Clients Count on Stratus

PCI Compliance in Multi-National Corporations

Strengthening security of mission-critical systems with VOS Auditor from Stratus and ARI

Business situation

Financial services organizations that handle large volumes of payment card transactions must safeguard critical information or face substantial penalties and loss of business. Security guidelines, such as the Payment Card Industry (PCI) Data Security Standard (DSS), are constantly evolving as technology and business processes change and new threats are discovered.

Three multi-national corporations set strategic objectives to strengthen the security of the fault-tolerant Stratus VOS systems supporting their mission-critical payment processes. Each company conducted a thorough internal audit to assess its current security practices with regard to the VOS system environment. In each case, the audit revealed vulnerabilities:

- **A major financial institution** with 200 million customers in more than 100 countries, needed to limit system access for technicians who handle production problems and record their activities.
- **A major US bank** with more than 6,000 branches nation-wide needed to control user access permissions on the production module and compare current system permissions to desired permissions.
- **A European entertainment operator** that served more than 15 million customers in 2008 needed to track the activities of Stratus system operators, each of whom had command-line access to all VOS system commands.

VOS Auditor helped close loopholes in security procedures, ensuring each firm passed its security audit on the Stratus system.

Quick Facts

Sold and Supported by Stratus

Solution profile
- Restricts unauthorized use of Stratus VOS system
- Incorporates company-defined security profiles for all users
- Automates process of managing user privileges/permissions
- Monitors user activities and issues immediate alerts upon any violation attempts
- Maintains secure, comprehensive audit trail of all activities
- Helps ensure PCI compliance

Products
- VOS Auditor security and auditing solution from Application Resources, Inc. (ARI)
- Stratus VOS operating system
- Stratus Continuum® and V-Series systems

Services
- Ongoing technical support from Stratus

The potentially far-reaching consequences of a security breach, whether due to a willful act or human error, compelled each organization to take proactive steps to tighten VOS system security. In each case, restricting access to the Stratus VOS system according to the individual user's specific role in the business was imperative, as was recording the system related activities of all users.

Business objectives

In seeking a solution, each company developed a similar set of objectives:

- Limit user access to the Stratus VOS system according to individual business need
- Verify user access rights against centralized configuration file
- Create an audit trail to track the activities of all system users
- Maintain transaction processing with no interruptions during security upgrades
- Minimize the impact on applications running on the production system

VOS Auditor security and auditing solution

Recognizing that a security breach could occur at any time, each financial services organization sought a proven security solution that could be deployed quickly and easily. Each determined that the VOS Auditor security and auditing

Count On Stratus™

solution met its urgent timeframe while achieving its business objectives. For more than 25 years, ARI and SoftMark have specialized in providing VOS tools for production systems in some of the world's largest corporations and are well versed in the rigorous security needs of these environments. Today, Stratus sells and supports these proven solutions. The modular VOS Auditor solution is designed to help organization enforce their security policies by limiting system access based on each user's security profile. Deployment requires no changes to VOS system applications and causes no disruptions in processing or user activities.

Customers rely on VOS Auditor to ensure that access to mission-critical VOS systems is based on business need, and that any attempts to violate security are blocked and immediately reported.

Each of the companies selected one or more of the following VOS Auditor modules[1]:

- **Access Control Manager (ACM):** controls user access to production system directories, files and programs while ensuring access rights are up-to-date and consistent with a centralized configuration file
- **MENU System:** Organizes VOS system applications behind an intuitive user interface that presents options to users according to their security profiles, and records all activities, including detailed information about any security violations
- **VOS Security Shell (VSS):** authorizes command execution for operators, system administrators and developers based on each individual's security profile and produces a log of all commands executed.
- **Alert Manager (LAMS):** monitors system elements, automatically executes user-defined corrective procedures and funnels critical alerts to the system operator

Business impact

Using VOS Auditor, the major financial institution developed a new procedure for handling production problems. Through the MENU system, the security officer enables the login ID for the repair technician. LAMS notifies the security officer when the technician logs in, while VSS records all technician activity and alerts the security officer of any violation attempts. Upon logging out, the technician's login ID is disabled. This new procedure shields the system from unauthorized use by limiting the technician's access to a one-time investigative event which is monitored by the security officer.

The major US bank used the ACM module to set up access permissions in a single configuration file to prevent unauthorized access to the VOS system. This centralized access control streamlines the process of updating permissions upon change of personnel. ACM enabled the bank to create scripts to scan all system directories, identify any deviations from desired permissions and automatically fix these security risks — a process that used to be manually intensive and fraught with error.

The European entertainment company deployed the MENU System as a way to eliminate unrestricted command-line access by hundreds of VOS system operators. Now, each operator is presented with different menu options based on his or her profile, and every menu option selected is recorded to a log file along with the user's id and the date and time. Management can review detailed operator activity and generate activity reports. By restricting menu options based on the operator's profile, the MENU system eliminated security gaps while simplifying use of the system by novice and experienced users alike.

The VOS Auditor security and auditing solution has been instrumental in securing the mission-critical Stratus systems that process payments for these industry-leading Fortune 500 companies. By eliminating security risks while producing a comprehensive audit trail, the VOS Auditor Security Solution enables each organization to satisfy corporate governance, regulatory and industry standards for payment processing system security.

About Stratus

Stratus Technologies focuses exclusively on helping its customers keep critical business operations online without interruption. Business continuity requires resiliency and superior availability throughout the IT infrastructure, including virtual environments. Stratus delivers a range of solutions that includes software-based high availability, fault-tolerant servers, availability consulting and assessment, and remote systems management services. Based on its 28 years of expertise in product and services technology for total availability, Stratus is a trusted solutions provider to customers in manufacturing, health care, financial services, public safety, transportation & logistics, and other industries.

[1] See your Stratus sales representative for complete information on all six VOS Auditor Solution modules.

X983-A

Stratus® Technologies

www.stratus.com