Anywhere Real Estate Flips Security Posture With CrowdStrike

Anywhere Real Estate is an $8 billion real estate conglomerate with its main hub in Madison, New Jersey. As a company **recognized for its innovation by Forbes**, Anywhere continuously upgrades its tech stack to boost productivity and protect its business.

Artificial intelligence is a great example. Over the past few years, the company has been on the vanguard of operationalizing AI, having introduced an agent-recruiting machine learning model to help determine which agents are likely to excel, among several other AI initiatives designed to empower agents, employees and homebuyers.

The company leverages its industry-leading dataset to power its AI initiatives. And critically, this data needs to be protected, as well as the company's endpoints, systems and reputation.

To that end, Anywhere recently upgraded its security stack to include CrowdStrike Falcon® Insight XDR for endpoint detection and response and CrowdStrike® Falcon OverWatch™ Elite for 24/7 managed threat hunting.

This is the story of how an innovative company thinks about security in the modern age, as evidenced by its evaluation, testing and implementation of the CrowdStrike Falcon® platform.

A Thorough Test of Security Vendors

With wire fraud attempts and other cyberattacks growing in speed and sophistication, Anywhere examined its security stack built on legacy tools for antivirus and endpoint detection and response (EDR).

One problem was alert fatigue, explained Brett Fernicola, Senior Director of Security Operations, Cybersecurity and Incident Response at Anywhere. "Our EDR had out-of-the-box rules, but we were getting up to 30,000 alerts per day."

To reduce the noise, he and his team began building their own detections, but they took a long time to write and test, pulling the team away from other tasks.

"We exhausted the amount of time and energy we could spend constantly tuning the product, so we started looking around for a new player … one that curated the data and provided built-in detections and threat intelligence so we didn't have to spend every waking hour ensuring the product functioned as desired," said Fernicola.

Anywhere

INDUSTRY

Real Estate

LOCATION/HQ

New Jersey, USA

CHALLENGES

- Anywhere Real Estate had a legacy security stack that was ineffective against modern threats.
- The company was getting upwards of 30,000 alerts per week, obscuring critical incidents.
- It wanted 24/7 managed threat hunting, but couldn't afford the service along with its legacy EDR and AV tools.

SOLUTION

Anywhere Real Estate uses CrowdStrike Falcon Insight XDR for endpoint detection and response and CrowdStrike Falcon OverWatch Elite for 24/7 managed threat hunting.

RESULTS

- Zero breaches with CrowdStrike
- One platform for modern endpoint security
- 500x fewer alerts
- 98% of alerts are true positives
- 24/7 managed threat hunting

Anywhere also wanted to consolidate to one security platform for endpoint protection and next-gen antivirus. Its legacy stack had multiple agents from multiple vendors — all competing for CPU and memory, which slowed things down and added complexity.

"The legacy AV mentality is to run scheduled scans on all files, but the juice isn't worth the squeeze," explained Fernicola. "With CrowdStrike, only the files being accessed or modified are inspected, which was a big win for us."

Finally, Anywhere wanted a fluid and easy interface to export data for threat hunting.

"In a breach scenario, we need our EDR product to be effective in the hands of a junior incident responder. They shouldn't have to be an expert in scripting or database languages to retrieve info and search for IoCs," said Fernicola.

With this long list of requirements, Anywhere compared CrowdStrike against other security vendors. During the test, Fernicola performed common malware and virus executions to ensure the basic functionality was there. He also did advanced red-team testing for lateral movement, dumping passwords and hashes, and other actions. The difference was clear when Fernicola tested data-exporting functionality.

"One security vendor absolutely failed," said Fernicola. "They collect all the data but there's no schema or documentation for exporting. For another vendor, the process required too many clicks and was too prone to errors."

Anywhere found the performance it needed in CrowdStrike.

"With CrowdStrike, we can easily export and search data for threats. Then, if we want to take the next step and go into the details, that process is straightforward," said Fernicola. "Plus, only CrowdStrike delivered a unified view of our security posture from one command console."

Consolidating with CrowdStrike

Today, Anywhere uses Falcon Insight XDR for endpoint detection and response. The **market-leading EDR product** was deployed rapidly without friction or reboots across 20,000 endpoints, including every Linux, Windows and Mac endpoint at the company, covering 100,000 users.

"It's two for one," said Fernicola. "We get an aggressive detection and blocking policy. "Plus, we can set it and forget it. If someone introduces a security risk, Falcon Insight will either block it or alert us right away if something nefarious happens."

Managed threat hunting was another major win for Anywhere. With only a handful of full-time security staff, Anywhere now relies on Falcon OverWatch Elite for 24/7 eyes-on-the-glass managed threat hunting with designated analysts. As a result, alerts have dropped by 500x.

"With our legacy tools, we struggled to know which alerts were valuable," said Fernicola. "OverWatch Elite takes the noise out of alerts. We now get around 200 alerts per month and 98% are true positives. There's no noise, no junk ... If it hits, it's a problem and we're investigating it."

For Anywhere, having experts watching over its environment provides peace of mind.

"With Falcon OverWatch Elite, we have experts watching over our environment 24/7. When something suspicious happens, we get a phone call so we can figure out what's happening and shut down the attack within minutes," said Fernicola. "That alone is worth its weight in gold."

"With Falcon OverWatch, we have experts watching over our environment 24/7. When something suspicious happens, we get a phone call so we can figure out what's happening and shut down the attack within minutes. That alone is worth its weight in gold."

–Brett Fernicola, Senior Director of Security Operations, Cybersecurity and Incident Response, Anywhere Real Estate

---

ENDPOINTS

20,000

CROWDSTRIKE PRODUCTS

- Falcon® Insight XDR endpoint detection and response
- Falcon OverWatch™ Elite managed threat hunting
- Falcon® Prevent next-generation antivirus
- Falcon® Firewall Management

By consolidating to the Falcon platform, Anywhere gets a single lightweight agent for modern endpoint security plus Falcon OverWatch Elite at a price it can afford.

"With CrowdStrike, we were able to sunset legacy AV, sunset legacy EDR and consolidate our budget to afford Falcon Insight with Falcon OverWatch," said Fernicola. "From a productivity and efficiency standpoint, there's tremendous value in consolidating on the Falcon platform."

Best of the Best

With its modern security stack in place, Anywhere further cements its reputation as a highly innovative company, hellbent on using technology to power and protect its business.

"We have the best of the best with CrowdStrike," concluded Fernicola. "For us, using the Falcon platform along with OverWatch puts us in the 99th percentile for security. As both companies continue to innovate, I look forward to seeing where this great partnership can take us."

ABOUT CROWDSTRIKE

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data. Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

CrowdStrike: **We stop breaches.**

Follow us: **Blog** | **Twitter** | **LinkedIn** | **Facebook** | **Instagram**

CROWDSTRIKE

we stop breaches

Learn more **www.crowdstrike.com**