CASE STUDY

The University of Auckland

OVERVIEW

Problem

With the university's increasing success and rate of growth and expansion, Russell Fulton, Security Engineer and Paul Wescott, Security Architect, 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. Additionally, both Fulton and Wescott knew they needed to improve their visibility of the complete scope of assets on the university's network, a growing problem with the sheer volume of devices expanding on a daily basis.

Solution

Despite the University of Auckland's many accolades and high rankings, they suffered from limited funding, a challenge that Fulton and Wescott knew they would need to consider when searching for a solution. In their ongoing search for a fitting solution, Wescott came across runZero (then called Rumble) by happenstance. They have appreciated that runZero was made by cyber security professionals, for cyber security professionals, making for an intuitive, easy-to-use solution.

Outcomes

Asset discovery with runZero 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. 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 its capabilities for CAASM and locating potentially exposed systems when time is of the essence to take steps toward remediation. 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.

CUSTOMER PROFILE

UNIVERSITY OF AUCKLAND
Waipapa Taumata Rau
NEW ZEALAND

Company size
12,000 employees, 45,000 students

Industry
Higher Education

Use cases

- Cyber asset discovery
- Cyber asset inventory
- Cyber risk management
- Incident response
- Cyber asset hygiene
- CAASM

"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 | THE UNIVERSITY OF AUCKLAND

PROBLEM

Since its founding in 1883, the University of Auckland has grown to become New Zealand's flagship, research-led university, known for the excellence of its teaching, its research, and its service to local, national, and international communities. Recently, they achieved the ranking of 68 in the world 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 the university's increasing success and rate of growth and expansion, Russell Fulton, Security Engineer and Paul Wescott, Security Architect, 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. "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," explained Fulton. Additionally, both Fulton and Wescott knew they needed to improve their visibility of the complete scope of assets on the university's network, a growing problem with the sheer volume of devices expanding on a daily basis. "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," said Fulton. Wescott added, "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." So 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 their cyber asset discovery, cyber asset inventory, cyber asset attack surface management (CAASM), and remediation efforts.

SOLUTION

Despite the University of Auckland's many accolades and high rankings, they 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," explained Fulton. While they did previously use Nmap, it wasn't a viable solution for them in the long run, specifically due to its lack of a central console to view and manage assets from, no history of when an asset was discovered or last seen, and absence of integrations with other tools like Tenable, LDAP, or cloud. They also leveraged 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," described Wescott. Fulton chimed in, "With Tenable, we were also highly constrained by license and the number of assets we can support." The university eventually adopted ServiceNow, but Fulton and Wescott quickly realized its shortcomings. "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," shared Wescott.

In their ongoing search for a fitting solution, Wescott came across runZero (then called Rumble) by happenstance. "I was going through my Twitter feed in the middle of the night. I saw something about this solution called Rumble. 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," explained Wescott. From the beginning, they enjoyed how easy it was to deploy and start using right away. "It is the easiest install I think I have ever done," recalled Fulton. Wescott then continued about his experience with their customer support, "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.'"

They have appreciated that runZero was made by cyber security professionals, for cyber security professionals, making for an intuitive, easy-to-use solution. "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," said Wescott. He went on to add, "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."

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," explained Wescott. They've 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," said Wescott.

OUTCOMES

Asset discovery with runZero's proprietary network scanner paired with leveraging 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. "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," explained Wescott.

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 when time is of the essence to take steps toward remediation 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 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," described Fulton.

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. "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."

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," said Wescott. He 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."

When asked to sum up their experience with runZero, Fulton said, "It's been a joy to work with. That includes the software, HD himself, and the whole runZero team." Wescott then jumped in to conclude, "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."

About runZero

runZero is a cyber asset management solution that is the fastest and easiest way to get to a full asset inventory with actionable intelligence. runZero can discover all of your assets: IT, iOT, and OT, no matter where they are: in the cloud, on premises, or remote. It is so easy to use, you can get started in minutes.

Gain a comprehensive view into your attack surface for improved cyber hygiene and remediation.

Visit https://www.runzero.com/try/signup/ to learn more.

Try runZero for free