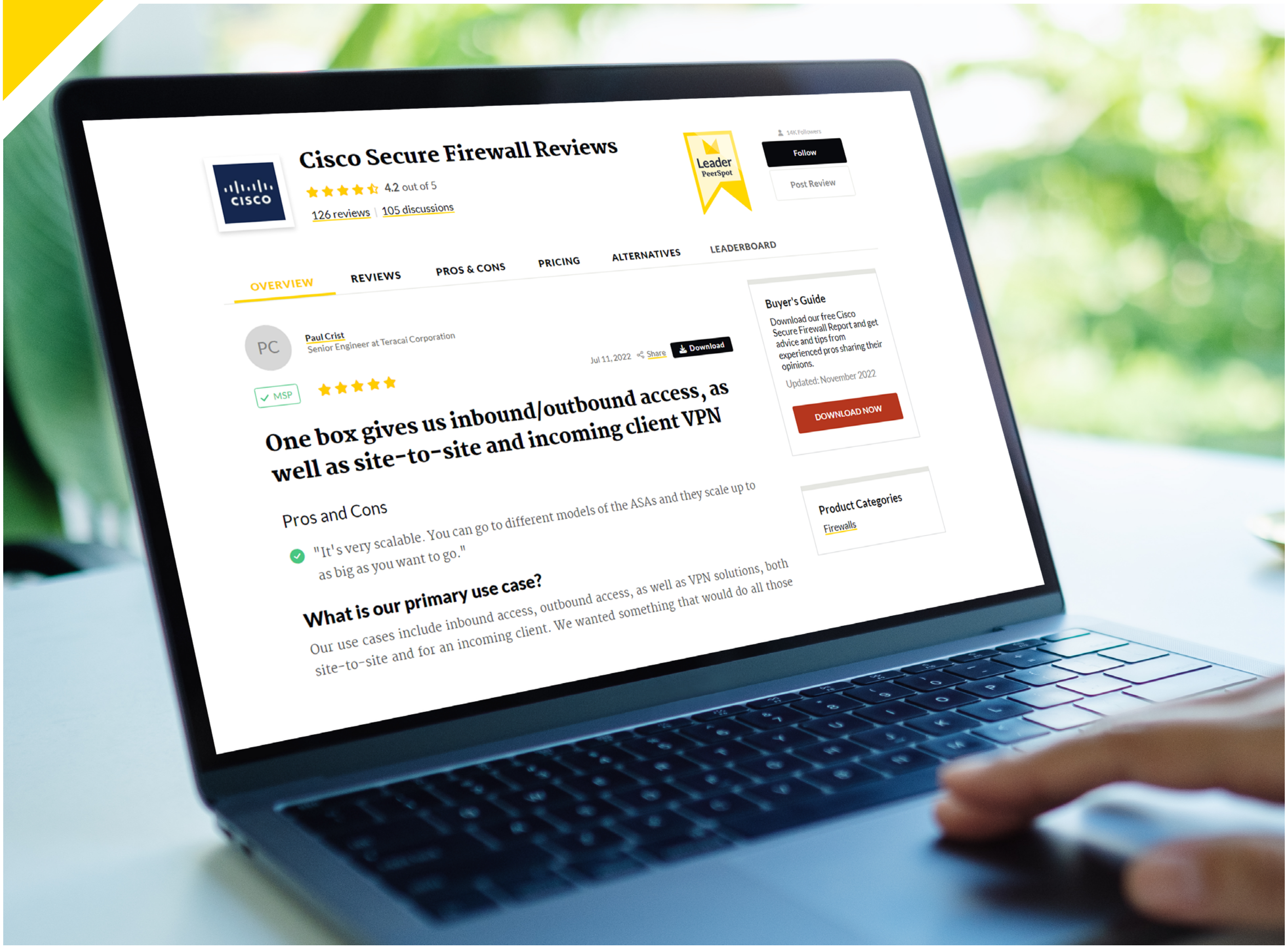
PeerPaper™ Report 2022

Based on Real User Reviews of Cisco Secure Firewall

The Elements of Security Resilience



Cisco Secure Firewall Reviews

4.2 out of 5

126 reviews | 105 discussions

Paul Crist
Senior Engineer at Teracai Corporation

Jul 11, 2022 Share Download

MSP ★★★★★

One box gives us inbound/outbound access, as well as site-to-site and incoming client VPN

Pros and Cons

✓ "It's very scalable. You can go to different models of the ASAs and they scale up to as big as you want to go."

What is our primary use case?

Our use cases include inbound access, outbound access, as well as VPN solutions, both site-to-site and for an incoming client. We wanted something that would do all those

Buyer's Guide

Download our free Cisco Secure Firewall Report and get advice and tips from experienced pros sharing their opinions.

Updated: November 2022

DOWNLOAD NOW

Product Categories

Firewalls

PeerSpot

CSO

Contents

Introduction

As cybersecurity professionals rise to the challenge of defending their organizations, they are pivoting from point solutions and security posture to a focus on security resilience. Not based on any single product, security resilience is a coordinated approach to securing all facets of a company. The goal is to enable a business to rebound quickly from security incidents, and maintain full operations despite short-term setbacks.

Realizing this objective requires having multiple, integrated security solutions working together. As users of the Cisco security portfolio explain in this paper, the elements of security resilience span risk reduction, visibility, insider risk mitigation and actionable intelligence. As these elements come together, they make it possible for an organization to remain resilient even in the face of a serious cyberattack.

Overview of Security Resilience

Security resilience is one of those concepts that most people understand intuitively, though they may find the details to be elusive. In practice, it's about being able to recover quickly from a cyber incident or comparable security problem. That means different things in different areas of a business, however. For Cisco, there are four main categories of security resilience:

- Operational—bringing business operations and relevant information systems back online as quickly as possible, with minimal data loss.
- Supply chain—averting or recovering from security issues that affect the supply chain, such as outages in ERP and logistics systems.
- Financial—minimizing the financial impact of a security incident, such as a ransomware attack on an accounting system.
- Organizational—making sure that people and organizational units can return to regular functioning in the wake of a security incident like a disaster that takes a communication and collaboration solution offline.

Realizing the goal of security resilience requires a broad-based, heterogeneous solution approach. Cisco security products can be deployed on-premises and in hybrid cloud environments—working with any cloud provider. Cisco security products work together synergistically, creating a "better together" effect across the ecosystem.

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."

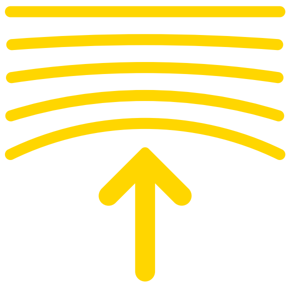
Read review »

Perspectives on Security Resilience

PeerSpot members shared many thoughts about security resilience in their reviews of Cisco security products. For example, a Cybersecurity Architect who uses Cisco ASA Firewall at a financial services firm with more than 5,000 employees said, "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."

"You definitely want resilience," said an ITS 1 who uses Cisco ISE at a government agency with over 10,000 employees. "You want to keep everything protected, especially in the day and age that we live in now. Information is power. Keeping our customers' and patients' information safe is our number one priority."

A Network Systems Manager who uses Cisco ASA Firewall at a software company with more than 5,000 employees put it like this: "Cyber security resilience has been extremely important for our organization because of our customers' demands for security. The ASA has really helped to accomplish that with the VPN. 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."



Increased Resilience

Administrator
at a university with
1,001-5,000 employees

★★★★★

> “I have integrated it for incidence response. If there is a security event, the Cisco firewall will automatically block the traffic, which is useful.”
>
> **Read review** »

“Cybersecurity resilience has been paramount,” said a Network Engineer who uses Cisco ASA Firewall at a university with over 1,000 employees. He added, “Because there is a threat of losing everything if ransomware or another sort of attack were to happen, the cybersecurity resilience has been top-notch.”

An Assistant ICT Manager who uses Cisco ASA Firewall at a transportation company with more than 50 employees explained why he finds Cisco products to be quite resilient. He said, “We’ve had problems due to power failures and our UPSs not being maintained and their batteries being drained. With the intermittent on and off, the Cisco ASAs, surprisingly, didn’t have any issue at all. The devices really stood on their own. We didn’t even have any issue in terms of losing configs.”

Elements of Security Resilience

Security resilience arises out of the interplay between four functional areas of security. These are risk reduction, visibility, insider mitigation and actionable intelligence. As the different factors come together in Cisco's "better together" ecosystem, greater resilience becomes possible.

Risk Reduction

Risk reduction occurs when the organization has done all they can, with regard to their technologies and policies, to reduce the attack surface within the organization. As a Senior Security Analyst who uses Cisco SecureX at a consumer goods company with more than 500 employees shared, "We use it to investigate threat incidents. It lets us better manage security incidents." On a related front, an Administrator who uses Cisco Firepower NGFW at a university with over 1,000 employees said, "I have integrated it for incidence response. If there is a security event, the Cisco firewall will automatically block the traffic, which is useful."

Risk
Reduction

Senior Security Analyst
at a consumer goods company
with 501-1,000 employees

★★★★☆

> “We use it to investigate threat incidents. It lets us better manage security incidents.”
>
> **Read review »**

Operational efficiency is a big part of risk reduction for a System Administrator who uses Cisco Secure Endpoint at a manufacturing company with over 200 employees. He said, “The way it is set up, with the console, I would get to know quickly that we have an issue. It increases operational efficiency because I don’t have to go from desktop to desktop. I’m also proactive instead of reactive. It has minimized security risks to our business.” He went on to explain that his setup has decreased their time to remediate security problems because they are focusing only on affected machines. He said, “It has decreased our time to detect.”

Further to the idea of efficiency, a Network Security Architect who uses Cisco SecureX at Lake Trust Credit Union, a financial services firm with more than 500 employees, said, “We use a lot of different Cisco security products to protect different areas of our entire infrastructure. SecureX basically gives us a single pane to all those products. We were trying to avoid going from product to product to product to product, either to research security events or just look at overall performance of those. SecureX covers every security product that we have.”

“In addition, compared to our previous firewall solution, the security is much better,” said an Information Security and Compliance Manager who uses Cisco Firepower NGFW at RSwitch, a tech services company with more than 50 employees. He added, “Through our monitoring, we now see all the information that we require on security, in terms of PCI. We can see exactly what is happening in our environment. We know what is going in and out. If an incident happens, it provides a notification so that we can do an analysis.”

Financial Corp, a financial services firm with over 10,000 employees, has found that Cisco AMP simplifies endpoint protection, detection, and response workflows, like security investigation, threat hunting, and incident response. Their Application Manager explained, “By using the solution, we’ve been able to divert attention towards the [other] tasks, saving us significant time and effort. It has obviously minimized security risks to the entire business, most importantly, endpoints, servers and other crown-jewel assets.”

Visibility

Being resilient is due, in part, to having extensive awareness of the IT estate and its attack surface. Ideally, the security toolset will provide visibility. A Technical Consultant who uses Cisco ASA Firewall at Zak Solutions for Computer Systems, a tech services company with more than 500 employees, framed the issue by saying, “Cisco has multiple products - not just firewalls. The integration between other items provides a powerful end-to-end solution. It’s nice and easy. There is one management system and visibility into all of the features. Using the same product is more powerful than using multiple systems.” Figure 1 depicts this capability.

Threat Visibility

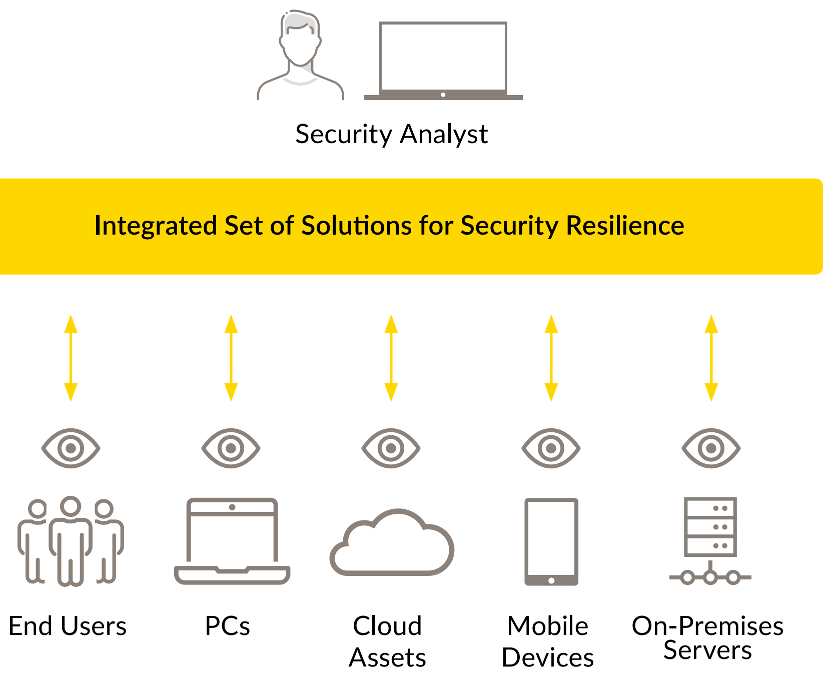


Figure 1 - An integrated set of solutions for security resilience can maintain visibility across a wide variety of digital assets, devices and end users.

"The most valuable features are actually the reporting with all the visibility," said a Senior Network Security Engineer who uses Cisco Umbrella at a tech vendor with over 200 employees. "It gives a hawk-eye view when we map AD [Microsoft Active Directory] with Umbrella. It gives us the visibility of every user, e.g., which sites and content are being used and who is accessing what. That has really been a good new addition for me."

A Network Administrator who uses Cisco Umbrella concurred, saying, "The best feature is the visibility. We're able to see the specific user names of whoever clicked on a certain link. It also gives us a threat detection level. It allows us to maintain more [awareness of] who's doing what they shouldn't be doing. The most valuable asset of it is giving us the ability to categorize who should have access to what type of sites."

Kevin S.
Network Administrator

★★★★★

"The best feature is the visibility. We're able to see the specific user names of whoever clicked on a certain link."

Read review »

Zaigham A.
Senior Network Security
Engineer at a tech vendor
with 201-500 employees

> “It gives a hawk-eye view when we map AD [Microsoft Active Directory] with Umbrella. It gives us the visibility of every user, e.g., which sites and content are being used and who is accessing what. That has really been a good new addition for me.”
>
> Read review »

Other notable comments about visibility include:

- “The integration of network and workload micro-segmentation is very good when it comes to visibility in our environment.” - Senior Network Security Engineer who uses Cisco Firepower NGFW at a small tech services company

- “Cisco NGFW’s ability to provide visibility into threats is good compared to other solutions. The visibility is quite impressive and gives us what we’re looking for, based on our security requirements.” - Information Security and Compliance Manager at RSwitch, a tech services company with more than 50 employees

- “Cisco ASA provides us with very good application visibility and control.” - Co-Founder of Multitechservers, a tech services company

- “It provides visibility and information to the organization about what is being accessed on the Internet as well as the applications that it is protecting.” – Technology Coordinator who uses Cisco ASA Firewall at a tech vendor with over 1,000 employees

Insider Mitigation

The traditional cyber perimeter effectively no longer exists. Digital assets, along with end users and their devices, are as likely to be outside the corporate network as they are inside it. This dramatic change has created an urgent need to defend against attackers posing as insiders. Actual insiders, such as employees and contractors, can also be a potential threat vector if their accounts have been taken over by malicious actors.

Zero Trust

As a result, many organizations are implementing, or at least considering “Zero Trust” security solutions. Zero trust, which is based on the policy of “Never trust. Always verify,” rejects all access requests until the user and device can be verified. After that, the user is only allowed the minimum possible access privileges. This approach is a key element of security resilience, as it mitigates insider threats. Figure 2 offers an overview of the model.

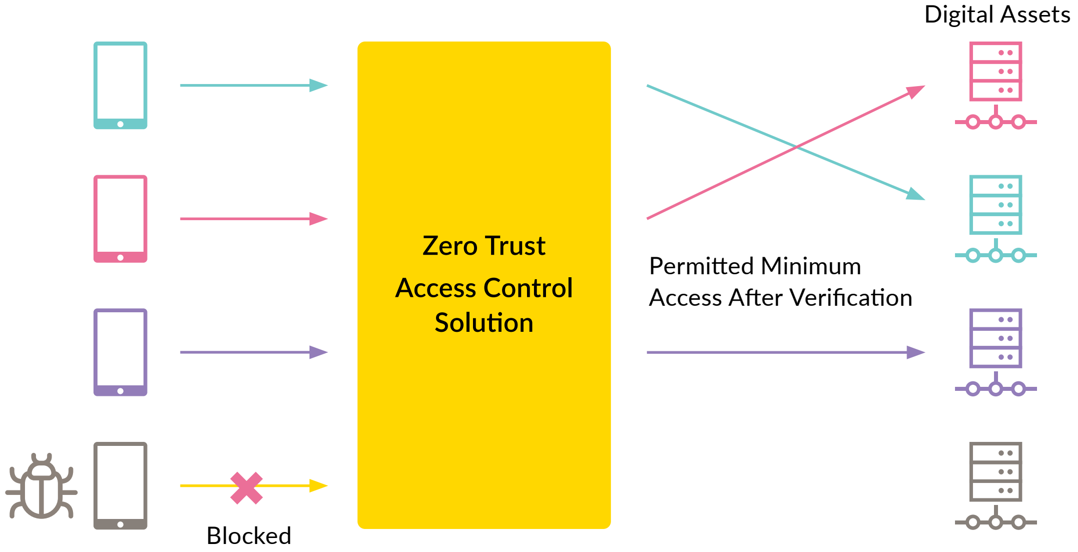


Figure 2 - Zero Trust works by not trusting any user or device until verified, and then only permitting the minimum access privileges.

Mohd. Asif K.
Co-Founder & Director at
VSAM Technologies

★★★★☆

“This is a comprehensive solution covering access to network to create a zero trust environment. It covers network access control, network segmentation and policy control.”

Read review »

PeerSpot members spoke of the growing appeal of Zero Trust. A Cyber Security Administrator who uses Cisco ISE at a small aerospace/defense firm, for instance, said, “Resilience is never a bad idea and it’s never too late to start working towards it or to begin the journey to Zero Trust. It’s very important in this day and age.”

For a Co-Founder & Director who uses Cisco ISE at VSAM Technologies, a small tech company, “The general usefulness of the product is not specific to a particular feature. This is a comprehensive solution covering access to network to create a zero trust environment. It covers network access control, network segmentation and policy control.”

“To leaders who want to build more resilience within their organization, I would say that it’s definitely worth moving toward a zero trust environment,” said a Principal consulting architect who uses Cisco ISE at a tech vendor with over 10,000 employees. He commented that Zero Trust is an updating of the old concept of least privileged access, but, as he explained, “The tools we have to implement it, such as Cisco ISE and firewalls, at the core and the ability to broker it out to the cloud as well, give us a lot more visibility and a lot more control over the traffic and our data, which is our biggest asset.”

A Network Architect who uses Cisco ISE at Tarrant Regional Water District, a small recreational facilities/services company, explained that ISE is strong in the Zero Trust model because it considers "everybody a foreign endpoint until they prove they belong on the network." He added, "ISE just seems to be built from the ground up to do that, whereas with other solutions, you have to 'shoehorn' that in.

"The fact that ISE considers all resources to be external is very important," said a Sr Wireless Network Engineer who uses Cisco ISE at a manufacturing company with over 10,000 employees. "We use ISE in our retail environments for our payment sleds. 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."

Actionable Intelligence

Avoiding attacks is one of the best ways to stay resilient. The problem never occurs in the first place! This is easier said than done in today's severe threat environment. However, with accurate and up-to-date intelligence, it is possible to anticipate threats and be prepared before they cause harm.

Up-to-Date Intelligence

IT Administrator/Security Analyst
at a healthcare company
with 11-50 employees

★★★★⯪

“We get the security intelligence feeds refreshed every hour from Talos, which from my understanding is that they’re the largest security intelligence group outside of the government.”

Read review »

A Systems Engineer who uses Cisco Firepower NGFW at a small tech services company explained, “If you configure Firepower correctly, it is good when it comes to threat visibility. It is proficient. It is the state of the art when it comes to blocking threats, network-wise.” He went on to say that if one uses Firewpower with SSO encryption, along with one’s own features, blocklists, security intelligence, intrusion prevention, and access control points, then Firepower can block most threats on the network.

“We get the security intelligence feeds refreshed every hour from Talos, which from my understanding is that they’re the largest security intelligence group outside of the government,” said an IT Administrator / Security Analyst who uses Cisco Firepower NGFW at a small healthcare company. He added, “My experience with Talos has been, they’re pretty on top of things. Another driving factor towards Cisco: We get feeds every hour, automatically refreshed, and updated into the firewall.”

Being able to set up Firepower so it discovers the environment is what stood out to a Cyber Security Practice Lead who uses Cisco Firepower NGFW at Eazi Security, a small tech services company. He elaborated, saying, “If that is happening, then Firepower is learning about every device, software operating system, and application running inside or across your environment. Then, you can leverage the discovery intelligence to get Firepower to select the most appropriate intrusion prevention rules to use for your environment rather than picking one of the base policies that might have 50,000 IPS rules in it, which can put a lot of overhead on your firewall.”

Conclusion

Security resilience is emerging as a critical goal for cybersecurity teams and operational stakeholders. Being able to rebound quickly from a security incident is not the result of any one product, however. The capability arises with a coordinated approach to security that cuts across the entire business and technology stacks. When multiple, integrated security solutions work together, resilience becomes possible in operations, the supply chain, and finance. The organization itself becomes more resilient overall. Getting there means taking a broad-based, heterogeneous approach.

Appendix: Description of the Products Mentioned in This Paper

- Cisco Secure Firewall ASA—The Cisco family of adaptive security appliances (ASA's) provides users with highly secure access to data and network resources - anytime, anywhere, using any device.

- Cisco Secure Firewall— The Cisco Secure Firewall portfolio delivers greater protections for networks against an increasingly evolving and complex set of threats.

- Cisco SecureX— SecureX is a cloud-native platform with XDR capabilities. It integrates the Cisco Secure portfolio with the client's whole security infrastructure, speeding detection, response, and recovery.

- Cisco Identity Services Engine (ISE)—The policy decision point for Zero Trust Architecture, ISE gathers intel from the stack to authenticate users and endpoints, automatically containing threats.

- Cisco Firepower NGFW—A Next-Generation Firewall (NGFW) that harmonizes policy and threat correlation across network, cloud, endpoints, email, web, and more; Enhances resiliency with superior threat defense against malware, with automatic daily security updates from Cisco Talos.

- Cisco Umbrella—A flexible cloud security solutions for users on and off the network offering flexible, cloud-delivered security. It combines multiple security functions into one solution, extending data protection to devices, remote users, and distributed locations anywhere.

- Cisco Secure Endpoint— Secure Endpoint offers advanced endpoint protection across control points, enabling businesses to stay resilient with powerful EDR and XDR capabilities.

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

Cisco has long established itself as the worldwide leader in technology that powers the internet, while building an open, integrated portfolio of cybersecurity solutions along the way. We believe that security solutions should be designed to act as a team. They should learn from each other. They should listen and respond as a coordinated unit. When that happens, security becomes more systematic and effective. Our customers have trusted us for years as both the world's largest provider of IT infrastructure and networking services and the world's largest enterprise cybersecurity business.

www.cisco.com