CISCO
SECURE

Case Study
Public

Zero Trust for Customer Zero

How Cisco uses Duo to secure its workforce

Like most modern organizations, Cisco has extended its network perimeter to include cloud applications and a mobile workforce.

To create a frictionless user experience that secures access to its applications and follows the principles of zero trust for the workforce, Cisco uses Duo Beyond. Cisco was able to deploy Duo to its entire user base in less than five months. With user and device trust established at every access attempt, application access was decoupled from the network, improving security and reducing reliance on the VPN.

According to Josephina Fernandez, Director of Security Architecture & Research at Cisco, "The world is continuing to evolve and we're seeing a need for companies to provide employees with a way to work securely from basically anywhere in the world."

Duo Beyond helps secure the three tenets of zero trust for the workforce – users, devices and applications. Cisco now has the ability to ensure users are who they say they are and their devices are healthy each time an access attempt is made – and this happens for every application. Establishing trust at the point of access every time doesn't have to be complex and burdensome; with zero trust security it's easy and consistent, improving security and boosting user productivity.

Customer Name
Cisco

Location
Global

Industry
Technology

Employees & Users
100,000+

© 2021 Cisco and/or its affiliates. All rights reserved.

Duo's zero trust for the workforce solution works like this:

First, the Cisco team uses Duo MFA to verify that the user is who they say they are. Self-enrollment and multiple authentication methods like mobile push and touch ID give users a lot of flexibility. This means that authentication can happen whether users are online or off and from any location. Additional user verification determines whether or not a user's behavior is normal. Duo's Trust Monitor feature takes into account each individual user's behavior and flags behavior determined to be unusual. For example, if two users log in at midnight, Trust Monitor can determine that it is normal behavior for the first user, but unusual for the second. In this case, the second user would be flagged and prompted for additional authentication or blocked.

"It's really important that you be able to establish user trust – but that's only half the equation. If their device isn't secure and you're allowing that device onto the network, you're allowing that device to access corporate resources," says Fernandez. To establish device trust – a crucial part of zero trust – Cisco uses the Duo Device Health app. It is a lightweight application that determines if a device is healthy and up to date. Every time a user tries to access an application, the Device Health app checks the device to make sure it meets hygiene standards like an up-to-date OS, screen lock and password protection and anti-virus is installed. If the device fails, the user is told why and how to self-remediate.

In one month, using Duo, Cisco performed 2.6 million health checks and users self-remediated 48,000 devices. **That's 48,000 times a potential vulnerability was patched without any effort from IT or impact on the help desk.**

"I haven't had to dedicate any additional resources from my team – that just speaks to not just the ease of implementation but also the low support costs of Duo," says Fernandez.

The second aspect of device trust is whether a specific device should have access to an application. Cisco uses Duo's Trusted Endpoints feature to designate devices that are managed by Cisco. Limiting sensitive application access to only corporate-managed devices adds another layer of defense in the event that credentials are compromised.

Finally, application access should be limited to only the users and devices who need them. This prevents the risk of lateral movement. The Duo Network Gateway solved a common challenge of on-premises and proprietary applications. Eliminating the need for a VPN, users can access applications directly and have the same checks in place.

According to Fernandez, "Before with VPN, we checked the user and device once coming in the door, and then that's it – especially if you're remote. You basically had free reign to move laterally across the network. The DNG instead makes sure that you and your device are secure on a per application basis. **I think that's a huge security win at no cost to the user – feedback has been great across the board."**

"It's not often that you can say you are improving security while also improving the user experience, but that's what we have achieved with this rollout"

Josephina Fernandez
Director, Security Architecture & Research, Cisco

© 2021 Cisco and/or its affiliates. All rights reserved.

True zero trust means access is continuously validated for every application.
"Since Duo is platform agnostic, we know that we can protect every application, regardless of where it lives. Duo's ability to easily protect any application reduces my team's effort, freeing them up to focus on other important work," says Fernandez.

Knowing that uniform policies run the risk of being too stringent for some scenarios and potentially too lax for others, Duo gives Cisco the flexibility to customize policies by application. This can include geographical location, device posture, approved networks and more. For example, a mobile phone may be able to check email while only corporate-owned devices on known networks can access sensitive R&D information.

Security is an ever-evolving challenge for organizations like Cisco. By having an easy to use solution in place that integrates with all types of applications and presents a simple user experience, the team is able to focus on more pressing matters.

For Fernandez, the agility of Duo means that her team is flexible enough to scale up quickly and respond to changes. "Our general workforce, our execs, and our help desk have all had really positive things to say. The best endorsement that we have gotten is the overwhelming number of emails from our users asking us to onboard even more applications to the zero trust architecture. It's clear that everyone just loves the Duo experience," she says.

As for the future, in addition to rolling out zero trust for all applications, Fernandez is looking forward to incorporating Duo's upcoming passwordless solution and further simplifying and securing the user experience. Her team is also focused on expanding the usage of zero trust beyond Cisco's immediate ecosystem to use cases such as the extranet partner landscape and onboarding acquisitions in a more seamless, less infrastructure intensive way.

Challenges

- Protect worldwide access
- Expand access to users securely
- Secure all users and devices
- Consistent experience for users

Solutions

- MFA prevents fraudulent login attempts
- Trusted Endpoints limits access to managed devices
- Trust Monitor detects abnormal login attempts
- Duo Device Health app ensures devices are safe
- Adaptive access policies block risky login attempts
- Duo SSO simplifies access with one username and password
- Duo Network Gateway provides access without a VPN

Results

- 100,000+ users and 120,000+ devices secured
- Deployed in 5 months
- <1% of users contacted help desk
- 2.6 million health checks a month
- 48,000 devices per month remediated
- 260,000 auths per month via DNG (VPN-less)

© 2021 Cisco and/or its affiliates. All rights reserved.