Facebook
How the Social Media Giant Secured Their Engineers and Protected More Than 10,000 Users
The Challenge

Facebook manages personal data for 1.19 billion active users across their platform; creating a clear case that the integrity of the personal data entrusted to them is integral to the overall success of the company.

Protect a billion users without losing (much) sleep.

This means shielding their developers from targeted malicious attacks while they’re accessing Facebook’s internal networks and databases during development in order to avoid security risks to their source code and user data.

Facebook’s internal security culture is focused on reducing friction and making security easy for their fast-paced developers. This required their security solution to be versatile, efficient and streamlined with their workflow process, which involved logging into a development server to write code.

With tens of thousands of SSH sessions a day, more than 60 individual interactive sessions and over 3,000 non-interactive authentications, they needed security that would support their needs without adding more friction.

Strong security required, without any hassle.

And, while they already used passwords, public and private key pairs, etc., they were looking for a stronger form of authentication that they could easily extend to their other Facebook employees. That’s when they turned to two-factor authentication as a solution; combining something they knew (a password) with something they had (authentication via a device, like a phone).

Facebook’s security team put extensive research into choosing the perfect two-factor authentication solution — but ran into several downsides of each option. With time-based tokens (i.e., RSA-provided) and Facebook’s code generator, developers typically had only 30 seconds to authenticate. These options were also not ideal for SSH use if two terminals needed to be open at the same time. Plus, the authentication method was annoying, as you could only authenticate via passcode.

With OTP (one-time passwords), they ended up with sync errors. If you hit your token several times on accident, you may end up out of sync, which is a huge usability fail. Tokens are also designed for infrequent use, which is good for VPNs for one session, but not good when opening multiple SSH sessions.

Biometrics provided extremely limited support for most devices, and had their own set of security problems, like false acceptance rates and replay problems. There was also the practical issue of how to use a biometric factor on a remote server when the user was local to their laptop.

PKI (Public Key Infrastructure) provided poor device support and used smart cards as the form of authentication, which were susceptible to smartcard proxy attacks. A hacker could intercept a smart card’s pin number and use a smartcard without the user’s knowledge. Plus, smart card management is a pain to integrate across multiple platforms and requires a lot of overhead.

Facebook’s security team ultimately needed a two-factor solution that was built better than these other methods — they needed usability, flexible options, fast deployment and strong security with minimal support overhead.
The Solution

Facebook’s Information Security Manager, John “Four” Flynn said that Duo was pushing usability, as well as pushing the usability envelope for authentication.

Duo’s two-factor authentication solution can be installed on phones as an app with Duo Mobile, and also supports a multitude of authentication methods for landlines and offline devices, including push, SMS, mobile and voice.

Duo’s two-factor is also cloud-based, eliminating the need for hardware and software install, making it both fast and easy to deploy, cutting down on support overhead for administrators.

Versatile two-factor authentication for custom security solutions.

The long list of integrations that Duo’s two-factor supports includes some of the most widely used platforms, applications and devices. The flexibility and versatility of Duo’s authentication service offers a great platform on which various other technology can be used to create a custom security solution. This prompted Facebook to enlist a third-party hardware token to support the most aggressive of their users that required very fast authentication.

In addition, Facebook needed to support the way engineers chose to login -- they found that they were running third-party software as their SSH clients, requiring a lot of custom scripts to login, and using SFTP often. They needed to support scripts that were run non-interactively without having someone authenticate.

Passwords created friction for their users, as most users wanted to use Kerberos, SSH certificates or keys to login. With the help of Duo Security, Facebook wrote separate keyboard interactive drivers and custom modules to direct authentication input.

Ultimately, Facebook needed a solution that provided the ultimate ease of usability and flexibility for their engineers with fast deployment with minimal support overhead. Strong security was a given. Duo Security and Yubico combined forces to provide a powerful two-factor solution that custom-fit Facebook’s security needs.

Duo grew organically at Facebook – from protecting 300 users to 10,000+ users.

Initially deployed on Linux servers, Duo’s two-factor spread organically within the organization to VPN, Windows servers, Splunk, OWA and others. Duo’s lightweight, cloud-based integration model has allowed Facebook to experiment with deployments efficiently for their production, financial and remote corporate VPN access systems.

So where is Facebook today with Duo? Facebook moving away from using time-based tokens provided by RSA SecurID completely in order to expand Duo to their entire organization with a full enterprise site license agreement, supporting more than 10,000 employees.
Protect all users, all devices and any application with Duo’s Unified Access Security (UAS).

**Trusted Users**
Verify users with advanced two-factor authentication and enforce user access policies to limit access to applications.

**Trusted Devices**
At login, Duo checks the security health of every device – including employee-owned devices. Customize access policies based on device risk.

**Every Application**
Protect cloud and on-premises applications, and simplify access with Duo's secure single sign-on (SSO) for both users and admins.

The Most Loved Company in Security

North America
866.760.4247

Europe, Middle East & Africa
+44 8003 585 309

Contact Us
duo.sc/contactduo