runZero

Case Study

Increased network visibility led to the discovery of over **50% more** assets.

Meet the Security Expert

Jason Waits

Chief Information Security Officer

Inductive Automation empowers the world's top companies within the energy, manufacturing, life sciences, and other critical industries with their unparalleled solution, Ignition, a universal industrial application platform for connecting all data, and designing and deploying industrial applications throughout an enterprise.

With thousands of global companies depending on Ignition every day, Waits and his team felt compelled to strengthen their security program and close security coverage gaps with the aim of decreasing third-party risk to their customers.

It was important for Waits to demonstrate that Inductive Automation was a trustworthy partner that their customers could count on for prioritizing security. They set out to find a formal asset management solution to reclaim control of their network.

inductive automation

Company Size

275 employees

Industry

Automation Machinery Manufacturing

Location

Folsom, California

Use Cases

- Cyber asset discovery
- Incident response
- Security hygiene

Problem

Scaling security features

At Inductive Automation, success translates to continuous, pragmatic company growth, where breaches and outages are minimized, vulnerabilities and insecure misconfigurations are proactively identified, responded to, and fixed. When Jason Waits, CISO at Inductive Automation, joined the organization over 7 years ago and discovered they didn't have a dedicated asset management tool, he knew a robust solution was necessary to take back control of their network.

When I started in IT at Inductive Automation, we didn't really have a dedicated asset management tool.

"We could sign into vCenter, see our VMs, or our EDR and Active Directory to see many endpoints. But at the end of the day, I would still run Nmap and map it out myself. It was a weak, hodgepodge approach that was scary because it didn't scale to keep up with our growth. I'm a big fan of asset management in general. It's difficult to secure things and prioritize when you don't know what you have. That was our big pain point."

Jason Waits
Chief Information Security Officer

RESEARCHING TOOLS

When Waits was promoted to head of security, he led the research efforts to understand all asset management options on the market. It was critical for them to find a comprehensive solution that could scan their entire network, offer network discovery for visibility into all IT, IoT, and OT assets on their network.

COMPETITORS COULDN'T MEET REQUIREMENTS

They tried many solutions, but they lacked detailed and accurate data, and in some cases, incorrectly identified devices as Linux boxes, among other issues:

Axonius didn't deliver enough value for the money, and the data they pulled was surface level.

Nessus wasn't the right fit due to performance issues; the UI/ UX lacked efficiency in that they needed to double-click into each host for more detail, and the data that the system reported back also lacked granularity.

JupiterOne wasn't a viable solution since it's a pure cloud security solution.

Solutions

Testing runZero for **free**

Inductive Automation discovered runZero and decided to test it out.

IMMEDIATE BENEFITS

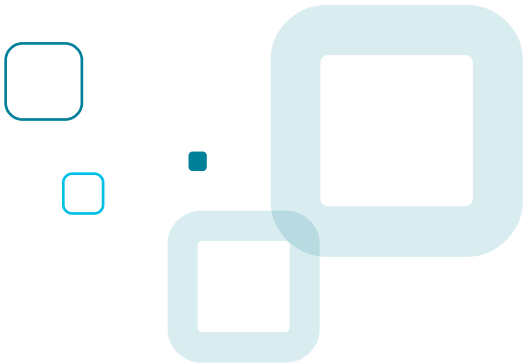
Inductive Automation became a customer and shortly after they renewed, runZero announced a CrowdStrike integration for providing insight into unknown assets lacking CrowdStrike EDR, which ultimately was the deciding factor for upgrading to the Enterprise tier.

"As soon as I turned on runZero's CrowdStrike integration and once I saw it working in action, I immediately deprecated Forescout."

SIGNIFICANT ASSET DISCOVERY

The team now enjoys runZero's cyber asset discovery capabilities for gaining visibility into what exists on their network. In fact, they have been able to discover over 50% more assets on their network, thanks for runZero.They also leverage runZero to accelerate remediation, taking advantage of the many out-of-the-box queries to expedite incident response.

I checked the runZero website and there was a free trial, which I love. I downloaded it and immediately scanned a couple of subnets. The UI/ UX was user friendly, and the classification was incredibly detailed.

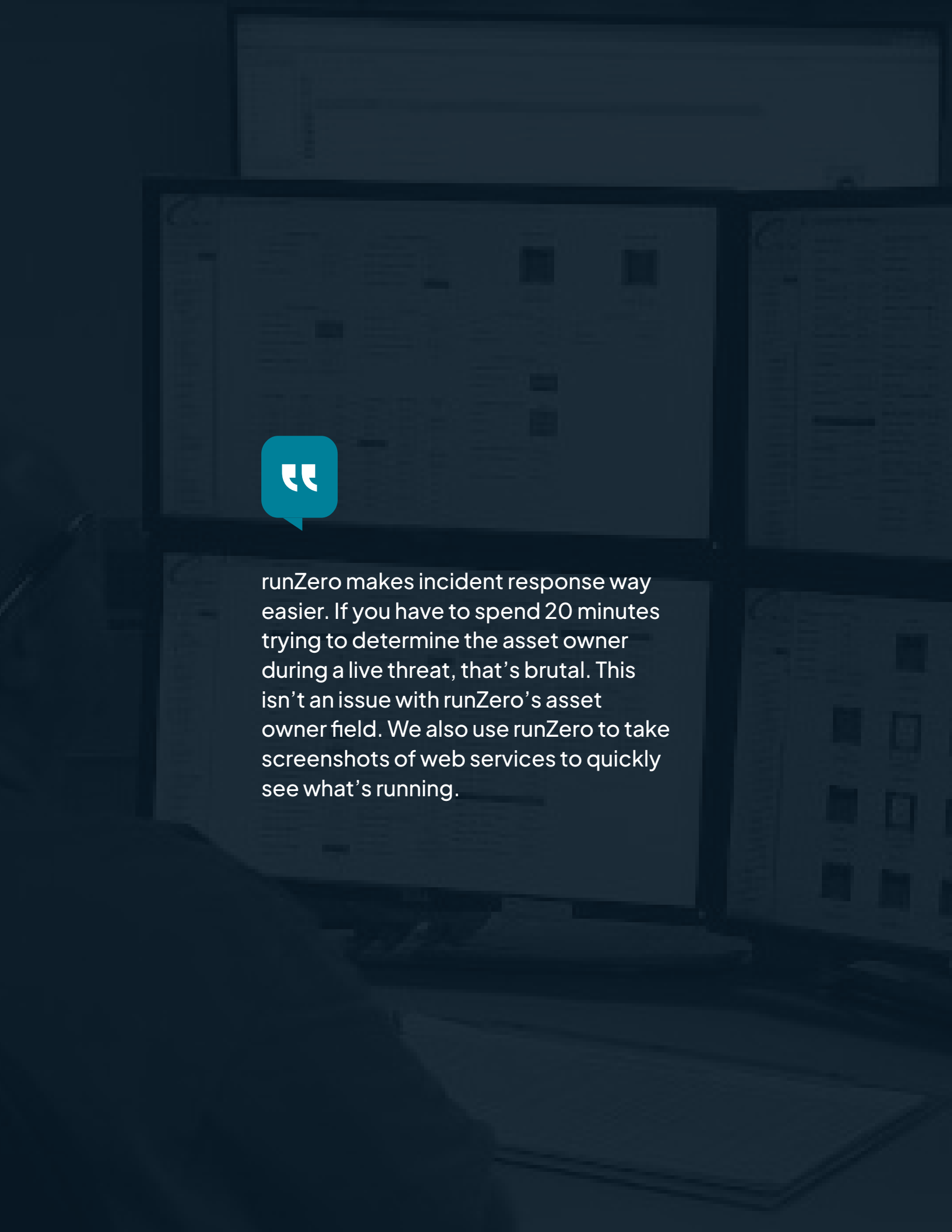


We absolutely use runZero to help speed up incident response. If there's a new open SSL vulnerability, runZero is quick to release some helpful queries. I'm a huge fan of that. I don't have to write the query, so one of my analysts can copy and paste that query should I be out of the office.

FEELING SUPPORTED

runZero's customer support team has provided Waits with the proactive, rapid response he needs to keep the Inductive Automation security program running smoothly.

"Your support team is fantastic. It's crazy how they reach out to tell me they fixed a bug I encountered that I didn't report. That's happened numerous times. And when I do submit a bug report, it's handled quickly."



runZero makes incident response way easier. If you have to spend 20 minutes trying to determine the asset owner during a live threat, that's brutal. This isn't an issue with runZero's asset owner field. We also use runZero to take screenshots of web services to quickly see what's running.

Outcomes

Increased **efficiency**

runZero has helped increase the efficiency of Waits and his team when it comes to asset discovery, incident response, and security hygiene, contributing to significant time savings of a few hours per week. This is valuable time where they can redirect their focus on other vital areas.

RUNZERO FOR THE WIN

Between offering valuable integrations, visibility into their network, and exceptional support, Waits and his team have developed the utmost trust and reliance on runZero. It has become such an integral part of Inductive Automation's security program that Waits and his team have incorporated runZero into their morning routines.

"runZero's release notes are morning reading for my team. I sign into runZero every day. I sit down, drink coffee, pop into runZero, CrowdStrike, Chronicle, and look for any fires as part of getting situated for the day."

COST-EFFECTIVE WITH NO COMMITMENTS

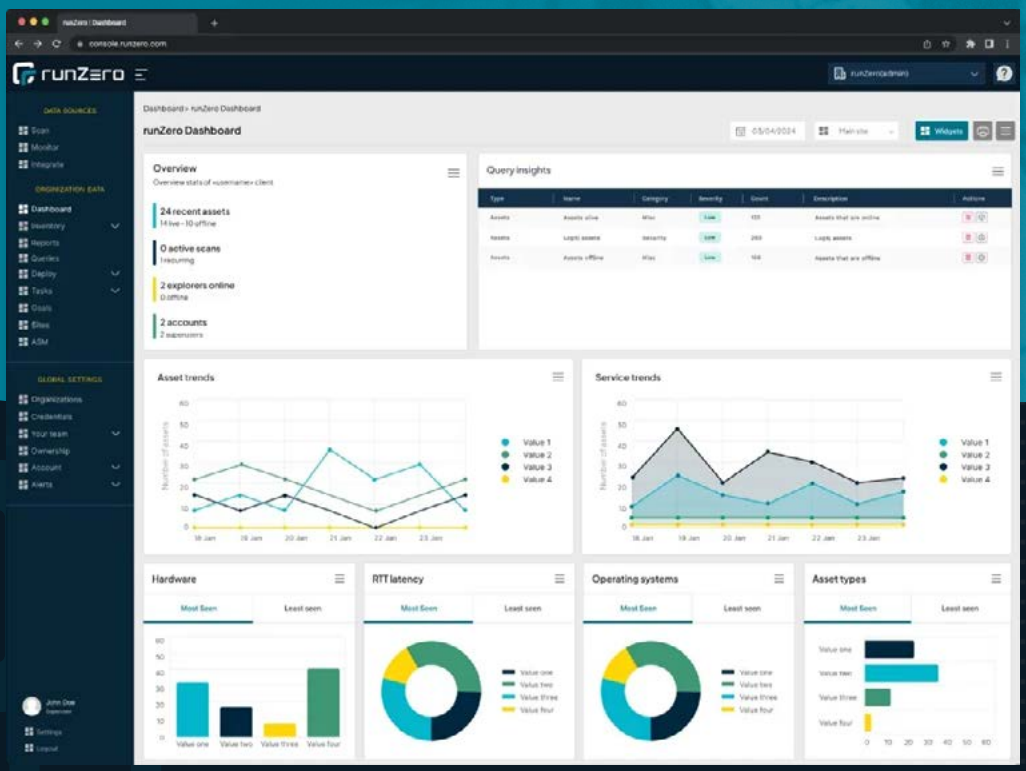
Additionally, runZero's unmatched capabilities and benefits are available at competitive pricing when compared to other solutions on the market. Inductive Automation found that runZero's total cost of ownership was 90% lower than other solutions they tested, and they were not required to commit to a multi-year deal. Together, this makes a significant difference for a smaller, mid-market organization like Inductive Automation.

Final Thoughts

Waits had a few parting words to sum up his experience so far with runZero:

> runZero sets a high bar for how I expect other tools to perform, from having a user-friendly UI/ UX, to clean, accurate data, I don't have to second guess.

Jason Waits
Chief Information Security Officer



About runZero

runZero delivers the most complete security visibility possible, providing organizations the ultimate foundation for successfully managing exposures and compliance. Rated number one on Gartner Peer Insights, their leading cyber asset attack surface management (CAASM) platform starts delivering insights in literally minutes, with coverage for both managed and unmanaged devices across the full spectrum of IT, OT, IoT, cloud, mobile, and remote assets. With a world-class NPS score of 82, runZero has been trusted by more than 30,000 users to improve security visibility since the company was founded by industry veteran HD Moore. To discover the runZero Platform for yourself, start a free trial today or visit the website.

Reduce overall risk by gaining visibility into your network.

Try runZero for Free