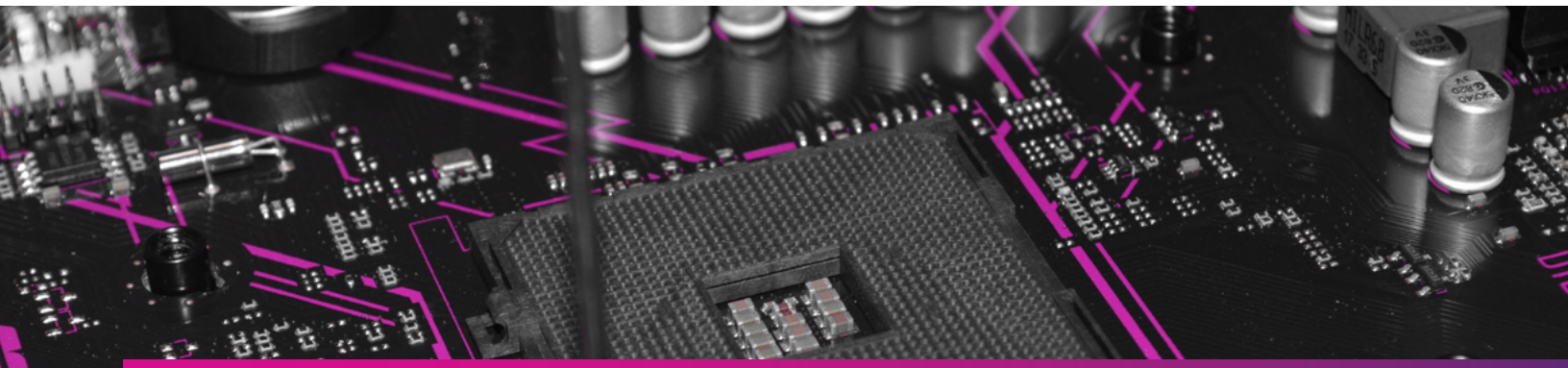

Case Study

Enterprise Technology Company Modernizes Its Security Environment

The client

For nearly half a century, the client has equipped organizations around the world with enterprise technology solutions. The company employs individuals from more than 100 countries and boasts revenues in the tens of billions each year.

The challenge: Address urgent concerns brought about from a failed audit

The client's IT leadership knew it was time to seek help when it failed an audit due to its more than 6,000 servers that had not been patched for more than five years. Despite multiple attempts at remediation the past few years, the team wasn't able to finish this large-scale project on their own.

They acknowledged a lack of vulnerability management standards — or even just a baseline understanding of the assets in their IT environment. Not having enough team members equipped with the necessary skill sets to solve these issues, the client team critically needed expert support, starting with a solid strategy.

Industry:

Technology solutions

CDCT provided:

- Comprehensive discovery using SnapStart
- Security remediation
- Patching automation and standardization
- Revamped infrastructure update processes
- Custom internal wiki library of methodologies and tool reports

CDCT services:

- Consulting Services in collaboration with Astellent
- Professional Services

The solution: Get perspective, fix the problems, and embrace new approaches

The client knew that the servers responsible for its audit fail were production systems that provide customer services; however, it didn't have any kind of current asset data. It was unsure what Operating System (OS) versions were active and what software was installed.

Insight Cloud + Data Center Transformation (CDCT) provided a complete discovery using our proprietary SnapStart engine to clarify and map the client's IT environment. Within just four weeks, we had a detailed picture of the elements that were end of life and where patches were available. SnapStart revealed more than four-year uptimes on several Red Hat® operating systems that were deemed end of life four and a half years ago.

Based on the discovery, we executed the first and second phases of the project: patching the client's Disaster Recovery (DR) and production systems. The client's boots-on-the-ground IT staff had, as is not uncommon, a fair number of legacy processes, particularly around their infrastructure layer. We built process and integrations around a tool set called Tanium to rapidly apply updates and worked closely with the client team to facilitate a cultural shift away from a "That's how we've always done it" pattern. We also built an internal wiki for the client that publishes all of the methodologies now in use, plus reports from Tanium and other tools.

Currently, Insight CDCT, alongside individuals from Astellent, are helping the client look at overall vulnerabilities, beyond OS, and perform cleanup activities (remediation and decommissioning) in preparation for cloud migration.

The benefits: Better security, visibility, and manageability in mere months

After years of the client trying to patch and remediate on its own, by working with us it was able to pass the audit, patch its entire DR environment in three months, and patch its production environment in another three. Many vulnerabilities have been addressed, and the client has far better visibility and insight into the environment. Managing the environment has become easier thanks to new automations, integrations, and processes. The company's security stance has been wholly improved, which benefits its own risk posture, as well as its customers' and partners'.

Our team holds weekly cadences with the client to ensure ongoing projects are moving along well. In a recent conversation, the client lead reported, "I'm so proud of myself for hiring you all."

Benefits:

Discovery and IT environment mapping in just

4 weeks

6,000+

servers patched in 6 months

Passed audit with flying colors

Automated and modernized security processes

Increased transparency

of methodologies, tool sets, and activities

Improved security and risk posture