

Key Facts

Company

Quinnipiac University

Industry

Higher Education

Country

United States

Employees

1,500

Students

8,500

Websitewww.qu.edu

Challenges

Given the tremendous growth of the university and the addition of several specialized schools and multiple campuses, Quinnipiac University needed a better way to secure and manage privileged access and view account activity.

Results

- Gains privileged-account visibility
- Reduced PCI audit time by two weeks
- Improves security with privileged-account controls
- Raises security awareness among admins

Products

One Identity Privileged Access Management solutions

One Identity Services


University raises the grade on securing privileged accounts

Quinnipiac University gained privileged user account visibility it lacked by deploying new privileged access management tools, with help from One Identity Services

Higher education poses a special class of IT security challenges because a university operates more like a small city. With its own public safety and health services, and payment-processing capabilities, a university must comply with numerous cyber-security requirements. In addition, every year's graduation sees about a quarter of the student population turning over, bringing new students, new devices and, potentially, new cyber threats. And that doesn't count the normal turnover among faculty and administrative staffs.

IT must also address the security challenges of students and staff connecting to campus networks with everything from their smartphones and gaming consoles to their tablets and laptops. Then there are countless flash drives making their campus rounds with contents that varies from term papers to pirated software, housing all sorts of potential viruses and malware that might infiltrate the campus network.

Brian Kelly, chief information security officer at Connecticut's Quinnipiac University, knows this all too well. "We've got about 10,000 users on



“Despite our firewalls as **boundaries**, the bad guys are now using compromised insider credentials to get in, so it’s critical we have **visibility** into who was doing what — and when and why — among our privileged users.”

Brian Kelly, Chief Information Security Officer, Quinnipiac University

campus, both students and staff, who make up a vast attack fabric that’s quite dynamic,” he says. “Our role is to protect them from themselves, while also protecting the university from the internet’s many threats.”

Taking a fresh look at security

In Kelly’s view, privileged-identity management is a core element in the layered, defense-in-depth model that he has now deployed at the university as a security best practice. But for years, the school had been using home-grown tools for privileged-identity management. University growth and the addition of two satellite campuses gave him plenty of reasons to consider a new approach.

One of those reasons is the changing nature of attacks. “Despite our firewalls as boundaries, the bad guys are now using compromised insider credentials to get in, so it’s critical we have visibility into who was doing what — and when and why — among our privileged users,” Kelley says.

To meet this challenge, Kelly chose One Identity’s Privileged Access Management Solutions,

which automate and secure the management of privileged accounts and passwords while recording all activity. “We just didn’t have enough visibility and insight into who was doing what, when and why. But with the addition of the One Identity Privileged Access Management Solutions, we now have that visibility plus the added security around our privileged accounts,” he says.

For implementation help, he turned to One Identity Services. “We evaluated alternatives, but the One Identity Services team really shined in helping us deploy and use the Privileged Access Management Solutions,” he says. “The team, their expertise and their responsiveness have all been extraordinary.”

Getting campus stakeholders on board

Kelly found the One Identity Services team especially useful in getting his key campus stakeholders, including server administrators and help desk staff, to understand and support the Privileged Access Management Solutions.

“I thought the benefits of the solution would be self-evident, but they weren’t,” he recalls.

“Fortunately, a workshop facilitated by the One Identity Services team was able to show our team that the solution was not adding friction to their roles and responsibilities, but actually adding a benefit by taking over the responsibility of managing those accounts.”

According to Kelly, the biggest benefits for the university are the enhanced security and new visibility into the activities of the privileged users. “We simply did not have that capability before, so we can’t quantify the amount of its impact, but it’s big,” he says. “In effect, the visibility that the Privileged Access Management Solutions provide is a new security perimeter for us.”

Gaining new visibility strengthens security

With the help of One Identity Services, Kelly’s team set up the Privileged Access Management Solutions to actively manage all their privileged accounts. In addition to managing the more high-risk server and domain administrative passwords, they record all session activity.

“We want to ensure that our users of high-risk assets are doing only what they are supposed to do, and we can prove that for compliance requirements,” Kelly says. “And, since the session management solution doesn’t provide them direct access to the systems, we can also ensure any malware or viruses won’t transfer from an admin’s computer to these high-risk assets.”

Overall, Kelly and his team rest much easier knowing that they’ve eliminated a big vulnerability with the extra security privileged-access management provides. Regulatory compliance has also been enhanced. “My team is more productive, leaving privileged- access management to One Identity’s Privileged Access Management Solutions,” he says. “And compliance is easier, saving us two weeks in our PCI audits alone.”

About One Identity

The One Identity family of identity and access management (IAM) solutions, offers IAM for the real world including business-centric, modular and integrated, and future-ready solutions for identity governance, access management, and privileged management.

Learn more at [OneIdentity.com](https://www.oneidentity.com)

“We evaluated alternatives, but the One Identity Services team really shined in helping us deploy and use the Privileged Access Management Solutions. The team, their **expertise** and their responsiveness have all been extraordinary.”

Brian Kelly, Chief Information Security Officer, Quinnipiac University