runZero

Case Study

Discovering nearly **20% more** assets than previously known.

Russell Fulton
Security Engineer

Paul Wescott
Security Architect

Meet the Security Experts

With the University of Auckland's increasing success, growth, and expansion, Fulton, Wescott, and their small team of 6 people struggled to keep up with supporting the university's need for overall cyber security, including desktop servers, applications, incident response, security architecture, and engineering.

Fulton and Wescott knew they needed to improve visibility into the complete scope of assets on the university's network. After reading about runZero on social media, the team quickly adopted the solution and never looked back.

UNIVERSITY OF AUCKLAND
Waipapa Taumata Rau
NEW ZEALAND

Company Size
12,000 employees • 45,000 students

Industry
Higher Education

Location
Auckland, New Zealand

Use Cases
- Cyber Asset Discovery
- Cyber Asset Inventory
- Cyber Risk Management
- Incident Response
- Cyber Asset Hygiene
- CAASM

Problem

High expectations in higher education

Since its founding in 1883, the University of Auckland has grown to become New Zealand's flagship, research-led university, known for excellence in teaching and researching.

Recently, the university achieved the ranking of 68 in the Quacquarelli Symonds (QS) World University Rankings, marking an enormous level of success for the university, and acting as a clear indicator of the excellence and global reputation of the university.

With an expanding university and growing demands, Fulton, Wescott, and their team realized they needed a viable security solution.

LACKING VISIBILITY AMID GROWING NEEDS

Both Fulton and Wescott understood they needed better visibility into the assets on the university's network, a growing problem with the sheer volume of devices expanding on a daily basis.

> Just simply, I had reached the point where I needed a team to do what I was doing just as one person. The amount of effort was far too high.

Paul Wescott
Security Architect

It's important to be able to be secure in our knowledge of what is going on.

"That was a huge issue with the university. With 45,000 students and 12,000 staff bringing roughly 20,000 devices on campus every day on top of the devices we already have on campus, it's the size of a small city."

Russell Fulton
Security Engineer

STARTING THE SECURITY SEARCH

With these pressing needs top of mind, the team began their search for a comprehensive cyber security solution that would support their small team in cyber asset discovery, cyber asset inventory, cyber asset attack surface management (CAASM), and remediation.

"We have so much stuff on our network, you just can't believe it. We've got research equipment, vacuum cleaners, everything you can think of. That's a lot to keep secure."

Paul Wescott
Security Architect

SCALING WITH LIMITED RESOURCES

Despite the University of Auckland's many accolades and high rankings, the team suffered from limited funding, a challenge that Fulton and Wescott knew they would need to consider when searching for a solution.

"We generally can't afford expensive tools, so we've usually had to build our own."

Russell Fulton
Security Engineer

WRONG TOOLS, WRONG RESULTS

While the team previously used Nmap, it wasn't a viable solution for them in the long run because the tool didn't offer:

- A central console to view and manage assets
- A history of asset discovery
- A supported integration with other tools, such as Tenable or LDAP

TRICKY TOOLS

The team used Tenable, but grew frustrated with its credential-less discovery capabilities, lack of detailed fingerprinting, inability to scan some assets using credentials, and its lack of a user-friendly user interface. Additionally, jerry-rigging Tenable to find vulnerabilities when there wasn't a specific CVE or signature was difficult.

"We would do Nmap scans a lot of the time, or we would try to do Tenable scans across the network, neither of which were particularly useful."

Paul Wescott
Security Architect

NOT A COMPLETE SOLUTION

The university eventually adopted ServiceNow, but Fulton and Wescott quickly realized its shortcomings.

With Tenable, we were also highly constrained by license and the number of assets we can support.

Russell Fulton
Security Engineer

ServiceNow is still ongoing, and we've yet to produce results. Also, there's only so many assets that we're licensed to actually discover with that, which is a fraction of the number of assets that we have on the University network. ServiceNow is a great tool, but it doesn't deliver for us the information that we need about all of our assets, in part because we have an asset limit. If you can only have a small window into some of your assets, that's not helpful.

Paul Wescott
Security Architect

Solutions

Introducing **runZero**

In their on-going search for a fitting solution, Wescott came across runZero (formerly Rumble) by happenstance.

"I was going through my X feed (formerly Twitter) in the middle of the night. I saw something about this solution called runZero. I was like, 'Oh that looks like what Russell is always saying he wants to build.' I sent it to Russell and by the next day, he had it up and running."

Paul Wescott
Security Architect

SIMPLE DEPLOYMENT

From the beginning, they enjoyed how easy it was to deploy and start using right away.

APPROVED BY SECURITY PROFESSIONALS

The team has appreciated that runZero was made by cyber security professionals, for cyber security professionals, making for an intuitive, easy-to-use solution.

It is the easiest install I think I have ever done.

Russell Fulton
Security Engineer

"runZero has always been super responsive. I mean, I don't think HD actually sleeps. When we first started with runZero, I might see something and report it in New Zealand time, which might be in the middle of the night in the US. Maybe 2 minutes later I'd hear back, 'Thanks for that, I got a new fix coming through, that'll be there tomorrow.

Paul Wescott
Security Architect

When we look at other tools, they're clearly designed by someone who's never had to use that tool.

"That's not something that we would say about runZero. It's designed very carefully to provide the information in a consumable way that people like us want to see it in. runZero is a really user-friendly, well thought out tool. It's also got a really good user interface that gives you the information that you're looking for in an easy to find way. On the other hand, every time I go into Tenable, they change how things work. I'm trying to find things and it's just not intuitive."

SUPPORTED INTEGRATIONS

The team has also taken advantage of runZero's integrations with Tenable and Active Directory to further enrich their asset data from these existing tools.

"Having as much information in one tool is very helpful to build a full picture of an asset. It means that we don't necessarily have to go and look in multiple places for information on an asset, which saves us time."

INTEGRATING WITH ACTIVE DIRECTORY

The team particularly enjoyed the Active Directory integration, as it provides information within runZero that they might otherwise not see.

"Interfacing with the Active Directory integration is really useful. If remote users are infrequently or never on the network and might never have their assets scanned, the Active Directory integration will still pull their information into runZero. This integration can find gaps in scanning caused by segmentation where LDAP details exist but an asset is not scanned. The Active Directory integration also provides much more accurate information about the operating system versions, and therefore improves the accuracy of the data."

Paul Wescott
Security Architect

Outcomes

Discovered more assets

Asset discovery with runZero's proprietary network scanner, paired with available integrations has provided the University of Auckland with comprehensive insight into the university network, helping them uncover significantly more assets than they knew existed, as much as 20% more to be exact.

By leveraging runZero, they've eliminated much of the manual labor and configuration work that was previously necessary when conducting manual scans with their former tools. This has resulted in saving over 20 hours per week in manual effort—a truly valuable benefit, especially when supporting hundreds of customers.

IMMEDIATE RESULTS AND BENEFITS

With this newfound knowledge and a clear map of the devices on the university network, the team has gained confidence in the solution. Relying on runZero's capabilities for CAASM and locating potentially exposed systems has enabled Fulton and Wescott to reap key benefits, including decreased time needed to find assets in their environment, and in turn, decreased incident response times.

We definitely found a lot more assets with runZero. I would say somewhere between 10% and 20%. With runZero, it's like night and day. It's like turning the light on and now you can see everything.

Paul Wescott
Security Architect

We recently learned of Microsoft announcing end of life for a large chunk of Windows 10. Our boss asked, 'How many assets of ours are affected?' About a half hour later, we could come back with a full report from runZero.

"We'll find out about these zero-day vulnerabilities, which seem to happen every other week. Whatever it is, there might be a query on runZero, which we can just go and use to find it. Sometimes runZero will tell you you're running a vulnerable version of it. Then we can go scan it with Tenable."

Russell Fulton
Security Engineer

BATTLING ZERO-DAY

runZero has been a valuable tool in their arsenal for quick zero-day vulnerability response, and has even helped reduce the number of gaps in their vulnerability scanning.

QUICK DETECTION AND TROUBLESHOOTING

The team experienced an instance where an insecure misconfiguration was detected and they were able to use runZero to determine which assets were affected and take immediate action.

"We had a network configuration where some IPv6 was being tunneled over IPv4. We use Shadowserver, which notified us that we had IP open to the world. It was using the 6 to 4 protocol. With that information, we were able to use runZero to find out all of the servers that were affected by that and then address that particular issue. That was a really helpful situation for us where runZero was a useful tool."

Paul Wescott
Security Architect

GAINING CONFIDENCE WITH RUNZERO

Wescott wrapped up his thought about leveraging runZero for obtaining a comprehensive view of their attack surface.

"It happens usually on a weekly basis that we'll find new vulnerabilities, whether it's some Atlassian issue or something to do with F5s. We know we've got F5s but do we know every one that we've got? So just being able to find all of the F5s and make sure and know they're all being patched gives us that peace of mind that we otherwise might not have. "

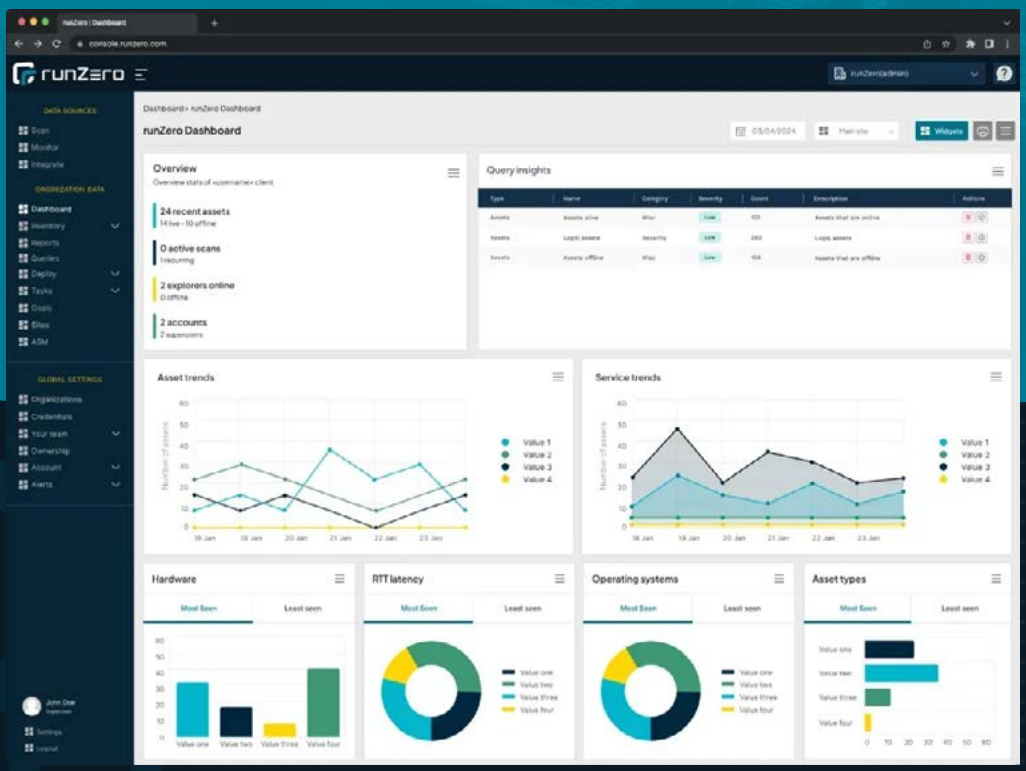
Paul Wescott
Security Architect

Final Thoughts

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

> It's one of the best tools that we have. It gives us the tools to be able to do our job in a really efficient manner and be able to get results and demonstrate these to our colleagues. We're really happy with the product. We think it's one of the best products out there. And we're two people who are highly critical of most of the products that we use.

Paul Wescott
Security Architect



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