runZero

Case Study

Notable risk reduction after discovering **2.5X more** devices than previously known.

Meet the Security Expert

Chris Russel

Chief Information Security Officer (CISO)

Russel and his team realized there were some key gaps in their security program that needed to be addressed, including their lack of complete, centralized network visibility.

Despite using Nmap and Tenable's Nessus, Russel determined York University needed a more robust security solution. Specifically, Russel observed Nmap's inability to provide a complete, centralized view into their environment without a lot of manual intervention, and Nessus' ineffectiveness for getting to a full cyber asset inventory, not to mention it was expensive.

After some research, York University discovered runZero and were immediately impressed with their interest and commitment in supporting the higher education sector.

YORK U

Company Size

6,400 faculty • 54,000 students

Industry

Higher Education

Location

Toronto, On

Use Cases

- Cyber asset discovery on and off campus
- Cyber asset inventory
- Cyber risk management and mitigation
- Cyber asset hygiene
- Asset ownership

Problem

High expectations in **higher education**

York University is a top international teaching and research university, boasting many impressive accolades. Living up to such high praise and recognition across the university community assigns great responsibility to all its members to strive for such excellence, and this proved to be a challenge for Chris Russel, Chief Information Security Officer (CISO), and his security team.

One of the main challenges that Russel and his team observed was the lack of a centralized view of all their assets in their environment. This was a challenge due to their large, highly complex and distributed environments of campus facilities, faculties, etc.

Our situational awareness was not the greatest in our environment, because by its nature it's very distributed, even for the managed devices IT looks after. There's no one view of any of it.

"There wasn't a place for us to easily get that type of information, so we had to make it ourselves with Nmap scans and map it to other sources of information so we can tell who's the contact point for a given endpoint. It's not just identifying endpoints but the other correlating bits of information, which is something we need in order to conduct any of our processes."

Chris Russel
Chief Information Security Officer (CISO)

Our incident response and vulnerability management suffered from a clunky way of us addressing and determining what we do once we know there's something that we need to address.

1. How important is that asset?
2. Who is responsible for it?
3. Where do we take it from there?

"Our actions were based on a lot of historical knowledge rather than authoritative sources, and that did not work well as we were rapidly growing our team."

SCALING WITH LIMITED RESOURCES

Similarly, Russel and his team recognized that their manual approach to incident and vulnerability detection and response wasn't scalable and needed an overhaul to save their small team with limited resources valuable time and effort.

"There was often a lot of manual review involved on our end. We wanted to automate this as much as possible because it doesn't scale if you need to have somebody review those things every time.

That's part of our objective. We have a very small team in security and a very large complex environment. So, we need to make as much use of automation as we can."

For something like Nmap, that's great. But it's really just a scanner. You can fit into a larger set of tools to help provide a better view, but on its own, it's not going to do that for you.

That's where our scripts came into play, where we could automate it as much as we could. But there was still a lot of piecing together that we had to do ourselves. It was a more reactive toolset than something that allowed us to track things well over time. Nmap is great, but it's really just the scanning aspect of it. It's not the whole picture that we need. It doesn't solve that problem.

TIME FOR NEW TOOLS

Russel and team had been utilizing a few security tools, one of which was Nmap. But they quickly realized its shortcomings of providing a complete, centralized view into their environment without a lot of manual intervention.

They had also been leveraging Tenable's Nessus, but that tool proved to be ineffective and unsuitable for getting to a full cyber asset inventory, not to mention it was expensive.

"For Nessus, we've used the scanner component mainly as the vulnerability scanner, and that's great for certain classes of vulnerability, detection, and so forth. But it's not something that's great for tracking overall asset inventory. We would get into looking at tens of thousands of assets that would actually add up quite a bit. So, it was very costly,"

Running with **runZero**

After some research, York University discovered runZero and were immediately impressed with their interest and commitment in supporting the higher education sector.

Russel and his team have enjoyed runZero's ease of deployment and use, helping them reap the benefits of the platform and get to value that much quicker.

PROVEN VALUE

runZero has already proven its value in a myriad of ways for the team, including increasing their speed to action for incident response, and the ability to rapidly detect and mitigate vulnerabilities.

It didn't really take a lot of training and getting up to speed to make it useful for us. Setting up scanners was fairly straightforward. That's not always the case with security tools. Usually there's a large ramp up in and getting value out of it. It was pretty much useful to us right away.

"It's simple, but it also has a lot of capability built into it. With a small team, we don't have enough time for training on a lot of different products. So having a tool that people can jump into very easily and quickly is helpful."

Our environment can be quite complex. When a new vulnerability comes out, finding out whether there are things that might be affected by it is not always easy or automatic to tell what's out there and what might be active. There may be devices offline that may come back online at some point when the person returns from vacation. We want to be sure that we don't miss things like that. A point in time isn't necessarily going to capture all that. So runZero is very helpful in those types of situations.

IMPROVED REPORTING WITH RUNZERO

runZero has also contributed to Russel's ease and speed in pulling reports for making critical decisions.

INTEGRATING WITH MDE

Russel and his team recently completed setting up a Microsoft Defender for Endpoints (MDE) integration. They noted some immediate advantages, including gaining visibility beyond the campus.

The team now has a clearer view into asset ownership since this information that they have set in MDE is synchronized with runZero, which has proven to be helpful in avoiding maintaining ownership in multiple locations with different tools. They have also gained the ability to find endpoints missing Microsoft Defender for Endpoints and it is now an easier task to identify and report on assets that are not yet onboarded to MDE/EDR. Finally, they have gained a consolidated, normalized view, enabling and accelerating security investigations.

"It allows us to bring AD/MDE onboarded assets into our runZero views and reports even if they are not on our campus network (such as laptops used with hybrid/remote working or servers hosted in cloud infrastructure), giving us a comprehensive asset picture that is not dependent on network location."

runZero's ad-hoc reporting has been invaluable. Sometimes our opportunity to get attention on a problem is fleeting. If I'm able to get some data quickly about a particular problem, I can strike while the iron's hot.

"If we're in a situation where we need to know, 'how many systems with this particular issue do we have out there,' and run a report on that, that would have been a lot of work in previous years before we had runZero to try to piece together the scanning. We wouldn't be very confident of the accuracy either because it would be lacking. We have some endpoints that are off the network that we wouldn't be able to necessarily see in a scan before, where now some of the data comes in through the integrations, we have with runZero."

Outcomes

runZero's **Impact**

DISCOVERED MORE ASSETS

A key outcome that the York University security team has witnessed is a measurable increase in visibility into their environment. Before runZero, they were aware of and managing roughly 10,000 assets. Now with runZero, Russel and his team have been able to discover and better protect 25,000 assets, including IoT devices, 2.5× what they had insight into before, or a 150% increase.

INCREASED VISIBILITY

This visibility with runZero is possible despite a constantly changing environment that continues to increase in complexity, a win that Russel doesn't take for granted.

"Part of it is that the environment changes a lot. We never really did have that clear visibility before, even through the networking management tools, which are great for managing the network but not so much for the devices in it. We can now truly see what's out there and track it over time."

IMPROVED EFFICIENCY

Another key value-add that Russel and his team have tracked the improvement of with runZero is an increase in their efficiency so they can do more with their limited time and resources.

"It's filling some gaps and allowing us to automate our processes where there would have been a big gap at this point in time, like when we're redesigning and revamping our security program. If we were to have a gap like that today, that would be a major issue in that we wouldn't be able to operate."

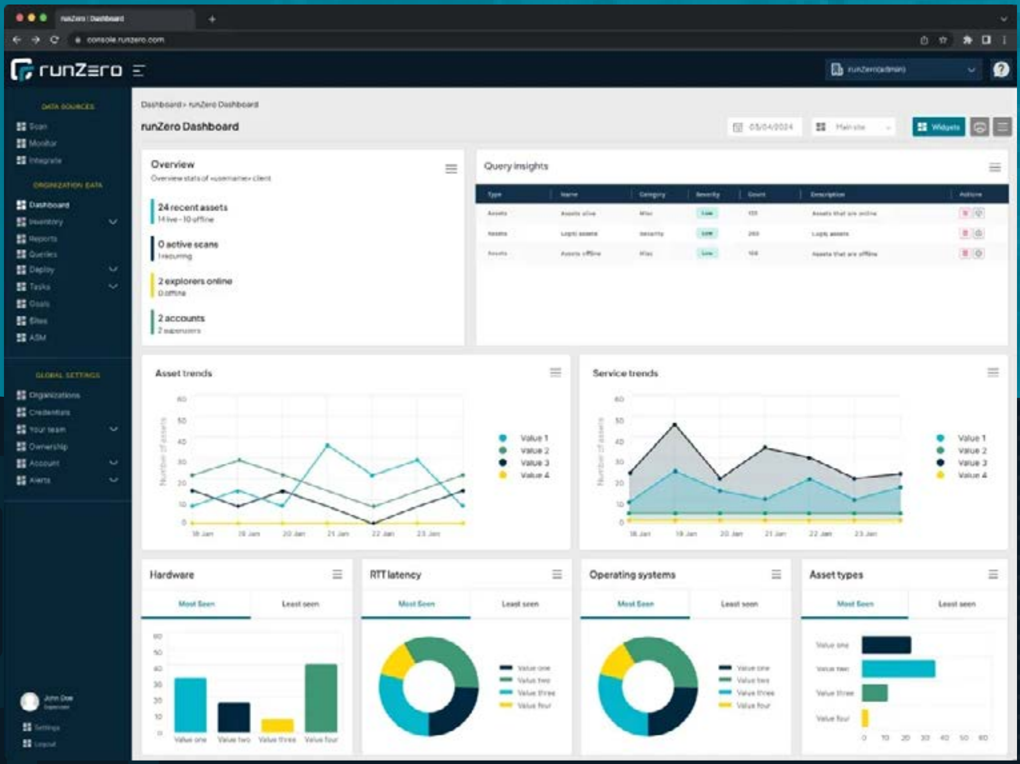
Of the assets that were the most visible to us, there were roughly 10,000 assets. Now we have a lot more out there, up to 25,000 assets in runZero that we're looking at and have the ability to get data on. There's a lot there and having the visibility beyond just the Windows devices that are Active Directory joined is a huge benefit.

Final Thoughts

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

> It’s a tool that we’re able to rapidly get up to speed with. It allows us to be agile and provide quick answers to a lot of our questions. It has vastly improved our awareness of our environment, which is necessary for understanding the risks and issues we have.

Chris Russel
Chief Information Security Officer (CISO)



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