CASE STUDY: Starwood Hotels Simplifies User Access Rights Controls for PCI and SOX with Access Auditor®

The Challenge

To help meet PCI and SOX requirements, Starwood Hotels wanted to automate the certification of user access rights and the identification and removal of user accounts left behind from terminated users.

The Solution

Access Auditor automated the re-certification process and the Fuzzy ID Identity Mapper enabled the discovery and removal of orphaned user accounts.

The Results

Within weeks, data from all key applications were imported, and user access reviews underway. SCC's Identity Mapper with the Fuzzy ID module linked user accounts from a wide variety of systems back to the same physical person, giving a true consolidated view into user access rights.

Security Compliance Corporation
120 Village Square, Suite 76
Orinda, CA 94563
(866) 657-4550
www.securitycompliancecorp.com
info@securitycompliancecorp.com

Background

Starwood Hotels & Resorts Worldwide, Inc. is one of the leading hotel and leisure companies in the world with over one-thousand properties in 100 countries and territories with 145,000 employees at its owned and managed properties. Starwood Hotels is a fully integrated owner, operator and franchisor of hotels, resorts and residences with the following internationally renowned brands: St. Regis(R), The Luxury Collection(R), W(R), Westin(R), Le Méridien(R), Sheraton(R), Four Points(R) by Sheraton, and the recently launched Aloft(R), and Element SM. The company boasts one of the industry's leading loyalty programs, Starwood Preferred Guest (SPG), allowing members to earn and redeem points for room stays, room upgrades and flights, with no blackout dates. Starwood Hotels also owns Starwood Vacation Ownership, Inc., one of the premier developers and operators of high quality vacation interval ownership resorts. For more information, please visit www.starwoodhotels.com.

The Challenge

As one of the largest travel companies in the world, Starwood Hotels faces a myriad of security and compliance requirements. With such a large number of hotels, compliance with the Payment Card Industry (PCI) security standards is a particularly important mandate. One of the crucial requirements of both PCI and Sarbanes-Oxley (SOX) compliance is the auditing of user access rights to key systems and applications.

Patrick Foley, Director of IT Compliance for Starwood Hotels, leads the global efforts for the hotel chain's PCI compliance. Foley sought an automated solution to address two primary requirements:

- Ensure that all users have the correct access to systems and applications
- Ensure that accounts for terminated users have been removed

Starwood already owned licenses, but had not yet deployed, another Identity Management (IDM) tool however, it would not help Starwood meet its PCI compliance requirements due to the lengthy and costly deployment required.

The compliance efforts were complicated by two important factors. First, Starwood utilizes a fully-outsourced IT department. While outsourcing saves costs on IT, it also creates compliance challenges such as integrating and aggregating trusted identity stores. The second factor was the lack of a consistent login ID across the various in-scope PCI and SOX applications. Most applications did not store a unique identifier that could link user accounts across various applications back to the same person. Some systems would contain little more than a user name. Without being able to link applications with a centralized identity store, it was very difficult to determine the organizational structure of each user, identify their manager, or even verify if the user was still an active employee.

The Solution

Starwood searched for a solution to automate the PCI and SOX requirements with a cost-effective identity access governance tool that was both easy to use and fast to deploy. Access Auditor from Security Compliance Corporation was the ideal fit for the world's leading hotel chain.

The initial project requirements were to quickly import data into the Access Auditor system and automate the periodic review of user access rights. Access Auditor's easy-to-use interface and intuitive design met Starwood's demanding objectives. Flexible workflow rules enabled multi-level approvals to map to existing business requirements. The look and feel of the web-based user interface remained consistent across all access reviews, minimizing the training required for approvers.

One of the major challenges Starwood faced was the lack of a uniform login ID or unique identifier for each person across disparate systems. Every user could have a different login ID on each application. An important requirement for Starwood's certification efforts was the ability to identify which login IDs belonged to which person. Access Auditor's Fuzzy ID module was the perfect solution. Using an intelligent name recognition algorithm, Fuzzy ID correlates Starwood's business owners with logins that were likely tied to each person, and presented a simple list for confirmation.

> *"Originally intended as a management testing tool for compliance purposes, we recognized its capabilities could be leveraged for achieving our most compelling access management requirements."*
>
> **Patrick Foley, Director of IT Compliance, Starwood Hotels**

The Results

Access Auditor provided Starwood Hotels with tremendous results to meet their PCI and SOX compliance objectives. Within a matter of weeks, data from all key PCI and SOX applications were imported, users linked with the Fuzzy ID module, and user access reviews underway. The entire process is seamlessly automated. Access Auditor tracks completion status for the access rights reviews and sends periodic reminders for approvers that have not yet completed their reviews. With a single click of the mouse, reports show user accounts that are still enabled but cannot be linked back to an active employee, allowing administrators to easily identify and remove orphaned user accounts.

The ongoing benefits of Access Auditor are equally impressive. User access data is refreshed/re-imported on a scheduled interval to give Starwood a single, up-to-date repository of user access rights across all key business applications. Since the data is automatically kept current, the next cycle of user access reviews can be initiated in seconds, leveraging all of the previous workflow and approver definitions.

Though used initially as a tool for user access reviews, Starwood quickly realized additional value. “Originally intended as a management testing tool for compliance purposes, we recognized its capabilities could be leveraged for achieving our most compelling access management requirements,” states Foley. Some of these extra capabilities include:

- Rule-based alerts to changes in user access rights.
- Ad-hoc reporting for user access, especially useful upon transfers and terminations to identify all active accounts for the newly relocated or departed employee.
- Separation of Duties (SOD) reporting and alerting.

Pat Foley sums it up, “Access Auditor helped Starwood succeed in the largest cleanup of user access rights that the company has ever undertaken. We continue to use Access Auditor not only for the original goal of automating user access rights reviews, but also supporting our ongoing day-to-day identity and access operations.”

“Access Auditor helped Starwood succeed in the largest cleanup of user access rights that the company has ever undertaken. We continue to use Access Auditor not only for the original goal of automating user access rights reviews, but also supporting our ongoing day-to-day identity and access operations.”

Patrick Foley, Director of IT Compliance, Starwood Hotels

Access Auditor Key Features

FEATURE	DETAILS	BENEFITS
Entitlement Reviews and Access Certification	• Managers and business owners certify access rights with a simple web-based solution • Flexible rules-based workflow defines custom approvers at various phases of a certification	• Provides company-wide attestation of employee access rights and privileges required for IT best practices and compliance-related audits (SOX, HIPAA, GLBA, ISO 27001, PCI, and others)
Fuzzy ID and the Identity Mapper	• Links users from disparate applications when no consistent login ID exists • Proprietary name-matching algorithms automatically identify the same user in multiple systems with no common attribute	• Solves one of IT's largest challenges, how to view access rights when no common attributes exist • Eliminates the need to modify applications to insert a unique identifier • Establishes a single repository of all access data across the entire enterprise
Role-Based Certifications and Role Definition Tool	• Defines roles and role memberships • Performs certifications by roles and exceptions to improve accuracy and relevance • Performs what-if scenarios to define cross-application enterprise roles	• Improves relevance of certifications by reviewing a handful of roles instead of hundreds of privileges • Defines and manages roles by comparing role memberships and exceptions
Consolidated View of User Access Rights	• Custom reports show real-time and historical data • Orphaned user accounts from transfers and terminations are detected and reported • Historical record of access rights compliance	• Reveals users with inappropriate combinations of access rights • Discovers orphaned or lost user IDs • Provides documentary evidence of meeting access-related compliance controls
Real-Time Access and SOD Alerting	• System monitors for changes to user access data • Simple interface for configuring custom alerts and actions • Comprehensive cross-application separation of duties reports and alerts	• Generates alerts if access data has changed since the last audit scan • Detects unauthorized changes to systems • Warns business owners if users violate separation of duties rules
Automated Discovery	• User access rights and group memberships are automatically discovered and processed • Support provided for wide variety of commonly used applications without product customization	• Consolidates user data from diverse systems and groups by user and application • Enables Access Auditor to provide a near real-time view of user entitlements

SCC
Security Compliance Corp

Security Compliance Corporation
120 Village Square, Suite 76
Orinda, CA 94563
(866) 657-4550
www.securitycompliancecorp.com
info@securitycompliancecorp.com

Security Compliance Corporation's (SCC) Access Auditor® automates the periodic review and certification of user access rights and entitlements. SCC's workflow engine provides the ultimate flexibility in defining and managing the periodic attestation of user access rights. The enhanced Identity Mapper™ utilizes a proprietary algorithm to link user accounts from disparate systems back to the correct person, even when common identifiers or login IDs do not exist. Access Auditor's consolidated view of user access rights enables customers to identify orphaned accounts left behind from terminated users, thus reducing the risk of fraud and audit findings. By automating labor-intensive tasks related to user access rights and separation of duties, SCC's customers improve security while minimizing the costs of compliance. Founded in February 2005, Security Compliance Corporation is based in Orinda, CA.

© Security Compliance Corp, SCC, Access Auditor, and the SCC logo are trademarks of Security Compliance Corporation. CNMC, Children's National, and the Bear logo are trademarks of The Children's National Medical Center.