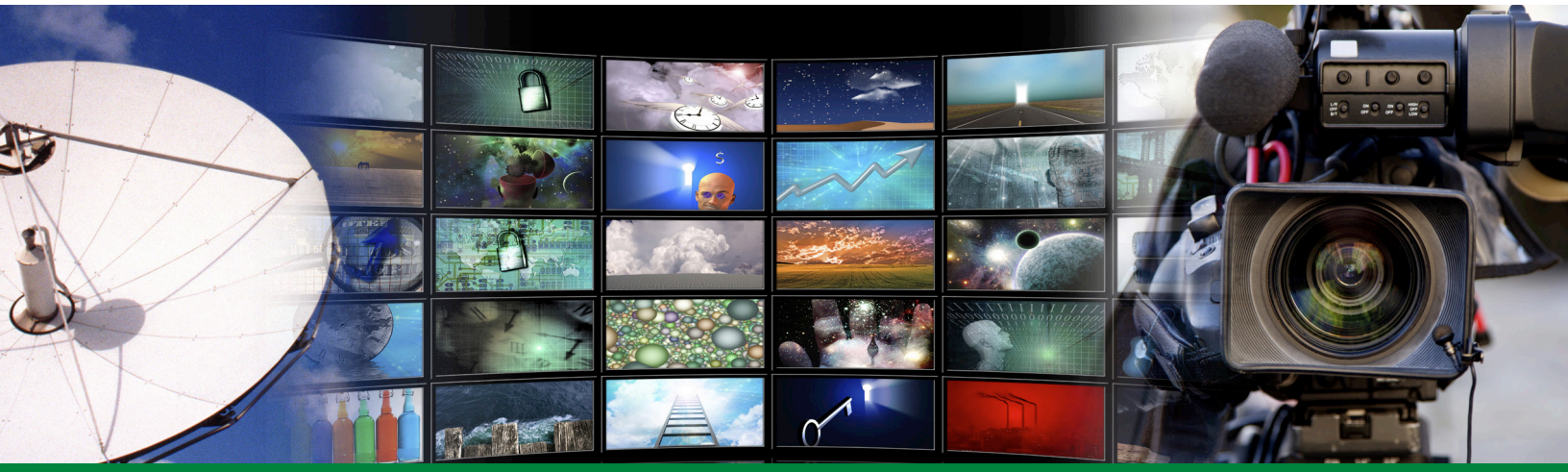
Case Study

VECTRA®
Security that thinks®



Broadcast news

Media outlets are juicy targets for hackers, and Tribune Media is doing all it can to protect its high-value assets, including television and radio stations, with strong defenses. Its newest defense is real-time detection and analysis of active network breaches.

Tribune Media gets the scoop on network breaches

Tribune Media defines itself as a 167-year-old persistent startup, and recent successes show they are a media company with canny survival skills. While many media outlets crashed and burned adjusting to an online, mobile world, Tribune Media excelled in engaging and connecting viewers across the nation with content across every distribution platform.

The Chicago-based media company is the nation's largest independent broadcaster with 42 television and radio stations that reach more than 70 million households. WGN America, the company's national entertainment network, is available in 73 million households. The company's other holdings include Tribune Studios, Gracenote and WGN-Radio. Altogether, Tribune Media's outlets are busy content engines producing local news, original programming and sporting events.

Know the unknown

"Every security organization's biggest challenge is knowing what you don't know," says Duane Smith, chief information security officer at Tribune Media. Smith joined the company in 2014, after the company spun out its newspaper business to focus on broadcasting and digital media.

"I was hired to build a security infrastructure from the ground up, and we had a lot of security tools in place," says Smith. "We were missing a solution that would give us real-time network visibility."

Tribune Media Group

Organization
Tribune Media

Industry
Media

Challenge
Detect security breaches at Tribune Media's headquarters and broadcast stations

Selection criteria
Real-time visibility into network breaches

Results
- Identified unexpected and unknown security threats
- Gained single view of threats across the enterprise network, including remote sites
- Prevented wasting time uncovering false positives

After hearing about the Cognito™ automated threat detection and response platform from Vectra® and its ability to detect and analyze network breaches in real time, Smith invited the Vectra team in for a meeting. Confident that Vectra would prove its value, the Vectra sales team offered to let Tribune Media test the platform—no strings attached.

"I immediately saw the value of Vectra," Smith says. "I was doing a lot of intrusion detection, and I was doing a lot of guesswork. Vectra took the guesswork out of detecting credible threats."

We'd be blind without Cognito

Modern attackers thrive on their ability to persist and spread through a network to eventually gain access to key assets, and a large media company has inherent complexity given the number of network sites and content traffic it manages. Cognito constantly analyzes traffic to detect all phases of these stealthy attacks, including internal reconnaissance, the lateral spread of malware, theft of account credentials, accumulation of data, exfiltration and other hidden communications. Detections are based on a combination of data science, machine learning, and behavioral analysis.

Tribune Media deployed an Vectra X-series appliance in its data center in Chicago, to provide real-time visibility into both internal and Internet-bound network traffic. To detect cyber attackers that might be hiding in its remote locations, the company is deploying Vectra S-series sensors at its 42 broadcast stations to provide expanded coverage and monitoring.

"When we first looked at Vectra, we thought we'd take a crawl, walk, run approach and put it in key sites as needed. But we realized that it had to be all or nothing or we'd leave ourselves open to problems at a remote site where I don't have a Vectra sensor," says Smith. "We can't have someone hack in on a TV station and upload videos before they go on the air. We'd be blind in those sites without Vectra showing us what threats are coming in and out of the network. My biggest nightmare was an attacker coming in from a remote station, spreading through the network and gaining access to key assets over time. The S-series solves that problem by protecting us everywhere."

A direct route to stop an attack

Cognito provides prioritized and contextual alerts to enable quick action to stop an attack. Alerts are automatically correlated by the host and displayed on the intuitive Threat Certainty Index™. Smith and his security operations team can quickly spot the specific hosts that pose the greatest risk to the network and immediately focus on detections that matter the most.

"Vectra is threat detection on steroids," says Smith. "Vectra does the homework for me. It will tell me, 'We think you're having an infiltration, such as a brute force,' and I can dig deep in and get to the real problem." From there, the team has single-click access to the threat details. "With Vectra, I can look at the packet captures and the traffic to find the root cause to potential security threats," he says.

In addition to detecting targeted attacks and insider breaches, the Tribune Media team can use Cognito to track misconfigurations, high-risk applications, or out-of-policy behaviors that can potentially enable or hide an attack.

Support that is second to none

The ability to detect and analyze network breaches in real time has differentiated Cognito from Tribune Media's other security products, and Vectra's post-sales support has made Vectra a staff favorite. The Vectra team quickly responds to any questions about features or functions with an immediate phone call and answers, which in turn helps the Vectra product team create product enhancements for the future based on the close relationship with Tribune and other customers.

Smith says that Vectra's responsiveness is much different from what he's experienced with other companies. "Anyone can sell me a good product, but who is going to be there after the sale? Vectra's aftersales support is second to none."

> *"Vectra is threat detection on steroids."*
>
> Duane Smith
> CISO, Tribune Media

VECTRA
Email: info@vectra.ai
Tel: 1 408-326-2020
vectra.ai