Data Equipment

Data Equipment secures sensitive data by leveraging strong access control with Duo

“We wanted to make access to our sensitive data more secure, with a centralized and user-friendly solution.”

Goran Tømte
CISO, Data Equipment

Project goals

- Secure sensitive data by implementing strong access control
- Achieve security while continuing to support a remote workforce
- Provide clients with a secure access solution that is easy to deploy, use and maintain

Why Duo?

- Data Equipment needed a better 2FA experience than what their existing solution provided
- Easy to deploy, manage and use
- Minimizes user friction without compromising security
- Can offer to customers as a managed service
- Works with all applications and secures SSO

Results

- Speed to security: It took only two hours to add Duo two-factor authentication (2FA / MFA) to existing solutions
- Enhanced security by providing visibility into security status of all devices accessing Data Equipment’s environment
THE CHALLENGE

Data Equipment had a secure access solution in place, but it wasn’t optimal for their needs. “We were looking for a solution that was easy to use — both from an IT administrator and an end user perspective — and that would also satisfy the needs of our diverse customer base,” says Goran Tømte, CISO at Data Equipment.

The IT security team agreed that a new solution must provide stronger authentication methods than their existing one.

CHOOSING A SOLUTION

Traditional two-factor methods like time-based tokens, code generators and SMS-based OTP (one-time passwords) were error-prone, had limited device support, and generally required a lot of overhead.

**Push authentication**, which allows users to authenticate using their mobile devices, was a much better fit for Data Equipment. It was not only cost-effective to implement and maintain, but also far more secure than other authentication methods.

“Simple yet airtight logins that will help our customers improve security without affecting user productivity were critical,” adds Tømte.

Another important requirement was the ability to authenticate offline. Data Equipment has a number of public sector customers whose workforce may occasionally be offline due to the nature of their job responsibilities. These users still need to run 2FA to securely log in to Windows computers. As such, offline MFA for laptops, desktops and servers was a must-have feature.

“Successful attacks take place in permitted traffic. To reduce the attack surface, we knew we had to establish trust at the application level. This meant strong access controls for applications, so that only authorized persons and devices have access to sensitive information,” adds Tømte.

Because Data Equipment employees use both personal and corporate-owned devices, it was especially important to conduct user verification. Whether bringing their own device or using one managed by their employer, both groups needed access to business applications including email, calendar, contacts, and other sensitive data.

“We wanted a solution that could provide insight into all devices that gain access to our environment, and that helps our teams assess potential risks associated with these devices,” says Tømte.

The solution was to also enable IT administrators to identify device vulnerabilities and enforce policies to reduce risks, such as preventing an outdated or jailbroken device from accessing applications. The company was committed to ensuring that sensitive applications were protected from risky devices.
We found Duo’s Device Health Application very efficient. In a matter of minutes, we were able to detect devices that needed updating.”

Petter Tidemand-Fossum  
Technical Manager, Data Equipment

Deploying Duo

Data Equipment thought that Duo Beyond was a natural choice, thanks to its ability to define access policies by user group and per application and identify company-owned versus personal devices.

One of the most important aspects among Data Equipment’s clients with a large remote workforce is securing access to the Windows environment. The process involves end users connecting remotely or virtually to a computer on the network to verify their identity via multi-factor authentication.

“We soon found out that Duo was the simplest solution we have ever implemented,” says Tidemand-Fossum. “Adding Duo’s two-factor authentication to remote desktop sign-in took just two hours. Some of our customers who chose other solutions for a 2FA configuration for RDP logins took between one and two weeks to complete the same task.”

“Many SaaS vendors require a license upgrade to get access to the single sign-on (SSO) feature. Duo SSO is included in every Duo edition,” says Tømte. This is also beneficial for users, as Duo’s SSO and MFA can easily be configured for each application to allow a seamless authentication experience.

Data Equipment’s clients also use Duo’s policy features, especially those that make it possible to step security up or down based on user type. Granular policies help ensure that users can access some resources with a single set of credentials but are prompted for more credentials when requesting access to sensitive resources.

“One of the key benefits for us as well as our customers is visibility,” says Tidemand-Fossum. “When administrators log into the admin portal, they can see where users are logging in from, what devices they are using and can easily identify when something goes wrong. Getting the same level of intelligence without Duo would require visibility through a number of logs,” says Tidemand-Fossum.

“This project showed us that zero trust is not about technology. It’s about mindset. And with technology that is intuitive and easy to maintain, it is much easier to change the security mindset,” concludes Tømte.