runZero

Case Study

New levels of insight deliver risk reduction and time savings.

Meet the Security Expert

Tracy Dallaire

Directory of Information Security

Dallaire and her team are dedicated to protecting their university community's data.

Throughout the COVID-19 pandemic and beyond, cybersecurity challenges have become increasingly prevalent in the post-secondary education sector.

In response, Dallaire and her team were searching for new tools to help them achieve McMaster University's comprehensive information security strategy.

McMaster University

Company Size

36,000 + students • 13,000 + staff

Industry

Higher Education

Location

Ontario, Canada

Use Cases

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

Problem

High expectations in **higher education**

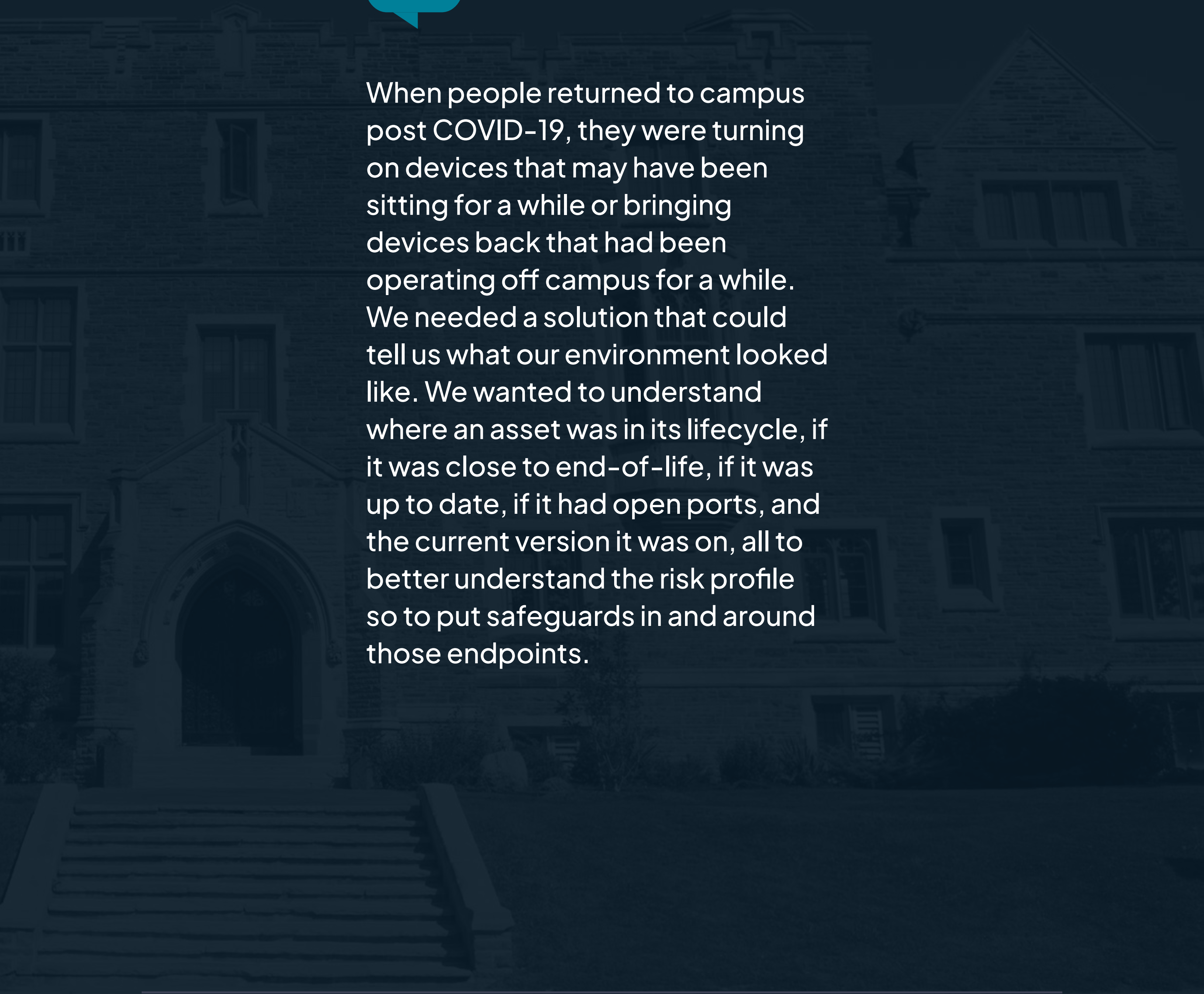
Dallaire leads a team of cybersecurity professionals focused on safeguarding the availability, integrity, and security of McMaster University's data.

POST-PANDEMIC ISSUES

There is an increasing trend of cybersecurity challenges, such as student scams and phishing attacks, in the postsecondary education sector. These challenges escalated during the transition from remote to in-person activities on campus as the university emerged from the COVID-19 pandemic. In response to these challenges, Dallaire and her team were searching for new tools to help them deliver the university's comprehensive information security strategy.

> "The postsecondary education sector is a complex environment from a cybersecurity perspective. Community members often use personal devices to connect to our networks, and there is a constant influx of new students, faculty, and staff, coupled with the introduction of research equipment and the retirement of old equipment."

Tracy Dallaire
Directory of Information Security



> When people returned to campus post COVID-19, they were turning on devices that may have been sitting for a while or bringing devices back that had been operating off campus for a while. We needed a solution that could tell us what our environment looked like. We wanted to understand where an asset was in its lifecycle, if it was close to end-of-life, if it was up to date, if it had open ports, and the current version it was on, all to better understand the risk profile so to put safeguards in and around those endpoints.

Solutions

Scanning for **vulnerabilities**

Dallaire and her team adopted the Cyber Asset Attack Surface Management (CAASM) solution by runZero to run automated scans of their network for vulnerabilities, leveraging runZero’s active, unauthenticated scanner.

DETAILED AND USEFUL SCANS

The solution allows them to conduct detailed, automatic scans of their environment while collecting valuable insights, such as account asset life cycles, end-of-life proximity, updates, open ports, software versions and more.

runZero’s active, unauthenticated scanner was easy to deploy, and it has quickly become a key part of our security program.

“runZero helps us understand what is operating in our environment down to detailed attributes, such as the version of Windows, patch level, if there are open ports, and more.”

Outcomes

Increased visibility, **decreased risk**

The implementation of runZero gave Dallaire's team a comprehensive view of the assets operating in their environment and their associated risks, helping to reduce overall risk. This newfound visibility empowered the team to make critical decisions, enhancing the university's information security.

LESS MANUAL WORK

Not only has runZero provided Dallaire's team with a new level of insight, but it has also been a significant time-saver for her team.

"runZero cuts out a lot of manual work, allowing our team to act more quickly and focus on higher-value analytics and strategy."

> At McMaster, we are using runZero to constantly stay on top of new vulnerabilities. It's another piece of intelligence that's helping us understand where and how to target efforts. It's becoming an ingrained part of our security program, our security operational activity, and our suite of tools that we use.

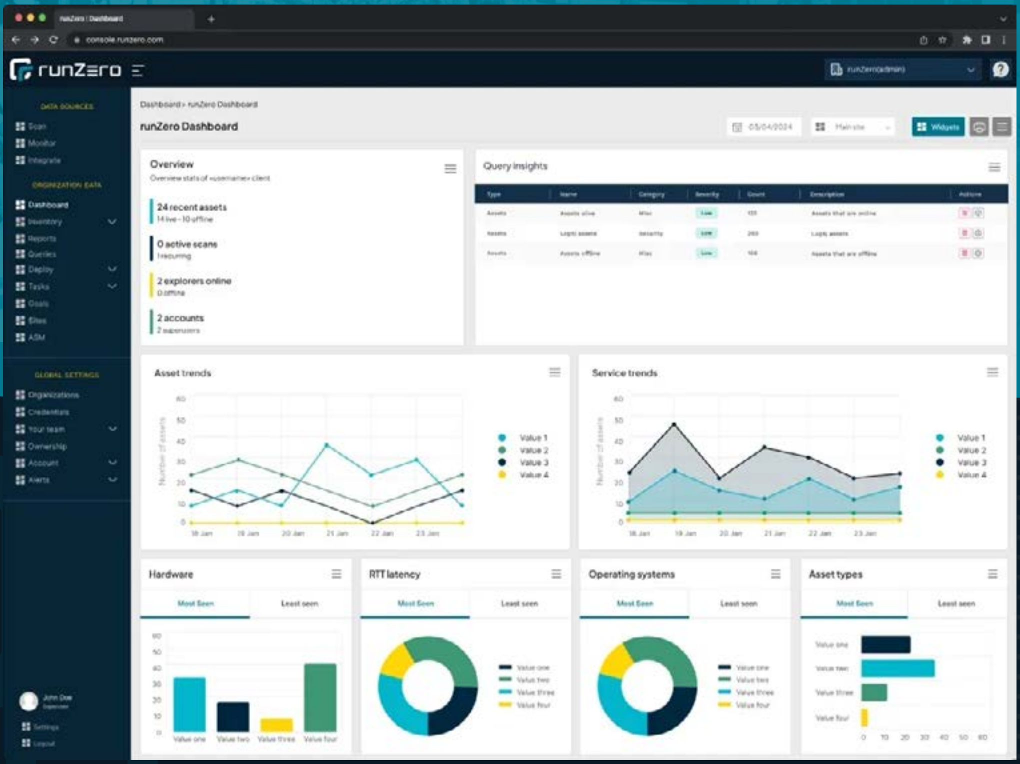
Final Thoughts

Dallaire had a few parting words to sum up her experience so far with runZero:

> Our team relies on runZero to remain vigilant in monitoring emerging vulnerabilities across our extensive network of information sources. The tool not only guides us in pinpointing precisely where and how to direct our security efforts but has seamlessly integrated itself into the very core of our security program, operational activities, and our suite of essential tools.

"Between the level of sophisticated intelligence it provides, speed of data acquisition and deployment, and ease of effective integration into our operating environment, I see a substantial return on value."

Tracy Dallaire
Directory of Information Security



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