RAPID7

CASE STUDY

Rapid7 Nexpose Helps Sierra View Medical Center Prioritize Risk and Remediate Fast

INDUSTRY:
Healthcare

SIZE:
1,100 employees

PRODUCTS:
Nexpose*, InsightIDR

CHALLENGE

- Lacked the real-time visibility and control needed to keep endpoints and servers protected.
- The data available to prioritize and assign remediation could be six months old.

SOLUTION

- Rapid7 Nexpose provides real-time visibility into how the virtual desktop environment is changing.
- The Real Risk Score streamlines remediation by prioritizing risk based on age, what exploits are available for it, and which malware kits are used.

It's no secret that the healthcare industry has become a favorite target for hackers over recent years. Patient data is a prized commodity on the cyber underground, and hospitals are seen as an easy target for ransomware attacks, given the mission critical nature of IT systems.

Scott Cheney, information security manager at Sierra View Medical Center, was well aware of these and other threats facing his organization. Sierra View is a state-of-the-art hospital in Porterville, California, reliant on 1,200 endpoints, 300 servers, and another 1,500 networked devices to offer the best possible care to patients. But Cheney was struggling to get the kind of visibility and control he needed to keep endpoints and servers protected.

IT in the dark

As the only full-time information security practitioner at the hospital, Cheney needed real-time automated insight into risk levels that he could share with the IT operations, networks, and systems staff helping him out day-to-day. And he needed a streamlined way to prioritize and assign vital remediation work to these colleagues in order to keep systems patched and resilient.

When he took the helm at Sierra View the only intelligence coming in was via quarterly and biannual scans from a third-party provider, meaning some of the data he and others were working from was up to six months old. It also came with a simple CVSS score, which lacked the granularity he needed to prioritize risk effectively. What's more, remediation was "nearly impossible" for Cheney and his colleagues, who were forced to work from a spreadsheet and manually prioritize what to fix.

"All we would end up doing is anything public facing and critical would get patched, and hardly anything internal would get patched," says Cheney. "It just wasn't happening before. It just physically wasn't possible to do what we're doing now with the old setup."

*Our award-winning Nexpose product has evolved into InsightVM, which utilizes the power of the Rapid7 Insight platform, our cloud-based security and data analytics solution. Learn more at www.rapid7.com/insightvm

Enter Rapid7 Nexpose and InsightIDR

To get the visibility he needed, Cheney opted for Rapid7 Nexpose and InsightIDR. Nexpose, the industry-leading vulnerability management platform, allows IT teams to see exactly where risk is in their organization, view data in real-time, and assign remediation tasks quickly and easily. InsightIDR, in turn, is an integrated detection and investigation solution that combines user behavior analytics, endpoint detection, and visual log search. Cheney was drawn to these products by the unified Rapid7 Insight Agent, which helped to ease deployment headaches. The agents also allowed him to avoid credentialed scanning on endpoints and, for the first time ever, get real-time visibility into how his virtual desktop environment changes—another big tick in the box for Cheney.

Sierra View was more than happy with the cloud delivery model in Nexpose. "IT is tired with getting more systems to manage and more servers to maintain, so anything cloud, especially when you can prove it works well, was received very easily for our organization," says Cheney.

Eye-opening visibility

It didn't take long for the IT staff at Sierra View to notice the difference. The real-time data generated by Nexpose has been a game changer for all concerned. Just as important is the detailed Real Risk Score that Nexpose offers, which goes way beyond the 1-10 of CVSS; it's a 1-1,000 risk score based around factors such as the vulnerability's age, what exploits are available for it, and which malware kits are used.

"Since Nexpose has been deployed it's been incredibly eye opening for our desktop teams and server teams to see the state of things. Having the real-time visibility in conjunction with the risk scoring is huge," says Cheney. "When we first got the info from the tool … it was overwhelming the amount of items it put up for us to fix, so definitely having the real-time risk score was important and helped us focus our efforts."

Cheney is so confident in the accuracy of the risk scores that the organization is using them to monitor progress and calculate the success of the overall project.

A one-stop shop

Liveboards are another key feature of Nexpose and one the Sierra View IT team has leveraged to good effect. Cheney checks them a couple of times a week to monitor the progress of projects with dynamic, real-time data. While he's looking at the "big picture," plans are afoot to roll this visibility out to the rest of the technical team. Given Cheney is not keen on authenticated scans, the dashboards provide a vital and detailed view of risk across the entire IT environment.

"They're the only place to go to find everything," he says. "Seeing the percentage of assets that can be exploited by a novice, for example … It's a scary one but there are no other tools that give us that information for our whole environment."

Remediation in a cinch

As for fixing the issues flagged by Nexpose, the Rapid7 platform's remediation workflow capabilities have turned a slow, inefficient, and manual process into a much smoother, more efficient setup. Before, it was nearly impossible to fix more than external and critical vulneraiblities, as Cheney's team had to manually work through a spreadsheet to prioritize and assign results. Remediation tasks can now be prioritized according to risk and handed to the desktop, VDI, server, or networking teams accordingly.

"For them to be able to sort it by highest risk and hit those items first is really important, because we're working with a mixed staff where they're worrying about IT operations full-time, not necessarily security full-time," he explains. "So for them to be able to come up with a quick idea of 'hey these are the two things I can try to work on this week' is really important."

The results speak for themselves. After just a month and a half, Cheney and his colleagues had resolved 12% of all server vulnerabilities and 7% of VDI bugs. Before Nexpose the IT organization was in a constant state of fire-fighting, with no idea what their progress was. Now they have visibility and control—which is great news for everyone concerned.

After just a month and a half, Cheney and his colleagues had resolved 12% of all server vulnerabilities and 7% of VDI bugs.