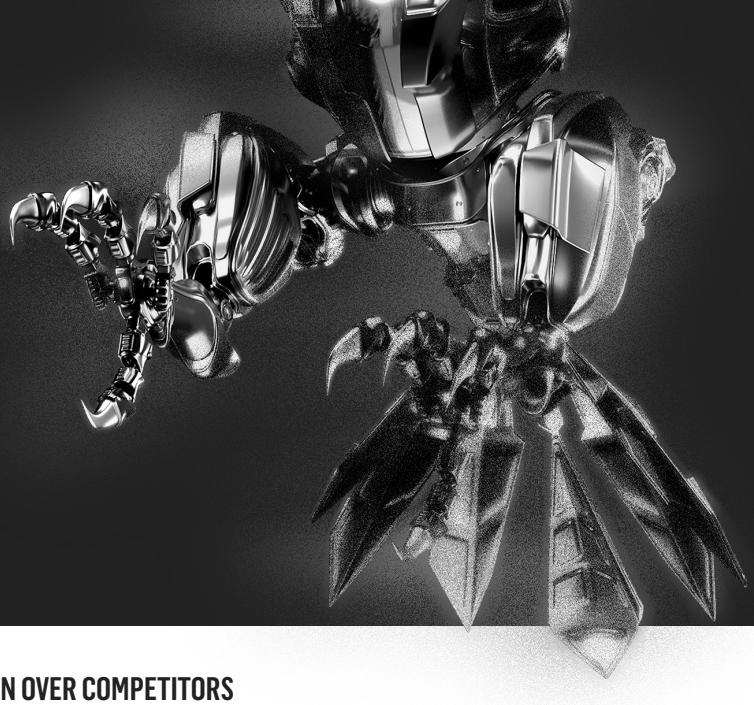
cybereason | CASE STUDY

Higher Education



INDUSTRY

Higher Education

SIZE OF ENTERPRISE

42,000 students and 6,000 employees across three main campuses and 59 satellite campuses

THE CHALLENGE

Newly-established security operations center (SOC) with only three full-time employees, including a ramping-up Threat analyst. Needed actionable visibility across a highly distributed attack surface across South Africa.

- Small security operations team wanting to upskill quickly
- Highly mobile, remote student body and workforce complicated the process of managing endpoint security
- Lack of visibility across a geographically-distributed attack surface
- Inability to detect sophisticated attacks and lateral movement of adversaries

SOLUTIONS

- The University conducted head-to-head comparisons of the Cybereason XDR Platform with competing solutions from CrowdStrike and Palo Alto Networks.
- Cybereason XDR proved to be superior in terms of price, user interface, fewer false positives, ability to conduct investigations and determine root causes faster, and speed and ease of remediation.

CHOOSING CYBEREASON OVER COMPETITORS

THE CHALLENGE

The first signs that the university needed to move away from signature-based endpoint detection were the 2020 SolarWinds supply chain attack and the following year's supply chain ransomware attack on Kaseya customers.

The university was a customer of both companies. Although they were able to mitigate these attacks without any damage, their Chief Technology Officer quickly realzed that signature-based detection was no longer enough for endpoint protection given the increasing sophistication of attacks and use of zero-day vulnerabilities

The COVID-19 global pandemic also complicated the university's ability to manage its endpoints and remediate incidents.

"Our employee base is now more mobile than ever, especially with COVID...," the CTO said. "Before COVID, employee machines would join our Active Directory and become part of the corporate network on a daily basis, and we could do software updates. It became much more difficult once people began moving away from campus."

The university leverages Druva's SaaS-based enterprise backup services for its endpoint backups. But the extreme cost of mobile and roaming connectivity in South Africa made it too costly for the university to conduct daily backups. "This is a problem for the university in terms of data loss," .

What the University needed was a unified threat detection and response platform that could ingest and correlate telemetry across remote endpoints, mobile devices, cloud platforms, and applications to predict, prevent, and end malicious operations.

THE SOLUTION

The university conducted an evaluation of Cybereason XDR and competing solutions from Palo Alto Networks and CrowdStrike by emulating real-world threats on an isolated network.

"We found it was simpler to troubleshoot and to actually mitigate threats with Cybereason," the CTO said. "The user interface was more intuitive and we were not prone to information overload. We could get through an investigation and get to a resolution in a more timely fashion."

The university also wanted a way to add bandwidth and experience to its strained SOC team. The best way to do that was to consider each vendor's Managed Detection and Response (MDR) services.

Cybereason's remediation capabilities were also superior to both competing solutions. "The information provided by Cybereason was much better and we were in a position to respond much more rapidly to issues that were identified," he said.

"What I liked from Cybereason is that you have one console to complete the entire investigation. With the other solutions we tested there were multiple dashboards and you had to drill through information for quite a significant amount of time before you would get an understanding of the specific threat and how that threat came to fruition," he said.

For his SOC team, the Cybereason MalOp™ (malicious operation) proved to be a significant force multiplier. "Investigating a MalOp is just so much simpler," he said. "Everything is put together in a very easy-to-interpret fashion and that proved to be extremely important for us having only one junior SOC analyst. There's just the right amount of information, and it's simple enough to understand."

> "What I liked from Cybereason is that you have one console to do the entire investigation. What we found with the other solutions we tested was there were multiple dashboards and you had to drill through information for quite a significant amount of time before you would get an understanding of the specific threat and how that threat came to fruition,"
>
> Chief Technology Officer, Higher Education

THE OUTCOME

Cybereason XDR produced far fewer false positives than the other solutions and saved the university SOC a significant amount of time that could be better spent investigating actual threats.

"With other solutions, there was a much more significant amount of false positives and with all of that noise, it became a very grueling process to investigate and resolve security threats," the CTO said. "The fewer false positives you get the more time it saves your analysts, especially for more junior people. So from my perspective, that's extremely valuable."

Although the university was also leveraging Kaspersky Endpoint Security, he said Cybereason XDR provided insights into more relevant threats.

"In terms of what we saw with Kaspersky, yes it was detecting quite a lot of basic viruses, but the world is changing where zero-day and ,more complex attacks are taking place on a daily basis," the CTO said. "We deal with things like phishing every day, so we're more concerned at this point with what they are trying to achieve with these attacks, and what information they are trying to get access to. The focus has changed significantly from just worrying about a virus in the fog."

The University has now deployed Cybereason on all Windows and Mac endpoints belonging to the university, with an interest in expanding to further Workspace, Identity, and Multi-Cloud modules in the future.