



**“The Cal State system’s the largest four-year public university in the country, we have half a million students, 23 campuses, and almost 50,000 employees. Protecting the data of half a million people keeps me pretty busy with different challenges every day.”**

**Ed Hudson**, Chief Information and Security Officer at Cal State University

### **Customer Challenge**

California State University’s team needed a streamlined approach to student, faculty, and staff personal data protection across 23 campuses.

### **Spirion Solution**

Automating personal data discovery addressed a significant data protection challenge across 23 California State University campuses.

### **Spirion Results**

Locating, classifying, and protecting data has become a routine part of the cybersecurity program at the California State University system. It all goes back to a simple idea: If you don’t know what you have, you can’t protect it.

# California State University Finds and Protects Personal Data Across 23 Campuses

## **Industry Challenge: Protect the Most Invaluable Student, Faculty, and Administration Asset, Personal Data, While Maintaining Academic Freedom**

If information is the lifeblood of academia, then personal data is the digital embodiment of the human self. When higher education institutions collect personal information, they possess the most invaluable assets of their student body, faculty, and administration. A student’s file offers an extensive view into their existence, including personal demographics, academic records, financial details, and medical data. This data inevitably puts their security at risk and has the potential to paralyze performance and cripple efficiency campus-wide. Educational institutions rank fourth only behind finance, healthcare, and public administration in the sheer volume of data breaches. This has led lawmakers to further regulate how large institutions collect and secure student data.

While data protection is essential across business, higher education institutions must maintain a careful balance between freedom and access to allow for education innovation and the often conflicting regulations, such as the California Consumer Privacy Act (CCPA).

## **The Need: A More Accurate and Secure Data Protection Program**

In 2015, the California State University (CSU) system confronted their extremely cumbersome information auditing process. While the team was asking the right questions to staff, faculty, and students — what kind of data do you have, what do you use it for, and how do you protect it — they needed a more efficient and accurate method of identifying and protecting server and endpoint data.

“The CSU is the largest four-year public university in the country, we have half a million students, 23 campuses, and almost 50,000 employees,” says Ed Hudson, Chief Information and Security Officer at the CSU. “Protecting the data of half a million people keeps me pretty busy with different challenges every day.”

## The Solution: Spirion Protects Privacy

Initially, Spirion was implemented as a more mature and systematic automated discovery process. The initial discovery process was lengthy, especially because endpoints can go missing, Hudson explained. "It is not unusual for a laptop or tablet to be left in a vehicle or in the back seat of an airplane. At CSU, we have a lot of endpoints, and many are mobile, therefore at higher risk for being lost."

After searching the endpoints, Hudson found many surprising pieces of data in large numbers and unexpected places. "When we first implemented Spirion, I expected to find personal data on finance and HR endpoints, but the discovery of nine million social security numbers on a research department employee's laptop was a shock. Fortunately, by following the path statement, I could see exactly where the data was on the endpoint." The discovery of this large trove of vulnerable data was not an isolated incident. Spirion also discovered 20 million credit card numbers on another endpoint.

Automating personal data discovery addressed a significant challenge across all 23 CSU campuses, but finding the data brought a new set of questions to the forefront – what type of data, how should it be safeguarded, who has access, and how can we adequately protect it?

The CSU information security team worked with Spirion to develop rules and regulations for engaging with and protecting data across the entire university system. It was important to clearly communicate the purpose and outcomes of data protection, while maintaining the balance between academic freedom and protection of personal data and intellectual property.

In addition to moving data that is inappropriately stored on the endpoint, the CSU needed to protect data that belonged on the endpoint. The CSU improved their endpoint protection by using Spirion on a regularly scheduled basis for automated personal data discovery. Spirion's search capabilities allows the CSU to change their strategy in response to the varying data privacy and regulatory requests.

## The Results: Discovering and Protecting Personal Data across 23 Campuses

Locating, classifying, and protecting data has become a routine part of the cybersecurity program at the CSU. For the CSU team, the program stems from a simple idea: If you don't know what you have, you can't protect it. The beauty of the new processes is the ability to quickly respond to auditors with accurate data inventory and movement reports that span all 23 campuses, and all environments. Instituting the data protection program was a large endeavor, but Hudson and the CSU team are committed to preventing misuse and reducing the risk associated with personal data. "You can't avoid an important project just because it is difficult," says Hudson. "I don't want to find myself on a witness stand saying, 'Oh, I didn't implement the most optimal security procedures because it was hard.'"

Higher education institutions must have an open flow of information that is protected from intentional and unintentional misuse. With Spirion, the CSU security team simplified a complex and inadequate process with the ability to find, identify, and quantify data. They are fully prepared for audits and successfully comply with the extensive education, financial, and state regulatory requirements.

**Talk to a Spirion data security and compliance expert today: [expert@spirion.com](mailto:expert@spirion.com)**

Spirion is the leader in data discovery, persistent classification, and protection of sensitive data on-premise and in the cloud. Since 2006, thousands of organizations worldwide have reduced their sensitive data footprint and proactively minimized the risks, costs and reputational damage of successful cyberattacks. Spirion provides greater command and control of sensitive data to leading firms across all industries from financial services to healthcare to public sector. Visit us at [spirion.com](https://www.spirion.com)