runZero

Case Study

Improved security posture with accurate asset discovery to detect missing EDR solutions.

Meet the Security Expert

Dan Paulmeno

Director of Managed Security Services

Kivu Consulting is an incident response consulting company that specializes in post-breach remediation, managed security services, and security program maturity support for their customers. They were witnessing the challenges their customers were facing with improperly deployed security rules and not knowing which assets were missing EDR agents.

Paulmeno and his team needed to provide their customers with a solution for asset inventory and management to impart vital insight into the assets on their networks. Additionally, they needed to be able to determine their level of risk to reduce their security vulnerabilities and prevent future attacks.

Company Size

72 employees

Industry

Computer Software

Location

Berkeley, California

Use Cases

- Cyber asset discovery
- Threat hunting
- Track down news-making vulnerabilities and exploits

Problem

Enhanced security offerings

Kivu Consulting prides itself on ensuring that their customers are protected from the minute they hear from Kivu Consulting.

While they already offered robust incident response and mitigation services to their customers, they saw an opportunity to broaden and enhance their services. They sought out an additional solution to empower their customers to be more proactive in their cyber security and strengthen their defense against ransomware and other attacks in the future. Kivu Consulting knew that with a highly capable cyber asset discovery, inventory, and remediation solution in place, they could become their customers' primary source for complete defense.

WRONG TOOLS AND OUTCOMES

During their research for an ideal solution, they observed that other solutions (like JupiterOne) didn't support key integrations with cloud and endpoint protection vendors, such as CrowdStrike and Microsoft Azure. Additionally, other solutions (like Tenable) were difficult to deploy and required a lot of manual effort, technical expertise, and training. It was important to the Kivu Consulting team to hone in on a solution that would provide visibility into the assets on their customers' networks and identify which endpoints lacked EDR. This new visibility would also provide Kivu Consulting and their customers with a blueprint for building a tailored security improvement strategy for their unique environments.

Solutions

Immediate asset **discovery**

Before introducing runZero to their security solution package for their customers, Kivu Consulting initially tested it internally. They deployed runZero during the mass work-from-home movement triggered by COVID-19 to discover unmanaged remote assets and to determine which devices were risky, outdated, out of compliance, or missing security controls.

We initially used runZero internally in a work-from-home environment during COVID-19.

"We were trying to track down everything and look for rogue assets and that was tough to deal with. With runZero, we were able to segment networks, see if work-from-home devices were still being used and put together a plan for returning them for reimaging and sending them back out. runZero was an invaluable tool early on, and these use cases and benefits sold our board to deploy it to our customers on a broader scale."

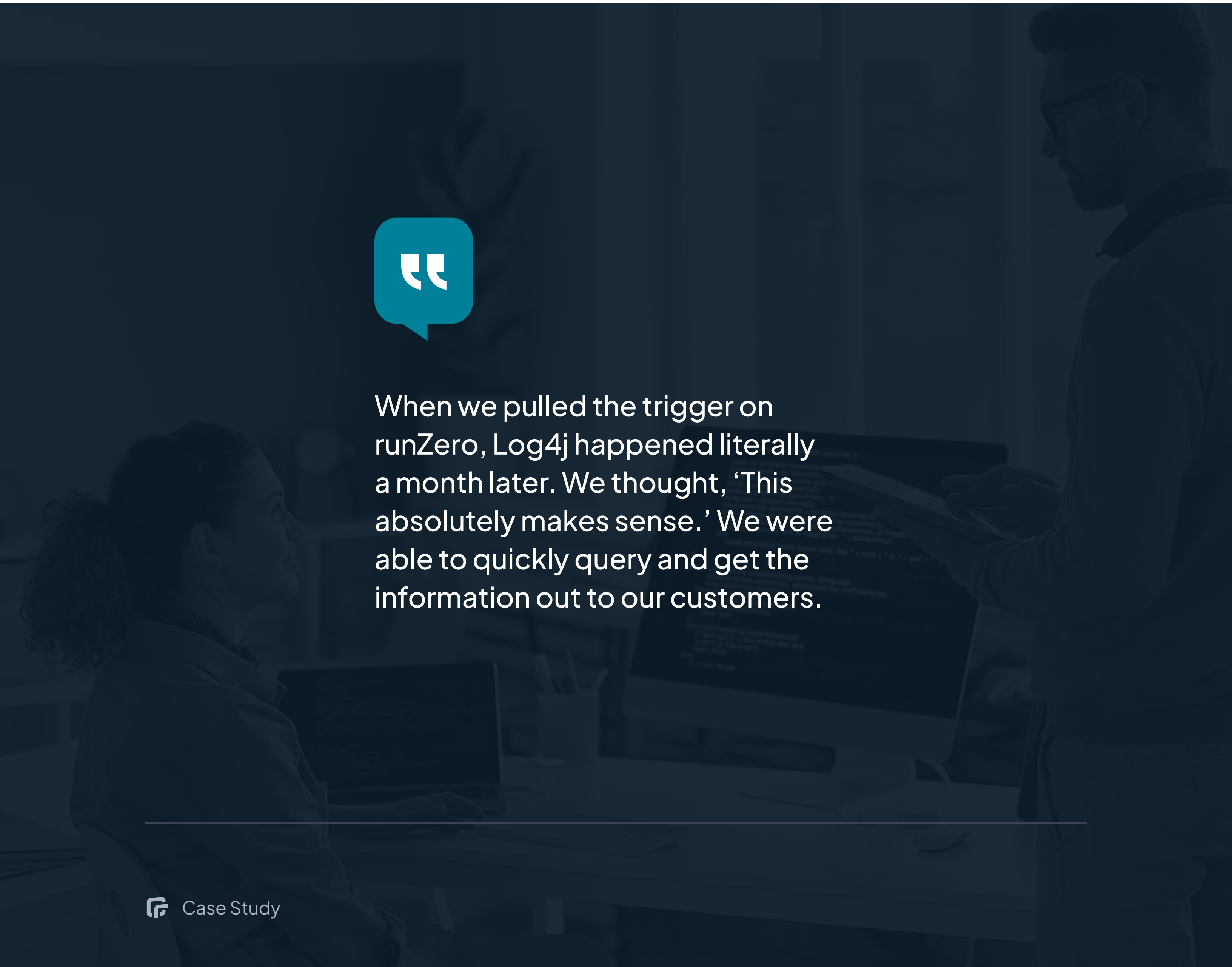
Dan Paulmeno
Director of Managed Security Services

RIGHT PLACE, RIGHT TIME

After deciding that runZero was the right fit, Kivu Consulting happened to roll out their new security solution during the initial emergence of Log4J. Luckily, runZero was firmly in place to quickly support Kivu Consulting and their customers through this zero-day vulnerability by using canned queries; there was no need to re-scan their networks.

NEW VULNERABILITY? NO PROBLEM

Since Kivu's adoption of runZero, many additional vulnerabilities and risky misconfigurations have appeared themselves, including ESXi, Nevada ransomware, publicly accessible RDP, Kaspersky, and SMBv1. With each new vulnerability and risky misconfiguration, runZero has proven to be a vital tool in Kivu's arsenal to get ahead of potential security threats and to take swift preventative action for their customers.



> When we pulled the trigger on runZero, Log4j happened literally a month later. We thought, 'This absolutely makes sense.' We were able to quickly query and get the information out to our customers.

Outcomes

Cost-effective **solutions**

runZero has been a source of cost savings for Kivu's Consulting's customers; runZero eliminates the need to pay for unnecessary security vendors.

INCREASED NETWORK VISIBILITY

Additionally, by having insight into the assets on their customers' networks and identifying endpoints without EDR solutions, Kivu Consulting can now effectively monitor the quantity of assets requiring EDR software. This insight ensures that their customers aren't overcharged. This also helps them improve the accuracy of their sales strategy, and thus their overall operational efficiency.

"We're now able to project better for accompanying renewals and quarterly true ups. We're able to stay ahead on our licensing count to make sure that we aren't charging any overages. So, from a revenue collection, runZero helps our team as well."

We support a university whose leadership wanted a comprehensive list of ALL endpoints on their network.

"With runZero's asset ownership feature, they now can see who owns assets and who doesn't and where these assets are going rogue. They can assign them to their team without buying an additional remote vendor to do all this auditing."

ONE-STOP SHOP FOR SECURITY

Between runZero's ability to report back granular data, like asset ownership and EDR saturation for full network visibility, canned queries to save valuable time during zero-day vulnerabilities, and ease of deployment and use, working with runZero has become an important competitive advantage for Kivu Consulting and their customers.

PROACTIVE CYBER SECURITY EFFORTS

Due to its dependability and key capabilities during the early, critical incident response hours, or advising customers with queries focused on Log4J, ESXi, Nevada ransomware, Kaspersky, and outdated SMB versions, runZero has become Kivu's go-to cyber asset discovery and remediation solution for a truly proactive approach to cyber security.

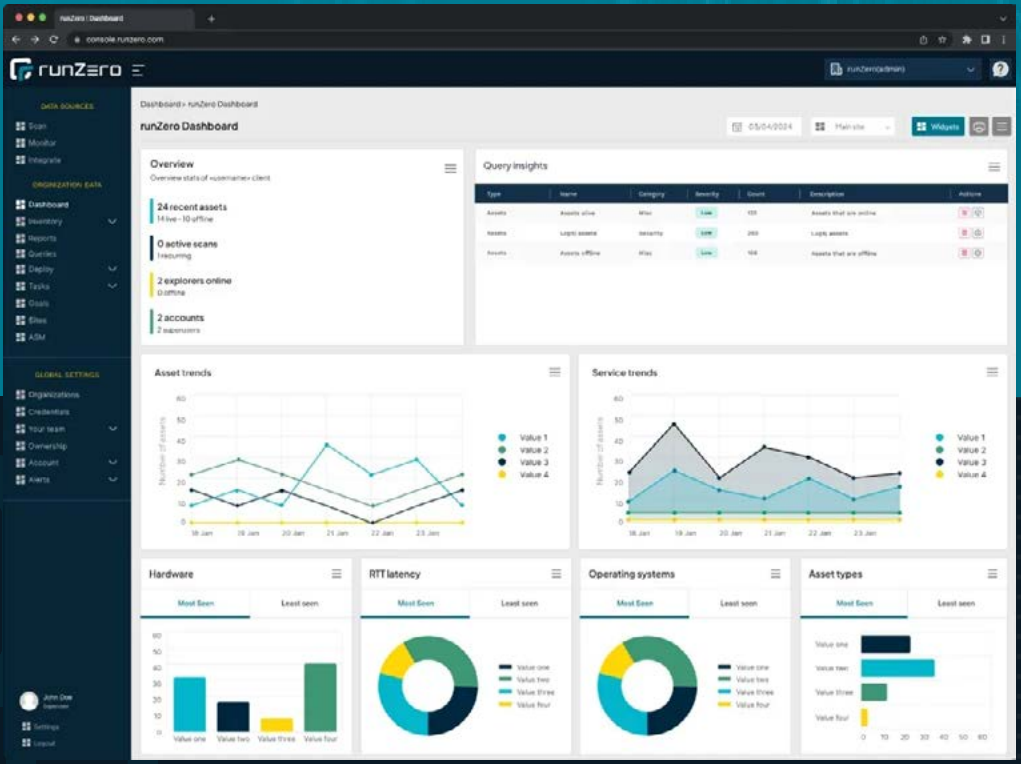
> We have clients coming out of incident response engagements where they're asking about some of these zero-day vulnerabilities and exploits. Oftentimes, runZero already has a search query in place for us. So, from a threat hunting and proactive security standpoint, these queries are a huge advantage in time saving and information gain.

Final Thoughts

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

> runZero has been the first place we go for most of our customers. With that threat, we can quickly pivot and check whether a customer is safe or if they need advisory. With the information you provide on your blog, you have become a one-stop-shop. We've developed a weekly ritual to check if there is a new vulnerability. We'll check runZero and CrowdStrike and then correlate data from the two. And that's been awesome.

Dan Paulmeno
Director of Managed Security Services



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