Colleges prepare to graduate to next-gen identity systems

The need for stronger security and more seamless access to virtual campus life prompts higher ed officials to consider agile, passwordless identity platforms.

EdScoop Report

Higher education IT administrators have always been challenged with managing who has access to their institution's resources. User profiles routinely blend together every semester as students work as campus employees, graduate students serve as faculty assistants and staff employees take online classes.

The challenge of identifying campus IT users—and controlling what resources they have access to—has become even more acute as students and faculty continue to adjust to remote learning conditions. That's forcing colleges and universities to take a closer look at more agile and automated security solutions that can authorize and authenticate users' identities quickly and ensure they can securely access the resources they need.

Universities in recent years have made headway trying to centralize the login credentialing process, both to reduce the friction users often experience and the burden on help desks to reset passwords. But while centralized login platforms can streamline how users enter the digital campus, tighter controls still must be put in place to regulate all the different resources users have to access to—from courseware to dining hall debit cards—depending on whether they're a student or staff, applicant or alumni.

Universities also are coming to terms with a weak link in every identity and access system: the relative ease for abusing traditional usernames and passwords.

That is why higher education IT administrators stand to benefit from robust identity authentication solutions that do not depend on a username and password, and instead allow organizations to establish tiered policies and requirements that can prompt for a second factor for authentication.

This not only reduces security risks, but also helps to lower IT and help desk costs and provide a more user-friendly experience, says Kelsey Nelson, Senior Product Marketing Manager at Okta.

The path to streamline identity and access

The University of Notre Dame represents what many higher education institutions have had to address, according to Nelson. As the university's digital infrastructure expanded, as did the risk of data breaches, it became an increasing challenge for the university's homegrown identity and access management (IAM) system—which dated back more than two decades—to keep up.

With more than 18,200 students, faculty and staff, the university recognized the need for a more robust and frictionless IAM solution so that its stakeholders could access resources to learn, teach, research and collaborate across the campus.

> “Ultimately you are pushing towards stronger security that is better for the end user. Imagine getting a security notification every time you sign in. Eventually the user will become numb to that and...circumvent your security.”
>
> **Kelsey Nelson**
> *Senior Product*
> *Marketing Manager*

The IT department also wanted a more efficient way to balance security and user experience, so the university, among other measures, implemented a multi-factor authentication solution. The cloud-based identity platform automates IT workflows and gives administrators greater visibility into daily IAM activities and account provisioning.

Establishing identities—and a user's role—is key for higher education institutions to help define a user where accesses intersect, Nelson says. For example, students and faculty need different access privileges to a given class's gradebook. And a graduate student can be a student one minute and serve in the role of an instructor the next minute. An IAM platform needs to recognize and control segmented access rights.

Stronger authentication and improved user experience

The push to adopt multi-factor and two-factor authentication solutions are helping higher-education organization strengthen their security and access, but this is also a stepping-stone to more effective and streamlined access controls.

"The challenge with MFA lies with low-assurance second factors, such as SMS, which are widely used but have well-documented weaknesses that are exploitable by hackers," Nelson explains. "Finding the balance between multi-factor and passwordless authentication tools will drive better user experience and strong security for organizations."

"What I hear from IT leaders from the higher education sector is a need for stronger security, without adding friction for students and for staff members," she says. "And that friction looks different for both of these end-user groups. If you lock everything down to make it really hard to get into for attackers, you are also making it more difficult for your end-user."

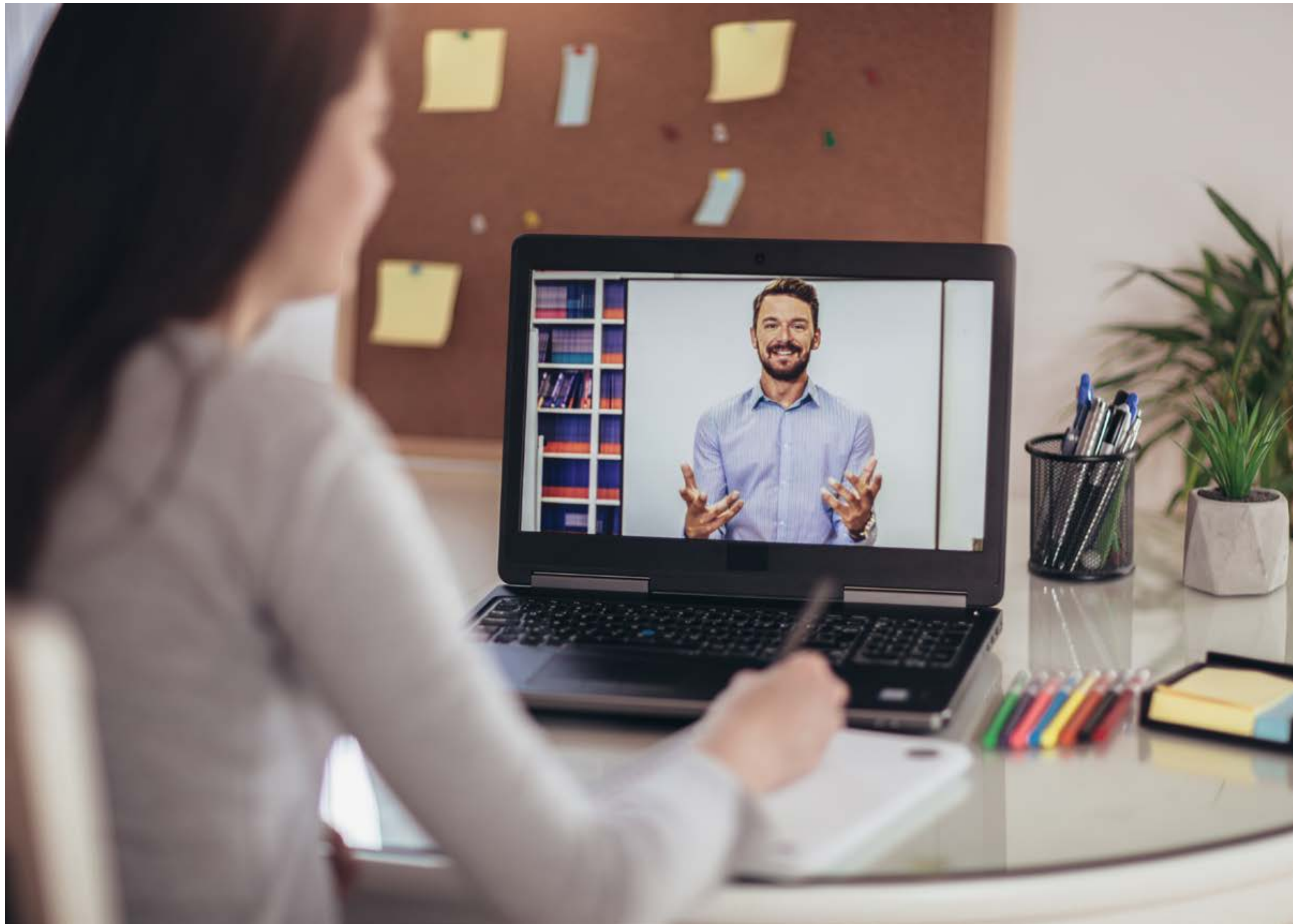
Colleges and universities are particularly vulnerable because of the overlapping and evolving nature of their users' roles.

Modern identity management and policy engines allow IT administrators to better define who a user is at a given time and change privileges as they move through their identity lifecycle. Additionally, with current automation technology, policy engines can deliver stronger identity hygiene. So, if a student changes a department, or a staff member audits a course, those permissions are updated accordingly.

"Ultimately you are pushing towards stronger security that is better for the end user," says Nelson. "Imagine you're an end-user and you're getting a security notification every time you sign in. Eventually the user will become numb to that and it's no longer going to add value. Additionally, if it's too hard, end-users are going to circumvent your security."

That's why IT security officials are increasingly looking for ways to abandon the need for passwords altogether, and adopt solutions that support a passwordless experience.

By 2022, Gartner predicts that 60% of large enterprises, and 90% of midsize enterprises, will implement passwordless methods in more than 50% of use cases—up from 5% in 2018.



Taking authentication a step forward

Redefining logins with passwordless authentication can reduce or even eliminate a majority of password-based attacks. Going passwordless is an evolutionary process and requires careful planning. But with phishing—and the use of compromised passwords—ranked as the leading threat action by a variety of security reports, passwordless authentication may be one of the most impactful steps that an organization can take to manage a range of security risks.

But it also offers advantages in streamlining users' experience as well. With a robust policy management solution, IT administrators use risk factors to designate instances when the user needs to authenticate only once using passwordless access, and other times when they need a second factor.

"For example, if a student loses their phone, a policy that requires they use the same application on their phone every time is not an effective policy," Nelson explains. "But in that same scenario, if that student meets other authentication factors—those can be network, application, geography, the resource they are trying to access or known user behavior—the system will double check their identity because it's a new phone, but won't need to check it again after."

There are several types of approaches to going passwordless depending on the use case:
Email magic links is an encoded one-time password (OTP) token or live link in the body of a secure email. This is common approach to password resets, but under passwordless authentication the password is removed, and the user is sent a secret, time-limited or user lifecycle limited, single-use link

Factor sequencing gives contextual awareness and intelligence to configure multiple authentication factors. When threat levels are low, the login experience can be streamlined with a simpler path to data and apps. When the risk level is high, the user is prompted to use a second authentication factor—like WebAuthn.

FIDO2/WebAuthn is a standards-based passwordless authentication framework that allows for web applications to simplify and secure user authentication by using registered devices (phones, laptops, et cetera) as factors. Any web application running in a browser that supports FIDO2/WebAuthn can take advantage of these authenticators to securely authenticate users.

Passwordless with device trust integrates with endpoint management systems to deliver a passwordless login experience on desktop and mobile.

According to Ant Allan, vice president analyst for Gartner, there has been increased demand for passwordless approaches over the last year.

"By 2022, Gartner predicts that 60% of large enterprises, and 90% of midsize enterprises, will implement passwordless methods in more than 50% of use cases—up from 5% in 2018.," Allan said in a March 2019 interview.

Colleges and universities are currently in the throes of rethinking how they will deliver a mixture of classroom and online learning experiences. That will inevitably require adopting more cloud services to reach students and faculty at home, but also an ideal opportunity to deploy more modern, cloud-based IAM platforms to better manage and protect their systems, resources, and most of all, their users.

Learn how to improve security and create a more efficient user experience for students and staff.

This report was produced by EdScoop and underwritten by Okta.

edscoop

okta