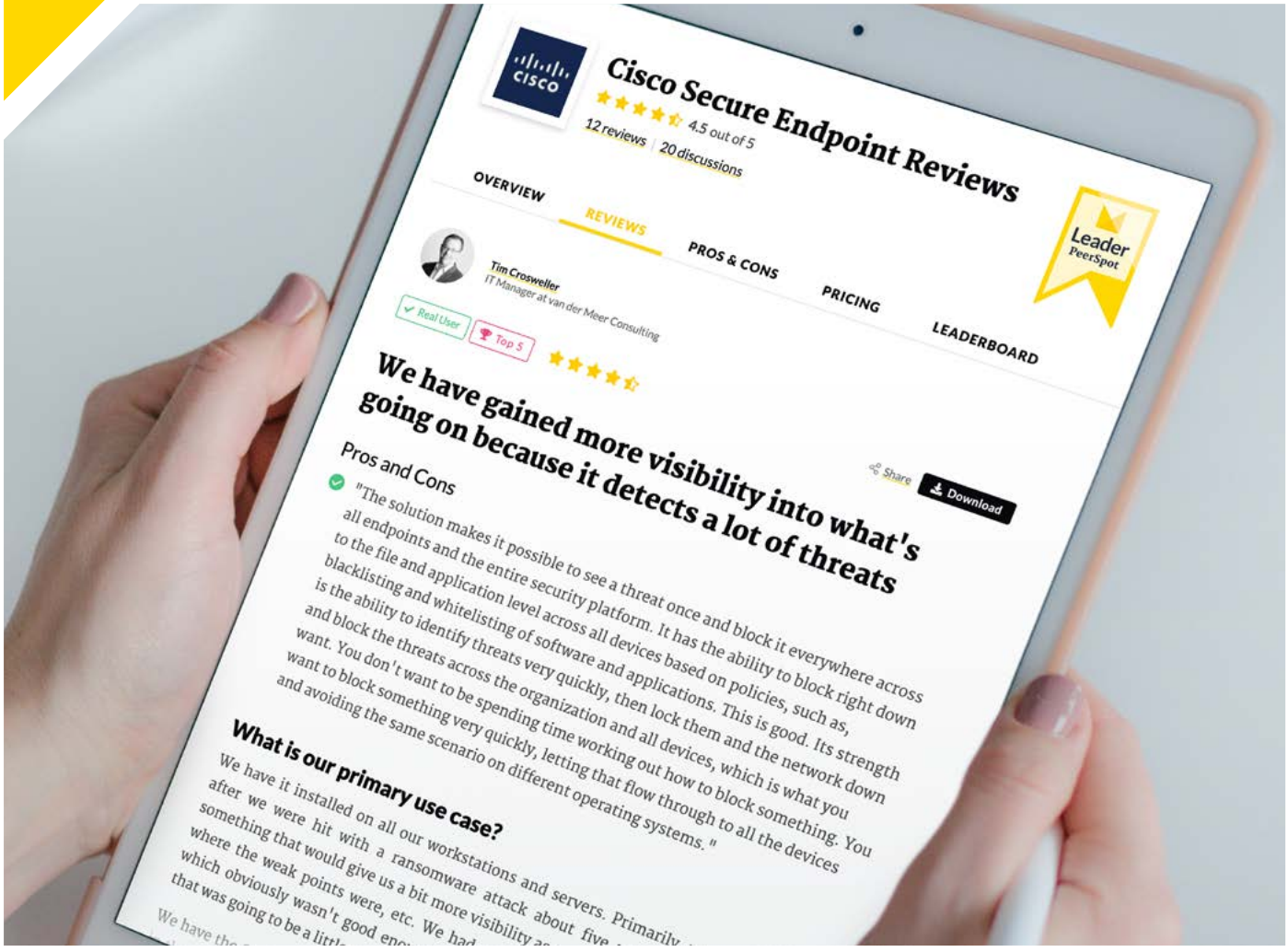
PeerPaper™ Report 2022

Based on real user reviews of Cisco Solutions

# Securing the Remote Workforce: From the Cloud to Endpoint




PeerSpot

CSO FROM IDG

# Contents

# Introduction

The events of 2020 dramatically changed how and where employees work. People are doing their jobs from just about anywhere, anytime – but it can take a lot to enable staff productivity without compromising security. Defending the whole remote work infrastructure can be challenging. Security teams work around the clock to protect remote workers, their devices, and their entire work environment.

IT and security professionals are under pressure to verify users, enable secure access, and defend the remote work environment from any threat. It's a mandate that spans everything from the cloud to the endpoint. This paper explores how companies are handling this unexpected mandate to support a large number of off-campus workers. It's based on real user reviews of Cisco products for user authentication, VPN, cloud security, email protection, and endpoint security on PeerSpot.

# Overview: The Remote Worker Security Challenge

The change in work location today could best be described as an inversion of the status quo. Until 2020, the majority of knowledge workers did their jobs within the confines of an office building or corporate campus. They logged in to a controlled network environment. When workers went home or traveled, the company made provisions for remote work. These provisions, which included technologies like Virtual Private Networks (VPNs), were intended for the relatively small portion of people who needed remote access at any given time.

This situation has been transformed in almost every imaginable way with large portions of workers now working from home (WFH). Nearly everyone is off campus today. And, what's more, the expectation is that far more people will continue on a WFH basis even after the strictures of the pandemic are lifted.

This new reality creates a variety of security challenges. Remote employees may be using consumer-grade internet connections to access the corporate network. They may be working on personal devices. The vast majority of network traffic is now supporting people off campus, rather than the other way around. Email threats like phishing are on the rise, while endpoints continue to be a prime target of attackers as they take advantage of pervasive remote work to gain access to the crown jewels of the enterprise.



**Works anywhere in the world**

# Mitigating Remote Worker Security Risks

IT managers and their counterparts in security have a big job on their hands in mitigating remote worker security risks. The remote work environment has expanded the attack surface. This means IT and security teams have to deal with more risks. The scale of the job is daunting, to say the least. The security practices once reserved for a few remote people now apply to almost every employee in the organization.

The need to ensure secure access and facilitate VPN use applies to far more end users today than it did in 2019. The requirements to secure user access and the endpoints they use daily are more extensive at the present moment. It's also essential to prevent users from reaching malicious sites or inadvertently downloading malware, as they fall victim to phishing attacks.

## Ensuring Secure Access

Remote access must be secure, regardless of the worker's location. That's a fundamental principle of the new WFH era. For example, a Board Member at a small computer software company uses Cisco AnyConnect for secure access to his company's network. He shared that "there are almost no problems with connectivity when using a third-party system."

> **"AMP will work anywhere in the world, as long as it has an internet connection. You get protection and reporting with it."**
>
> Read review »

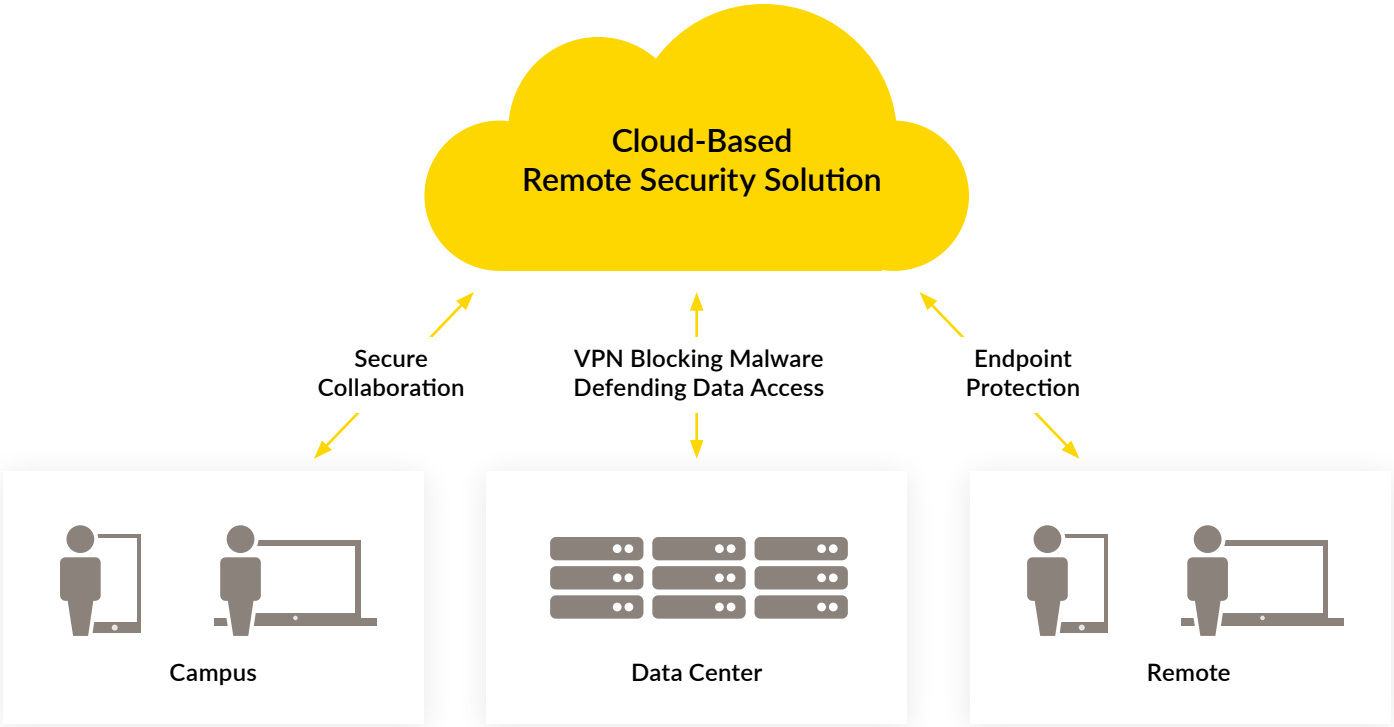



Figure 1 – A cloud-based security solution can protect data assets, end users, and endpoints across the campus, data centers, and remote work sites.

## Requiring and Facilitating VPN Use

The VPN is a core requirement of remote work, so companies must make them easy to use and readily available. In this context, the InfoSec Consultant at Thorntons referred to her solution as "easy to deploy for staff to use VPNs." An IT Administrator at Vodafone, similarly referred to Cisco ASA as "a stable solution with good monitoring and VPN capabilities." He added, "The VPN and monitoring are the most valuable features."

A Head of Solutions Delivery (Systems) at a health, wellness, and fitness company with more than 200 employees felt that Cisco AnyConnect is "absolutely a product that I can recommend." He said, "For me, it is straightforward to establish my VPN connection and then do my work." Figure 1 offers a simple example of how a solution like this can work.

"The visibility that we have into the endpoint and the forensics that we're able to collect give us value for the price."

Read review »

Cisco Umbrella is the preferred solution for a Global Security Manager at a manufacturing company with over 500 employees. As he put it, "Architecturally, for the deployment, you should consider if you want it on roaming clients or if you want it central. If people are connecting back through a VPN, it's then probably on every single client. Looking at how we're all working now with COVID, having a roaming client deployment gives you that added layer of protection because you're not dependent on the users connecting back to corporate VPN. They're always protected."

"One of the best features of AMP is its cloud feature," shared a Security Officer at a healthcare company with more than 50 employees. He added, "It doesn't matter where the device is in regard to whether it's inside or outside of your network environment, especially right now when everybody's remote and has taken their laptops home. You don't have to be VPN'ed into the environment for AMP to work. AMP will work anywhere in the world, as long as it has an internet connection. You get protection and reporting with it."



**20%**
less time spent on patching

## Defending Digital Assets, Endpoints, and End Users

PeerSpot members talked about the need to defend digital assets, endpoints, and end users no matter where anyone – or anything – is located. This was a consistent theme in user reviews with regard to remote work. A CIO who uses Cisco AMP at Per Mar Security Services, a security firm with over 1,000 employees, put it this way: "The most valuable thing about the solution is a feature that's not in the actual product set itself. It's peace of mind. We take a look at security holistically, multilayered."

**Stops malware before it reaches endpoints or networks**

He then shared, "We start from the edge and perimeter and work all the way down to the client. I feel we've deployed best-of-breed in each of the slices of the security layer. For the endpoint, Cisco gives us good clarity about what our endpoints are actually doing. So when we get bad actors into the network, we get quick visibility into which devices are compromised." An IT Manager at van der Meer Consulting, a construction company with more than 50 employees, has a comparable situation. He uses Cisco Umbrella and AMP for Endpoints to provide the first line and last line of defense against advanced threats. The advantage of this approach is that "it is looking at attacks from a different point or source."

## Defending Data Access

Data security, never an easy area of security, can be particularly problematic in a WFH environment. Employees still need to access corporate data. However, the risk of a malicious actor gaining entry to a sensitive database increases when everyone needs a remote session to work with its data. A Security Team Leader at a tech services company with over 500 employees explained his approach to defending data access by saying, "Even if devices become infected in other ways, Umbrella prevents connections to an attacker's servers. [We can] stop data exfiltration and execution of ransomware encryption."

## Defending Endpoints

Sending nearly everyone home to work has expanded the definition of an endpoint and stretched the concept of endpoint defense to extremes. The situation facing the

Per Mar Security Services CIO is representative. He said, "The visibility that we have into the endpoint and the forensics that we're able to collect give us value for the price. We have about 800 endpoints that we protect with it and that number is growing, because around the end of 2019 we started playing around with deploying AMP onto cell phones, both Android and iOS. It doesn't impact the devices. It is an agent-based solution, and we see no performance knock on cell phones." He then revealed, "The other thing that we really like, from the agent standpoint, is that our end-users are not capable of turning the tool off. That was very critical for us."

Email security solutions now play a significant role in endpoint protection. A Director of IT Security who uses Cisco Email Security at a health, wellness, and fitness company with over 10,000 employees explained, "If it's an unknown hash (after it identifies the file by hash value) and not found in the databases, then it automatically uploads that file to Threat Grid for sandboxing and analysis. That layered approach with respect to treating the files as they come in works well, whether via network, email or found on endpoint." He further shared, "This works well because the information found on a single endpoint, for example, can then immediately take action on an email by blocking that identified malicious file."

"The solution simplifies endpoint protection, detection, and response workflows, such as security investigation, threat hunting, and incident response," said the IT Manager at van der Meer Consulting. He added, "We have policies and procedures in place now at the HR user level and also at the machine

**"The solution simplifies endpoint protection, detection, and response workflows, such as security investigation, threat hunting, and incident response."**

**Read review »**

level to make sure that certain procedures are followed and those procedures are put in place. From that point of view, Cisco gives us confidence." For the tech company Security Team Leader, the value came from the fact that the solution "stops threats over all ports and protocols – even direct-to-IP connections." He liked the fact that Umbrella can "stop malware before it reaches your endpoints or network."



**Gives great value for price**

## Preventing Users From Reaching Malicious Sites

The risk of employees visiting malware-laden websites is always a concern, but extensive remote work has made the risk much harder to manage. A Sr. Network Engineer at a small real estate/law firm has found a solution with Cisco AMP and its Device Trajectory feature. He said, "It shows everything that's going on, on a computer. It shows the point in time when a virus is downloaded, so you can see if the user was surfing the internet or had a program open. It shows every running process and file access on the computer and saves it like a snapshot when it detects something malicious."

"The most valuable feature is that it secures our network against malicious websites," said a Network Engineer who uses Cisco Umbrella at LADWP, an energy/utilities company with more than 5,000 employees. He then commented, "If we do have an instance of malware then it is unable to home back to these types of sites." The IT Manager at van der Meer Consulting similarly noted, "Our webpage/portal records all instances of programs accessed on the computer, everything accessed on the internet, all the system processes, and any programs that are running. It then scans them for potential issues."

"The most valuable feature is that it secures our network against malicious websites..."

Read review »

## Blocking Unwanted Internet Connections

Blocking unwanted internet connections is another urgently needed countermeasure in a WFH environment. The IT Manager at van der Meer Consulting said Cisco AMP for Endpoints makes it possible to see a threat once and block it everywhere across all endpoints and the entire security platform. As he explained, Cisco AMP for Endpoints has the ability to block right down to the file and application level across all devices based on policies, such as "allow lists" and "block lists" of software and applications. This user related that the solution was able to identify threats very quickly and then "lock them and the network down and block the threats across the organization and all devices, which is what you want."

## Preventing Email Attacks

Email, given its prevalence as a cyberattack vector, is especially worrisome for security managers in the remote work context. With users on personal devices, it can be difficult to detect and respond to phishing and other forms of email attack quickly enough to stop them before they do damage. For example, according to the health and wellness Director of IT Security, business email compromise involving executive impersonation is a common problem at this firm. He also contends with phishing and malware delivery by email. He uses Cisco Cloud Mailbox Defense (CMD) to contain these threats. He said, "Having Cisco's solution gives us a fast way to track and identify."

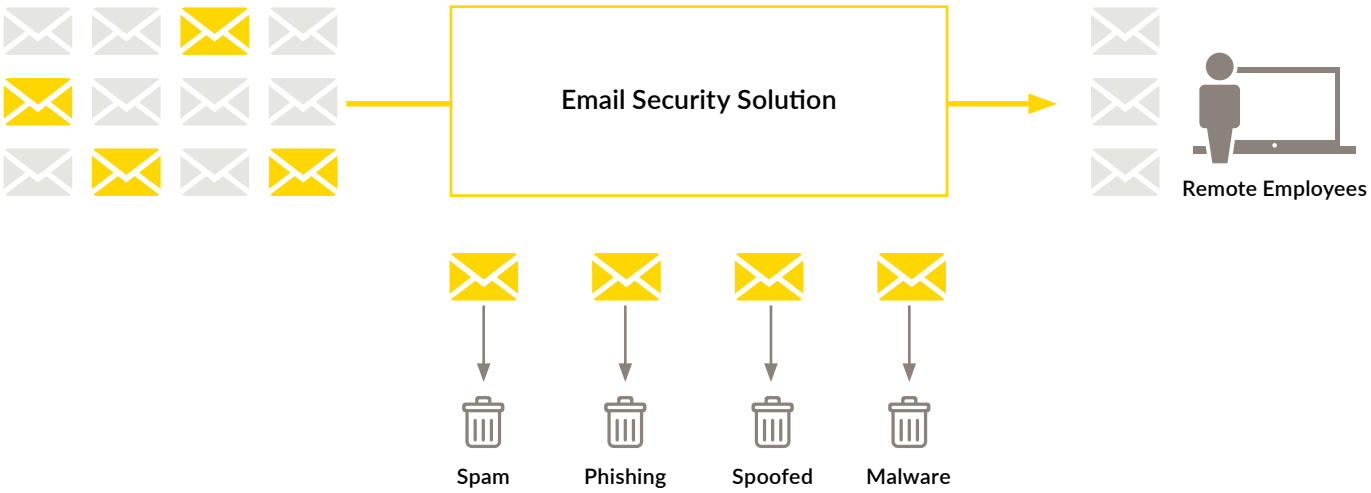



Figure 2 – Email security solutions authenticate senders and filter out spam, phishing attack emails, messages from spoofed addresses, and email that contains malware.

Other notable comments on preventing email attacks included:

- "We get over 100 million emails a month. This filters them down and allows only somewhere about three million emails, which is a great help." – Chief Information Officer at Sacramento County, a government agency with over 10,000 employees

- "With our previous solution, you had no way to be sure that you were not missing something, if there were not any files left, passwords/data stolen, connections made to different machines, booby traps or scheduled tasks left, etc. With Cisco AMP, if it manages to execute, I can say, 'How did we get this file?' With one click, I can block it from being downloaded from the internet and being emailed in/out of our environment." – Technical Team Lead Network & Security at Missing Piece BV, a small tech services company

- "It helps to protect the network against ransomware and phishing attacks." – Presales Engineer at DataProtect, a tech services company with more than 50 employees

> **"With one click, I can block it from being downloaded from the internet and being emailed in/out of our environment."**
>
> Read review »

## Defending Against Internet Attacks

Malware, never a good thing, is all the more dangerous when it can take up residence on remote workers' devices. From there, malware can make its way into corporate networks and wreak havoc on critical applications and data. As WFH becomes the norm, security teams are fighting to defend their digital assets against malware. For a Sr. Network and Security Consultant at a media company with over 1,000 employees, this means deploying Cisco Umbrella for more than 2,000 users. He said, "We have multiple sites, and we have some remote users in different locations. Cisco Umbrella is a fitting solution for internet or DNS-based attacks. It is a very good solution for that, and especially for remote users. It has a malware protection engine."

Speed of malware alerts is what mattered to a Technical Team Lead at Missing Piece BV, the small tech services company. As he explained, "With our previous solution, if it was known malware, we would get an alert. If it was an unknown malware or ransomware, our users were our detectors. Then, it might take hours before they could say, 'Hey, something's not working for me.' Cisco AMP will get you that same alert within minutes of an incident occurring."

## Checking For Patch Compliance

Patch management, an absolutely critical element of any cybersecurity program, also grows more difficult as workers head home. If they are not on the corporate network, it may be hard to know what needs patching. PeerSpot members are finding solutions, however. For instance, the law firm Sr.

> "The solution has decreased our time to remediate."
>
> Read review »

Network Engineer remarked that the Cisco AMP's Orbital Advanced Search feature shows which software packages are vulnerable.

He said, "Once you know that information, you can proactively patch the computer or apply updates to it so that it does not become infected. It alerts you to an infection, and then you can say, 'Oh, these other computers could be infected by that too.' Orbital detects those computers." In his case, the solution reduces the amount of time spent on patching by about 20 percent. The IT Manager at van der Meer Consulting shared that he "can roll out an update to all devices and not have to worry about having reboots, particularly for servers."

His organization has 120 devices, plus an extra 60 work-from-home devices at the moment. He shared, "The scalability is good because we were able to go from 120 devices to 180 very quickly. Therefore, we are able to push devices out very quickly, as needed. There are no issues from my point of view. The solution has decreased our time to remediate."

**"We are able to push devices out very quickly... The solution has decreased our time to remediate."**

**Read review »**

# Conclusion

IT team members and their colleagues in security have had to adapt quickly to a major change in the way employees perform their jobs. People are working from home, and doing so just about anywhere except on the main corporate campus. Away from a place that was designed for digital productivity and security, employees are instead relying on home internet connections and even personal devices for sensitive tasks.

Mitigating remote worker security risks is a multi-faceted challenge. With the right tools, IT managers and security professionals are able to ensure secure access to digital assets. This may involve the use of VPNs as well as technologies that defend digital assets, endpoints, and end users. Data access protections are critical, as are solutions that prevent users from downloading malware or reaching malicious sites.

Email security grows in importance with widespread remote work, as attackers are finding it easier to impersonate employees when so many people are at home. Patch management programs face similar difficulties, as it can be unclear which devices people are using and what software is running on them. PeerSpot members are finding their preferred tools to be essential in devising and implementing the varied security countermeasures required to defend remote workers, their devices, and the corporate data assets they need to do their jobs.

# About PeerSpot

**User reviews, candid discussions, and more for enterprise technology professionals.**

The Internet has completely changed the way we make buying decisions. We now use ratings and review sites to see what other real users think before we buy electronics, book a hotel, visit a doctor or choose a restaurant. But in the world of enterprise technology, most of the information online and in your inbox comes from vendors. What you really want is objective information from other users. PeerSpot provides technology professionals with a community platform to share information about enterprise solutions.

PeerSpot is committed to offering user-contributed information that is valuable, objective, and relevant. We validate all reviewers with a triple authentication process, and protect your privacy by providing an environment where you can post anonymously and freely express your views. As a result, the community becomes a valuable resource, ensuring you get access to the right information and connect to the right people, whenever you need it.

www.peerspot.com



# About Cisco

Cisco (NASDAQ: CSCO) is the worldwide leader in technology that powers the Internet. Cisco inspires new possibilities by reimagining your applications, securing your data, transforming your infrastructure, and empowering your teams for a global and inclusive future. Discover more at newsroom.cisco.com and follow us on Twitter at @Cisco.

Cisco Secure Remote Worker is a simple, scalable, integrated security solution that delivers the strength and breadth of the Cisco platform approach to protect your workforce everywhere. We verify the identity of all users before granting access to corporate applications with secure and easy multi-factor Authentication with Cisco Duo. We enable secure access to the enterprise network for any user, from any device, at any time, in any location with Cisco AnyConnect Mobility Client (VPN). And we enable coordinated defense against threats with Cisco SecureX – a platform built into Cisco Umbrella for internet security, Cisco Cloud Mailbox Defense for email security and Cisco AMP for Endpoints for endpoint security.