



---

## Overview

### The need

With a constantly changing student population, IT staff faced an ongoing administrative challenge to manage user accounts and confirm users had the right access to the right systems at the right time.

### The solution

Working with Pontis Research, the university deployed an identity management solution from IBM that reduces the time and complexity of managing user accounts and access privileges.

### The benefit

IT staff were able to uncover and close out thousands of inactive accounts, confirm compliance with regulations, and efficiently manage a fluid user population.

---

# Chapman University

## *Reducing risk and confirming appropriate user access*

Located in Orange, California, Chapman University is a private, midsized university with approximately 8,000 undergraduate and graduate students from 60 countries.

### **Battling complex and continually evolving user access requirements**

Despite having a homegrown automated identity management system, Chapman University faced significant challenges when it came to managing access to systems and data. The legacy system didn't provide the flexibility or capabilities the IT staff needed to easily manage often complex and evolving relationships with users.

For example, students require different access rights as their relationship with the university changes from applicants to students to alumni. Parents who manage the "business relationship" between the student and the university need access to financial information, but can't access their child's educational records without the student's express permission. Faculty members may require access to student educational records for a semester, but are prohibited from viewing financial aid data.

---

*The IBM Business Partner ecosystem gave Chapman University IT staff valuable knowledge and expertise as they worked to strengthen and streamline identity management processes. "IBM has built a strong relationship with companies like Pontis Research, and this relationship really benefits us in the long term," says Helen Norris, chief information officer, Chapman University.*

---



---

## Solution components

### Software

- IBM® Security Identity Manager

### IBM Business Partner

- Pontis Research Inc.
- 

“We have to provision users at the right time and provide them only with access to the things that they need for their role at that time,” says Helen Norris, chief information officer, Chapman University. “When students leave the university, we have to shut off some of their access, but we still want to maintain a relationship with them and continue to manage them within our pool. We needed a tool to help us better manage these relationships.”

## Taking a holistic approach

Working with IBM Premier Business Partner, Pontis Research, the university replaced its existing solution with an identity management solution from IBM. Key to its decision was IBM’s ability to meet the organization’s needs both today and in the future.

“Chapman University had an immediate need to improve identity management for their students, faculty and staff; however, in the future, they may need to support additional scenarios including authentication of federated identities,” says Vinita Bhushan, enterprise security architect and president, Pontis Research. “By using the IBM Security suite, they gain a holistic solution that supports them as they grow.”

Today, IBM® Security Identity Manager software helps the organization effectively manage relationships with approximately 9,500 students, faculty, staff and community members. The solution simplifies and automates the creation, modification and termination of identities across the lifecycle of each relationship.

IT staff can also easily extend user access to new university systems, without having to build custom integrations for each Active Directory. For example, in recent years, Chapman University has expanded its Health Sciences department, adding pharmacy, physical therapy and psychology programs. Many of these programs provide community clinics, and IT staff must manage user access to the supporting clinical systems based on Health Insurance Portability and Accountability Act (HIPAA) guidelines.

“We’re growing, adding more students and new programs,” says Norris. “The IBM solution is scalable and sustainable, and can grow with us.”

---

*“We can manage our fluid user populations and keep people in the community while addressing compliance requirements and better protecting our data.”*

—Helen Norris, Chief Information Officer,  
Chapman University

---

### **Reducing risk while building relationships**

For Norris, the most important benefit realized has been a reduction in the university’s risk. Using IBM Security Identity Manager software, IT staff were able to uncover and close out thousands of inactive accounts, which could pose a substantial security risk if compromised.

“In the past we created an account for every applicant and that became very difficult to manage,” says Norris. “We found that we had thousands of unused accounts. Now, we can better manage our risk by confirming that we don’t provide access to people who don’t need it.”

In addition, the solution’s advanced capabilities help IT staff confirm that the university doesn’t inadvertently share student data when it shouldn’t be shared.

“It’s important for us to confirm compliance with FERPA [Family Educational Rights and Privacy Act],” says Norris. “With the IBM solution, we can minimize access to student data, and only give access to the people who need it. It also helps us audit access to confirm we haven’t inadvertently provided the data too broadly.”

Ultimately, Norris says, the platform enables the organization to build stronger relationships with its students, and continue those relationships even after students graduate.

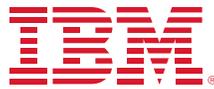
“We can manage our fluid user populations and keep people in the community while addressing compliance requirements and better protecting our data,” says Norris.

### **Take the next step**

To learn more about IBM Security software, please contact your IBM representative or IBM Business Partner, or visit the following website: [ibm.com/security](https://ibm.com/security)

For more information about Pontis Research Inc., visit:  
[www.pontisresearch.com](https://www.pontisresearch.com)

For more information about Chapman University, visit:  
[www.chapman.edu](https://www.chapman.edu)



---

© Copyright IBM Corporation 2015

IBM Security  
Route 100  
Somers, NY 10589

Produced in the United States of America  
June 2015

IBM, the IBM logo, and [ibm.com](http://ibm.com) are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at [ibm.com/legal/copytrade.shtml](http://ibm.com/legal/copytrade.shtml)

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

**Statement of Good Security Practices:** IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.



Please Recycle