Inductive Automation

DUO CUSTOMER SUCCESS STORY: **TECHNOLOGY**

Inductive Automation streamlines application access as part of an effective, scalable, zero trust strategy.

“

Duo is one of the most powerful tools in my arsenal, empowering my team to solve many problems at once with minimal administrative overhead. This allows us to enhance security without losing productivity. Duo has been instrumental in laying the foundations for a zero trust architecture that virtually any company could benefit from.”

Jason Waits
Director of Cybersecurity

The Organization

Founded in 2003 and headquartered in Folsom, California, Inductive Automation creates supervisory control and data acquisition (SCADA) software designed to remove all technological and economical obstacles, so that organizations can quickly and confidently turn great ideas into reality.

The Challenge

The threat landscape is constantly changing as cybercriminals increasingly launch new, innovative attacks. Credential theft, phishing emails, ransomware, and other threats have become much more pervasive and far more sophisticated. But it's not just on the surface where things are changing. Below that layer, an ever-expanding attack surface has become a cause for concern.

For Jason Waits, Director of Cybersecurity at Inductive Automation, the overwhelming growth in the number of assets was equally important. "While some people are focused on the threats out there, the landscape underneath is shifting so fast that our attack surface is rapidly expanding. Whether it's new servers, SaaS services or Chrome extensions, there's been an explosion in potential attack surfaces that needs to be managed."

Inductive Automation was experiencing its own growth surge which created some challenges for the software vendor. Initially, there were a lot of homegrown applications run on-premises in a controlled environment. However as the company started to expand, employees began to use virtual private networking (VPN) which led Waits to consider implementing multi-factor authentication (MFA) for secure remote access. "That's where I first got the idea to look at the market and figure out how I could do it in a way that was fairly seamless and would afford us that security without getting in the way. That's why I found Duo," said Waits.

Securing remote access to the company's VPN with MFA was the first use case. Next, Waits wanted to streamline employees' work lives so he made the decision to implement single sign-on (SSO). "People were coming in every day and signing into five, six, seven apps and I felt I could make that easier while bundling in security. Whenever I can help solve business problems and layer some security in, that's a pretty big win."

To access applications in the company's SSO portal, employees were using passwords to authenticate. Passwords still come with extensive risk, however, as attackers continually try to steal, guess, and even bypass the passwords. There was also the worry of "Push fatigue," and the risk of users accepting a fraudulent push when persistent attackers spam users until they tire of the requests to authenticate and simply accept. This led Waits to look into the passwordless market. "I wanted to get away from passwords and shift more emphasis to a strong factor that requires a physical presence in front of the device such as FIDO security keys, Windows Hello or Apple Touch ID."

Like many organizations, Inductive Automation is embracing the zero trust tenet of strong access requirements through identity and device verification. Moving away from simply using an IP address or password to control access to resources and including a second factor that shows a physical presence at the device in use appeals to Waits. So does checking device health. "We want to ensure that when computers connect, they are running endpoint protection, firewall and disk encryption are enabled, the OS is up to date, and they have a password set."

The Solution

Securing application access for remote workers

To solve the company's challenges around enabling secure remote access, streamlining permissions to multiple applications, and reducing user reliance on passwords, Waits selected Duo Beyond. With Beyond, he can achieve his security goals and further extend the organization's zero trust framework. He began by implementing Duo MFA to provide the growing number of remote users with secure VPN access to the corporate network. Waits selected Duo Push as the preferred authentication method and rolled Duo out to employees. "Kicking off Duo was one of my very first initiatives and largely it went extremely well. We were able to send out the enrollment emails and get people to set up their Duo app. It was pretty much seamless for us."

Streamlining the user experience

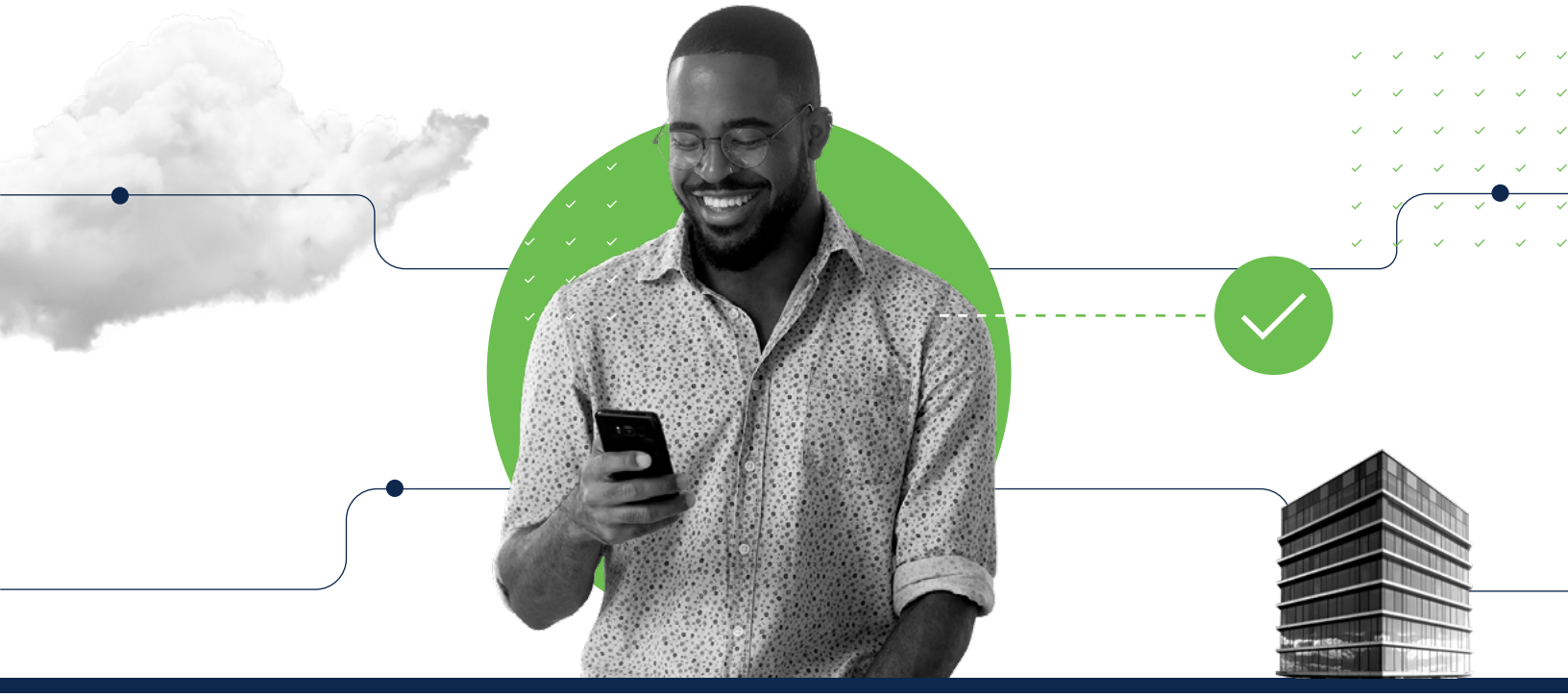
With single sign-on already included in Inductive's Duo license, Waits built an on-premises SSO portal and began adding core applications such as Gmail, Confluence, Slack, Office 365, and others. Eventually he migrated the portal to Duo Cloud SSO which enabled the company to reduce not only its data center footprint, but also the number of servers to patch. "We had a trio of load balanced servers we no longer have to maintain, so it allows us to do more aggressive data center maintenance without taking down our SSO portal." In addition, moving to the cloud helped with disaster recovery. Waits' goal was to simplify the data center and have robust business continuity and disaster recovery planning without rebuilding all the different services.

Reducing Risk

To address security concerns around passwords, Waits looked at different passwordless solutions but found that while vendors "talked the talk" about the benefits they provided, none offered a concrete solution that delivered on the promises. Disappointed, he turned to Duo after hearing about the company's solution for passwordless at a user conference. "It was exactly what I was looking for, which was a simple and elegant way to use YubiKeys or Windows Hello or Touch ID to replace the password. It simultaneously simplifies a user's life and takes the risky password off the table."

Embracing Zero Trust

Duo sits at the center of Inductive's zero trust strategy. Waits likes having strong user and device trust and health, and then wrapping that into Duo's access control engine. He's taken a very identity-centric approach to security and wants to avoid a reliance on perimeter security in favor of identity-based and app-based controls. "I wanted to collapse the controls as close as I could to those sources, so identity has been one of the key areas I've focused on. That's why we've embraced Duo and every single Duo feature that's come out since then."



“I wanted to collapse the controls as close as I could to those sources, so identity has been one of the key areas I’ve focused on. That’s why we’ve embraced Duo and every single Duo feature that’s come out since then.”

Jason Waits
Director of Cybersecurity
Inductive Automation

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

cisco The bridge to possible

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.