HITACHI
Inspire the Next

University of California San Francisco Modernizes Secure Access

CASE STUDY

Challenge: The institution needed to replace its legacy identity system deeply entangled with core business processes.

Solution: UCSF chose Hitachi ID to modernize its identity access management and provide increased secure access from anywhere.

Outcome: Security strategy now matches UCSF's culture of innovation and excellence with improved flexibility, efficency and governance.

INDUSTRY
Higher Education

REGION
North America

PRODUCT
Hitachi ID Bravura Security Fabric

After twenty-years it was time for the University of California San Francisco (UCSF) to strengthen security and empower greater access to knowledge by modernizing a decades-old identity system. Based on mainframe technology, the system was being phased out–its software authors and maintainers long since gone. Paired with another major IT project plus complex higher education challenges like cyclical onboarding and siloed IT purchasing, the university faced an endeavour. How would UCSF replace a legacy identity system so deeply entangled with core business processes to prepare for the future?

The Challenge

UCSF is not one but two top down organizations. Both a university, with an array of education requirements, and a hospital, with its own interlaced medical teaching needs, population is broad. Like many universities, UCSF's changing population required massive on-boarding and deactivations when classes began and ended, placing huge strain on staff.

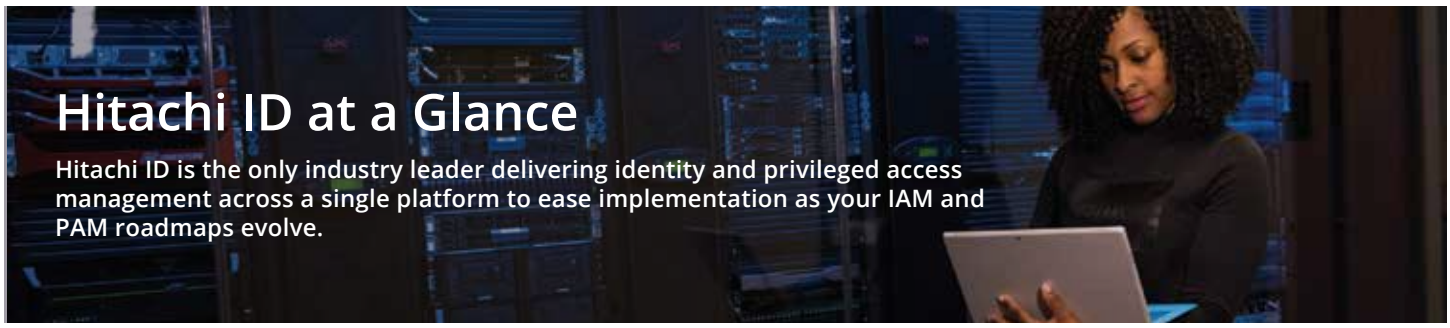
Multiple data sources combined with loose affiliations for members including students, teachers, staff, residents, nurses, doctors, researchers, guests, volunteers and contractors made the quality of the data unreliable. Some departments inconsistently used central identity provisioning for SaaS applications like Box and DocuSign. Each member could also have multiple changing affiliations within UCSF, like graduates who work in the hospital.

Distance learning introduced added risk. Bad actor logins plus access challenges like firewall issues in China or students in Africa connecting mainly from smartphones with slow and spotty connectivity was a concern.

UCSF was also replacing a thirty-five-year-old system to centralize human resources and academic solutions for all personnel and payroll transactions. It needed to maintain existing systems and synchronize across both new and old systems of record during the migration. The new personnel system also required extra unique identifiers and processes tied to user names. Those names often change with marriage, divorce, and gender, introducing yet another impact to IDs, email addresses, aliases, and more.

Across all applications and services, UCSF needed one data source to automate provisioning, synchronize systems of record, and streamline appropriate access through the identity lifecycle with a highly secure yet publicly accessible identity solution.

> "With Hitachi ID as our identity provider, we significantly improved our flexibility, efficiency and governance. Our security strategy now matches our culture of innovation and excellence."
>
> Kevin Dale, Senior Manager, Identity and Access Management, University of California San Francisco



Hitachi ID at a Glance

Hitachi ID is the only industry leader delivering identity and privileged access management across a single platform to ease implementation as your IAM and PAM roadmaps evolve.

The Solution

UCSF prioritized must-have features including password management, good connectors including one for Active Directory, group management, identity lifecycle, access management, and governance. Kevin Dale, Senior Manager, Identity and Access Management, University of California San Francisco, brought the project from concept to completion.

UCSF chose Hitachi ID as the best solution to modernize its identity access management and provide increased security access from anywhere. They found Hitachi ID offered the reliability, technology, extensive expertise and professional services it needed to locally deploy at a cost that met their requirements.

“Beyond a magic quadrant, an analyst like Gartner can offer in-depth insight on solutions to meet your strategic goals,” says Dale. “Prior to sending out a request for proposal, cast a wide net and talk to many vendors.”

Dale advises to prioritize features and technology then eliminate vendors who don’t fit your needs. Get demonstrations and talk with peers and reference clients to help validate your decision. Finally move ahead with a proof of concept to determine how the short-listed solution works for you.

Budgets for universities, even those with a hospital, are much smaller than those of corporations. While autonomous IT funding across the centers and individual schools combined with ambiguous organizational structure is typical, the University and the Medical Center jointly fund and use central IT including networking, identity access management and business apps. The identity modernization budget, driven by a request for proposal with a small plan for contingency, was fixed. Since tribal knowledge had left the organization and old systems were without good documentation created an element of the unknown, the team also budgeted for some ongoing enhancements.

“Fixing the scope and price is the only way to avoid a multi-year, multi-million-dollar white elephant project,” said Dale. “Getting an accurate scope takes time and effort to capture but failing to define it will result in a project you may think is agile but really is just ruinously expensive and lengthy.”

An experienced partner will help develop an efficient deployment and test plan that’s tried and true. To get to an accurate estimate, USCF clearly defined the full project scope through discovery and by outlining precise requirements and acceptance criteria. They created clear test paths and enough time to test deliverables prior to going live. Though each sprint added extra time and cost for testing and migration, the sprints added transparency and confirmation they were implementing to plan.

The Outcome

With one identity system to rule them all, UCSF leveraged faster near-time processing and simplified integrations through an ecosystem of over one hundred connectors. Automation saved notable time and effort onboarding and deactivating, and enabled appropriate access based on birthrights, roles, workflows and notifications. The team strengthened security through enhanced access control with attestation, self service requests, credential management, delegated administration and approvals. Easier support, upgrades and enhancements put UCSF in control of identity access to empower teaching and learning.

Nine departments worked to promote adoption across the campus. Spearheaded by the IT team, stakeholders worked in business and governance groups. They outlined concrete deliverables including replacing the mainframe, introducing the Hitachi ID solution, production deployment, automating and standardizing provisioning and deactivations, federation via Shibboleth and multi-factor authentication. The stakeholders frequently communicated prioritized outcomes linked to timelines to help foster partnerships with staff. They trained everyone on how to use the new Hitachi ID solution and augmented skills as needed.

“It’s a long term investment and you have to think about the future,” says Dale. “With Hitachi ID as our identity provider, we significantly improved our flexibility, efficiency and governance. Our security strategy now matches our culture of innovation and excellence.”

With a modern Hitachi ID identity solution, UCSF simplified and improved data protection and access while reducing security risk. Improved control has better positioned UCSF to provide access for its members today and ever growing population into the future.