

Customer Success Story



WASHINGTON STATE EMPLOYEES CREDIT UNION

Washington State Employees Credit Union

Banking on the Lumension Vulnerability Management solution to create a strong enterprise wide security posture to remove all potential risks and gain long-term costs and operational benefits.

Background

Washington State Employees Credit Union (WSECU) is the second largest credit union in the state with more than \$1 billion in assets, over 150,000 members and more than 500 employees. The 19 branches statewide contain a mixed PC and Citrix environment with 150 servers and about 700 PCs and laptops. Ranked within the top two percent of financial services organizations for its quality member services, WSECU puts a high priority on making sure that member needs are met and sensitive data is kept secure.

WSECU Vice President of IT Tony Hildesheim directs a team of 25 IT professionals that all play a role in maintaining the organization's keen focus on security. Additionally, the credit union has an expert enterprise risk management team that meets once a month to make core decisions about how it will continue to adopt smart security measures.

Protecting Data on all Fronts

WSECU bases its approach to securing the organization on the premise that security is a company-wide program that requires everyone's diligence, according to Hildesheim.

"One of our members' primary needs is total data protection, which we support with our security systems and policies," says Hildesheim. "The money that we have is actually data. It exists in the form of bits, meaning that as an organization security is a top focus area for strategic IT investment."

Well aware that financially-motivated hackers know data is money too, Hildesheim needed to address the pervasive risk of exploitation from network vulnerabilities by continuously removing all potential threats. To accomplish this, Hildesheim sought out a comprehensive vulnerability management solution that could execute on WSECU's strategic approach of creating a strong security posture enterprise-wide.

Building Patch and Vulnerability Automation

In 2003, WSECU signed on with Lumension to deploy its vulnerability management product, which includes key functionality for asset discovery and inventory, network- and agent-based assessment scans, automated remediation and ongoing policy compliance audits.

To integrate the patch and vulnerability management process, Hildesheim adopted the Lumension Patch and Remediation™ (formerly PatchLink Update and Security Management Console) component of the Lumension Vulnerability Management™ solution — a comprehensive solution designed to define mandatory baselines, discover and assess network resources, patch and remediate vulnerabilities, and centrally audit and report on the effectiveness of its vulnerability management approach.

After evaluating a variety of patching tools from vendors, including Altiris, Hildesheim explains that

Lumension far surpassed the competition in its ability to proactively manage threats by automating the collection, analysis and delivery of patches. Lumension offers WSECU the flexibility to pick and choose which patches to deploy with the ease to roll them out all at once, if needed.

“Patching is a huge part of our security strategy,” says Hildesheim. “We need to control the patching for our environment, rather than turn on Windows Update for all of our computers, because we have a lot of applications that have dependencies on each other. Before deploying patches, we need to run a test to make sure they won’t affect our core systems. Lumension allows us to do this very effectively.”

Audit Ready Security Systems

To test the efficiency of its overall security architecture, WSECU conducts regular audits with the help of external consultants. In a recent audit, the credit union set out to bring its core processes and technologies further into alignment with the ISO 27001 Standard. With the help of mission critical



tools including Lumension’s risk management solution, WSECU built and executed an information security management system in compliance with the ISO Standard, according to Hildesheim.

In the heavily-regulated financial services industry, Hildesheim relies on Lumension’s top notch reporting functionality to validate compliance with security polices as required by a host of regulatory bodies, including the Washington State Department of Financial Institutions (DFI) and the National Credit Union Administration (NCUA). Lumension facilitates compliance reporting through continuous monitoring of nodes and a full range of operational and management reports that track vulnerability assessment and remediation results.

During the first quarter of 2008, WSECU conducted another internal audit to evaluate the effectiveness of its security tools with the goal of exposing any gaps.

“We were at a critical juncture during this last assessment as we had created a sizeable budget to completely revamp our security suite,” explains

Hildesheim. “Of all the security products we had in place, Lumension’s solution was the only one we kept. It fits our needs perfectly and aligns with the aggressive approach we take on security.”

From the assessment, the credit union not only validated the importance of using Lumension technology to proactively eliminate operating system and application vulnerabilities, but it completed the deployment of the Lumension Vulnerability Management solution by adding the Lumension Scan™ product. Lumension’s centralized management capabilities give Hildesheim and his team the comprehensive view of the organization’s network vulnerabilities through intensive agent and network-based scans of each managed endpoint.

Additionally, WSECU’s IT team has been able to seamlessly push out applications to individual desktops using the Lumension Developers Kit™ (formerly PatchLink Developers Kit). By utilizing this tool, Hildesheim’s team can quickly create intelligent change packages to dynamically identify and correct a variety of problems from simple configuration issues and proactively block Zero-day threats. These packages can be uploaded into the Patch and Remediation repository, once created, for automatic deployment, continuous validation and ongoing status reporting.



Global Headquarters

15580 N. Greenway-Hayden Loop, Suite 100
Scottsdale, AZ 85260 USA
phone: +1.888.725.7828
fax: +1.480.970.6323

www.lumension.com

Vulnerability Management | Endpoint Protection | Data Protection | Reporting and Compliance