April 2025 | Business Value White Paper, sponsored by Vectra AI

The Business Value of Vectra AI

Christopher Kissel
Research Vice President,
Security and Trust Products, IDC

Ladislav Kinda
Consultant,
Business Value Strategy Practice, IDC

Table of Contents

BUSINESS VALUE HIGHLIGHTS

Click any link and look for the ➤ symbol on the corresponding page. Use the Return to Highlights button to return this page.

40%
more efficient SOC teams

391%
three-year ROI

6-month
payback period

60%
less time assessing and prioritizing alerts

52%
increase in identified potential threats

50%
less time investigating alerts

51%
less time monitoring and triaging alerts

40%
less time tuning threat use case rules and correlation

37%
less time identifying new threat use cases

$793,000
reduction in annual network security related productivity losses

Executive Summary

Vectra AI has proven to be a valuable asset for organizations across various industries, enhancing their security postures and operational efficiency. Through interviews with seven organizations, IDC has gathered insights into the significant benefits and experiences these organizations have had with Vectra AI. This white paper provides a comprehensive overview of these benefits, with the support of direct quotes from the interviewed organizations.

Vectra AI helped these organizations achieve a higher level of security, creating a more responsive environment in which security staff can focus on high-priority tasks by providing:

- **Enhanced threat detection and response,** reducing security incidents and operational disruptions
- **Increased operational efficiency,** allowing security teams to focus on genuine threats
- **Improved business continuity and compliance,** ensuring network availability and regulatory adherence
- **Substantial cost savings** by retiring legacy security tools and optimizing staffing

Situation Overview

The network detection and response (NDR) market is expanding rapidly due to the growing need for advanced threat detection and response capabilities. NDR solutions use AI and ML to identify and mitigate sophisticated cyberthreats that traditional security measures might miss. This proactive approach is crucial in today's evolving threat landscape.

Key drivers of the NDR market include the adoption of cloud services and the complexity of network environments. As organizations move to the cloud and adopt hybrid infrastructures, comprehensive visibility and real-time threat detection across all network segments become essential. NDR solutions provide this visibility, enabling swift detection and response to threats, thereby minimizing potential damage.

Advancements in the NDR market include integrating network telemetry with individual identities (e.g., email addresses, login information) to enhance threat detection precision. NDR solutions also monitor specific session protocols (e.g., FTP, HTTPS) to detect anomalies, providing deeper insights into network activities. Vendors such as Vectra AI focus on application-specific protocols to create comprehensive visibility and historical references, strengthening security posture. More than that, Vectra AI is looking at how telemetry from devices, applications, and network protocols interrelate — allowing accepted behavior but flagging anomalous behavior indicative of a multi-vector attack.

Integrating NDR with other security technologies, such as security information and event management (SIEM) and extended detection and response (XDR), enhances overall security. By correlating data from multiple sources and providing a unified view of security events, NDR solutions streamline incident response processes and improve security operations efficiency. As the threat landscape evolves, the adoption of NDR solutions will increase through the need for advanced, AI-powered threat detection and response capabilities.

Vectra AI Overview

Vectra AI is a notable player in the NDR market with its advanced capabilities in detecting and responding to cyberthreats. Founded in 2011, Vectra AI has evolved to offer comprehensive detection and response solutions, including cloud detection and response and managed XDR. The platform excels in gathering and correlating telemetry from various sources, including on-premises, cloud, hybrid, and IoT/OT environments. Vectra AI's focus on domain-specific behavior and identity-based anomalies enhances its ability to detect lateral movements and expedite investigation times. The platform reduces the blast surface by identifying and mitigating potential vulnerabilities before threat actors can exploit them.

A key strength of Vectra AI is its integration capabilities. The platform supports a wide range of integrations with SIEM, SOAR, endpoint detection and response (EDR), web/email, and firewall solutions, ensuring seamless operation within existing security infrastructures. Vectra AI's Attack Signal Intelligence uses AI/ML models to build behavior-based profiles, normalize threat detections, and correlate to specific entities — hosts and accounts — to assign urgency scores, which helps in prioritizing critical threats. This approach significantly reduces alert noise and enhances the efficiency of security operations.

Vectra AI also offers robust response capabilities, enabling automated and manual responses through existing endpoints, firewalls, and identity providers. The platform's ability to correlate Active Directory, Entra ID, and cloud identity logs with network telemetry provides a comprehensive view of security events. Vectra AI's focus on coverage, clarity, and control ensures that organizations can effectively manage and mitigate cyberthreats, making it a valuable asset for enhancing overall security posture.

The Business Value of Vectra AI

Study Firmographics

IDC conducted research that explored the value and benefits for organizations using Vectra AI to enhance their security posture, improve operational efficiency, and achieve business continuity. The study included seven interviews with organizations that use Vectra AI and have experience with and/or knowledge about the platform's benefits and costs. In-depth interviews by IDC covered a variety of quantitative and qualitative questions about the impact of Vectra AI on these organizations' IT and security operations and business results.

Firmographics data, per **Table 1** (next page), includes the average numbers of employees, IT staff, and business applications and annual revenue. This data provides context for the analysis and highlights the scale of the organizations involved. The average number of employees is 28,900, with a median of 17,000 and a range from 5,000 to 80,000. The average number of IT staff is 950, with a median of 300 and a range from 30 to 2,750. The average annual revenue is $15.3 billion, with a median of $15 billion and a range from $900 million to $37 billion.

TABLE 1

Firmographics of Interviewed Organizations

Firmographics	Average	Median	Range
Number of employees	28,900	17,000	5,000–80,000
Number of IT staff	950	300	30–2,750
Total number of business applications	4,900	1,000	150–15,000
Total number of TBs	109,000	7,500	150–500,000
Annual revenue	$15.3B	$15.0B	$900.0M–$37.0B
Verticals	Telco, Education, Pharmaceutical, Cosmetics, Industrial Engineering, Luxury Goods, Construction		
Countries	United States (2), India, Netherlands, Italy, France, Switzerland		

n = 7; Source: IDC Business Value In-Depth Interviews, January 2025

Choice and Use of Vectra AI

The organizations selected Vectra AI for various reasons, including the need for an end-to-end solution to address NDR and EDR challenges. They sought to enhance security with behavior-based detection methods, moving beyond traditional antivirus solutions. Vectra AI's network monitoring capabilities and integration with existing security software were crucial for decentralized operations.

Additionally, after experiencing significant security incidents, the organizations recognized the need for advanced threat detection to improve their overall security posture:

Telecommunications:
"Network detection and response was challenging due to its pervasive nature, especially with global IoT proliferation. Endpoint detection and response and device management were also significant challenges. We sought a solution to proactively handle everything end to end."

Luxury goods:

"Our organization adopted Vectra AI seven to eight years ago as one of the first customers in Switzerland. We aimed to enhance our detection of malicious activities through behavior-based methods rather than traditional signature-based ones. Antivirus solutions were inadequate for the sophisticated threats we faced, so we needed a network-level behavioral approach to strengthen our security."

Construction:

"We are a decentralized company with a small head office of around 100 full-time equivalents (FTEs) and 130 operating companies across the Netherlands, the UK, North America, Canada, and Germany. We centralized basic IT services but lacked network monitoring. To enhance security in depth, we chose Vectra AI for its network monitoring and integration with other security software, which we already use for endpoint protection."

Cosmetics:

"We adopted Vectra AI after experiencing a significant ransomware attack that encrypted our files. Although it didn't disrupt sales, restoring from backup was time consuming and costly. This incident highlighted the need for advanced threat detection and motivated us to enhance our security posture with Vectra AI."

Business Value and Quantified Benefits of Vectra AI

IDC's Business Value research evaluates and quantifies the benefits for companies in adopting Vectra AI to enhance their security posture, boost operational efficiency, and ensure business continuity. In-depth interviews with study participants revealed that Vectra AI significantly improved threat detection and response capabilities, leading to fewer security incidents and minimal operational disruptions. The platform also increased the productivity of security teams by automating threat detection and reducing false positives. Participants highlighted various Vectra AI features and functionalities that enhanced proactive threat management, provided comprehensive visibility, and streamlined security operations, resulting in substantial cost savings and resource optimization.

Organizations using Vectra AI reported significant operational and security benefits. They experienced increased efficiency by minimizing false positives and providing true positive alerts, allowing their SOC teams to quickly identify and respond to abnormal behavior. The platform's speed of investigations, valuable metadata collection, and threat identification capabilities enhanced team efficiency. Vectra AI's out-of-the-box detection capabilities reduced the need for tailored detections, saving time and effort. Additionally, Vectra AI provided end-to-end threat coverage, eliminating guesswork in tracking threat origins and destinations and improving incident prioritization and response.

Overall, organizations saw improved threat detection rates, reduced downtime, and fewer incidents:

Cosmetics:
"We're far more efficient now. We've tuned Vectra AI to minimize false positives, a major issue with security tools. The top 3 criteria I look for are true positive alerts, minimal false positives, and the ability to tune the tool. Unlike other competitors we've tried, which we couldn't fine-tune, Vectra AI provides fewer than 20 alerts a day. Our SOC quickly identifies abnormal behavior and suspicious alerts, ensuring rapid response and efficiency."

Industrial engineering:
"The most significant benefits we saw with Vectra AI are the speed of investigations, the valuable metadata collected during detection, and the ability to identify threats, which makes our team more efficient."

Luxury goods:
"Vectra AI provides out-of-the-box detection capabilities, eliminating the need for tailored detections. This saves time, effort, and tuning, while the platform manages everything, significantly reducing our operational burden."

Telecommunications:
"Vectra AI helps proactively identify threats and provides end-to-end coverage from endpoints. It eliminates the guesswork of tracking threat origins and destinations, offering complete mapping. The platform allows incident prioritization and quick response setup, enhancing security and network detection management. These features make it invaluable for proactive threat management."

Manufacturing:
"We saw improved threat detection rates, reduced downtime, and fewer incidents. Specifically, our mean time to detect and mean time to respond both improved, leading to fewer unplanned outages. For both KPIs, we observed reductions of 50%–60%."

Further, organizations using Vectra AI reported several key business benefits. The platform simplified compliance with government security regulations, ensuring licenses remained secure. It also improved ROI by minimizing downtime and protecting companies' reputations and revenue. One organization reported that Vectra AI ensured 100% network availability, crucial for maintaining trust and business continuity. The platform reduced the need for multiple tools and extensive manpower, providing robust and timely threat detection. Vectra AI protected intellectual property, client data, and overall data, preventing reputational damage and potential sales impact.

Additionally, it enhanced visibility into network activities, increasing confidence in promptly detecting breaches and critical events:

Telecommunications:
“With Vectra AI, we see three key business benefits. First, compliance: As a telco operator, we must meet government security regulations and report incidents monthly. Vectra AI simplifies this, ensuring our license isn’t jeopardized. Second, ROI: Incidents harm our reputation and revenue. Even a five-minute downtime is unacceptable in today’s digital world. Lastly, security: Vectra AI ensures 100% network availability, crucial for maintaining trust and business continuity.”

Cosmetics:
“My team focuses primarily on Vectra AI for real incident detection, reducing the need for multiple tools and extensive manpower. We handle 200 alerts daily with fewer people than other teams. Vectra AI gives me confidence that if someone breaches our network, we’ll detect them within hours. Before Vectra AI, we had no visibility; now, we have robust, timely threat detection.”

Luxury goods:
“Vectra AI protects our intellectual property, client data, and overall data, preventing reputational damage and potential sales impact. Vectra AI enhances our security posture, contributing to the improvement of our business results.”

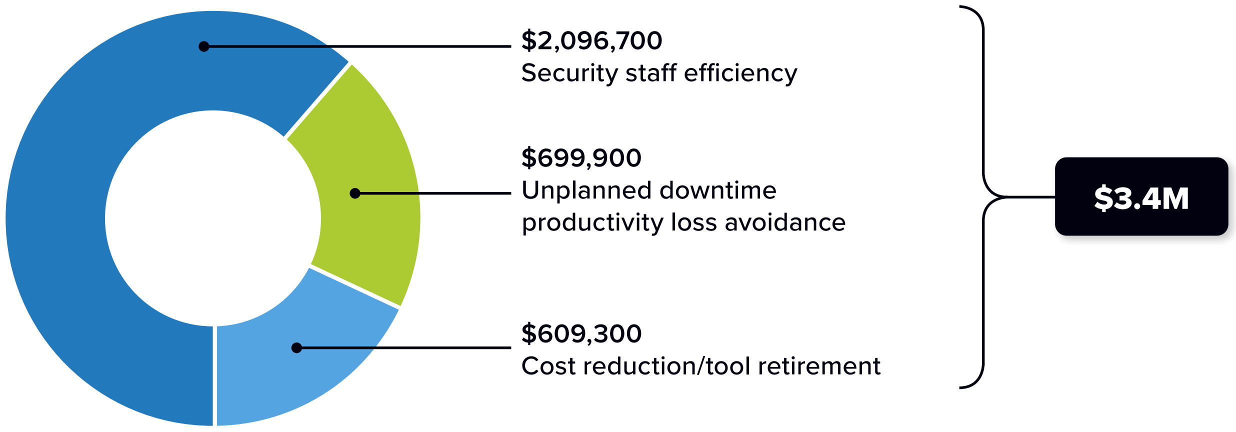
Education:
“We now have much greater visibility into what’s happening in our environment and network. Our confidence has significantly increased, knowing that we will promptly discover any breach or critical event that we need to be concerned about.”

Cosmetics:
“Before Vectra AI, we received no alerts and only learned of Red Team’s access through their annual reports, which consistently showed they had domain admin and root access. The first year with Vectra, we detected, expelled, and completely defeated the Red Team. Vectra is my top security tool.”

This paper presents the quantified benefits of using Vectra AI on a per-average-organization basis. The average annual benefits per organization amount to $3.4 million (see **Figure 1,** next page). These benefits fall under three main areas: security staff efficiency, unplanned downtime productivity loss avoidance, and cost reduction/tool retirement. Specifically, security staff efficiency benefits amount to $2,096,700 per organization, unplanned downtime productivity loss avoidance amounts to $699,900 per organization, and cost reduction/tool retirement amounts to $609,300 per organization.

FIGURE 1

Average Annual Benefits per Organization

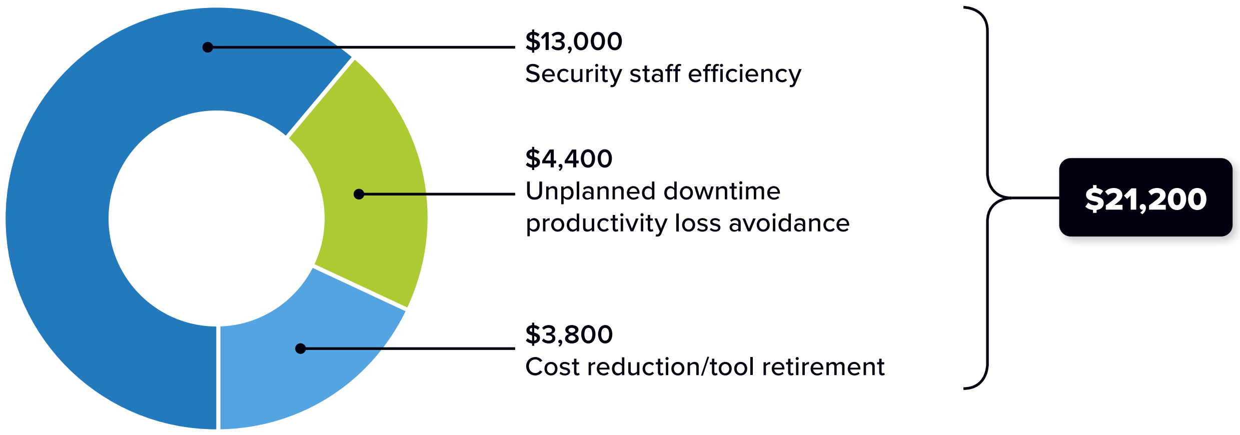


n = 7; Source: IDC Business Value In-Depth Interviews, January 2025

On a per-100-user basis, the average annual benefits of using Vectra AI amount to $21,200. These benefits also fall under three main categories: security staff efficiency, unplanned downtime productivity loss avoidance, and cost reduction/tool retirement. Specifically, security staff efficiency benefits amount to $13,000 per 100 users, unplanned downtime productivity loss avoidance amounts to $4,400 per 100 users, and cost reduction/tool retirement amounts to $3,800 per 100 users (see **Figure 2**).

FIGURE 2

Average Annual Benefits per 100 Users



n = 7; Source: IDC Business Value In-Depth Interviews, January 2025

Security Staff Benefits with Vectra AI

Organizations using Vectra AI reported significant benefits for their security staff. The platform enabled teams to focus on threat hunting rather than managing complex technologies, reducing operational workload and training requirements. Vectra AI's precision and clarity in identifying real threats significantly reduced false positives, allowing quicker and more relevant incident responses. SOC teams prioritized Vectra AI alerts, ensuring rapid investigation and response to suspicious activities.

The platform also allowed security staff to dedicate more time to higher-priority detections and responses, achieving substantial efficiency in threat identification, monitoring, and triaging, even with smaller teams and budgets:

Education:
"Vectra AI has enabled our security teams to focus on threat hunting rather than building and operating technologies. Its platform replaced the need for deep operational and technological expertise, such as Linux, software compilation, and writing kernel patches. This shift has eliminated the operational workload and training requirements, allowing us to concentrate on our core competencies."

Construction:
"With Vectra AI, we're able to act much quicker and with more relevant information on occurring incidents. It's more precise and provides better clarity on whether an alert is a real threat, a genuine incident, or a false positive. The implementation has significantly reduced the number of false positives."

Cosmetics:
"The SOC team prioritizes Vectra AI alerts above all others. We aim to review each Vectra AI alert within 15 minutes, with notifications sent directly toteam members' phones via Teams. Our experienced team can quickly discern normal activity from suspicious activity. If an alert appears suspicious, the team immediately initiates an investigation."

Luxury goods:
"SOC staff now dedicate their time to dealing with higher-priority detections and responses rather than spending excessive time on operational tasks."

Cosmetics:
"A benchmark report indicated our security budget should be significantly higher, with a headcount of 20. However, our actual budget is much lower, and we have only seven full-time employees. Despite this, Vectra AI has enabled us to achieve over 60%–70% efficiency in threat identification, monitoring, and triaging. If we relied on another competitor tool, we would need nearly double the staff for monitoring alone."

Vectra AI significantly improved SOC team efficiency by reducing alert fatigue and false positives, allowing teams to focus on genuine threats. Its AI and ML capabilities automated threat detection and response, minimizing manual investigations. Vectra AI's automation of threat detection freed up security staff to concentrate on strategic threat hunting and proactive defense measures rather than being bogged down by routine alerts. **Table 2** shows that the required number of full-time equivalents for equivalent security activities reduced from 43.3 to 26.1, a 40% improvement. Similarly, the value of staff time for equivalent security activities dropped from $4,331,900 to $2,610,000, also a 40% improvement.

TABLE 2

SOC Team Efficiency

Efficiency Benefits	Before Vectra AI	With Vectra AI	Difference	Benefit
Required FTEs for equivalent security activities	43.3	**26.1**	17.2	40%
Value of staff time for equivalent security activities	$4,331,900	**$2,610,000**	$1,721,900	40%

n = 7; Source: IDC Business Value In-Depth Interviews, January 2025

Vectra AI significantly improved the efficiency of security analyst teams by streamlining event analysis through automated threat detection and reduced false positives. Vectra AI's ML capabilities provided detailed insights and prioritized threats, minimizing manual investigations. Its integration with third-party tools enabled comprehensive visibility and faster threat identification. Vectra AI's real-time alerts and curated detection capabilities allowed analysts to quickly assess and investigate incidents, reducing the time they spent on subsequent analysis. This enabled more proactive threat management and strategic planning, allowing security analysts to focus on high-value tasks and improve overall security operations. **Table 3** (next page) shows that the required number of FTEs for equivalent security activities reduced from 11.1 to 6.2, a 44% improvement. The value of staff time for equivalent security activities dropped from $1,111,100 to $625,000, also a 44% improvement.

TABLE 3

Security Analyst Team Efficiency

Efficiency Benefits	Before Vectra AI	With Vectra AI	Difference	Benefit
Required FTEs for equivalent security activities	11.1	**6.2**	4.9	44%
Value of staff time for equivalent security activities	$1,111,100	**$625,000**	$486,100	44%

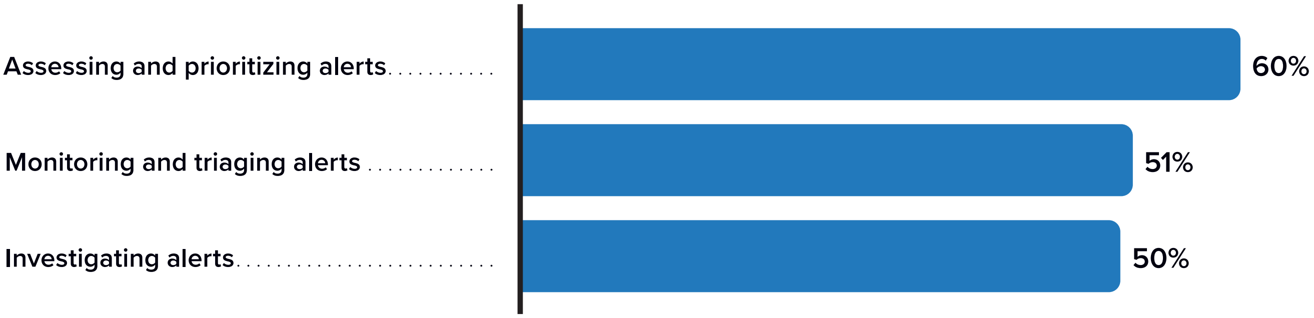
n = 7; Source: IDC Business Value In-Depth Interviews, January 2025

A more detailed view of the specific tasks where security analysts saw benefits shows that Vectra AI enabled security analysts to work more efficiently in investigating, monitoring, triaging, assessing, and prioritizing alerts. The reduced time analysts dedicated to these tasks allowed them to focus on higher-value activities, enhancing overall security operations. Specifically, the time to investigate alerts reduced by 50%, the time to monitor and triage alerts dropped by 51%, and the time to assess and prioritize alerts fell by 60%. **Figure 3** presents these findings.

FIGURE 3

Security Analyst Specific Task Benefits

(Reduction of time dedicated to tasks)



n = 7; Source: IDC Business Value In-Depth Interviews, January 2025

Vectra AI enhanced the efficiency of security engineer teams by automating threat detection and reducing manual workload, enabling them to focus on strategic tasks. Vectra AI's ML capabilities provided detailed threat insights, allowing engineers to design and implement more effective security measures. Its integration with existing tools, such as Microsoft Sentinel, improved system resiliency by offering comprehensive visibility and proactive threat management. Vectra AI's real-time alerts and curated detection capabilities freed up engineers to spend more time on system design, security architecture, and enhancing overall network security. This shift significantly boosted their efficiency, allowing them to concentrate on high-value activities and strategic initiatives, making them 32% more efficient **(Table 4).** The required number of FTEs for equivalent security activities reduced from 5.2 to 3.5, a 32% improvement. The value of staff time for equivalent security activities dropped from $522,700 to $355,000.

TABLE 4

Security Engineer Team Efficiency

Efficiency Benefits	Before Vectra AI	With Vectra AI	Difference	Benefit
Required FTEs for equivalent security activities	5.2	**3.5**	1.7	32%
Value of staff time for equivalent security activities	$522,700	**$355,000**	$167,700	32%

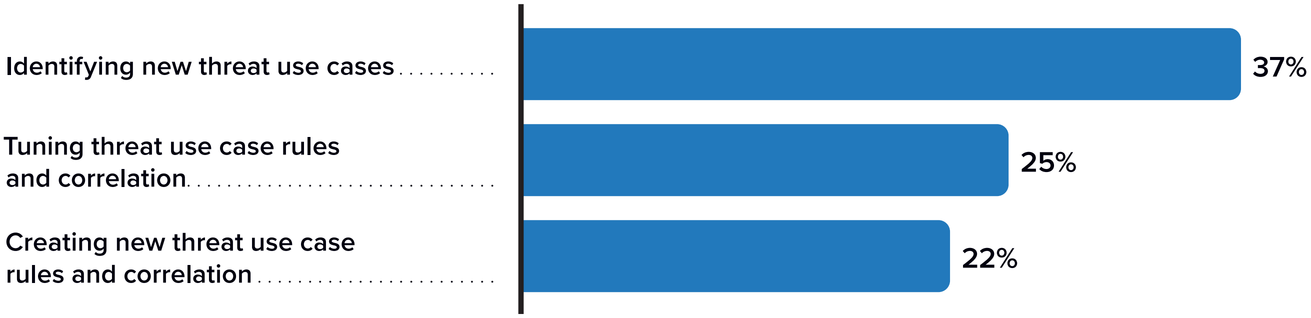
n = 7; Source: IDC Business Value In-Depth Interviews, January 2025

A more detailed view of the specific tasks where security engineers saw benefits shows that Vectra AI enabled security engineers to work more efficiently in creating new threat use case rules and correlation, tuning threat use case rules and correlation, and identifying new threat use cases. The reduced time for these tasks allowed engineers to focus on higher-value activities, enhancing overall network security. Specifically, the time to create new threat use case rules and correlation reduced by 22%, the time to tune threat use case rules and correlation dropped by 25%, and the time to identify new threat use cases fell by 37% (see **Figure 4,** next page).

FIGURE 4

Security Engineers' Specific Benefits

(Reduction of time dedicated to tasks)



n = 7; Source: IDC Business Value In-Depth Interviews, January 2025

Organizational Security Outcomes with Vectra AI

Organizations have seen significant security benefits with Vectra AI. It has been crucial in preventing major security incidents, particularly for organizations targeted by bot attacks and phishing. Vectra AI's alerts enabled swift action during a massive phishing attack, preventing a major incident. The platform enhances proactive detection capabilities, identifying and mitigating risks early in the kill chain. Since implementing Vectra AI, organizations have blocked multiple attacks on the same business day, minimizing the impact to isolated PCs rather than entire production lines.

Vectra AI's early detection capabilities allow for quick reactions, limiting the impact of incidents and ensuring business continuity:

Cosmetics:

"Without Vectra AI, we would have faced major security incidents. Our company, being a prime target for bot attacks and phishing, has benefited immensely from Vectra AI's alerts. Last year, a massive phishing attack saw over 70 users compromised. Thanks to Vectra AI and our SOC team, we swiftly shut down and reset passwords, preventing a major incident. Vectra AI's protection has been crucial in safeguarding our operations."

Luxury goods:

"We've significantly enhanced our proactive detection capabilities with Vectra AI, especially during the initial phases of the kill chain. This improvement has allowed us to identify and mitigate risks before they escalate into impactful breaches."

Industrial engineering:

"Before Vectra AI, we had three incidents over three years, with recovery times of up to a week. Since implementing Vectra AI in 2019, despite increased attack frequency and complexity post-2020, we've blocked four attacks on the same business day, some within an hour.

The impact has been minimal, affecting only isolated PCs rather than entire production lines. Previously, a single incident could shut down an entire plant for a week."

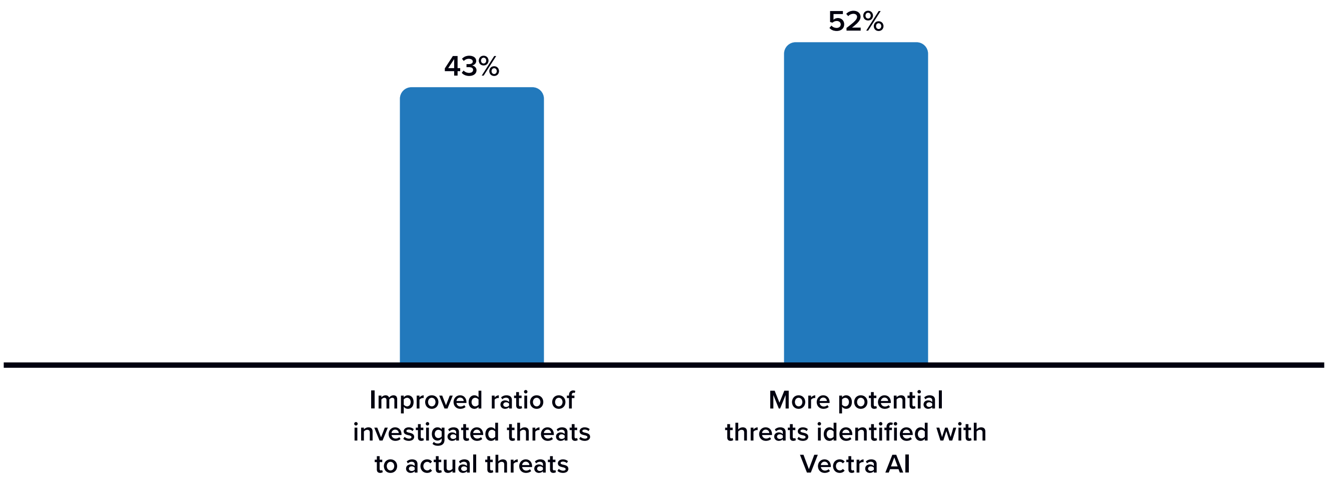
Construction:

"Vectra AI really helps in detecting incidents or events in an early stage. With that, we can limit the impact because the sooner we know what's going on, the quicker we can react."

IDC's research on Vectra AI revealed significant improvements in security metrics for organizations. The platform enhanced the ratio of investigated threats to actual threats by 43%, further confirming the reduction of false positives, and increased the identification of potential threats by 52% (see **Figure 5**). These improvements allowed security teams to focus on genuine threats, reducing false positives and operational workload, leading to fewer security incidents and minimal disruptions. Overall, Vectra AI's advanced detection capabilities and comprehensive visibility significantly bolstered organizational security posture and operational efficiency.

FIGURE 5

Security Metrics Improvements with Vectra AI



n = 7; Source: IDC Business Value In-Depth Interviews, January 2025

Unplanned Downtime Benefits and Environmental Stability

Vectra AI significantly reduced unplanned downtime and enhanced environmental stability for organizations. By automating threat detection and providing real-time alerts, Vectra AI enabled faster identification and mitigation of potential issues. One organization reported a significant reduction in unplanned downtime incidents due to Vectra AI's proactive threat management. Another organization noted the virtual elimination of downtime incidents, maintaining continuous system availability.

Vectra AI's integration with existing tools ensures comprehensive visibility and stability, minimizing disruptions and ensuring the reliability of critical systems and applications:

Manufacturing:
"Vectra AI enabled us to reduce the mean time to detect and respond, which increases the availability of business applications, resulting in less operational disruption."

Cosmetics:
"Previously, we experienced annual downtime lasting several days. Since implementing Vectra AI, downtime due to incidents has been virtually eliminated, with no incidents causing downtime in years."

Luxury goods:
"Vectra AI significantly enhances our security posture, especially in our AWS and cloud environments, where its ease of configuration and curated detections allow us to address threats from day zero. While it complements other tools, its capabilities to deliver insights and reduce manual effort have been particularly impactful during our cloud migration."

Vectra AI's proactive threat management enhances system stability and helps minimize disruptions to ensure continuous availability. Organizations reported significant reductions in the number of impactful network security breaches, the average duration of impact of breaches, and the number of impacted users per breach. Specifically, the number of impactful network security breaches per month reduced from 1.7 to 0.5 (69.4% improvement), the average duration of impact of breaches dropped from 28.0 hours to 4.3 hours (84.8% improvement), and the number of impacted users per breach fell from 65 to 15 (76.9% improvement). These improvements led to substantial productivity loss avoidance. Vectra AI helped organizations virtually eliminate costs associated with staff productivity losses, reporting on average a 99.9% reduction in productivity losses due to security breaches. This translated to $793,000 of productivity loss avoidance for the average organization (see **Table 5,** next page).

TABLE 5

Unplanned Downtime Productivity Loss Avoidance

Productivity Loss Avoidance	Before Vectra AI	With Vectra AI	Difference	Benefit
Number of impactful network security breaches per month	1.7	**0.5**	1.2	69.4%
Average duration of impact of breach (hours)	28.0	**4.3**	23.7	84.8%
Number of impacted users per breach	65.0	**15.0**	50.0	76.9%
Average productivity loss during breach	57%	**4%**	53%	93.4%
Annual productivity loss avoidance benefits	$793,600	**$600**	$793,000	99.9%

n = 7; Source: IDC Business Value In-Depth Interviews, January 2025

In addition to the organizational security and staff efficiency benefits, organizations also managed to save or avoid significant costs by retiring old security tools by adopting Vectra AI. On average, organizations reported savings of $690,000 annually.

ROI Summary

IDC's Business Value methodology gathers data from organizations currently using Vectra AI. The ROI analysis shows that organizations have achieved significant gains and savings from Vectra AI staff efficiency, cost savings, and downtime benefits. The investment in implementing and using Vectra AI, along with associated migration, training, and support costs, has resulted in a 391% ROI over a three-year period, with a payback period of six months. The discounted benefits over three years amount to $8,054,900 per organization, while the discounted investment costs are $1,640,300 per organization, resulting in a net present value (NPV) of $6,414,600 and an ROI of 391% (see **Table 6,** next page).

TABLE 6

Three-Year ROI Analysis

Three-Year ROI Analysis	Per Organization	Per 100 Users of Vectra AI-Protected Applications
Discounted benefits	$8,054,900	$50,100
Discounted investment	$1,640,300	$10,200
NPV	$6,414,600	$39,900
ROI	**391%**	**391%**
Payback	**6 months**	**6 months**
Discount factor	12%	12%

n = 7; Source: IDC Business Value In-Depth Interviews, January 2025

Challenges/Opportunities

Vectra AI has significant opportunities in the NDR market due to its advanced AI/ML capabilities, strong integration with various security technologies, and comprehensive visibility across on-premises, hybrid, and cloud environments. Its focus on identity-based anomalies and domain-specific behavior enhances threat detection and response, making it a valuable asset for organizations.

However, Vectra AI faces challenges in requiring additional certifications, such as GDPR and FedRAMP. Vectra AI faces competition from larger vendors, and there is the possibility of NDR becoming a feature within larger platforms, such as XDR or SIEM. Additionally, its pricing model based on the number of IPs may be a barrier for some potential customers.

Overall, Vectra AI's strengths in advanced threat detection, integration capabilities, and comprehensive visibility position it well in the NDR market, but addressing the aforementioned challenges could further enhance its market standing.

Conclusion

Vectra AI has demonstrated substantial value for organizations by significantly enhancing their security posture and operational efficiency. The platform's advanced AI- and ML-powered threat detection and response capabilities have enabled organizations to proactively identify and mitigate sophisticated cyberthreats, resulting in fewer security incidents, reduced operational disruptions, and improved business continuity. Integrating Vectra AI with existing security infrastructures, such as SIEM and XDR, has further streamlined security operations, allowing security teams to focus on high-priority tasks and strategic initiatives. The quantifiable benefits, including increased SOC team efficiency, reduced false positives, and substantial cost savings, underscore the platform's effectiveness in optimizing security operations and ensuring robust protection against evolving threats.

Overall, the adoption of Vectra AI has led to significant improvements in security metrics, such as reduced mean time to detect and respond to threats, minimized unplanned downtime, and enhanced visibility into network activities. Organizations have reported substantial productivity gains, cost savings, and a high ROI, with a payback period of just six months. The platform's ability to provide comprehensive threat coverage, automate threat detection, and integrate seamlessly with existing tools has made it an invaluable asset for organizations seeking to enhance their security posture and operational resilience. As the threat landscape evolves, Vectra AI's advanced capabilities position it well to meet the growing demands for proactive and efficient threat management.

Appendix 1: Methodology

This project utilized IDC's standard Business Value/ROI methodology, gathering data from organizations currently using Vectra AI.

Based on interviews with organizations using Vectra AI, IDC performed a three-step process to calculate the ROI and payback period:

1. **IDC gathered quantitative benefit information during the interviews using a before-and-after assessment of the impact of using Vectra AI.** In this study, the benefits included data warehousing–related cost reductions and avoidances, staff time savings and productivity benefits, revenue gains, and end-user productivity.

2. **IDC created a complete investment (three-year total cost analysis) profile based on the interviews.** Investments go beyond the initial and annual costs of using Vectra AI and can include additional costs related to migrations, planning, consulting, and staff or user training.

3. **IDC calculated the ROI and payback period.** It conducted a depreciated cash flow analysis of the benefits and investments for the organizations' use of Vectra AI over a three-year period. ROI is the ratio of the 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:

- Multiplying time values by burdened salary (salary + 28% for benefits and overheads) quantifies efficiency and manager productivity savings. For this analysis, based on the interviewed organizations' geographic locations, 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 per year for non-IT staff members. IDC assumes that employees work 1,880 hours per year (47 weeks x 40 hours).

- IDC calculates the net present value of the three-year savings 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 the assumed cost of money and the assumed rate of return.

- Because IT solutions require 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 IDC Analysts

Christopher Kissel

Research Vice President, Security and Trust Products, IDC

Chris Kissel is a research vice president in IDC's Security and Trust Products group, responsible for cybersecurity technology analysis, emerging trends, and market share and forecast reporting. Kissel's primary research area is security operations and AI security analytics. The major technology groups within this practice are SOAR, firewall automation, network detection and response, threat detection and investigation response, threat intelligence, and cloud-native XDR. Kissel also contributes to the IDC SIEM and exposure management practices. The AI analytics service effectively covers the processes security operations analysts employ to monitor, detect, remediate, and mitigate threat actors attempting to attack a network and how AI algorithms can be used to enhance detection and response processes

More about Christopher Kissel

Ladislav Kinda

Consultant, Business Value Strategy Practice, IDC

Ladislav Kinda is a consultant in the IDC Business Value Strategy practice team. Kinda conducts customized business value research and consulting projects for clients across various technology domains. His primary focus is assessing the return on investment from their adoption of enterprise technologies. Kinda's research delves into how organizations leverage digital technology solutions and initiatives to enhance efficiency and drive business growth.

More about Ladislav Kinda

Message from the Sponsor

VECTRA®

Vectra AI is a global cybersecurity AI company that provides organizations network protection for advanced cyber-attacks.

When attackers bypass existing controls to gain access to data center, campus, remote work, identity, cloud, or OT environments, Vectra AI stops them from becoming breaches. With 35 patents in AI threat detection and the most vendor references in MITRE D3FEND, organizations worldwide rely on Vectra AI to stop attacks others can't.

Click here for more information

IDC Custom Solutions

IDC Custom Solutions produced this publication. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis that IDC independently conducted and published, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. This IDC material is licensed for external use and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.

IDC

IDC Research, Inc.
140 Kendrick Street, Building B, Needham, MA 02494, USA
T +1 508 872 8200

idc.com

in @idc

X @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.
With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.

©2025 IDC. Reproduction is forbidden unless authorized. All rights reserved. CCPA