VECTRA AI

Customer Story | Higher Education

How Texas A&M University System Saved $7 Million in One Year with Vectra AI

Texas A&M University System saves $7 million in one year with the Vectra AI platform.

THE TEXAS A&M UNIVERSITY SYSTEM

Organization
The Texas A&M University System

Industry
Higher education

The Challenge
Protect high value academic and research data

Selection Criteria
Increase speed and efficiency of threat detection and incident response

The Results

- $7 million saved in one year by eliminating the need for post-breach forensic analysis.
- $4.2 billion in total expenditures protected, safeguarding critical research and partnerships.
- 7 network cyberattackers detected and mitigated in one year, preventing potential breaches and securing vital assets.
- One person can investigate up to 50 threats in just two hours, dramatically increasing operational efficiency across a network of 250,000 users.

The Aggies may be known for football, but the Texas A&M University System is also an academic and research powerhouse.

The A&M System encompasses 11 university campuses, seven state agencies and numerous research institutes. Its research is as varied as tackling global hunger, advanced manufacturing, animal diseases that crossover to humans, and nuclear science. For a cyber thief, stealing that research is the ultimate touchdown.

The Challenge

A drought of cybersecurity talent

"One of the biggest challenges we faced was the lack of cybersecurity talent, which is a huge global issue right now," says Dan Basile, executive director of the Security Operations Center at the A&M System. "It's difficult to hire and retain skilled cybersecurity professionals."

"The other challenge is that we spend $4.2 billion in total expenditures," Basile added. "Vital research is performed with many important organizations like the U.S. Department of Energy, NASA and the U.S. Department of Defense. This makes us a target for nation-state cyberattackers."

Cut costs by detecting attackers fast and early

For the A&M System, whose network supports about 250,000 people at any given time, Vectra AI's Network Detection and Response (NDR) solution has proven to be the fastest, most efficient way to stop cyberattackers that evade perimeter security and spread inside the network in search of key assets to steal or damage.

The A&M System's Security Operations Center successfully detected and mitigated seven network cyberattackers in one year with Vectra in their toolkit. And there was little need for expensive post-breach forensic analysis, which only provides a rear-view mirror of an attack, often months after cybercriminals have made off with your crown jewels.

"You're looking at about $1 million every time you call in consultants to perform post-breach forensic analysis," Basile explained.

"By eliminating this, Vectra AI saved the A&M System $7 million in a year and we cut threat investigation times from several days to a few minutes."

The Solution

Automation creates opportunities

By closing the cybersecurity gap between network perimeter security and post-breach forensics, the A&M System can detect attacks faster and eliminate the need to analyze and chase down hundreds of thousands of NetFlow threat logs.

"Since deploying Vectra AI, our team can monitor the entire A&M System network for cyberattackers and run the Security Operations Center with incredible efficiency, despite having an extremely lean staff," Basile says.

Vectra AI has also been instrumental in helping the university overcome the cybersecurity skills shortage. Student interns who are interested in studying and developing careers in cybersecurity are trained to use the Vectra AI platform, with AI-driven Attack Signal Intelligence, as Tier-1 analysts in the Security Operations Center.

"Vectra AI is so intuitive and easy to use that interns can decide in a few minutes whether to act on a threat detection themselves or escalate it to a Tier-2 security analyst for further investigation," says Basile. "So the highly-skilled employees who used to be Tier-1 analysts are now working as Tier-2 analysts. This is where Vectra really shines."

"We continue to shrink our threat detection times with Vectra and student interns are now viable members of the security operations team," Basile adds. "That is massive in higher education. It's a big win for both students and the university."

How Vectra AI finds the highest-risk threats with certainty

By monitoring all internal network traffic, Vectra AI's NDR solution provides visibility into the actions of all devices – including BYOD and IoT – and automatically puts the most relevant information in context into the hands of the security operations team.

When active cyberattackers are found inside the network, Vectra AI automatically scores, prioritizes and correlates each threat detection with the compromised hosts and key assets that are under attack.

Vectra AI consolidates thousands of events and historical context to pinpoint the hosts that pose the biggest threat. With Vectra AI, analysts see the data that matters in full context, which speeds-up incident response.

Security analysts can instantly see which devices infected hosts are communicating with and how. Access to metadata in captured packets further accelerates threat analysis so security teams can take fast, decisive action.

"Vectra AI saved the A&M System $7 million in a year and we cut threat investigation times from several days to a few minutes."

DAN BASILE
Executive Director of the Security Operations Center, The Texas A&M University System

The Results

Millions saved with efficient threat detection

Since implementing Vectra AI, the Texas A&M University System has achieved outstanding results, including:

- $7 million saved in one year by eliminating the need for post-breach forensic analysis.
- $4.2 billion in total expenditures protected, safeguarding critical research and partnerships.
- 7 network cyberattackers detected and mitigated in one year, preventing potential breaches and securing vital assets.
- One person can investigate up to 50 threats in just two hours, dramatically increasing operational efficiency across a network of 250,000 users.

Armed with Vectra AI, the Texas A&M University System protects its critical operations and research, staying ahead of sophisticated threats while maintaining operational excellence.

"Since deploying Vectra AI, our team can monitor the entire A&M System network for cyberattackers and run the Security Operations Center with incredible efficiency, despite having an extremely lean staff"

DAN BASILE
Executive Director of the Security Operations Center, The Texas A&M University System

Read more customer stories

About Vectra AI

Vectra AI is the leader in AI-native security and observability. Vectra AI delivers organizations real-time visibility into their network, clear insight into which behaviors matter, and the ability to act before risk becomes impact. By connecting on-premises, multi-cloud, identity, SaaS, edge, and IoT/OT infrastructure, Vectra AI helps organizations reduce exposure, accelerate detection and response, and automate security operations with AI. With over a decade of AI and ML innovation, 39 patents and a Leader in the 2025 and 2026 Gartner Magic Quadrant for Network Detection and Response, Vectra AI empowers security teams to stay ahead of emerging AI powered attacks, increase operational efficiency, and prove resilient in an increasingly complex, AI-driven world. For more information, visit www.vectra.ai.

For more information please contact us: Email: info@vectra.ai | vectra.ai