



Western Corporate Federal Credit Union (WesCorp)

Leading Edge Credit Union Establishes Leading Edge Security for Members

Nowhere is data security more critical than at financial institutions, which capture, move and update confidential information worth billions of dollars each day. At WesCorp (Western Corporate Federal Credit Union), the focus is on providing members with quality services backed by leading edge systems and world-class expertise. WesCorp is the largest corporate credit union in North America with more than \$24 billion in assets and 1,000 member organizations.



In recent years, WesCorp made significant investments in implementing the best perimeter security technologies such as firewalls and intrusion detection to protect its sensitive member data. However, the Chief Information Security Officer, Christofer Hoff, knew this would not be enough.

According to the 2004 Computer Security Institute /Federal Bureau of Investigation Computer Crime and Security Survey 78% of information theft is committed by trusted employees. Hoff needed to establish more aggressive security policies and boost employee compliance. He needed a solution that would monitor data changes, while maintaining the high level of trust created among employees.

SECURING THE INFORMATION THAT WESCORP RELIES ON

WesCorp selected IPLocks Information Security Platform to provide the visibility, monitoring, and real-time notification required for effective database security operations and business continuity. IPLocks is more comprehensive, less intrusive, and delivers a greater level of detail than WesCorp found with other database security products. It alerts management to business risks from security violations and suspicious data activities, and also provides the audit trail required for today's changing government regulations.

WesCorp member databases change each day, either as a result of financial transactions, customer information updates or internal application installations and patches. Yet with each change comes new potential holes that can compromise

data integrity and security. IPLocks examines patch levels, accounts, permissions, grants, configuration settings and a myriad of other settings that can provide unintended access to data or holes in security.

The ongoing vulnerability checks discover previously unknown security holes across 70 unique databases throughout WesCorp. Because databases are dynamic, with new configurations, software updates and potential exposures appearing every day, these continual checks are essential for ultimate security and confidence. With each regular assessment, IPLocks delivers a report of the health and vulnerability of all corporate databases, along with recommended actions to improve the status. Hoff can drill down into specific alarms, or view a series of assessments to determine the progress of the assets' health.

“The missing piece was a way to understand who or what is accessing the data to ensure the security, integrity and availability of the database and assets.”

Chris Hoff
CISO/Director of Enterprise Security



Because employees need constant access to member data, WesCorp utilizes IPLocks to enforce proper use of the database through continuous monitoring. With the ability to discover, define and implement company-specific policies, WesCorp can minimize enterprise risk and increase confidence in both data assets and its own employees. IPLocks monitors metadata, permissions, content and transactions. This provides Hoff with an audit trail of both specific actions and series of transactions to determine whether data activities are out of the ordinary.



Additionally, WesCorp proactively manages its access-control changes, as well as the movement of all data, providing a record of who accessed specific information across the enterprise. This monitoring ensures that security policies, change management processes and best practices are followed throughout the company. It also provides insight into performance constraints on the system so WesCorp can make the appropriate resource changes as the organization grows.

WESCORP RESULTS

With IPLocks in place, WesCorp has established a security baseline and updated policies to detect and deter negligence, while also providing employees with the data access they need. For the first time, WesCorp conducts continuous monitoring of database changes and transactions. This helps Hoff's team to better understand the movement of member information throughout the organization.

The reports provide management with new views of asset health across the company, as well as new levels of details for greater insight. Together, the assessment, monitoring and auditing improve data confidence and ease the pain of corporate

“WesCorp is now conducting database security audits around the clock to ensure our members’ financial information remains safe.”

Chris Hoff
CISO/Director of Enterprise Security

governance. IPLocks is also less intrusive and easy to maintain because all of WesCorp's databases can be monitored from a single instance. Hoff needs fewer resources to discover critical assets that need protection, allowing his team to focus on other initiatives.

Today, Hoff is confident that WesCorp's member information is secure from both external and internal threats. But because data is always changing, his work is never done. WesCorp's next step is to leverage IPLocks' software that learns user behavior in order to discern between normal data access activities and malicious acts. With this knowledge, the software will be able to detect specific threats and automatically alert managers. The result will be faster response to unexpected changes in activity.

This commitment to leading edge systems and excellence is good news for member credit unions. Knowing they can place their trust and, ultimately, financial future in WesCorp is a very safe investment.



2665 North First Street, Suite 110 | San Jose, CA 95134 | Telephone: 408.383.7500 | www.iplocks.com

IPLocks and the IPLocks logo are trademarks of IPLocks, Inc. All rights reserved. Any unauthorized use or reproduction of the IPLocks logo is prohibited. ©2005 IPLocks, Inc.