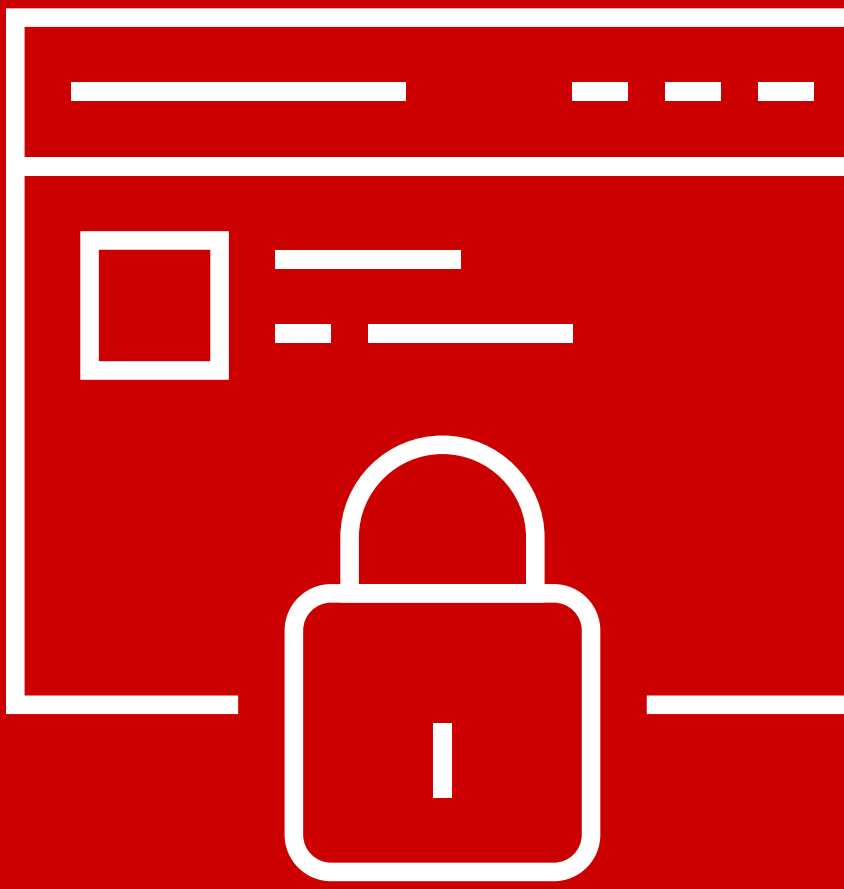
PeerPaper™ Report 2023

7 Ways CDW & Cisco Security Can Protect Businesses

Based on Real User Experiences with CDW & Cisco Security



PeerSpot

Contents

Introduction

Success in cybersecurity is only partly about establishing savvy and smart policies. Effective cyber defense comes from working with the right partners and selecting the best technology solutions. This is what CDW brings to the table as one of the world's leading Cisco Gold Partners. No other Cisco partner offers CDW's combination of expertise and experience. This paper explores these extraordinary capabilities, reviewing seven ways that CDW & Cisco Security can help protect businesses. Based on real user reviews from PeerSpot, it examines how Cisco fortifies organizations by boosting security resilience, establishing trust, providing deeper visibility, and more.

CDW & Cisco Security: Partnership Overview

As Cisco's largest U.S. National Direct Integrator Partner and the first worldwide partner to achieve Cisco Security Master status, CDW offers the broadest range of Cisco security expertise across multiple technologies. CDW develops innovative, industry-leading technologies while also providing a full lifecycle of solutions and services that help organizations manage, optimize, secure, and transform their businesses.

CDW supports the four core "pillars" of Cisco Security:

- Firewall, featuring the Cisco Firewall product portfolio
- Breach protection and extended detection and response (XDR)
- User protection, using Cisco Duo, Cisco Umbrella and Cisco Identity Services Engine (ISE)
- Cloud protection

For details about the Cisco products referenced in this paper, see the Appendix.

Cybersecurity Architect
at a financial services firm with
5,001-10,000 employees

"Cybersecurity resilience has helped us be able to react and respond in a quick fashion to anything that may be happening or any anomalies within the environment."

Read review »

7 Ways CDW & Cisco Security Can Help Safeguard Businesses

CDW & Cisco Security brings harmony to networks, workloads, and application security while providing comprehensive threat visibility and end-to-end security across the entire network. CDW's expertise extends to improving data protection and identifying, categorizing, and managing IT security vulnerabilities to minimize their attack surfaces. Working this way, CDW leverages high impact solutions in seven ways that help customers safeguard their digital assets in hybrid cloud or multicloud environments:

#1 – Building Security Resilience

Resilience, the ability to bounce back quickly and fully from a cybersecurity incident, is a critical goal of most cybersecurity programs. Cisco users on PeerSpot spoke to this need in their reviews, with a Cybersecurity Architect who uses Cisco Security Firewall at a financial services firm, for example, remarking, "Cybersecurity resilience has helped us be able to react and respond in a quick fashion to anything that may be happening or any anomalies within the environment."

Cybersecurity Resilience

This user further reflected that Cisco Security Firewall's IP blocking was the product's most valuable feature for resiliency. He said, "It gets rid of things that you don't need in your environment. Its resilience helps with being able to react and self-heal."

A Network Systems Manager who uses Cisco Security Firewall at a large software company shared, "Cyber security resilience has been extremely important for our organization because of our customers' demands for security." In his case, the Cisco Adaptive Security Appliance (ASA) has helped accomplish resiliency for their virtual private network (VPN). He offered a further comment on this, though, which was, "My advice to leaders who are looking to build resilience is don't go cheap, and make sure you have backup solutions and high availability."

Augustus H.
Senior Infrastructure Engineer
at a insurance company with
10,001+ employees

"Making sure that data is secure is good for the company and beneficial to the customer."

Read review »

"Cybersecurity resilience is very important for our organization," said a Senior Infrastructure Engineer who uses Cisco Security Firewall at a large insurance company. Being in the healthcare insurance industry, they have a lot of customer data going through their data center under multiple government contracts. He added, "Making sure that data is secure is good for the company and beneficial to the customer."

#2 – Establishing Trust

Trust is foundational to effective cybersecurity. Cisco products, as implemented by CDW, enable organizations to establish trust with users and devices. As a Dynatrace Architect who uses Cisco Duo Security at a large hospitality company put it, "The solution improved trust models within our organization, significantly changing how people view connecting to the network." At the same time, he did not think the technology had an impact on employee morale, which can be an issue when a trust solution disrupts the user experience.

A Network Engineer 2 who uses Cisco Duo Security at a large tech vendor explained, "Duo has allowed us to add an additional layer of security to our organization. It prevents people from gaining access unless they have their credentials as well as a device. It has allowed us to establish trust for every access request and secures our environment. We are confident and comfortable with the way the solution handles this. We have tried other solutions, but they've not met our expectations."

How does Cisco Duo establish trust? According to a Systems Engineer Virtualization at a large engineering company, "Duo Security seems to work for establishing trust for every access request, no matter where it comes from." A Network Technician who uses Cisco Duo Security at a comms service provider likewise noted, "Duo Security establishes trust for every access request, no matter where it comes from." In their case, they limit where users can access their networks. He added, "It helps to make sure whoever we're letting in is who they're supposed to be."

"Duo Security considers all resources to be external," said a Network Engineer at a large recreational facilities/services company. This is a "good idea" in his eyes, "because everything is done in a completely untrusted model." Figure 1 depicts this approach to establishing trust.

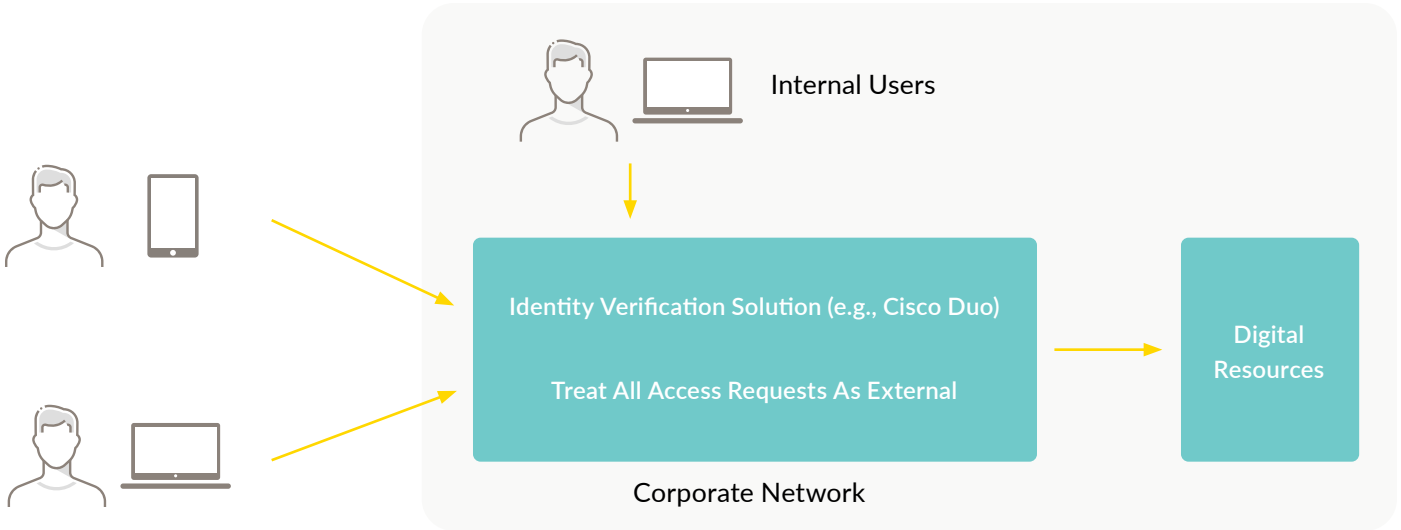


Figure 1 - Establishing trust works well when every access request is treated as if it were external.

Patryk R.
Dynatrace Architect at a hospitality company with 10,001+ employees

"The solution improved trust models within our organization, significantly changing how people view connecting to the network."

Read review »

The “everything is external” approach is a step toward establishing a zero-trust network architecture (ZTNA), which is a common goal for network security at this time. A VP Enterprise Architect who uses Cisco Duo Security at a large financial services firm explained, “Duo Security does a great job of establishing trust for every access request, no matter where it comes from. It is very important for our organization that the solution considers all resources to be external because it frames the activity as zero trust, and that’s how we run our network to zero trust across the board.”

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

“[Duo Security] does a fantastic job at securing access to applications and networks. It is streamlined and straightforward.”

Read review »

#3 – Securing Access

Cisco users on PeerSpot place importance on securing access to networks and applications. The tech vendor’s Network Engineer 2 framed the issue like this: “Duo Security does a good job of helping to support our organization across a distributed network. It does a fantastic job at securing access to applications and networks. It is streamlined and straightforward.”

Secure Access

Petroleum Development Oman, a large energy/utilities company, operates a data center that hosts over 1,000 applications. Their Infrastructure Planner discussed how Cisco Security Firewall protects and secures the company’s services. He said, “It was a requirement from our security and compliance team that any traffic going to the data center needs to be checked and secured.”

"It's great across a distributed network for securing access to all our apps and the network," said a Sr Wireless Network Engineer who uses Cisco ISE at a large manufacturing company. "We don't have to worry about which system is going through which access layer or which security system. We can just put everything into ISE. We don't have to separate the switches from the routers to the wireless. It's all just 'one-stop, go.' It used to be that our switches were in a separate system for authentication routers and the wireless was all on EAP [Extensible Authentication Protocol]. It was confusing. ISE consolidated all that."

Secure access is part of the emerging secure access service edge (SASE) paradigm that many organizations are now implementing. A Vice President Information Security & Compliance who uses Cisco Umbrella at a large tech vendor addressed this process when he said, "One of the main use cases of Cisco Umbrella kicked in during the COVID pandemic, as a SASE deployment - secure access, secure edge. Most of the users within a company started working from outside the company and that is when Umbrella became deployed a lot."

#4 – Offering Cloud Management

Single Pane of Glass

Cisco customers appreciate the ability to manage their security tools in the cloud. To this point, a Network Security Consultant who uses Cisco Umbrella at a large tech services company said, "Cisco Umbrella provides a cloud management system. We can manage every client from a single workspace because they're in our portal. The single pane of glass management is user-friendly."

"I think cloud management is key," said the President of TKD Consulting, a large consultancy that uses Cisco Meraki MX. "The cloud management and support are the two things that make the product great." A Senior Manager (Enterprise Services) who uses Cisco Meraki MX at a software company simply stated, "Ease of management is the best thing about the solution. Cloud management is pretty much the driver."

#5 – Defending Against Email Threats

Email has emerged as one of the most dangerous attack surfaces that security managers need to defend. From malicious links to malware attachments, email is problematic on many levels—but also essential for business and a challenging technology when it comes to enforcing security policies. As a Network Administrator who uses Cisco Umbrella commented, "Everyone really just wants to be able to click and do what they do, just like at home. But for the IT side of it, it [Umbrella] does benefit us by limiting all of the extra activity. It does give us some comfortability that we aren't going to wake up, or even come in in the afternoon, and the whole network is down because someone went to buy some shoes or they clicked on a malicious email and caused a chain reaction."

For the CTO of Intelcom, a small tech services company, the most valuable feature of Cisco Umbrella for email security is its DNS security. Why? Because, as he said, "All the threats nowadays are coming from email servers. We also have the DSA solution to limit the threats coming from ransomware. Combining all of these with [Cisco] Talos [threat intelligence] provides the best security solution." Figure 2 shows this process in action.

Figure 2 - An email security solution, such as the one included in Cisco Umbrella, blocks messages containing malicious links and attachments.

"It enables us to go granular in the customization of blocking some categories on the DNS," said an IT Security Operations Manager who uses Cisco Umbrella at BeyondTrust, a large tech vendor. "Sometimes we get a malicious URL in a phishing campaign on the email side. Blocking a domain across the whole company in one minute is definitely great. To block a DNS request very quickly you just add the domain to the Global Block List and in one second it's blocked." He added, "Managing all the DNS aspects from one portal is definitely great from a security perspective."

Brian L.
IT Director at a university with 10,001+ employees

"It has reduced malware and mitigated risks associated with email links and various other factors, resulting in cost savings."

Read review »

Other notable comments about defending email using Cisco products included:

• "The solution also helps us remediate threats more quickly. Examples are when an email campaign comes in with malicious links, or if they're on a website like Facebook which is full of junk that doesn't need to come through." - Network and Security staffer who uses Cisco Umbrella at Dublin Intermediate School

• "It has reduced malware and mitigated risks associated with email links and various other factors, resulting in cost savings." - IT Director who uses Cisco Umbrella at a large university

• "We were looking to deal with email phishing attacks and brute force attacks, and the like, and Duo has helped a lot. We're more secure with multi-factor and have seen the number of phishing attacks and brute force attacks go down." - MSP Director who uses Cisco Duo Security at a small tech services company

#6 – Eliminating Security Gaps

There will always be gaps in security. No security team can defend everywhere, all at once with equal efficacy. For this reason, security managers value solutions that eliminate security gaps. For instance, the Chief Digital Officer of Talent Garden, a large tech company that uses Cisco Umbrella, shared that his company's employees are scattered throughout more than 20 locations, including homes and hotspots. "We had to cover the security gap," he said. "We needed to be sure that regardless of the location our employees would be covered by the security features."

BeyondTrust found that it had a gap when it came to blocking non-malicious traffic from DNS request queries. Their IT Security Operations Manager explained that they can address this issue with Cisco Umbrella. He said, "DNS is very important from a security perspective. Securing this layer, specifically for the remote users and the remote workforce that we're seeing today, is definitely a big gap that needed to be filled."

DNS security was also the source of a gap in security for a Senior Network Engineer who uses Cisco Umbrella at a large educational organization. He said, "We use it for roaming clients. We also push all our DNS traffic to Umbrella. We do not allow any other DNS traffic. We were looking to bridge the gap for DNS security, especially for mobile clients. We wanted to be able to put that roaming client on their PCs and kind of bring that together."

"We don't have to worry about when something goes down," said an Enterprise Architect who uses Cisco Security Firewall at a small tech services company. He elaborated, saying, "Instead of saying, 'Oh my gosh, this went down and now we have a gap here,' it has automatic failovers and built-in redundancy. So, it says, 'I don't have a gap anymore.' This is one less thing to worry about, which was a big benefit for me. If our security group comes back, and says, 'Hey, this is down.' Then, it is like, 'Yeah, we got it covered.'"

Senior Network Engineer
at a educational organization with 1,001-5,000 employees

"We use it for roaming clients. We also push all our DNS traffic to Umbrella. We do not allow any other DNS traffic. We were looking to bridge the gap for DNS security, especially for mobile clients."

Read review »

Eliminates Security Gaps

#7 – Providing Deeper Visibility

Security analysts and network security managers need visibility into what's happening in their infrastructure. Cisco users praised the company's security portfolio for this capability. A Systems Engineer who uses Cisco Security Firewall at a small tech services company, for example, has customers who have migrated from Cisco ASA to Cisco Firepower. "They have benefited from the change because they have much more visibility into the network," he said.

Specifically, they often use an ASA as a Layer 3 to 4 firewall. "We allow networks and ports," he added, "but a Firepower firewall has the default intrusion prevention engine, so you can allow it to https on port 443, but it can also look into the packet, with deep packet inspection, and see if there is malicious code that is trying to be pushed into your system."

The shift from ASA to Firepower, going from Layer 3 to Layer 7, also delivered visibility benefits to the tech services company's Systems Engineer. He commented, "The dynamic access policy functionality, and the fact that in Firepower 7.0 the feature has one-to-backward compatibility with the Cisco ASA Firewall, is a game-changer. Our customers have begun to transition from Cisco ASA to Cisco Firepower. They gain through the visibility they get from a next-generation firewall. They get more visibility and a more secure solution."

"It provides visibility," shared a Head of Network Administration Section who uses Cisco Security Firewall at Zemen Bank S.C., a large financial services firm. "It has been helpful for packet inspection and logging activities for all kinds of packets, such as routing packets, denied packets, and permitted packets. All these activities are visible on Cisco ASA."

Mitku B.
Head of Network Administration Section at Zemen Bank S.C.

"It has been helpful for packet inspection and logging activities for all kinds of packets, such as routing packets, denied packets, and permitted packets. All these activities are visible on Cisco ASA."

Read review »

Increased Visibility

Conclusion

Organizations that engage with CDW & Cisco Security find that they are achieving robust security outcomes by using the Cisco Security portfolio. CDW's unique achievements as a Cisco Gold Partner enable the company to deliver on firewall, breach protection, user protection, and cloud protection. These are the core focus areas for Cisco Security. As PeerSpot members who use Cisco Security products share, there are seven principal ways Cisco helps them protect their businesses: boosting security resilience, establishing trust, providing deeper visibility, defending against email threats, securing access, offering cloud management, and eliminating security gaps. As CDW & Cisco Security delivers on these capabilities, customers will realize gains in their security postures while improving the efficiency of their security operations.

Appendix: Cisco Products Referenced in this Paper

- Cisco Firewall—Cisco produces a wide range of firewall products that protect resources on customer networks.
- Cisco Duo Security—A two-factor authentication (2FA) solution that verifies user identities and establishes device trust.
- Cisco Umbrella—A flexible solution for cloud-delivered security that combines multiple security functions into one, e.g., data protection for devices, remote users, and distributed locations.
- Cisco ISE (Identity Services Engine)— A network access control solution that uses policy-based decision making to determine a device's network access rights.
- Cisco Meraki MX—An enterprise software-defined wide area network (SD-WAN) appliance.

About PeerSpot

PeerSpot is the authority on enterprise technology buying intelligence. 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

About CDW ServiceNow Solutions

CDW has over 20 years of experience delivering Cisco solutions to Enterprise, Commercial and Public Sector customers. CDW provides unmatched Cisco expertise and experience as the first worldwide partner to achieve Cisco Security Master status as well as Cisco's largest U.S. National Direct Integrator Partner. In addition to creating and developing innovative, industry-leading technologies, CDW has the experience, experts and services to help organizations craft a combination of the right tools and the right plan that can mitigate security risks, increase visibility, unlock the power of their solutions and be better prepared for the evolving threat landscape.

A Fortune 500 company and member of the S&P 500 Index, CDW was founded in 1984 and employs approximately 14,900 coworkers. For the trailing twelve months ended June 30, 2023, CDW generated Net sales of approximately $22 billion. Learn more about CDW.