Case Study

Keyfactor Enables End-to-End Encryption for the Largest University System in the US

Company Overview

Unisys is a global managed security services provider that handles IT and security projects for international and local organizations. Its services help organizations overcome obstacles to successfully navigate business transformations such as AI adoption, cloud migration, and application modernization, ultimately becoming more agile and reaching their greatest potential.

Challenges

Securing communications for the largest university system in the US

Viewing security certificates as a checkmark on a compliance to-do list is the wrong way to think about them, according to Unisys Field CISO Gary Landau. “Today, certificates are critical infrastructure,” he says. “They are essential to every operation and every connection within a business.”

At California State University, the challenges were clear:

Security: Without comprehensive end-to-end encryption, the network was vulnerable to potential breaches.

Visibility: The team lacked visibility into certificate statuses, expirations, and potential vulnerabilities.

Automation: The manual process of updating security certificates on thousands of servers was time-consuming and error-prone.

Industry

IT Services and Consulting

Location

Blue Bell, Pennsylvania

Pain Points

Lack of end-to-end encryption meant the university’s network was vulnerable to ransomware and other security breaches

IT team lacked visibility into certificate statuses, expirations, and potential vulnerabilities

Manual process of updating security certificates on thousands of servers was time-consuming and error-prone

California State University is the largest university system in the US, and it has the largest PeopleSoft instance. They used to manage security certificates by relying on manual SSL offloading at the perimeter, which was inefficient and insufficient. This approach left the system vulnerable to ransomware and other security concerns.

"If you're in charge of securing an environment and your customer is concerned about ransomware, you need to have a comprehensive security program in place," says Landau. "Part of that comprehensive program means end-to-end encryption because if an attacker got into the environment, you need to at least make sure they can't see the data in transport."

The scale of California State University's system made this project particularly challenging. They have over a thousand servers and there was no mechanism to automatically update the certificates across their environment. In addition, the system's endpoints use different types of certificates and keys.

"We needed a solution that could support all of the different variations," Landau explains. Unisys set out to find an option that would fit California State University's needs.

Solution

Finding a partner to support a large, diverse environment

Unisys selected three solutions and ran pilot tests for all three, seeking the best answer for a system of such great size and diversity.

"Keyfactor was the only one that worked," says Landau. Not only did Keyfactor work, but it supported multiple certificates and was the easiest to implement. "Keyfactor was the only solution that supported all the certificate types we were going to use, successfully deployed them automatically, and had tech support that was able to support us and answer any questions we had," he continues. "They were a good team; they're responsive and know what they're doing."

Increasing automation was an absolute necessity, and Keyfactor addressed that as well.

Solution

Unisys uses Keyfactor Command to automate certificate deployment and renewal, enabling end-to-end encryption that saves time, reduces human error, and minimizes security risks for California State University.

Results

Automating certificate installation on servers saves thousands of hours and reduces human error

End-to-end encryption helps meet regulatory requirements around sensitive data and personal information

Automated certificate updates close security gaps and ensure operations aren't impacted by costly maintenance downtime

Products

Keyfactor Command

"Today, certificates are critical infrastructure. They are essential to every operation and every connection within a business."

"Other solutions didn't have complete automation, which meant that we would have to do a lot of customization or manual effort to get the certificates deployed," Landau says. "Ultimately, we selected Keyfactor for the comprehensive automation. We needed a solution that could automate and Keyfactor was the one that did it."

Business Impact

Transforming security while building trust

Saving thousands of hours through automation

The results are clear for Landau and his team: Keyfactor delivered the capabilities required to install certificates and enable end-to-end encryption. Without Keyfactor, the project wouldn't have been possible.

It's hard to imagine completing the project manually. "If we'd had to do it manually across a thousand-plus servers, I'm guessing it would've taken a thousand hours of someone's time," Landau says. "Having a system that can automate saves all of that." Increased automation also saves costs by reducing the time and human resources necessary to maintain the system, and it prevents the inevitable mistakes that occur with manual work.

Reducing risk and disruptions to operations

Another significant impact was the reduction of business risk for California State University. Keyfactor's automation and transparency reduce any potential impact on business operations, preventing interruptions when deploying new systems. "Certificates can now be renewed every 90 days—or every month or every week if we want," says Landau. "There's no business impact and no intervention required on our part." Keyfactor helped close the security gaps and increase continuity, which helps build trust between campuses and vendors that access the network.

There's a legacy idea that encryption isn't necessary if an organization handles SSL offloading at the perimeter. Today's regulatory environment has changed that. "It's an antiquated thought. There are also insider threats, plus cloud computing, making that whole notion of what's inside your network a different animal. Today, it's important to have end-to-end encryption—it's key for regulatory

Gary Landau
Field CISO at Unisys

"Keyfactor allowed us to reduce business risk. [California State University] now has more trust with the campuses that are connecting to the data and the vendors that are connecting to the data. There's more trust in the fact that their connections are secure."

compliance around sensitive data or personal information," Landau explains.

That example demonstrates why organizations need a partner to help them navigate and adjust their lifecycle management solutions over time.

The more often certificates need renewal, the harder it will become for an organization to manage them manually or with a spreadsheet. "The only way to do it is through an automated certificate lifecycle management system, and Keyfactor has been the best one," Landau says.

"If we'd had to do it manually across a thousand-plus servers, I'm guessing it would've taken a thousand hours of someone's time," Landau says. "Having a system that can automate saves all of that."

About Keyfactor

Keyfactor brings digital trust to the hyper-connected world with identity-first security for every machine and human.

Contact Us

- www.keyfactor.com
- +1.216.785.2946