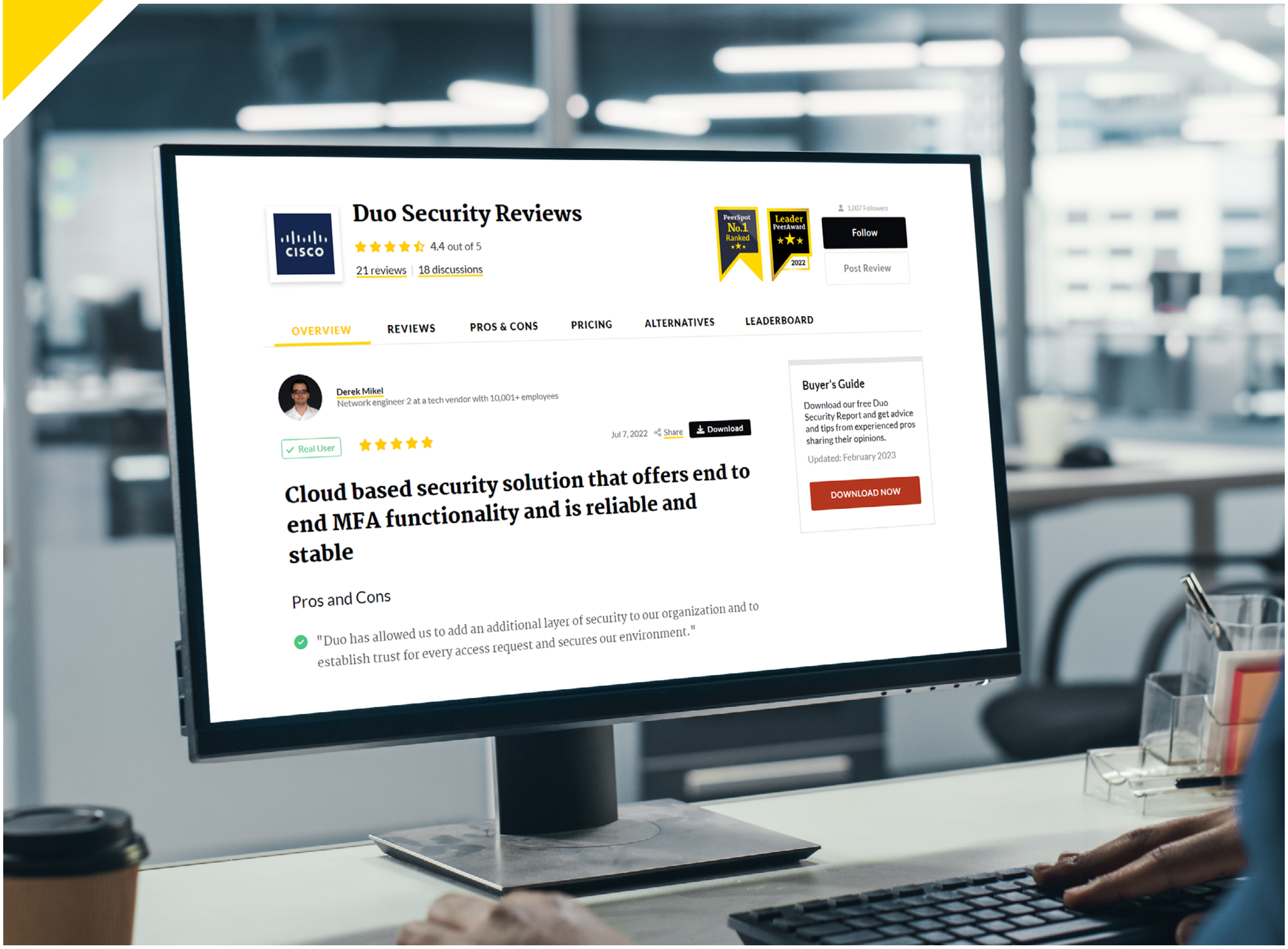
PeerPaper™ Report 2023

Based on Real User Experiences with Cisco

How Cisco Customers Are Getting Practical About Zero Trust



Duo Security Reviews

★★★★☆ 4.4 out of 5

21 reviews | 18 discussions

Derek Mikel
Network engineer 2 at a tech vendor with 10,001+ employees

✓ Real User ★★★★★ Jul 7, 2022

Cloud based security solution that offers end to end MFA functionality and is reliable and stable

Pros and Cons

✓ "Duo has allowed us to add an additional layer of security to our organization and to establish trust for every access request and secures our environment."

Buyer's Guide

Download our free Duo Security Report and get advice and tips from experienced pros sharing their opinions.

Updated: February 2023

PeerSpot

CSO

Contents

Introduction

The zero trust security model is gaining significant traction in the enterprise, though it is often described in vague terms like “Zero trust is a journey.” This perspective can be frustrating for IT professionals who face practical challenges such as making zero trust a core security element of digital transformation initiatives. However, as PeerSpot members are discovering when they work with Cisco on zero trust planning and deploy the Cisco Security solutions, they’re already on that journey. By utilizing Cisco products for multi-factor authentication (MFA), micro-segmentation, and network segmentation, which are three critical elements of a zero trust architecture, they are well on their way to realizing a zero trust approach in their organizations. This paper explores how PeerSpot members are adopting these components of zero trust, as well as their viewpoints on zero trust in general.

Zero Trust Overview

Zero trust is a security model that forms the basis for security controls and practices. It is an idea, not a product, with the foundational rule, “Never trust. Always verify, and enforce the principle of least privilege.” If a user or device requests access to a digital resource, like a database or a network segment, the standard zero trust policy is “deny by default.” This stands in contrast to many existing security policies that grant broad, general access to a wide range of digital assets once the user has passed a basic username/password authentication process. Instead, after the user has been verified, only then will a zero trust-architecture grant limited access privileges, often confined to a single network segment. Figure 1 shows a simple reference architecture for zero trust.

Zero trust adoption is growing, with digital transformation initiatives as one of its main drivers. Digital transformation is about using technology to reinvent the customer relationship for the purpose of gaining competitive advantage. Its success depends on strong security. Transformative initiatives may require, for example, that end users be able to access networks and data from anywhere at any time on any device. Without zero trust policies in place, the risk of unauthorized access increases. Additionally, without a cohesive approach to security, more administrative burden, including manual management of access privileges, is placed on overworked IT teams.

Zero Trust

Ronnie S.
CTO at Charter

"As far as remote access, simple access, and authentication to gateways, it [Cisco Duo] was perfect. It has very strong network connectivity, which works reliably and well. It was very easy for people to connect, and the app worked as it should."

Read review »

Zero trust adoption is also mandated in certain government IT projects. In May, 2021, US President Biden issued an Executive Order on Improving the Nation's Cybersecurity, which specifically stated, "The Federal Government must adopt security best practices; advance toward Zero Trust Architecture."

The order recommends that Federal agencies that are in scope (e.g., non-Department of Defense entities) follow the Cybersecurity & Infrastructure Security Agency (CISA) Zero Trust Maturity Model. According to the CISA, the model is "one of many roadmaps for agencies to reference as they transition towards a zero trust architecture." Additionally, government agencies can adopt zero trust based on the National Institute of Standards (NIST) Special Publication (SP) 800-207, which provides systematic guidelines for updating network security and developing a Zero Trust Architecture.

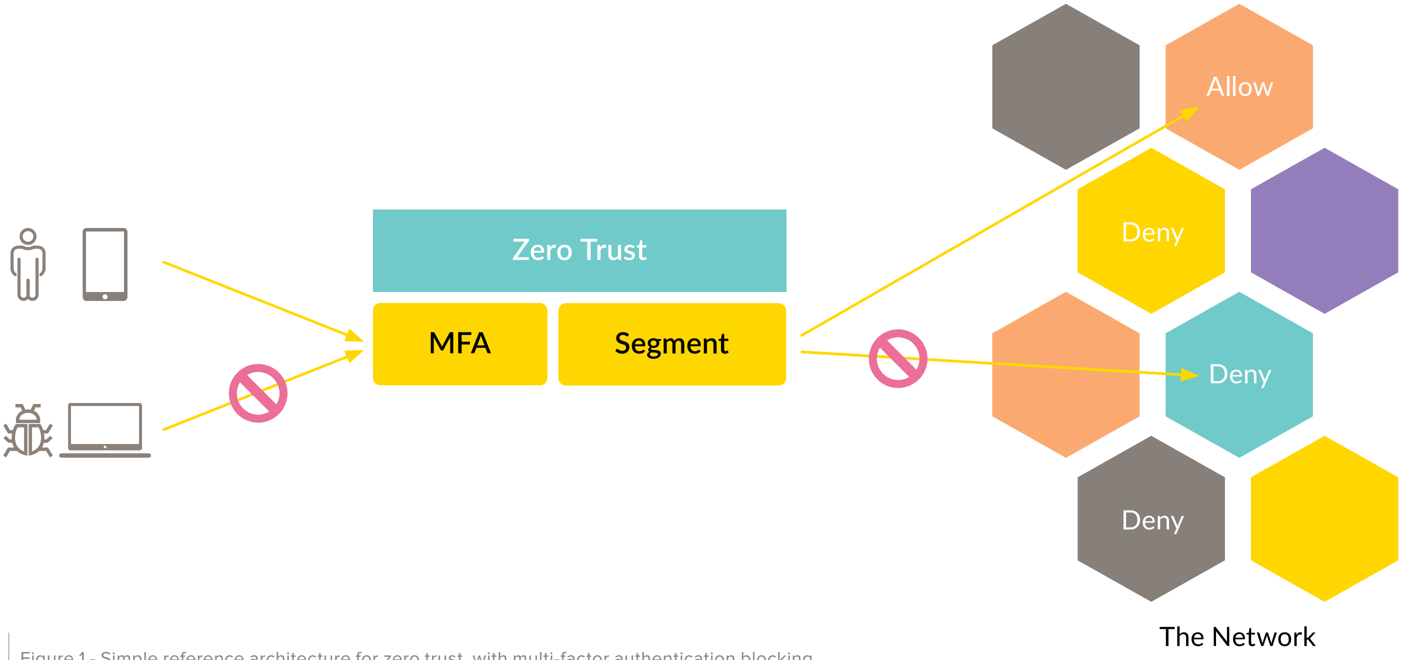


Figure 1 - Simple reference architecture for zero trust, with multi-factor authentication blocking non-verified users and network segmentation allowing minimum access privileges.

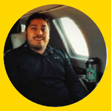
Cisco Customer Perspectives on Zero Trust

PeerSpot members are using Cisco technologies to implement zero trust security. For some, Cisco serves as a trusted advisor on zero trust security matters. A Network Infrastructure Specialist who uses Cisco Identity Services Engine (ISE) at a small tech services company, for Instance, relied on Cisco to detect the need for missing elements of their network security architecture that they had not noticed during a health check.

The Co-Founder & Director of VSAM Technologies, a small tech company, felt that Cisco ISE covers access to the network to create a zero trust environment through network access control, micro-segmentation, network segmentation, and policy control. He said, “Having secure network access control will always make it safer and help organizations in attaining a zero trust environment.”

According to a Sr. Wireless Network Engineer who uses Cisco ISE at a manufacturing company with over 10,000 employees, “We want our payment system to be secure. Zero trust is our whole thing. It’s great that everything is external to ISE and then everything has to go through the system.”

“By eliminating trust, it helps us with audits, including CJIS [Criminal Justice Information Services] because we have a law enforcement division, and [we are] trying to conform to the NIST standards,” said a Network Architect who uses Cisco ISE at Tarrant Regional Water District. He added, “A lot of government agencies are becoming more familiar with the Zero Trust model and ISE makes our audits go a lot faster and a lot smoother than they used to.”



Homer M.
Network Administrator at a retailer
with 1,001-5,000 employees

★★★★⯪

“Duo has helped us remediate threats more quickly by having one spot to look at.”

Read review »

Adam B.
Network Architect at Tarrant
Regional Water District

★★★★☆

“We consider everybody a foreign endpoint until they prove they belong on the network. ISE just seems to be built from the ground up to do that, whereas with other solutions, you have to ‘shoehorn’ that in.”

Read review »

This user went on to explain that Cisco ISE is built on a strong zero trust model. As he put it, “We consider everybody a foreign endpoint until they prove they belong on the network. ISE just seems to be built from the ground up to do that, whereas with other solutions, you have to ‘shoehorn’ that in.”

A Network Engineer at a manufacturing company with over 1,000 employees felt that Cisco Secure Access by Duo was “really great for remote workers and a hybrid workforce nowadays for people who are trying to access their VPN or any applications from outside of the company.” He then said, “It helps us make sure it’s someone who should be accessing those things. It does a good job. It’s definitely a factor in achieving that Zero Trust.”

Cisco Duo received several acknowledgements by PeerSpot members for multi-factor authentication, a key element of zero trust user verification. A Senior Aerospace Engineer who uses Duo Security at a manufacturing company with over 10,000 employees said, “We have a high level of confidence in the platform, especially for identifying potential logins from unexpected geolocations. The data associated with logs is very helpful to make that determination. It’s very important for us that Duo considers all resources to be external, especially as we lead up to zero trust. It needs to be like that.”

Securing Remote Access: A Top Use Case for Zero Trust

Recent trends in network access are putting pressure on security teams and their partners in network and IT operations to implement zero trust principles. The need for secure access and remote access, which are both on the rise, translate into the use of multi-factor authentication and other elements of zero trust. The CTO of Charter, a small software company, put it this way: “As far as remote access, simple access, and authentication to gateways, it [Cisco Duo] was perfect. It has very strong network connectivity, which works reliably and well. It was very easy for people to connect, and the app worked as it should.”

Furthermore, he commented that Duo applies and maintains network connectivity across campus and remote locations. He added, “It eliminated trust for remote access, but not from inside our organization. Remote access from people’s homes and branches is also strong. Network connectivity is its strength and it does that well.”

Securing Remote Access

Secure Access That’s Easy for Users

“It provides security for the remote workers and it helps to improve enterprise security in a very easy way,” said a security operations center (SOC) and Security Services Director who uses Cisco Umbrella at Bestel, a comms service provider with more than 500 employees.

Secure access that is reliable, simple to scale, and easy to install is what mattered to a Technical Solutions Architect who uses Cisco ISE at a wholesaler/distributor with more than 200 employees. The Vice President, Information Security & Compliance at a tech vendor with over 1,000 employees is using Cisco Umbrella to implement a SASE (Secure Access Service Edge) model. This started during COVID, when most users within client firms started working from outside their offices.

Integrated Technologies Increase Visibility

Cisco solutions help customers focus on implementing key aspects of zero trust for end users and their devices. For a Sr. Consultant who uses Cisco ISE at a tech services company with over 10,000 employees, this means being able to deploy worldwide and integrate with Microsoft 365. Global access control for such commonly used applications is essential for success with zero trust as part of digital transformation.

Increased Visibility

CTO
at a tech vendor with
11-50 employees

★★★★☆

> “The solution offers 100% telemetry coverage. The telemetry you collect is not sampled, it’s not intermittent. It’s complete. You see everything in it, including full visibility of all activities on your endpoints and in your network.”
>
> Read review »

Global access needs global awareness, which is what a CTO of a small tech vendor put into practice with Cisco Secure Workload. He said, “The solution offers 100% telemetry coverage. The telemetry you collect is not sampled, it’s not intermittent. It’s complete. You see everything in it, including full visibility of all activities on your endpoints and in your network.”

Device and User Support

Support for Diverse Types of Devices and Users

An Accounting Executive at a small tech services company uses Cisco ISE for the device authentication and application access controls that zero trust requires. In his case, he has groups of employees with separate application access needs, such as accounting people accessing accounting software and salespeople accessing sales management software, and so forth. Users are not entitled to access applications outside of their work area. This means device authentication against access control policies.

As he put it, “In my case, I’ve got a Windows laptop and I’ve got an Apple product and those have unique identifiers, unique back addresses. It would say that this is my profile so I could get to those apps with either device, 24/seven. That’s how granular the ISE or these NAC Solutions can get. That you have to have that same device.”

Verifying Users with Multi-Factor Authentication (MFA)

User verification is at the heart of zero trust. Companies that want a reliable verification method are turning to multi-factor authentication, as delivered by Cisco Secure Access by Duo. PeerSpot members put the use case in perspective, with a Networks and Infrastructure Manager at a financial services firm with more than 200 employees, for example, sharing, “Prior to implementing Duo Security, our users were not using multi-factor authentication. They were simply authenticating with a username and password. That was not secure enough, which is why we implemented the second level of authentication.”

The Networks and Infrastructure Manager added, “Having a single solution for multifactor authentication makes it comfortable for the users. They only need to train on one product.”

“Duo has helped us remediate threats more quickly by having one spot to look at,” said a Network Administrator who uses Duo Security at a retailer with over 1,000 employees. He went on to say, “We can see whether a user authenticated it from somewhere or if they were denied a two-factor request.” A Solution Engineer who uses Duo Security at FirstLight, a tech services company with more than 200 employees, likewise noted, “We get fewer threats to remediate due to the two-factor authentication, which does not allow as many threats through. It does a good job of establishing trust for every access request.”

Multi-Factor Authentication

Mark S.
Solution Engineer
at FirstLight

"We get fewer threats to remediate due to the two-factor authentication, which does not allow as many threats through. It does a good job of establishing trust for every access request."

Read review »

Multi-factor authentication is a "massive part of a proper defense strategy" for a hospitality company with over 10,000 employees. Their Dynatrace Architect explained, "Having Duo makes it easier to implement and manage that two-factor solution. For a CDC director at STC, a comms service provider with over 10,000 employees, the benefit from Cisco Duo came from its ability to deliver multi-factor authentication, "which gives another layer of protection."

In his case, his company has thousands of people who access the network from outside. He said, "It's hard for us to know which one is legitimate and which one is illegitimate. Having two-factor authentication with Duo helps us to implement a second layer of authentication so that we know for certain that the people who are accessing accounts are legitimate."

The CDC director at STC put this issue into further context when he said, "People use very weak passwords, so it's very easy for attackers to get in and compromise accounts. This is why we need two-factor authentication and why we are with Duo Security. It helps us to not only rely on the username and password but also implement another layer of protection. Attackers are not going to be able to compromise accounts because of the two-factor authentication."

Other notable comments about multi-factor authentication included:

- "It [Duo] authenticates users so that you can know they're legitimate in the network. It can be used for mobile banking. For example, when you're doing mobile or internet banking with your phone, when it uses OTP [one-time password], it is using Duo Security." - Vendor Business Manager EMEA who uses Duo Security at Westcon-Comstor, a tech services company with over 10,000 employees

- "We can ensure whomever is logging in isn't someone else who might be sharing a username or password. Duo has enabled us to mitigate rogue access requests to our network." Network Engineer who uses Duo Security at an aerospace/defense firm with more than 200 employees

- "Duo allowed us to greatly enhance our security. Now, not only do users have to know their username and password, but they also have to be able to receive the second-factor authentication in order to get in. The same goes for anyone trying to break in." - IT Security manager who uses Duo Security at an energy/utilities company with more than 200 employees

Anderson R.
Network Engineer at a aerospace/
defense firm with 201-500 employees

★★★★½

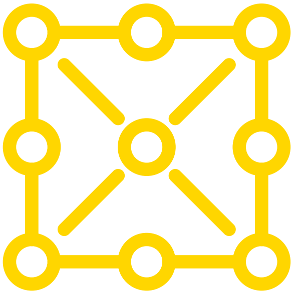
"We can ensure whomever is logging in isn't someone else who might be sharing a username or password. Duo has enabled us to mitigate rogue access requests to our network."

Read review »

Network Segmentation and Micro-Segmentation

Network segmentation is a significant operational factor in zero trust success. Security managers can reduce the attack surface area by limiting verified users access only to the network segment they need. Segmentation restricts an attacker’s ability to move laterally across networks and compromise digital assets as he or she moves along.

PeerSpot members are employing Cisco security products for this purpose. A Regional Presales Consultant (INS Division) at GBM, a computer software company with more than 500 employees, uses Cisco Secure Workload for micro-segmentation, for instance. A hospitality company with over 10,000 employees uses Cisco ISE for access control for a distributed network. Their Network Engineer explained, “It allows you to segment things and allows only certain devices to access the network.”



Network Segmentation

This user also shared, “[It’s about] protecting the network infrastructure from exploits and really allowing us to segment IoT [Internet of Things] devices and the corporate network. And because [on] the corporate network, once you get into it, there really isn’t anything protecting against accessing critical storage systems, accessing mission-critical servers, [or] our sales numbers, it’s super important that we have the ISE so that we’re only allowing the things that we want into the network that we trust.”

Ed M.
Network Engineer at a hospitality company with 10,001+ employees

★★★★½

> **“It allows you to segment things and allows only certain devices to access the network.”**
>
> **Read review »**

A Sr. Architect who uses Cisco ISE at a pharma/biotech company with over 10,000 employees similarly noted that zero trust “ensures that if the device is not allowed to access something then ISE won’t let that device access that resource. This is mostly for segmentation security.”

The Tarrant Regional Water District, which is considered critical infrastructure by the federal government, uses Cisco ISE to protect supervisory control and data acquisition industrial control systems. Their Network Architect who remarked, “ISE helps us do that by segmenting them off from the rest of the network.”

Wireless segmentation of users for Remote Authentication Dial-In User Service (RADIUS) with Cisco ISE is the use case for a Solution Architect Telecom at a manufacturing company with over 10,000 employees. Likewise, a Sr. Wireless Network Engineer at the same company uses Cisco ISE primarily for virtual local area network (VLAN) segmentation for RADIUS users on their wireless networks.

“We use ISE for security group tagging in terms of guests and visitors who access the network to make sure that they actually go through this to control their privilege access to ensure they don’t actually access the internal network, etc.,” said a Senior Software Engineer who uses Cisco ISE. He elaborated, commenting, “Our clients use ISE as a form of security policy management so that users and devices between the wired, wireless, and VPN connections to the corporate network can be managed accordingly.”

Conclusion

Zero trust is being broadly adopted, driven by increasing needs for secure and remote access as well as an evolving threat environment. PeerSpot members are able to execute the core zero trust principles through their use of the Cisco Security solutions. They are deploying multi-factor authentication, which enables the critical verification step of the zero trust principles of “never trust/always verify.” The ability to segment networks with Cisco products is another vital factor in making zero trust a reality. With segmentation and micro-segmentation, organizations can enforce the zero trust principle of limiting access based on least privilege. As the comments in this paper show, Cisco Security customers are making sizable progress toward zero trust implementations.

About PeerSpot

PeerSpot is the authority on enterprise technology. As the world's fastest growing review platform designed exclusively for enterprise technology, with over 3.5 million enterprise technology visitors, PeerSpot enables 97 of the Fortune 100 companies in making technology buying decisions. Technology vendors understand the importance of peer reviews and encourage their customers to be part of our community. PeerSpot helps vendors capture and leverage the authentic product feedback in the most comprehensive way, to help buyers when conducting research or making purchase decisions, as well as helping vendors use their voice of customer insights in other educational ways throughout their business.

www.peerspot.com

PeerSpot does not endorse or recommend any products or services. The views and opinions of reviewers quoted in this document, PeerSpot websites, and PeerSpot materials do not reflect the opinions of PeerSpot.

About Cisco Secure

Cisco Secure is built on the principle of better security, not more. It delivers a streamlined, customer-centric approach to security that ensures it's easy to deploy, manage, and use — and that it all works together. We help 100 percent of the Fortune 100 companies secure work — wherever it happens — with the broadest, most integrated platform. Learn more about how we frustrate attackers and not users... to simplify experiences, accelerate success, and protect futures at cisco.com/go/zero-trust.