

Case Study

How Topcon saves time and reduces risk with faster, more accurate cyber asset attack surface management.





Joe Denton

Information Security
Operations Manager

Leading Topcon's security evolution.

Joe Denton manages global information security operations for international manufacturer Topcon, which develops innovative solutions across the healthcare, agriculture, and infrastructure sectors. Joe's team is focused on maintaining Topcon's security posture, with a wide array of responsibilities ranging from investigating incidents to ensuring the corporation stays up to date on implementing security controls and best practices.

Joe and his colleagues faced several challenges related to tracking and managing cyber assets across the global Topcon group. These included limited visibility due to decentralized data, data inaccuracies, and laborious manual data processing for analysis and reporting. They wanted to find a more efficient, accurate, and comprehensive asset management solution.



Company Size

3,000 employees

Industry

Manufacturing • Agriculture • Healthcare

Headquarters

Global

Use Cases

- Asset inventory
- Attack surface management
- Exposure mitigation
- Mergers and acquisitions

The Problem:

Decentralized, incomplete asset data and slow, inefficient processes.

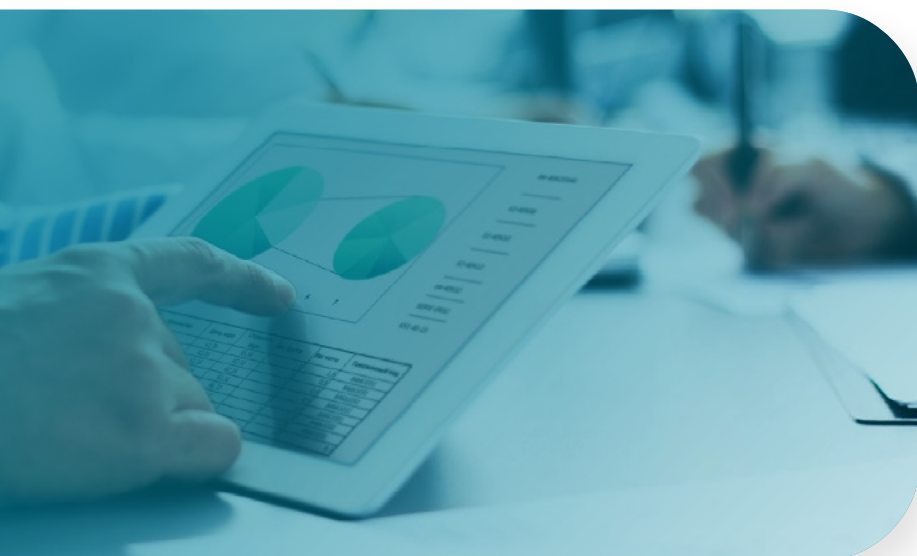
Global manufacturer Topcon has multiple subsidiaries, and Joe Denton's team is responsible for information security across the whole organization. Previously, the security team was using Lansweeper along with a series of disparate spreadsheets to track and manage cyber assets across all locations and business units.



Before, we were simultaneously using everything and nothing for asset inventory and management. We had some Lansweeper instances, but they were underutilized and not fully licensed for the scope we needed. Beyond that, it was spreadsheets — and in some cases, guessing.

Joe Denton

Information Security
Operations Manager



Denton identified three key drivers for upgrading Topcon's asset discovery and management capabilities:

1. Gaining greater data visibility and accuracy

Decentralized data made it hard to get a comprehensive, accurate overview of assets. Manually checking, updating, and compiling information from different sources was inefficient and time-consuming, and increased the risk of errors.

"The main problem was not having accurate data. Spreadsheets get out of date very quickly if you're not updating them often enough."

Lansweeper wasn't meeting Topcon's needs. "Lansweeper's requirement for administrative credentials to fully access asset details can be inconvenient and potentially insecure, and its integrations are limited."

2. Generating fast, reliable asset reporting

"We kept getting asked by different vendors about how many Windows assets or Linux assets we have. To be frank, it was really difficult to answer those questions. Each took at least an hour because we had to manually sort through the data. We wanted an easier way to extract and share this information with confidence."

3. Streamlining and speeding up asset discovery

The Topcon team was using Active Directory to track down assets. *"We had to skim and scrape to figure out exactly where, across multiple locations, a particular server or asset might exist."*

"We didn't know exactly how many Macs we have in our environment. Our guesstimate was anywhere between 90-120. We really needed to clarify and make sure we weren't overpaying for licenses."



Sometimes we would acquire a new company and not have a full scope of what assets it was bringing in.

"We'd get an idea from documentation left by the previous team, but it was never robust. So we'd discover surprises like a Windows 2003 machine that's been there for 10 years but wasn't listed."



The Solution:

Installing runZero as the single source of truth for cyber assets.

Topcon decided to upgrade to a cyber asset attack surface management (CAASM) tool. Denton and his colleagues considered Lansweeper and Armis, but ultimately chose runZero.

The major deciding factors were not needing administrative credentials to perform discovery — “a game changer” — and the robust level of integrations runZero offers, which provide powerful contextual information on assets.

runZero provides both active scanning and passive discovery across managed and unmanaged assets in all environments: IT, OT, IoT, mobile, cloud, and remote.



The level of asset detail we found with runZero compared to Lansweeper wasn't just like comparing apples to apples — it was apples to oranges.

“Plus, we have several tools that already integrate with runZero. Being able to get all that context without having to spray credentials everywhere made choosing runZero a no-brainer.”

Simple, speedy deployment.

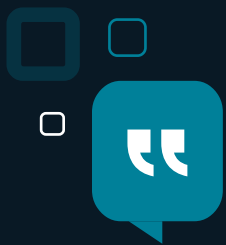
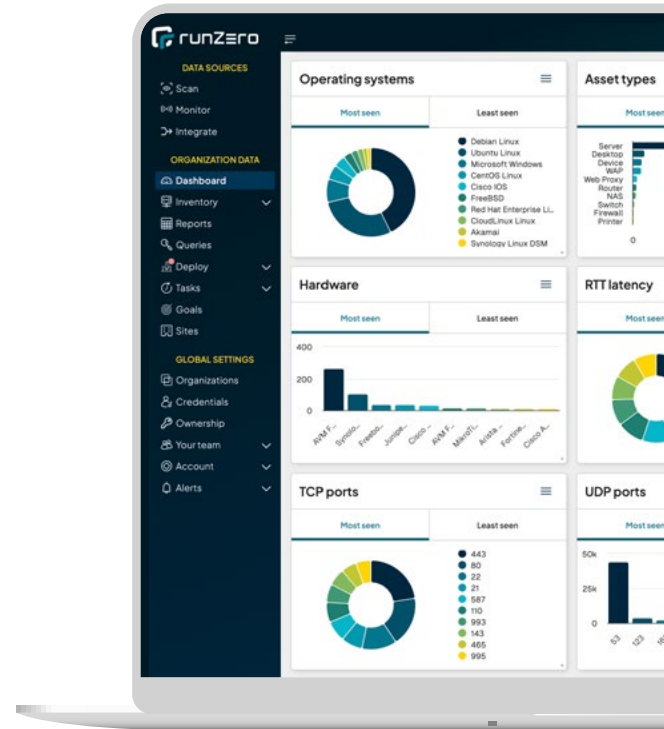
Denton was impressed with the ease and speed with which he and his team were able to deploy runZero — meaning they could start generating and using powerful information very quickly.

“I honestly can’t stress enough how incredibly easy implementing runZero was. It’s just point and click, install, and run a scan — that’s pretty much it. Then all that powerful data is available for you to take advantage of however you choose.”

Multiple integrations with existing tech stack.

Denton particularly values runZero’s built-in integrations with many of Topcon’s existing security applications and systems, including Active Directory, Microsoft Intune, Rapid 7, and VMware, plus a custom integration with EDR solution Carbon Black.

“The context that runZero’s integrations gives you is fantastic. It’s like having a one-stop shop for any asset.”



While you can get a lot of information from a general scan, it doesn’t give you the asset’s full context. For instance, a general server scan won’t tell me the vulnerabilities on that server. But now I can look at a list of vulnerabilities in runZero along with context from Rapid 7 and Active Directory. That’s invaluable, because you can mesh all that data together into powerful insights.

The Outcome:

Improved data quality, efficiency savings, and reduced risk.

Implementing runZero has given Topcon centralized asset data that is more comprehensive, detailed, and accurate than ever before, with the ability to find, manage, and analyze assets across all locations much faster and more easily. Greater data visibility and accuracy have boosted data confidence and operational efficiency — saving both time and money — while helping reduce risk.

Greater data visibility and accuracy.

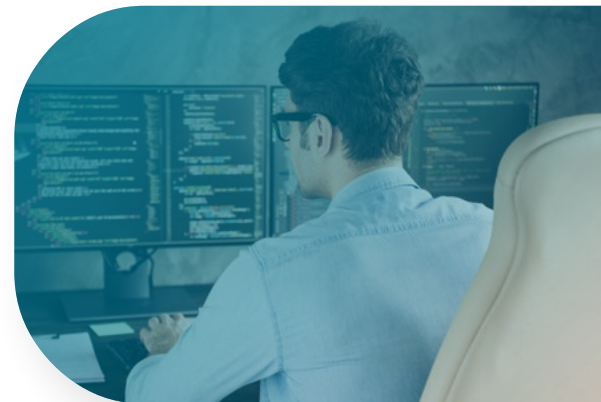
runZero has given Denton's team much greater visibility over Topcon's assets: what they are, where they are located, what they're connected to, how much they're being used — and any risks they pose.

Having centralized, up-to-date data makes it easier and faster to identify security gaps and take action when needed. For example, Denton's team is currently using runZero to review end-of-life operating systems, and decide which services and servers to migrate or disable — a far harder task without runZero's data.

"We know more about these assets: they're not just out there in the ether. We're more certain of where they are, that they're online, and potentially or actively in use. It became like a puzzle and we're filling in the blanks with different puzzle pieces."



runZero has revealed so many details we didn't even know about, particularly around legacy assets and outdated software. It's good to have greater visibility, with concrete details we can drill down into.



Significantly reduced asset discovery time and a single source of truth.

Using runZero, the Topcon team can find assets much faster — and without needing to switch between multiple tools.

“runZero has reduced our asset discovery time significantly.”

Faster, more accurate asset reporting.

Answering vendors’ questions about Topcon’s assets is now 200x faster — and the team has full confidence in the data accuracy.

“One vendor wanted a count of Windows desktops, Windows servers, Linux desktops, Linux servers, and Mac operating systems. It took me less than 20 minutes to pull all that data together. Before, it would have taken at least an hour and involved some guesswork.”

Increased endpoint protection and improved security controls.

By using runZero to reduce gaps in endpoint protection across all locations, Topcon has strengthened its security controls.

“We used runZero with all of our teams worldwide to identify assets that didn’t have our EDR solution, Carbon Black, installed, then we created internal tickets to resolve that. Now we’re pretty confident in our level of Carbon Black coverage. So that’s been very fruitful for us.”

Swift response to new vulnerabilities.

Topcon has benefited from access to runZero’s rapid responses whenever new vulnerabilities are publicly identified.



We finally got a true count of the number of Macs we have in our environment by using runZero.

“We’d guesstimated 90–120, but we’ve actually got around 60. It’s good to know because we can ensure we’re not overpaying for licenses.”

“We no longer have to use Active Directory to figure out where an asset is, because that information is already there in runZero, ready to go.”

“Now, I rarely touch Active Directory, or even Intune. I’ll just go to runZero and see if the asset is there first. I’ll only check other tools if I need to dive deeper into the asset for some reason.”

Final Thoughts

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

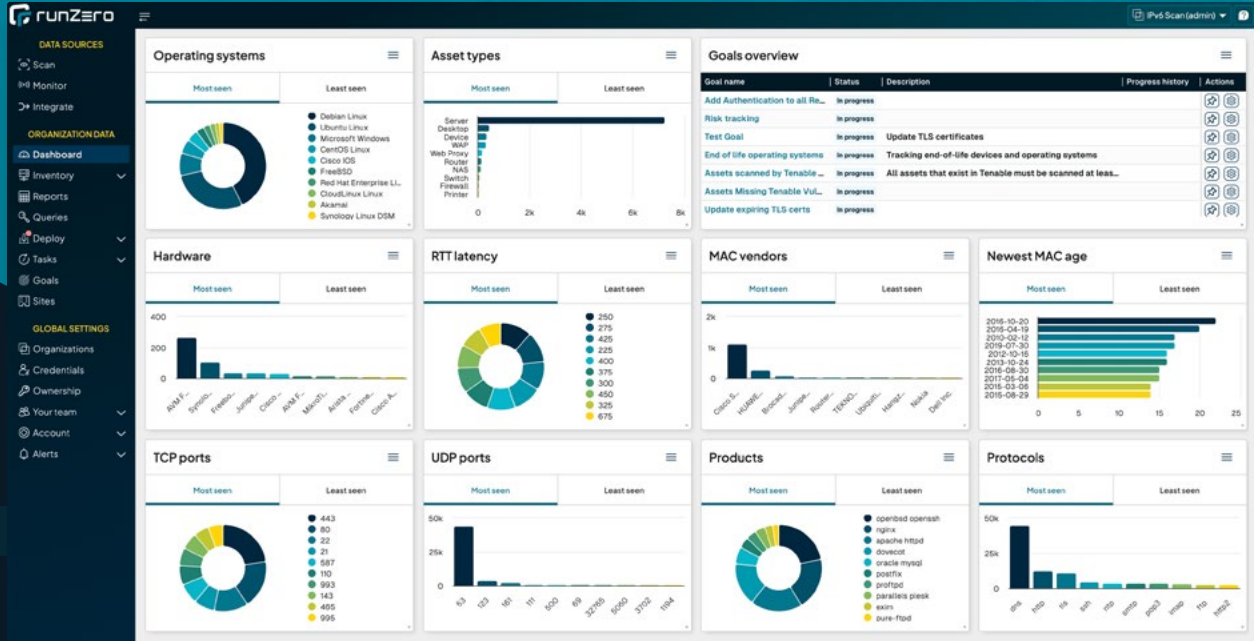


The runZero team is really on top of vulnerability research and has helped us find a couple of vulnerabilities that we didn't even know existed in our environment. For example, alerting us to the Cisco smart install service, which had a remote code execution vulnerability against it. We found out that was enabled on a few of our devices, although luckily nothing was exposed online.

"We hadn't even known about that vulnerability, yet thanks to runZero we already had a ticket to remediate the issue. It was great."

"We love runZero — it's a very, very helpful tool with powerful data, and the runZero team has been really good to us. We're keen to look at how we can further use it to reduce our overall risk posture. The runZero team is always iterating and adding to the tool, so there's always something new to explore."





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 total attack surface management 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](#).

See and secure every asset. Even the unknowns.

Try runZero for Free

