salty cloud

STACHE

Securely Share & Store Sensitive Credentials

saltycloud.com

Saltycloud is a Public Benefit Company

Sharing Sensitive Data While Safeguarding It Requires a Robust Data Manager Designed with Security in Mind

STACHE is a sensitive data manager for items such as passwords, numbers, procedures, and keys that provides a streamlined, secure, and cloud-based solution for highly distributed or regulated environments to protect data while allowing collaboration and escrow capabilities amongst colleagues.

Secure Data Management for Any Use Case

Whether you're storing a personal email login, sharing the office credit card with your team, or retrieving a highly sensitive credential in times of need, STACHE was purpose-built to help you manage and protect sensitive data.

Credential Management

Create, access, edit, and organize data entries and groups.

Colleague Collaboration

Share individual entries and create groups using a series of permissions. Additionally, stay aware of shared sensitive entries with a trip-wire alert that notifies other owners when they are accessed.

Access Administration

Manage your organization's data when the owner is not available or responding to a lawful request on a entry-by-entry basis. Unencrypted field searches and MofN approval mechanisms allow for controlled retrieval of encrypted entries.

In a Recent Report Analyzing 277 Separate Breaches, System Admins Were the #1 Internal Actor Accounting for 26% of Breaches[1]

In today's security landscape, no one person should have unhindered access to the organization's vault of sensitive entries. Contrary to personal password managers, STACHE employs administrator rules, including audit logs, for entry retrieval that ensure the proper chain of command approval.

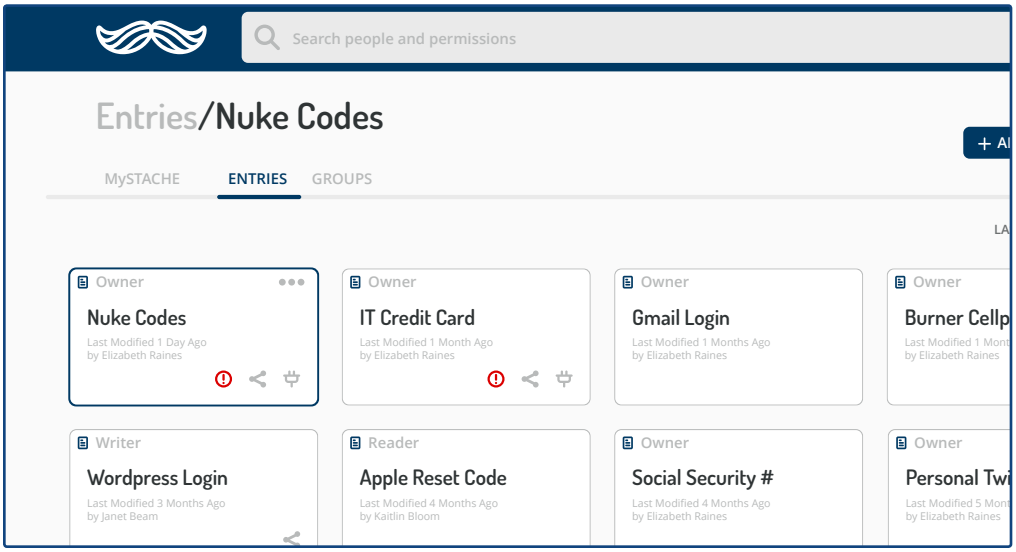
1. Verizon Data Breach Investigation Reports (DBIR), 2017

API Features for Automated Processes

STACHE comes equipped with a read/write API that allows for greater customization and automation with your existing systems. You can easily store and escrow S/MIME digital certificates issued via InCommon using built-in API capabilities. The STACHE write API can further streamline things like account and resource provisioning on campus as well as other workflows.

Layers of Encryption at Rest and In Transit

All data stored on STACHE is encrypted and vetted using government-grade encryption standards (FIPS 140-2). On the backend, STACHE uses a Hardware Security Module (HSM) to encrypt data entries with a Data Encryption Key (DEK) that uses an AES-256 algorithm with a SHA-256 hash. While at rest, this data is also encrypted by a separate AWS generated and managed key (KMS). When data is in transit, the original DEK encryption remains, but the AWS-KMS key is replaced with an AWS-TLS encryption key for transit. At all times, STACHE is layering data with at least two levels of industry standard AES-256 grade encryption keys.



Key Features

- Cloud-Based Architecture
- Two-Factor Authentication
- SAML & LDAP Integration
- REST API Integration
- Write API Integration
- MofN Admin Workflow
- FIPS 140.2 Compliant

Ready to STACHE?

Contact us to get a personalized demo. STACHE is proven to securely manage sensitive data at large, distributed organizations while being lightweight and robust enough for small security or IT teams.

SaltyCloud delivers proven security solutions designed for highly distributed and regulated environments including DORKBOT Vulnerability Search Service and ISORA IT Risk Assessment. Our products are in use at over 400 Universities across US, Canada, Australia and beyond.

saltycloud™