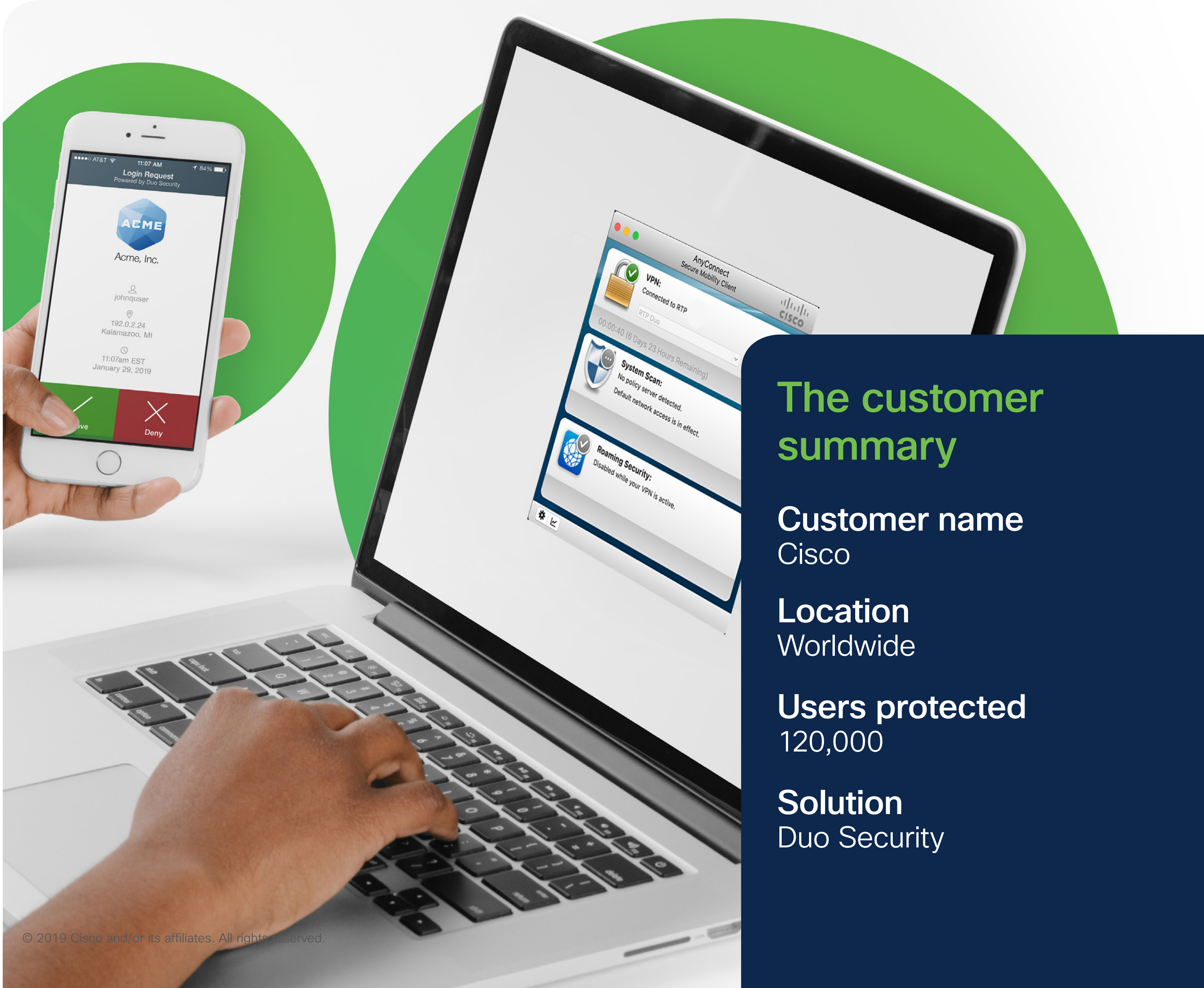
Case study
Public

Duo + Cisco: Workforce Zero Trust

With zero-trust security from Duo, Cisco protects access to 3,000 applications for 120,000 users and 400,000 devices worldwide



The customer summary

Customer name
Cisco

Location
Worldwide

Users protected
120,000

Solution
Duo Security

Security

- Secure access attempts by employees, contractors and vendors located all over the world

Zero trust

- Implement zero-trust approach to protect all applications by validating users and devices

Tools

- Use security tools that foster productivity while protecting critical data and resources

Data protection is Cisco's No. 1 priority

Almost every business on the planet is a Cisco customer. Customers entrust a lot of information on and about their networks to Cisco, and protecting that data is priority No. 1 for Steve Martino, Cisco's Chief Information Security Officer. With customers, employees, and contractors all over the world, the organization wanted to put security tools in place that give employees the flexibility they need while ensuring they can trust they're secure. According to Martino, "One of the most important aspects of the way we try to deliver security is to make it not a hindrance, but an enabler of the business; an easy experience for our users and an almost invisible experience for our customers." For Cisco, a zero-trust framework is a necessity to provide the security and flexibility needed to serve its customers.

Like most large, international enterprises, Cisco's 120,000 employees and contractors use different types of devices – laptops, personal phones, tablets, etc. – and access applications from locations around the world. Meanwhile, more applications are moving to the cloud. This creates unique challenges for modern IT organizations: keeping an 'always on' environment while also securing new types of applications and devices. Cisco wanted a way to gain insight into the users and devices accessing its applications and put access-based controls in place to reduce the risk of breaches while also increasing productivity.

Finally, as the largest single security company on the planet, customers look to Cisco for guidance on how to use security tools and implementation best practices. Cisco wanted to lead the way on designing and implementing a robust zero-trust approach for the workforce so customers would have a model to emulate. This meant continuously validating every user and device for every access attempt in a frictionless way that would not hamper productivity or upset users.

Implementation approach

- Prioritized change management and communication strategy
- Enabled flexible self-service to make it easy for users to enroll
- Integrated into O365 rollout for a secure, borderless experience and to encourage enrollment

Business results

- Protecting over 120,000 employees, contractors and vendors – only 1% needed support
- Continuously validate health and trust of over 400,000 access devices
- Visibility into who and what is on the network for faster responses to risks

Implementation Approach

According to Shane Harms, IT manager, “MFA is important and drives your trust in the user, but zero trust is about enabling a borderless experience for our users.” To truly ensure that users can have the same experience accessing applications regardless of location or device, and to enable a zero trust for the workforce environment, the team deployed Duo.

Rolling out a new technology to 120,000 users globally can often take organizations multiple years. The Cisco IT team was determined to complete its Duo rollout in a much shorter period of time. The small project team consisted of two people, and they knew they had to be efficient and strategic in their approach.

The team took key steps to implement a robust program with Duo:

- To not pull attention too far to one area, the team had two active workstreams: technical implementation and change management for users
- They focused on communicating the importance of MFA and why they were rolling out Duo. Cisco also used it as an opportunity to reinforce the importance of security in people’s personal lives and integrating MFA where possible into banking and other online accounts.
- Duo replaced an existing MFA solution and the team was concerned users might get frustrated with the change and be slow to enroll. The team integrated it into the company’s Office 365 rollout to present a compelling user experience.
- Pairing Duo with an easier way to access key work resources from any location positioned security as a user experience improvement and not a barrier.
- The team enabled robust self-service resources for enrollment and support - making the process painless for users.
- Evaluating device health to ensure every device attempting to access an application is secure and up-to-date. Attributes can include screenlocks, operating system version, encryption status, whether it is corporate-owned or not, and more.
- Fully enabling secure BYOD by putting application-specific access controls and policies in place to grant access based on device health, type of device, location and sensitivity of the application.

> “People thought Duo was easy to install, deploy, adapt to and use and I think that is a testament to the great design focused on usability and deployability that Duo has put in place.”
>
> **Steve Martino**
> Chief Information Security Officer

Business results

With Duo's help, the Cisco team implemented a rather large change in a short period of time. And because Duo was easy for end users to adopt, it created minimal burden on IT staff. Cisco achieved its goal of securing a diverse workforce and environment in a way that improved employee flexibility and productivity.

Enabled zero trust for the international workforce:

- Every user, device and access attempt is continuously validated
- Employees and contractors worldwide have secure access to applications
- Employees have the flexibility to securely work from anywhere at any time to meet customer needs

Implemented a security solution that was easy to administer and use:

- An implementation team of two rolled out Duo to 120,000 users in less than six months
- 70% of users enrolled with Duo within 48 hours of receiving an invitation
- Only 1% of users opened helpdesk tickets and needed support
- The implementation team received positive user feedback – users embrace Duo and appreciate the ease of use and security it provides

As the largest security vendor on the planet, Cisco became a proving ground for their products:

- Demonstrated how Duo can be rolled out at enterprise scale easily and quickly
- Ensure that the over 400,000 access devices being used are healthy and up to date
- Duo policies secure 5 million access attempts each month

Create a zero-trust framework that goes beyond MFA:

- Cisco protects 3,000 applications with Duo – ensuring the right users and devices can securely access the right applications
- Duo notifies users if a device is at-risk and allows self-remediation
- Visibility into who and what is on the network gives the security team the speed and agility to respond quickly to threats
- Duo's forward-looking features enable cutting-edge approaches to ever-evolving security challenges

Going forward

Cisco will continue to be a proving ground for the tools and capabilities that Duo builds to help customers securely embrace new ways of working and overcome new challenges as they arise. Deploying Duo is part of Cisco's zero-trust security strategy, and ensures the company has an optimal framework in place that will continue to evolve its security strategy and how it detects and responds to threats. "We have internally been talking about how do we do zero trust for four or five years right now. I think for the first time we feel like we have all the technology pieces to actually make this a reality. So I think we're sitting here saying, we have a really exciting opportunity going forward," states Harms.

Learn more

To learn more about Duo Security, visit:
http://www.cisco.com/go/mfa

"Security isn't static–as we move forward, Duo is going to be a critical enabler in allowing us to have adaptive trust."

Steve Martino
Chief Information Security Officer

"Zero Trust is not just about the technology and security, it's about enabling our business and workforce to do what they need to do for our customers, wherever they need to do it."

Shane Harms
Cisco IT Manager