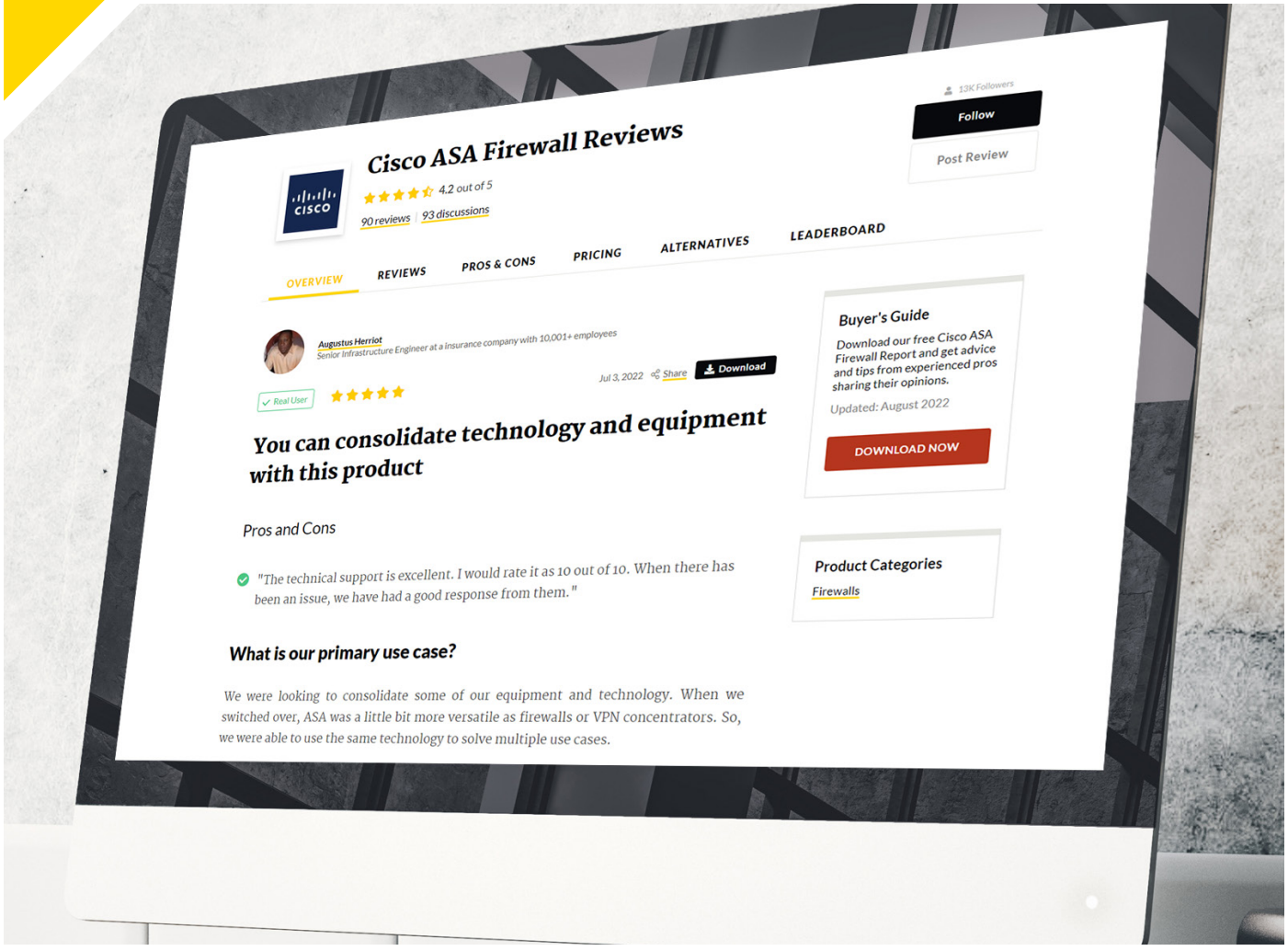
PeerPaper™ Report 2022

Based on Real User Reviews of Cisco Security Products

Assembling the Elements of a SecOps Strategy



PeerSpot

CSO

Contents

Introduction

Security Operations (SecOps) is where cybersecurity policy meets practical reality. SecOps teams are responsible for monitoring firewalls and other security tools, enforcing security policies, tracking threats and responding to security incidents and alerts. People, process, and technology must come together to enable SecOps to work. Ultimately, success with SecOps is about responding quickly, but also efficiently, to threats.

While each organization does SecOps in its own way, a consensus has emerged regarding the core elements of a SecOps strategy. In this paper, real users of Cisco security products on PeerSpot weigh in on what these elements are and how they work together to deliver effective SecOps. They include productivity, analytics, visibility, detection, incident response and more.

Except where noted, the companies described in this paper have fewer than 500 employees.

SecOps Overview

The term “security operations” refers to two overlapping areas of activity. In the broader sense of the term, SecOps refers to any type of work on the operational side of cybersecurity. This is distinct from cybersecurity policy, which is about setting the rules. SecOps is about enforcing those rules and defending an organization against malicious cyber actors.

The narrower, more commonly accepted view sees SecOps as a discrete team, or set of teams who use SecOps tools and processes to monitor cyber defenses and respond to cyber incidents. For some, SecOps is indistinguishable from the people and tooling that comprise the security operations center (SOC). On one side there are threat detection inputs, as shown in Figure 1, processed by the SecOps teams and leading to incident response workflows.

However one understands SecOps, the fundamental issues are always the same. SecOps is about mounting the most effective cyber defense, in operational terms, using the most economical allocation of resources. SecOps always involves the choreography of people and technology in the pursuit of a strong security posture.

Peace of mind

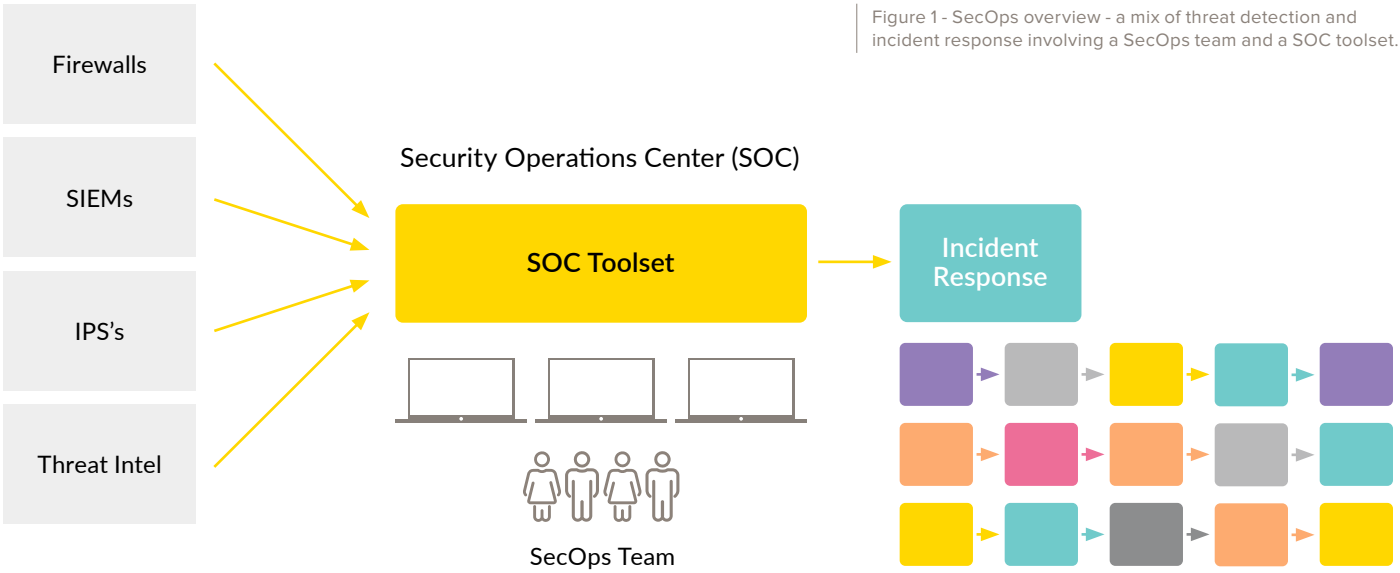


Figure 1 - SecOps overview - a mix of threat detection and incident response involving a SecOps team and a SOC toolset.

Elements of a SecOps Strategy

Despite the fact that the word "operations" is part of SecOps, it can be challenging to get a SecOps program running right. Success requires working from a complete, coherent SecOps strategy. The elements of such a strategy include concepts like productivity, visibility, alerting, threat detection and analytics. Automation and integration are critical, too, as are robust threat detection and incident response capabilities. All of these factors need to be thought through and aligned in their execution if SecOps is going to work as envisioned.

Productivity

There are never enough SecOps people. Whether the constraints come from budget or availability of trained personnel, this core reality of SecOps translates into a compelling need for SecOps team members to be as productive as possible. Achieving this goal is partly a matter of tooling, as the CEO of NPI Technology Management, a tech services company, explained. He said, "At the end of the day, the solution [Cisco Secure Firewall] offers good productivity enhancement to a company."

For a CISO / Associate Vice President - IT Infrastructure who uses Cisco Secure Firewall at a pharma/biotech company with more than 500 employees, being able to determine active versus inactive users led us to increased productivity through visibility. In their case, they found a return on investment (ROI) from their firewall due to improved productivity. Specifically, as he put it, "The change to Cisco Secure Firewall has reduced the time it takes for our network guy to generate our monthly report. It used to take him many hours where he can now have it done in an hour."

Provides application visibility and control

> **"Cisco Secure Firewall Management Center saves us time in terms of management and troubleshooting."**
>
> **Read review »**

"Cisco Secure Firewall Management Center saves us time in terms of management and troubleshooting," said a Network & Security Engineer at Oman LNG L.L.C., a natural gas company with more than 500 employees. He added, "Instead of individually deploying a policy on each firewall, we can easily push a policy to as many firewalls as we want by using Cisco FMC. We just create a policy and then select the firewalls to which we want to push it."

In quantitative terms, Cisco SecureX enabled Missing Piece BV, a tech services company, to reduce its workload by 20 to 30 percent, according to their Technical Team Lead Network & Security. He remarked, "We're 50 to 70 percent more efficient in investigations. It really saves a huge amount of manual checking. It has probably saved our compliance officer 10 percent of his time as well." A Technology Director at Shawnee Heights USD #450, an educational organization, felt that Cisco SecureX had saved his organization in between 30 to 40 percent in investigation tasks.

Intelligence and Data Analytics

Intelligence and data analytics are elements of a SecOps strategy because SecOps stakeholders need to be aware of how they are performing in the context of the overall threat environment. As a Cyber Security Practice Lead who uses Cisco SecureX at Eazi Security, a tech services company, explained, "SecureX definitely provides us with contextual awareness throughout our security ecosystem, since it allows us to integrate multiple threat intelligence feeds, as well as multiple security appliances and platforms. This enables us to have all the threat intelligence and threat event data in one place."

"Talos continuously enriches intelligence so that you get information about upcoming threats on time," said a Project Engineer who uses Cisco Secure Firewall at Telindus B.V., a tech services company. He elaborated, saying, "It's important that you have something in the background that is continuously enriching intelligence so that you get information about upcoming threats on time. That keeps you protected as soon as possible when a Zero-day happens."

> **"We're 50 to 70 percent more efficient in investigations. It really saves a huge amount of manual checking."**
>
> Read review »

> "The fact that you can have a single solution that combines endpoint intelligence with email intelligence, firewalls, and publicly available intelligence is really helpful."
>
> Read review »

Regular updating of intelligence was what stood out for an IT Administrator / Security Analyst who uses Cisco Secure Firewall at a healthcare company. "We get feeds every hour, automatically refreshed, and updated into the firewall," he said, then adding, "If I had to rely on one security intelligence, which I wouldn't, but if I had to, I'm sure it would be Talos. The fact that it gets hourly updates from Talos gives me some peace of mind."

When it comes to network security, a Network engineer at a manufacturing company praised Cisco Secure IPS's deep learning intelligence ability to filter packages and traffic coming to networks and to different workstations in networks. On a related front, Missing Piece's Technical Team Lead was pleased that Cisco SecureX combines multiple sources of security intelligence, "making it easy to correlate events in our environment with those outside of it. The fact that you can have a single solution that combines endpoint intelligence with email intelligence, firewalls, and publicly available intelligence is really helpful. I didn't expect there to be a product in which you can so easily change between the different parts of your security with a single click, allowing you to go from publicly available security intelligence into, 'How's it looking in my environment?'"

Visibility

SecOps team members need to see what's happening all around them. A Technical Consulting Manager who uses Cisco Secure Firewall at a consultancy with over 10,000 employees put it this way: "Firepower provides us with application visibility and control. We have a standard evaluation procedure with around 136 criteria. We have a team that does the evaluation and there were viruses reported."

A CSD Manager who uses Cisco Secure Firewall at BTC, a comms service provider with more than 5,000 employees, similarly commented, "The traffic inspection and the Firepower engine are the most valuable features. It gives you full details, application details, traffic monitoring, and the threats. It gives you all the containers the user is using, especially at the application level. The solution also provides application visibility and control."

Reports allow us to constantly monitor our environment and take corrective steps

Zero-day prevention and detection

The biotech CISO offered an example, saying, “Previously, with each application, we would prepare and develop a report based on our knowledge. E.g., there are a couple business units using the SAS application, but we lacked visibility into the application layer and usage. We used to have to configure the IP or URL to give us information about usage. Now, we have visibility into concurrent SAS/Oracle sessions.”

He went on to say that the solution gives his team more visibility into the inbound/outbound traffic being managed, which is a new experience. They find it effective because they are using Office 365 as their productivity tool. He said, “When users are accessing any of the Office 365 apps, this is directly identified and we can see the usage pattern. It gives us more visibility into our operations, as I can see information in real-time on the dashboards.”

Alerting and Reporting

Alerts and reporting are the lifeblood of SecOps. The tool-sets generate alerts and reports, and the SecOps workflows process them. SecOps analysts interpret them and react. As Oman LNG's Network & Security Engineer shared, "On one screen, we can see the whole firewall activity. We can see policies, backups, and reports. If our management asks for information about how many rules are there, how many ports are open, how many matching policies are there, and which public IP is there, we can log in to Cisco FMC to see the complete configuration."

"Standard reports allow us to constantly monitor our environment and take corrective steps," said a Head of Information Communication Technology who uses Cisco Secure Firewall at National Building Society, a financial services firm with over 1,000 employees. In particular, this user valued the reports generated according to the rules that his team put in place to either block traffic or report suspicious attempts to connect to the network. He said, "They would come standard with any firewall and we're always monitoring them and taking any corrective steps needed."

Ease of use matters in this context, as well. Missing Piece's Technical Team Lead related that his manager can "look at everything himself without him having to ask for me to create a report and without having to have access to the files themselves." This includes retrospective data. "He has a dashboard and can say, "I want to see the last week, last month, etc." He gets all the widgets and all the information for whatever period he wants. He can use that within his report to show the auditors how we're dealing with our security."

> **"On one screen, we can see the whole firewall activity... We can log in to Cisco FMC to see the complete configuration."**
>
> Read review »

> "The malware detection, threat defense, sandboxing, VPN, and mail security have all been valuable features of Cisco Secure IPS."
>
> Read review »

Threat Detection

Detecting threats is one of the main purposes of SecOps. In this regard, PeerSpot members acknowledged the value of solutions that enabled them to detect the presence of threats targeting their IT estates. For example, a Programming Analyst at a tech services company described Cisco Secure Firewall as "a stable, advanced threat detection solution with a straightforward setup." Specifically, the feature he found most valuable is the intrusion prevention system (IPS) advanced threat detection for removing ransomware and malware.

Other notable comments about threat detection include:

- "The anomaly detection capabilities are awesome." - Senior Network Security Engineer who uses Cisco Secure IPS at a wellness & fitness company with over 10,000 employees

- "You can do zero-day prevention and detection. It's quite useful." - Senior Network / ITOps Engineer who uses Cisco Secure IPS at a leisure/travel company

- "The malware detection, threat defense, sandboxing, VPN, and mail security have all been valuable features of Cisco Secure IPS." - Information Technology Manager who uses Cisco Secure IPS at Agricorp, a government agency

Incident Response

When a security incident occurs, the SecOps team needs to take action. Having the right tools helps incident response processes run smoothly—achieving the desired outcomes without expending excessive amounts of time or resources in the process. For instance, according to Missing Piece's Technical Team Lead, "The ribbon feature is quite useful. The solution is great at helping you maintain context around incidents as you navigate different consoles. It's immensely valuable due to the fact that, as you navigate between products and between pages, the ribbon stays with you. I can open a case there and I can also share it with my colleagues."

Eazi Security's Cyber Security Practice Lead likewise noted that the ribbon allows his team to do threat hunting and build a kind of casebook from their threat hunting investigation. He said, "We feel that SecureX Ribbon features will affect collaboration within our team or across teams. The ability to pivot between SecureX Cisco Threat Response and different Cisco security products from one location will make the business of investigating security events and threats easier."

Integration

Threat detection and incident response, among other SecOps workloads, require integration across multiple systems. This includes connecting SecOps tooling with detection equipment like firewalls as well as linking incident response solutions with email systems and beyond. For these reasons, integration is a key element of SecOps strategy.

Cisco Secure Firewall's automated policies definitely save us time

PeerSpot members spoke to this need, with a Deputy Manager who uses Cisco Secure Firewall at Star Tech Engineering Ltd, a computer software company, observing, "All Cisco security technologies have API integrations. We have all Cisco security products for all our customers integrated into SecureX for overall visibility of threat detections across all security appliances. Cisco Advanced Malware Protection is a good example. It is not just a product but a capability that has been integrated into multiple products or technologies."

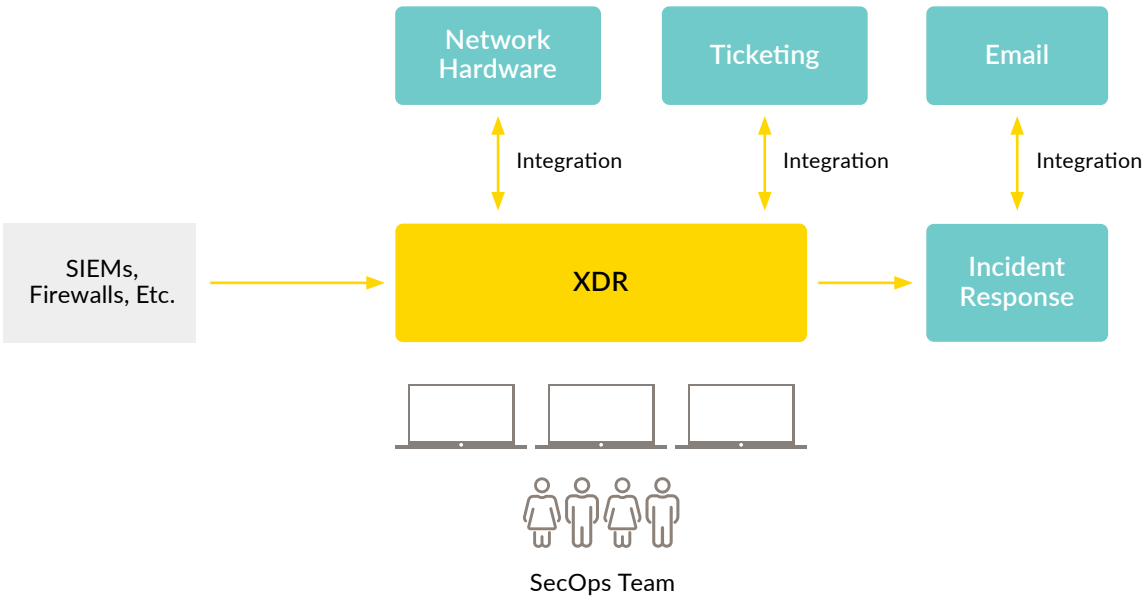


Figure 2 – integration between SecOps products like Extended Detection and Response (XDR) tools and network hardware, ticketing systems, email solutions and more is essential for effective SecOps.

As he further explained, “If a threat is detected in one place that can be blocked everywhere, almost at the same time, then the integration is very good. If we look at something like Cisco Umbrella, then we see Umbrella integrated with Cisco Meraki appliances, both on firewalls and access points. So, there does seem to be a good level of integration.” An Administrator who uses Cisco Secure Firewall at a university with over 1,000 employees simply stated, “It is a flexible solution and can be easily integrated with your network hardware. It is a very useful product.”

> "Automated policy application and enforcement saves significant time when adding devices, users, or new locations."
>
> Read review »

Automation

SecOps workflows achieve their objectives best when they include automated processes. As it is with so many areas of SecOps, technology needs to make up for a lack of people. BTC's CSD Manager framed the issue by saying, "Automated policy application and enforcement saves significant time when adding devices, users, or new locations."

He offered an example, which involved a bank needing to deploy more branches. Automation saves time in this kind of situation. He added, "When you add more users or you add more devices, when you create a profile of the policies, they will be available in a matter of minutes, regardless of the number of branches or users or applications. It reduces the time involved in that by 75 percent."

Other users revealed that automation saved them time, with Star Tech Engineering's Deputy Manager saying that Cisco Secure Firewall's automated policy application and enforcement "have freed up time for us, on the order of 30 percent." A Network Specialist at a financial services firm with more than 500 employees concurred, saying that Cisco Secure Firewall's automated policies "definitely save us time. I would estimate on the order of two hours per day." Automation saved the Technical Consulting Manager 90% of his team's time.

Conclusion

There is no single factor that will make a success of SecOps. Rather, a strong SecOps program will be one that brings together people, process and technology to enable fast, accurate and efficient detection and responses to threat. In practice, this means building a SecOps capability out of the core elements of SecOps strategy. For PeerSpot members who use Cisco security products, SecOps strategy involves tooling that facilitates user productivity through automation, integration and visibility. The toolset has to provide intelligence and data analytics, alerting and reporting. The right mix of these elements will lead to effective threat detection and incident response—working toward the strengthening of the SecOps capability and the overall improvement of an organization's security posture.

Appendix: Cisco 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 Management Center** — The Cisco Secure Firewall Management Center (FMC) is an administrative nerve center for managing critical Cisco network security solutions. It provides complete and unified management over firewalls, application control, intrusion prevention, URL filtering, and advanced malware protection.

- **Cisco Secure IPS** — The Cisco Secure IPS (formerly known as Firepower Next-Generation IPS) provides network visibility, threat intelligence, automation and industry leading threat effectiveness used to protect the network where the firewall can't go.

- **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.

About PeerSpot

PeerSpot (formerly IT Central Station), 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

About Cisco

Cisco has long established itself as the networking leader, while building an open, integrated portfolio of cybersecurity solutions along the way. 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, easy to manage, and easy to use – and that it all works together.

We're driven by the fact that people and our customers are at the heart of what we do. Cisco Secure empowers the security community with the reliability and confidence that they're safe from threats now and in the future on the SecureX platform. We help 100 percent of the Fortune 100 companies protect what's now and what's next with the most comprehensive, integrated cybersecurity platform on the planet. Learn more about how we simplify experiences, accelerate success, and protect futures at cisco.com/go/secure.