra, we were not detecting anything coming from the vendor we are paying to test our security."

- **Faster identification to reduce risk:**
  "On the business side, the most significant benefits of Vectra for us are identifying misconfigurations and identifying rogue systems that shouldn't be on the network .... With Vectra, we've minimized the severity of security events because it gives us quicker identification of security events before they get really bad."

Interviews with Vectra customers demonstrated the strong value they are achieving, reflected in security-related staff and cost efficiencies, as well as tangible value gained by minimizing risk associated with security breaches and unexpected outages.

Overall, IDC projects that study participants will realize average annual value of $2.62 million ($108,700 per 1,000 users) (see Figure 1 next page) that is nearly evenly divided between:

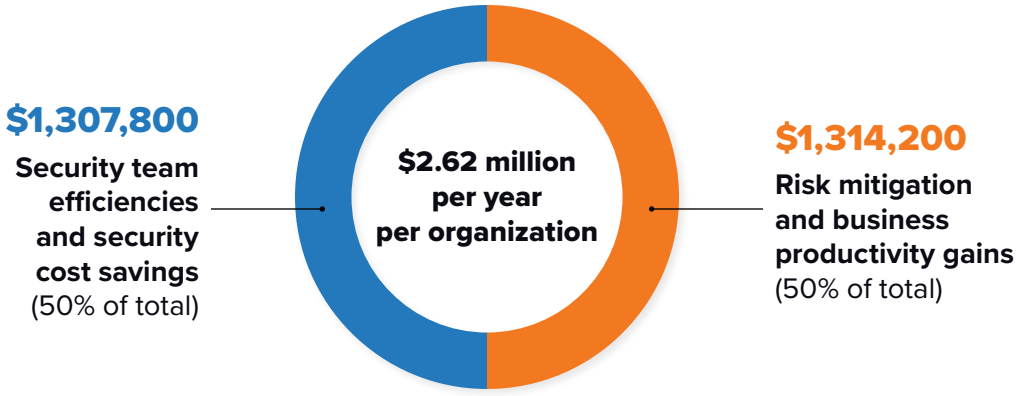
- **Risk mitigation and business productivity gains:**
  Study participants have not only significantly reduced exposure to business risk that could carry hundreds of thousands or millions of dollars of costs but also markedly lowered costs to their business in terms of lost employee productivity. IDC calculates that interviewed Vectra customers will on average gain $1.31 million per organization ($54,500 per 1,000 users) in higher user productivity by reducing the frequency, duration, and impact of security breaches and unplanned outages.

- **Security team efficiencies and security cost savings:**
  Study participants have also realized substantial efficiencies for their core security operations teams, including incident management and network security analyst teams, through AI-enabled functionality of Cognito that enables more targeted, efficient, and ultimately successful threat identification and remediation efforts. IDC estimates that these security staff productivity gains alongside security solution cost reductions will be worth an average of $1.31 million per organization ($54,200 per 1,000 users).

Interviews with Vectra customers demonstrated the strong value they are achieving, reflected in security-related staff and cost efficiencies, as well as tangible value gained by minimizing risk associated with security breaches and unexpected outages.

FIGURE 1

Average Annual Benefits per Organization



Source: IDC, 2020 | n = 9

Enhanced Security Capabilities

Minimizing business risk associated with security breaches and unplanned operational interruptions is directly tied to study participants' ability to rapidly identify, prioritize, and address actual security events. For interviewed organizations, trying to separate out real threats in a timely and accurate way is a major challenge. With huge volumes of data and large numbers of users accessing their networks, arriving at actionable conclusions about potential threats can become either impracticable given resource constraints or infeasible without the ability to accurately prioritize potential threats. For interviewed Vectra customers, this is where the AI- and data science-driven functionalities of the Cognito platform positively impact the basic foundations of their abilities to ensure security.

Chief among interviewed organizations' challenges is that their security teams are swamped with too much information about too many potential threats, without a clear means of prioritization. This can cause substantial amounts of staff time to be misallocated in investigating non-threats and can allow more actual threats to slip through the cracks as resources are directed elsewhere.

Study participants explained that Cognito from Vectra changes this dynamic by robustly prioritizing actual threats, allowing for more non-threats to be ignored, thereby enabling more targeted and useful investigations by security teams:

→ **Ability to investigate more, proactively identify actual threats:**
"We're constantly investigating threats. With Vectra, we're probably investigating 100 threats for every 1 real security threat. We're investigating a lot more now with Vectra because it's easier. Previously, it was less than 20 to one because we couldn't find them .... With Vectra, we're proactively identifying probably 98% of threats compared with a lot less—probably 25%."

We're investigating a lot more now with Vectra because it's easier. Previously, it was less than 20 to one because we couldn't find them...."

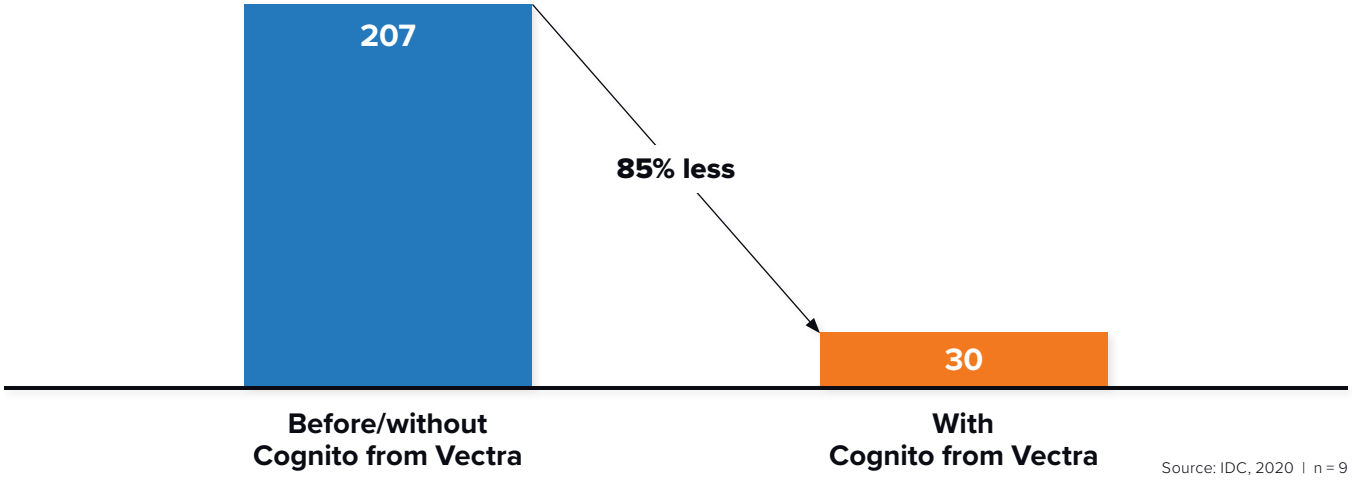
→ **Telemetry enables substantial improvements in investigative capabilities:**
"Vectra gives us a completely different view that we didn't have before .... We are investigating more with Vectra—probably 10% of what we cover without Vectra. What was happening before is unquantifiable because we didn't have that telemetry."

As shown in Figure 2, Cognito from Vectra enables security teams to target their investigations much more effectively and robustly with enhanced prioritization. Study participants reported a much lower ratio of investigated threats to actual security threats, demonstrating the efficacy of the Cognito platform in helping them focus on issues that are more likely to become impactful events. On average, interviewed Vectra customers reported lowering this ratio by 85%, bringing down the ratio from over 200:1 to 30:1 in terms of investigated threats to actual security events.

FIGURE 2

Ratio of Investigated Threats to Actual Impactful Events

(Ratio of investigated threats to threats that become security events)



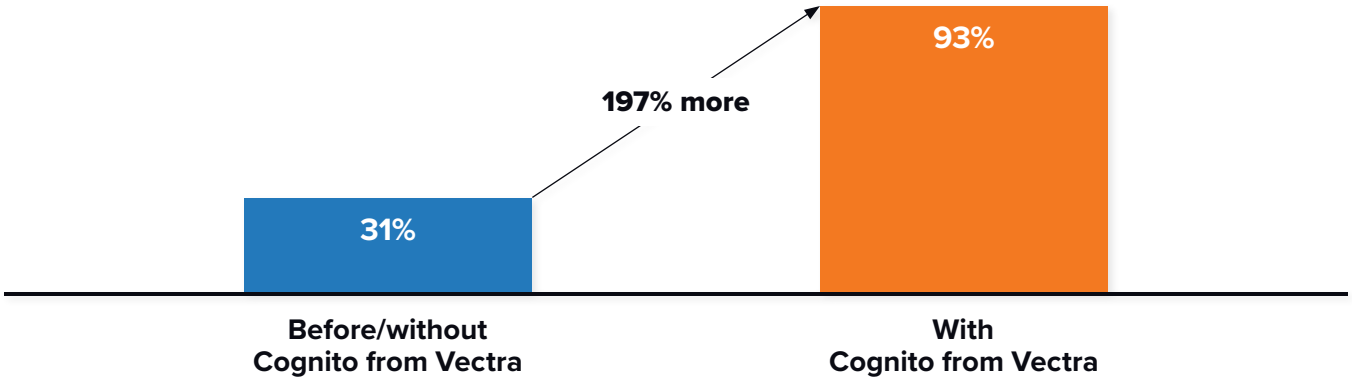
Source: IDC, 2020 | n = 9

The ability with Cognito from Vectra to prioritize threats more effectively as well as AI- and data science-driven prioritized alerting functionalities also enable study participants to take a more proactive approach in terms of threat identification and resolution. One interviewed organization commented: *"What's really nice about Vectra is that it really points out lateral attacks. So if a machine gets attacked and it's starting to go through a mirror attack, Vectra is really great at doing a scan and finding vulnerable machines."* Another noted its ability to be more proactive in remediation: *"Before Vectra, an investigation would realistically take about 2 hours. If something was malicious, it would be able to encrypt pretty much our whole estate. Now, we know in minutes, and then we can automatically isolate that endpoint or that server, which means that containment is very quick."* Figure 3 (next page) demonstrates the substantial impact that the Cognito platform has had on study participants' ability to proactively identify actual threats, going from only around one-third (31%) to nearly all actual threats (93%), which is nearly a threefold (197%)increase in threats proactively identified.

FIGURE 3

Success in Proactively Identifying Threats

(Percent of threats proactively identified before becoming security incident)



Source: IDC, 2020 | n = 9

Study participants also linked their ability to effectively remediate security threats or events to their use of Cognito from Vectra, especially in terms of rebuilding servers or workstations. One study participant noted: *"To rebuild workstations/servers when a security event impacts our systems—and we have to rebuild—we're talking about 5 or 6 people for about a week, 100%, with Vectra. Before Vectra, it would probably be like 10 people working on it for a couple of weeks, 100% before we could restore service."* Overall, interviewed Vectra customers reported completing these types of rebuilding efforts 39% faster on average, enabling a fast return to full functionality for affected infrastructure and environments.

Reduced Business Risk

Study participants reported that as a result of enhanced security capabilities achieved with Cognito from Vectra, they have greatly reduced their exposure to business risk. They explained that limiting risk carries benefits that are very tangible—that is, reduced cost to their businesses of lost employee productivity associated with security breaches and unplanned outages—as well as less immediately tangible reputational damage that can have huge potential business ramifications and costs.

Interviewed Vectra customers reported that a major security event or unplanned outage carries average costs of almost $1 million per hour ($884,000) in terms of lost revenue and productivity, as well as costs to address and remediate the problem. Study participants uniformly linked their use of Cognito from Vectra to greatly reducing risk associated with these types of major events. One study participant explained: *"Every quarter, I present to the board the risk and threats that we see regarding the ones we had to take actions, and the ones that we didn't have to take actions because they were prevented …. A serious security breach could potentially cost us millions of dollars and we've reduced that risk by close to 100% with Vectra."* Thus, through effective prioritization with Cognito, study participants can more effectively intervene to limit potential damage associated with these types of events.

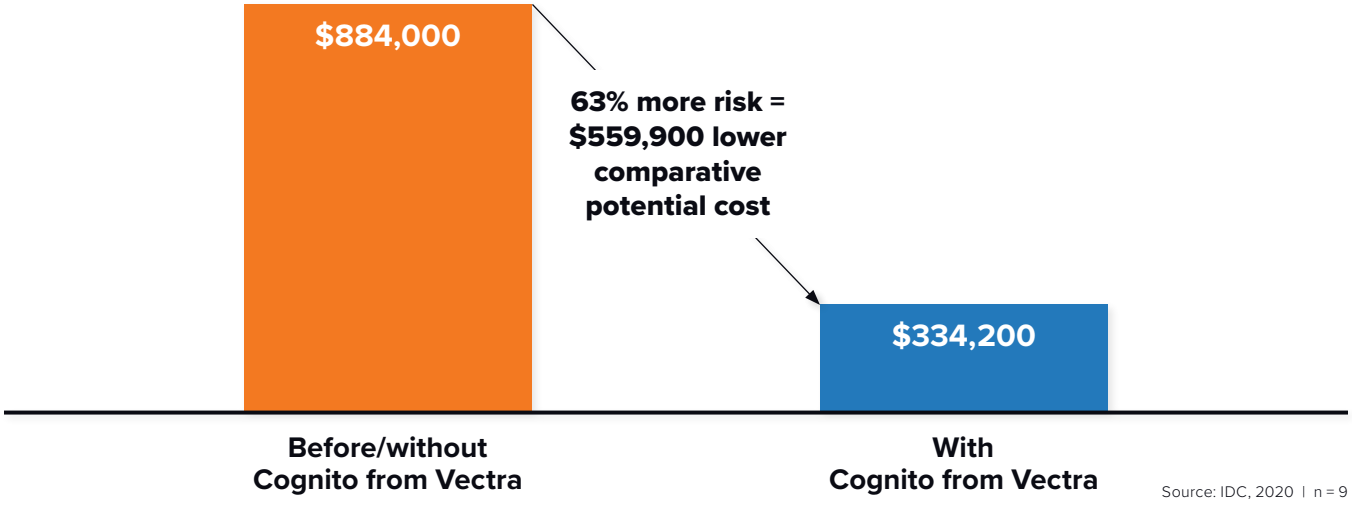
"A serious security breach could potentially cost us millions of dollars and we've reduced that risk by close to 100% with Vectra."

On average, study participants told IDC that they have reduced the likelihood of suffering a major security event or unplanned outage by 63% with Cognito from Vectra. As shown in Figure 4, such risk minimization brings down the imputed cost of such an event by $559,900, demonstrating the major value for study participants of limiting business risk from these types of impactful, major security events. This type of risk minimization also reflects well on the overall efficacy of their security programs, which are first and foremost focused on avoiding these types of security-related events.

FIGURE 4

Success in Proactively Identifying Threats

($ cost per impactful security event/unplanned outage)



Source: IDC, 2020 | n = 9

Study participants also linked their use of Cognito from Vectra to significant reductions in costs associated with security breaches and unplanned outages that are impactful but not worst-case scenarios. They attributed these benefits to the same enhancements in security functionality already discussed, including more targeted, proactive, and effective threat identification, prioritization, and remediation. One interviewed organization commented: *"Vectra provides visibility and information into network health and use and identifies file-sharing incidences that shouldn't be happening. Because it's giving that visibility, we're able to address those activities, and that helps prevent breaches and threats because we see them before they become a problem."* Another interviewed Vectra customer noted: *"Vectra gives us a completely different view that we didn't have before .... Before Vectra, we might have picked up a threat later in the attack chain or incident life cycle. With Vectra, we see it a lot earlier and can investigate and resolve something before it ever becomes an incident."*

Table 3 demonstrates the extent to which study participants have actually reduced the frequency and impact of impactful security breaches, bringing down their frequency by an average of 57%, needing 75% less time to respond, and losing an average of 89% less productive employee time to security breaches.

TABLE 3

Impact on Security Breaches

Average per Organization per Year	Before/ Without Cognito from Vectra	With Cognito from Vectra	Difference	Efficiency with Cognito from Vectra
Number of impactful security breaches per year	11.9	5.1	6.8	57%
Mean time to repair (MTTR, hours)	13.2	3.3	9.9	75%
Hours of lost productivity per user per year	1.1	0.1	1.0	89%
Value of lost productive time per organization per year (FTEs)	14.4	1.6	12.8	89%
Value of lost productive time per organization per year	$1.01 million	$0.11 million	$0.90 million	89%

Source: IDC, 2020 | n = 9

Likewise, Table 4 shows the impact of Cognito from Vectra on unplanned outages affecting employees using business applications. On average, study participants reported losing 85% less productive time due to these types of outages.

TABLE 4

Impact on Unplanned Downtime

Average per Organization per Year	Before/ Without Cognito from Vectra	With Cognito from Vectra	Difference	Efficiency with Cognito from Vectra
Number of impactful unplanned outages per year	31.1	17.9	13.2	43%
Mean time to repair (MTTR, hours)	7.2	5.8	1.4	20%
Hours of lost productivity per user per year	0.6	0.1	0.5	85%
Value of lost productive time per organization per year (FTEs)	7.9	1.2	6.7	85%
Value of lost productive time per organization per year	$550,400	$81,200	$469,200	85%

Source: IDC, 2020 | n = 9

Security Team Efficiencies

Study participants described leveraging the Cognito platform from Vectra to make their security teams much more effective and productive. These gains are reflected in significant improvements in security KPIs as well as reduced exposure to business risk, but also in terms of these teams' ability to handle more expansive security environments with increased efficiency and accuracy. Interviewed organizations also noted that use of Cognito has freed up security team members to do higher-value work.

Efficiencies for security operations teams relate to capabilities gained from use of Cognito from Vectra, including the delivery of timely and actionable insights about potential threats based on AI- and data science-driven analysis. As a result, security teams have more signal and less noise as they prioritize and address actual threats, which not only saves time but also frees them up to either handle broader environments or support other security and business projects.

Security teams have more signal and less noise as they prioritize and address actual threats, which not only saves time but also frees them up to either handle broader environments or support other security and business projects.

Interviewed organizations described with specificity how Cognito from Vectra helps their security teams work more efficiently and effectively:

- **Repurpose staff time from manual correlation work:**
  "We've moved 50% of three people's time to other things with Vectra … [because it] correlates many events and identifies relationships between events. It's something that you can't do manually without a lot of work."

- **Ability to monitor full ecosystem:**
  "With Vectra, we can monitor all 21,000 devices on our network. Before, we were doing the best we could, but only monitoring around 15% of devices. I can't imagine humans doing what Vectra does."

- **SOC efficiencies:**
  "Vectra helps with our security efficiency because it handles detection activities, so we can get by with a Level 1 analyst instead of having a Level 3 analyst to find these things. [As a result], we can basically get rid of our managed security operations center, for which we pay like $200,000/year."

Table 5 (next page) summarizes the positive impact of the Cognito platform from Vectra on interviewed organizations' security teams. Overall, IDC found that study participants require 51% less staff time on average to secure equivalent environments with Cognito, including 57% average efficiencies for network security analyst teams and 41% average efficiencies for incident management teams. This level of efficiency can also be viewed as a productivity gain of more than two times (103% more productive), reflecting their ability to work in a more targeted and efficient manner. This not only allows affected security teams to provide higher-quality security services but also frees up staff time to support business operations more broadly.

TABLE 5

Impact on IT Security Teams

Average per Organization per Year	Before/ Without Cognito from Vectra	With Cognito from Vectra	Difference	Efficiency with Cognito from Vectra	Productivity Gain with Cognito from Vectra
Incident management teams per organization per year (FTEs)	8.0	4.8	3.2	41%	69%
Network security analyst teams per organization per year (FTEs)	12.3	5.3	7.0	57%	132%
Overall impacted IT security teams per organization per year (FTEs)	23.5	11.6	11.9	51%	103%
Staff time required (per FTE basis)	3,809	1,880	1,929	51%	103%
Value of staff time required for equivalent effectiveness per organization	$2.35 million	$1.16 million	$1.19 million	51%	103%

Source: IDC, 2020 | n = 9

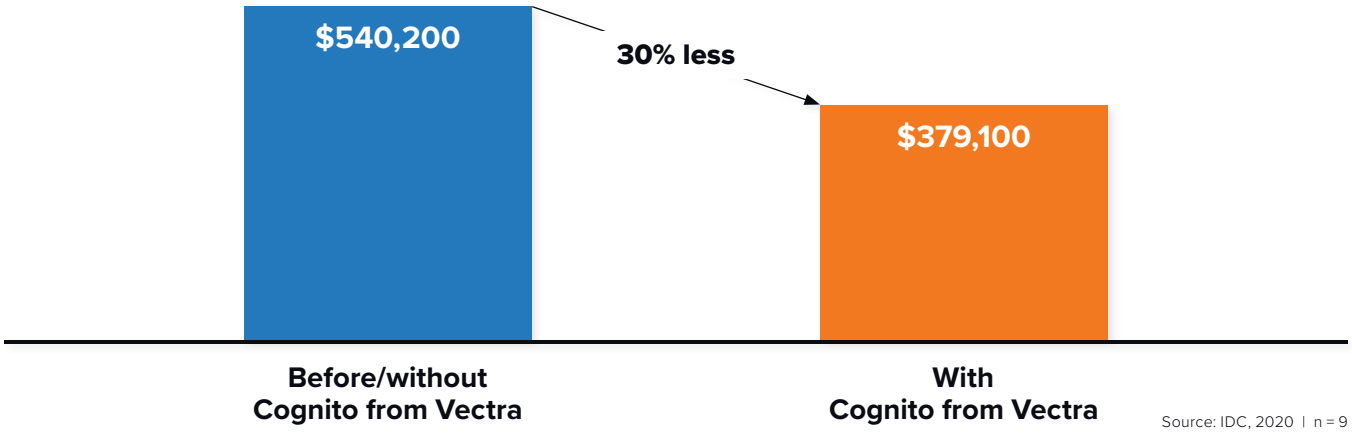
Security-Related Cost Savings

Interviewed Vectra customers also attributed security-related cost savings to their use of the Cognito platform. As an initial matter, use of Cognito from Vectra has allowed them to retire certain other security solutions as they consolidate on the more functional Cognito platform. As shown in Figure 5 (next page), IDC calculates that study participants have lowered their direct costs of security tools by 30% with Cognito, saving an average of over $150,000 per year per organization. Further, study participants also connected their use of Cognito to the ability to leverage cloud environments to capture additional cost savings related to infrastructure and staff time: *"Vectra helps us move more effectively to the cloud because we're setting up a lot of our traffic and compute in the cloud. We have Vectra monitoring a lot of the cloud attacks and cloud traffic—it's going to help us do that."*

FIGURE 5

Annual Cost of Security Tools

($/year)



Source: IDC, 2020 | n = 9

ROI Analysis

Table 6 presents IDC's analysis of the benefits and costs associated with interviewed organizations' use of the Cognito platform from Vectra. IDC calculates that study participants will realize average discounted benefits worth $6.27 million per organization over three years ($259,900 per 1,000 users) in higher employee and security team productivity levels, reduced business risk, and security-related cost reductions. These benefits compare with average three-year discounted investment costs of $1.36 million per organization ($56,500 per 1,000 users), which would result in an average three-year ROI of 360% with payback occurring in an average of five months.

TABLE 6

Three-Year ROI Analysis

	Per Organization	Per 1,000 Users
Benefit (discounted)	$6.27 million	$259,900
Investment (discounted)	$1.36 million	$56,500
Net present value (NPV)	$4.91 million	$203,400
ROI (NPV/investment)	360%	360%
Payback	5 months	5 months
Discount factor	12%	12%

Source: IDC, 2020 | n = 9

Challenges/Opportunities

Vectra competes in a crowded cybersecurity landscape, which can be difficult to differentiate in. Security vendors have used the terms *artificial intelligence* and *analytics* so interchangeably that the greater meaning could get lost (and yes, syndicated research firms such as ours share some blame for the commoditization of these terms). Basic statistical baselines are established in security platforms such as EDR, SIEM, and intrusion detection systems/ intrusion prevention systems (IDS/IPS).

Another place where competition is intense is in network detection and response (IDC uses network intelligence and threat analytics to be more inclusive of different types of network detection strategies such as deception, deep packet insights and emulation, and full packet capture). The network itself is an excellent control plane: security platforms can be developed to measure session entropy, HTTP tunnels, indications of beaconing, and suspicious port behavior. In this sense, Vectra competes with other network detection and response companies, SIEM, EDR with an IaaS backplane, extended detection and response (XDR), and possibly even the public cloud service providers.

There is a silver lining in the competition though. Enterprises are really only looking at two things: the time to detect an adversary, which includes the time spent on poorly qualified alerts, and the time to respond to an incident, including temporary blocking, patching, and integration with workflow. Security tools must work over multiple environments, must provide discrete value, and must work in concert with other IT and security platforms. With the enterprises that IDC spoke with, Vectra demonstrated consistent, definable value.

Conclusion

One of the misnomers about cybersecurity tools is they are developed to find indicators of compromise. This simple proposition gets turned on its head as the network itself is unstable, often adapting to new users, shadow IT, software and application upgrades, and physical conditions such as load balancing and extreme conditions such as power outages. Each new condition can cause tools to be noisy or inaccurate.

In addition, cybersecurity tools happen in what is still human security operations centers. An expertly designed tool not only finds evidence of an attacker but also gives the analyst the tools to investigate the event. In reality, cybersecurity tools need to chain indicators of compromise into a meaningful version of the truth, determine the probability of an oncoming attack, and trigger the right response. Cognito from Vectra does this.

IDC's research with organizations using Cognito from Vectra demonstrates the platform's value in minimizing costs associated with business risk as well as empowering security teams. Study participants deployed Cognito to address specific challenges related to securing their business and IT environments, chief among them needing to find a way to effectively and efficiently identify, prioritize, and address security threats. Through AI- and data science-driven assessments, Cognito from Vectra enables more accurate identification of actual threats, allowing for more targeted threat investigation and remediation efforts and earlier more proactive identification of actual security issues.

As a result, security teams are more productive and effective, and organizations incur lower actual business costs from security breaches and unplanned outages while reducing the potential cost of major security events. Based on these interviews, IDC projects that interviewed Vectra customers will realize a strong return on their investment of more than 4.5 to 1 (360% three-year ROI) through enhanced and more robust security operations.

Appendix: Methodology

IDC's standard ROI methodology was utilized for this project. This methodology is based on gathering data from current users of the Cognito platform from Vectra as the foundation for the model. Based on interviews with organizations using Cognito, IDC performed a three-step process to calculate the ROI and payback period:

- **Gathered quantitative benefit information during the interviews using a before-and-after assessment of the impact of Cognito.** In this study, the benefits included IT- and security-related cost reductions and avoidances, staff time savings, and productivity benefits.
- **Created a complete investment (three-year total cost analysis) profile based on the interviews.** Investment costs include the actual cost of Red Hat training courses as well as staff time required to take and complete the courses.
- **Calculated the ROI and payback period.** IDC conducted a depreciated cash flow analysis of the benefits and investments for the organizations' use of Cognito over a three-year period. ROI is the ratio of the net present value (NPV) and the discounted investment. The payback period is the point at which cumulative benefits equal the initial investment.

IDC bases the payback period and ROI calculations on a number of assumptions, which are summarized as follows:

- Time values are multiplied by burdened salary (salary + 28% for benefits and overhead) to quantify efficiency and productivity savings. For purposes of this analysis, IDC has used assumptions of an average fully loaded salary of $100,000 per year for IT staff members and an average fully loaded salary of $70,000 for non-IT staff members. IDC assumes that employees work 1,880 hours per year (47 weeks x 40 hours).
- The net present value of the three-year savings is calculated by subtracting the amount that would have been realized by investing the original sum in an instrument yielding a 12% return to allow for the missed opportunity cost. This accounts for both the assumed cost of money and the assumed rate of return.
- Further, because the Cognito platform from Vectra requires a deployment period, the full benefits of the solution are not available during deployment. To capture this reality, IDC prorates the benefits on a monthly basis and then subtracts the deployment time from the first-year savings.

Note: All numbers in this document may not be exact due to rounding.

About the Analysts

Christopher Kissel
Research Director, Security & Trust Products, IDC

Chris is responsible for cybersecurity technology analysis, emerging trends, and market share reporting. His primary research area is Cybersecurity Analytics, Intelligence, Response, and Orchestration (AIRO). The major technology groups within this practice are SIEM, device and application vulnerability management, threat analytics, and automation and orchestration platforms. Chris affectively covers the processes that security operation center (SOC) analysts employ to monitor, detect, remediate, and mitigate threat actors attempting to attack a network within a security and vulnerability management and security analytics paradigm.

More about Christopher Kissel

Matthew Marden
Research Director, Business Value Strategy Practice, IDC

Matthew is responsible for carrying out custom business value research engagements and consulting projects for clients in a number of technology areas with a focus on determining the return on investment (ROI) of their use of enterprise technologies. Matthew's research often analyzes how organizations are leveraging investment in digital technology solutions and initiatives to create value through efficiencies and business enablement.

More about Matthew Marden

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

IDC Research, Inc.
5 Speen Street
Framingham, MA 01701
USA
508.872.8200

idc.com @idc

Doc. #US47016020