University of British Columbia

The University of British Columbia is a major research university in Canada that consistently ranks among the top 20 public universities in the world, with over 65,000 students and almost 20,000 faculty members and staff.

The Challenge

Cyber criminals often target educational institutions with phishing attacks. Across the industry there is an increase in the sophistication and frequency of phishing attacks. Despite best efforts, even the more technically savvy users do not always recognize a phishing attempt.

To ensure that the protection is comprehensive, the InfoSec team required a multi-factor authentication (MFA) solution that could integrate with a wide variety of on-premises and cloud applications. This meant that the MFA solution must support modern and legacy authentication protocols while providing a consistent user experience. In addition, the team also required the solution to comply with security controls for regulations such as PCI-DSS and HIPAA.

The solution must also provide adaptive access policies that are aware of user role, target application, user device type, and login context. A reasonable level of protection at low friction is appropriate for many use cases to encourage user cooperation and reduce security fatigue, while particular applications require the most stringent possible access policies.

For example, the team was able to integrate Duo with the VPN solution and programmatically combine VPN access rules with multiple MFA profiles. MFA challenge policy would vary according to the role that a user assumes when connecting to VPN.

Depending on the application and risk context, the university has enforced Duo's adaptive access policies, such as ensuring that authenticator devices have screen lock enabled, allowing different authentication methods based on the needs of each department, enabling "Remember Me" device policies for specific applications and checking every device that enters the network. Finally, Duo has out-of-the-box integrations with the Shibboleth and CAS Identity Providers, two of the major implementation requirements.

The Solution

Deployment and Administration

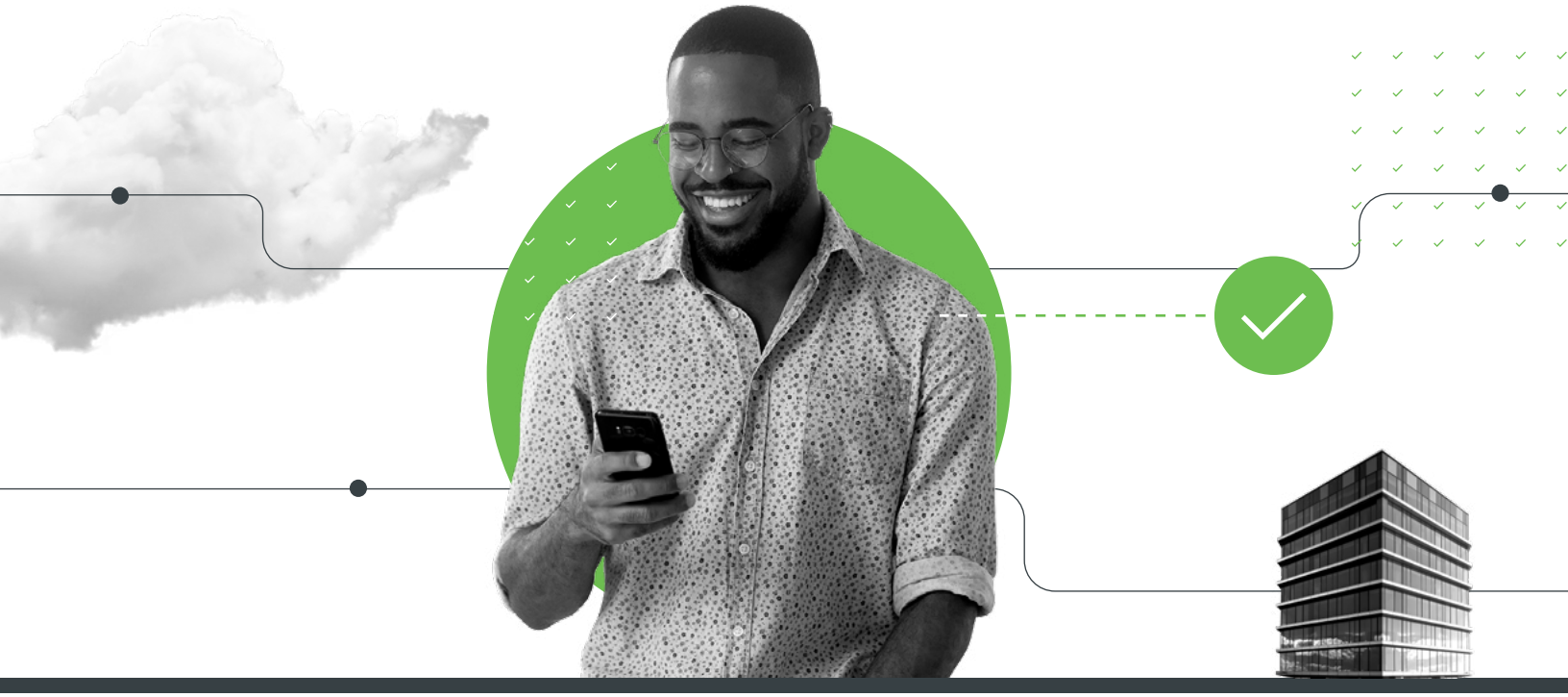
The InfoSec team deployed Duo and enrolled over 40,000 users in a phased approach over a year. Duo comes with an authentication proxy with LDAP and Radius connectors, which was used in a variety of use cases for MFA and also to manage risks around primary authentication against AD. The proxy was implemented in high-availability (HA) mode for load balancing.

To reduce the friction and service support risks of the MFA rollout, a custom integration was built between the Duo API and the organization's directory services to synchronize users and groups for hundreds of departments, set fine-grained access policies, and enable phased onboarding. This custom synchronizer allowed for a flexible user enrollment schedule across various departments and facilitated the IT change management process.

For example, certain user groups that access sensitive applications were required to enroll into MFA at the time of application login, while other user groups were prompted to enroll before a cutoff date, with soft reminders upon login that leads to a mandatory enrolment. When users become employees and when they leave, MFA challenge is applied and removed automatically, with lifecycling logic to prevent loss of access while transitioning between jobs. The result was an orderly rollout without inducing a deluge of IT helpdesk calls and with minimal impact to end users.

To support a diverse community of users and minimize administrative overhead, the InfoSec team has delegated access management to each department's IT desk by subsets of user population and/or applications. This helps enforce the principle of least privilege access and reduce the risk of providing too much access for the wider user population.

After the deployment of Duo, the use of compromised credentials has been observed to drop significantly, up to 95%.



“One of the most attractive things about Duo was that it holistically solved MFA across all our applications … We’re able to standardize the platform, the process behind the platform, and the end-user experience.”

Mark Schooley
Senior Director, IT Operations & Engineering
Box

Start your free 30-day trial and quickly protect all users, devices and applications at **duo.com**.

Duo Security, now part of Cisco, is the leading multi-factor authentication (MFA) and secure access provider. Duo comprises a key pillar of the Cisco Zero Trust offering, the most comprehensive approach to securing access across IT applications and environments, from any user, device, and location. Duo is a trusted partner to more than 25,000 customers globally, including Bird, Facebook, Lyft, University of Michigan, Yelp, Zillow and more. Founded in Ann Arbor, Michigan, Duo also has offices in Austin, Texas; San Francisco, California; and London.