Auckland University of Technology Gets Complete Patch Management with Secunia Corporate Software Inspector

Auckland University of Technology (AUT) is a New Zealand institution with a focus on industry-relevant teaching and impactful research. The university currently teaches more than 26,000 undergraduate and postgraduate students, across three campuses – who all depend on secure and reliable IT.

Business Challenge

With the university's focus on innovation, third-party applications are prevalent across its IT infrastructure, which includes a wide variety of different platforms and operating systems.

Any of these applications may include a software vulnerability, which needs to be patched with an application update. But when multiple vulnerabilities compete for attention, it can be difficult to know which applications to deal with first.

"We were patching our third-party applications on an ad-hoc basis," says Roy Cullum, Director of Infrastructure Service at AUT. "We just created packages in Microsoft SCCM. But we didn't have complete visibility to know what, when, and where to patch, so it was difficult to prioritise. We needed a way to discover third-party applications, prioritise vulnerabilities, create and customise patches, and apply them as soon as possible."

In addition, the university wanted a complete solution that could bring all patch management under the same central process - with Microsoft System Center Configuration Manager (SCCM) and Microsoft Windows Server Update Services (WSUS) at its core.

"While our priority was being able to apply patches faster, it was important that we could integrate third-party patching with our existing process," adds Cullum. "That meant finding a solution that worked alongside the systems we were already using to handle operating system and Microsoft application updates."

Solution

As Cullum and his team began searching for a new way to handle third-party patching, he discovered Secunia Corporate Software Inspector (Secunia CSI). It was a solution that met all of his requirements, with extensive Microsoft SCCM and WSUS integration for an easier to manage workflow.

"Secunia CSI seemed to tick all the boxes," he says. "It integrated with SCCM, could scan Mac and Linux systems as well as our Windows estate, and allowed us to package and customise patches quickly and easily. But we were also drawn to Secunia's experience in the security community, and Secunia CSI would give us the advantage of their strong vulnerability assessments – ideal for prioritising our patching."

The university's next step would be to test Secunia CSI first-hand. To do this, Cullum contacted EMT Distribution, an experienced distributor for the APAC region.

"EMT Distribution was highly responsive to our queries, and we planned a free trial," says Cullum. "We set up Secunia CSI on our test environment, and found that the documentation was easy to follow and sufficiently thorough."

Since Secunia CSI is a cloud-based solution, it is easier to implement and maintain than its on-premise counterparts. This was attractive to the university, which could not commit the time or resources to a more complicated implementation.

"We were able to implement Secunia CSI and get the SCCM integration working from the documentation alone. This ease of setup and administration – along with the support we received from EMT Distribution – gave us the confidence we needed to decide on the product."

Results

Since implementing Secunia CSI, the university has been able to more easily discover vulnerable applications, prioritise patching with real-time intelligence, and apply patches efficiently.

In particular, the Secunia Package System (SPS) plays a key role in rolling out updates across the infrastructure. SPS is a platform for installing, configuring, uninstalling, and deploying updates, including those that are not security-related.

"With SPS, we can respond much faster, especially for products where silent update packages can be created automatically," adds Cullum. "Even where we have to create silent packages ourselves, it's still much easier and quicker to deploy than making a separate SCCM package for every update on an ad-hoc basis."

In addition, Secunia's CSI dashboard equips the university with the detailed intelligence it needs to make informed decisions about patching.

"CSI dashboard and custom reports give us useful insight into the current state of our environment. We're more aware of the criticality of each vulnerability, which helps us prioritise and take the necessary action."

However, what the university values most is that Secunia CSI is the most complete solution for third-party patching, with discovery, intelligence, and patch deployment integration coming together in a single package.

"Secunia CSI is a more complete patch management solution than the other options we evaluated," concludes Cullum. "It gives us the intelligence we need to see what, when, and where to patch. We can deploy those updates in the same way as our Microsoft updates, on the same patching cycle. And we can even respond quickly outside our normal cycle. It's all together in the same place."

Secunia CSI provides

- Industry-proven IT security protection
- Microsoft SCCM and WSUS integration
- A customised dashboard for at-a-glance intelligence
- Expert intelligence from the Secunia Research Team
- Quick and easy installation and maintenance
- Flexible patch deployment using the Secunia Package System (SPS)