Secure

Securing What's Now and What's Next

20 Cybersecurity Considerations for 2020

Contents

Introduction

Security leaders, while supporting business growth and digital transformation, struggle with a multitude of challenges. We know this because you tell us, both in ongoing conversations and as part of our annual benchmark survey. Some challenges are focused on security, such as needing better visibility or automation, or striving for greater simplicity of management and response. Some are related to the success of your business, such as wanting to support growth and transformation no matter which cloud application is needed, or which mobile device is being used. Other challenges relate to making investments now that will remain relevant into the future as your organization changes.

And all of that is in addition to the everyday demands of the day job, such as detecting and blocking advanced threats. It's difficult to manage sophisticated threat actors and the ever-expanding attack surface at the same time. Your challenges go beyond just having to do more with a limited budget, and extend into maintaining brand reputation, board and stockholder confidence, and recruiting expertise to match cyberattack tactics, techniques and procedures (TTPs), to name a few.

You have to provide users the access they need while meeting these security, complexity, and budget challenges. You also need to lower technology overhead, avoid major breaches, hunt down threats before they infiltrate your network and exfiltrate your data, spend security budget smarter, and win over more customers.

According to the World Economic Forum, cyberattacks are perceived as the #2 global risk of concern to business leaders in advanced economies, second only to fiscal crises.[1]

By conducting our sixth annual survey of 2,800 IT decision makers from 13 countries, we've continued our annual tradition of going deep into your world to compile key benchmark statistics.[2] We also spoke at length to a panel of CISOs to analyze the findings and build a list of 20 considerations for 2020. This report provides valuable takeaways and data you can share with other members of your C-suite, or your board of directors, to make concrete recommendations for improving your organization's security posture.

Because we know there's nothing certain except uncertainty in this industry, we styled this report's sections as questions you might be asking yourself as you prepare for the year ahead. If these questions resonate with you, or provoke additional areas of inquiry, we'd love to hear from you at security-reports@cisco.external.com. Meanwhile, we hope the report will help you navigate this year's security challenges.

To see all of the reports in our Cybersecurity Report Series, go to: cisco.com/go/securityreports.

---

[1] "This is what CEOs around the world see as the biggest risks to business," World Economic Forum, 2019
[2] Countries surveyed are Australia, Brazil, Canada, China, France, Germany, India, Italy, Japan, Mexico, Spain, the UK, and the U.S.

20 Cybersecurity Considerations for 2020

1. Who in your organization provides executive support and clear focus?

Over the years in our survey, we've measured four critical practices for fostering a mutually beneficial relationship between executives and the security organization. This exercise evaluates top-down security buy-in, where we've found a slight downward trend from last year. Looking at these results:

· Eighty nine percent of respondents said that their **executive leadership still considers security a high priority;** however, this is down slightly (7%) across the preceding four years.

· The percentage of organizations who have **clarified the security roles and responsibilities within the executive team** has fluctuated over the past few years – landing at 89% this year. Considering cybersecurity's growing visibility and the dire need for security leaders at top levels, clarifying roles and responsibilities needs to remain high.

· The incorporation of cyber risk assessments into overall risk assessment processes is down by 5% from last year, but is still high with 91% of respondents saying they use them.

· Although down by 6% from last year, executive teams establishing clear metrics for assessing the effectiveness of security programs is still rather high with 90% of our respondents doing so.

Over four years, these responses are slightly down, which may indicate: 1) that the scope of security responsibility is changing, 2) that communication with the executive team isn't as clear as it used to be, 3) that executive management has other business priorities, or 4) that CISOs and executives are re-evaluating their metrics.

And although these numbers are down, they are still very high. Perhaps this is because security has now become operationalized, but requires a greater voice at the executive table. **The fact that the numbers are still very high indicates a continuing strong relationship between executives and security professionals.**

Every organization is different in terms of the executive makeup – and there are many different styles of executive leadership. The role of a CISO is to have conversations and engage with the business by demonstrating that well-designed security will give value back to the business.

Mick Jenkins MBE, CISO for Brunel University London

2. How might you decide which metrics matter most?

As we just noted, 90% agreed their organization's executives had established clear metrics for assessing the effectiveness of their security program. Establishing clear metrics is an integral activity for a security framework, and it isn't an easy task to agree across multiple executives and security teams how to measure operational improvement and security outcomes.

IT decision-makers responding to our survey rated **time-to-detect highest as a key performance indicator (KPI). However, when you're reporting to the C-suite or board of directors, time-to-remediate ranks just as important,** as it represents an aggregate of total impact that may include: system downtime, records affected, cost of investigation, lost revenue, lost customers, lost opportunities, and out-of-pocket costs (Figure 1). It can also be a proxy metric for the overall effectiveness of the IT organization, as remediation can require a lot of collaborative work across departments.

Figure 1: Metrics used to report an impactful breach internally to the C-suite or board of directors (N=2800).

Metric	Value
Time to detect	56.6%
Time to patch	52.0%
Time to contain	52.4%
Time to remediate	57.2%
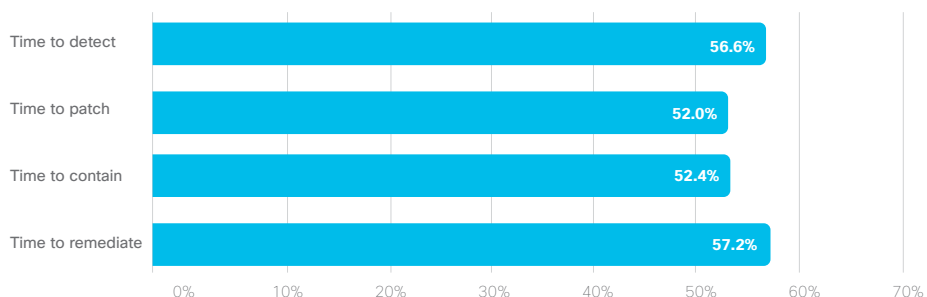
Source: Cisco 2020 CISO Benchmark Survey

3. What primary considerations drive spending on a limited budget?

Predominantly, we heard that the best way to allocate security spend is through outcome-based objectives and metrics. Sixty one percent are using this planning method, a 10% increase from the previous year and an encouraging trend (Figure 2).

Figure 2: What organizations use to determine and/or control security spending (N=2799). Percentages are rounded.

Source: Cisco 2020 CISO Benchmark Survey
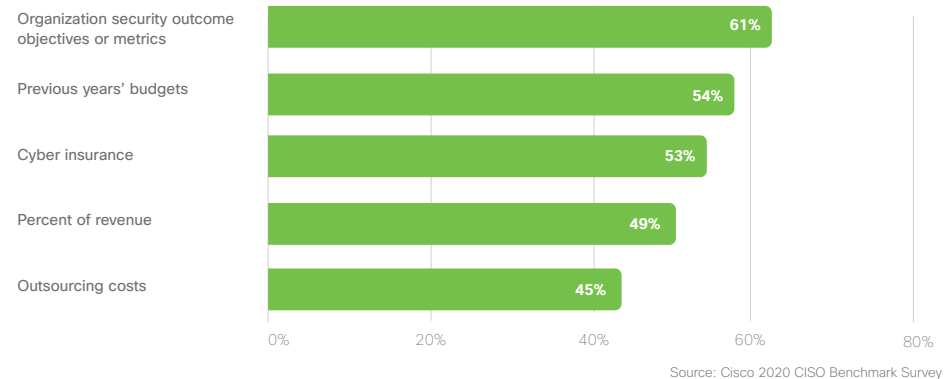
'Percent of revenue' and 'outsourcing costs' were the least used factors to determine security budgets. Fifty-four percent base spending on the previous years' budget. Although this may not seem like a precise way to quantify security costs – especially when the average cost of a data breach globally ($3.92M) is rarely factored in – if your budget is flat year over year or you have predictable SaaS subscriptions, your forecasted budget will probably see very little change.[3]

---

[3] [2019 Cost of a Breach Report](), Ponemon Institute

When incidents are detected, you must quickly determine root cause (i.e., Respond and Recover) — but just as importantly understand the long-term fix that may be architectural in nature. You then need to address Identify, Protect, and Detect to prevent future incidents.

Marisa Chancellor, Senior Director,
Security & Trust Organization, Cisco

4. What's the right balance for spending on trust verification and threat detection?

In exploring how security budgets are spent, we surveyed our respondents on five categories (Identify, Protect, Detect, Respond, and Recover) that describe the lifecycle of cybersecurity defense and breach management:

· **The category Identify** saw a rise in expenditures from 21% to 27% from 2019 to 2020

· **Protect and Detect** remained basically the same at 25% and 18% respectively

· **Spending in the Respond and Recover categories** declined somewhat in the same timeframe to 15% and 14% respectively

Figure 3:   Security spending by lifecycle category. Percentages are rounded.
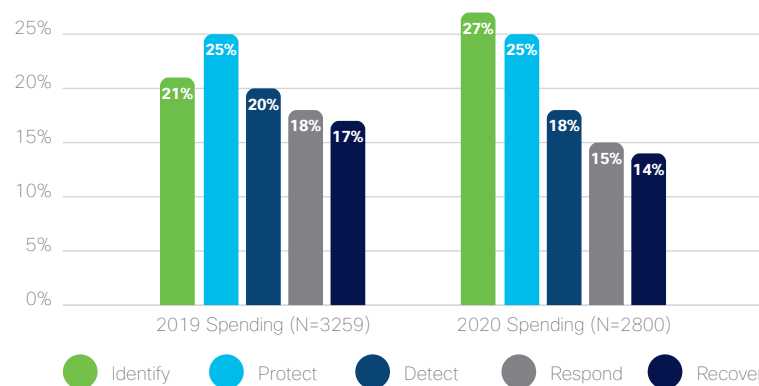
Source: Cisco 2020 CISO Benchmark Survey

This trend shows that **organizations are spending more on prevention versus being reactive** in their cybersecurity posture. Enterprises are always trying to find the right balance between being proactive and being responsive and resilient, and that pendulum swings back and forth every year. Last year, organizations may have been concentrating their efforts on the basics (asset inventory, discovery, etc.). And theoretically, if you spend right on Identify, Protect and Detect up front, you shouldn't need to spend as much on Respond and Recover, as they aren't needed as often.

5. What can measuring the business impact of security breaches tell you?

In our survey, we asked about various breach impacts including downtime, records, and finances.

To what extent are organizations having to endure downtime from major breaches? We compared different organizational sizes, and the results were very similar across the board. Large enterprises (10K or more employees) are more likely to have less downtime (0-4 hours), as they will likely have more resources available to help respond and recover. Small to mid-sized organizations dominated the 5-16 hour recovery timespan, and catastrophic downtimes of 17-48 hours were similarly low for organizations of all sizes (Figure 4).

Figure 4: For the most severe security breach managed in the past year, the number of hours systems were down correlated with organizational size (N=2265). Percentages are rounded.

Hours of downtime   ● 0-4 hours   ● 5-16 hours   ● 17-48 hours
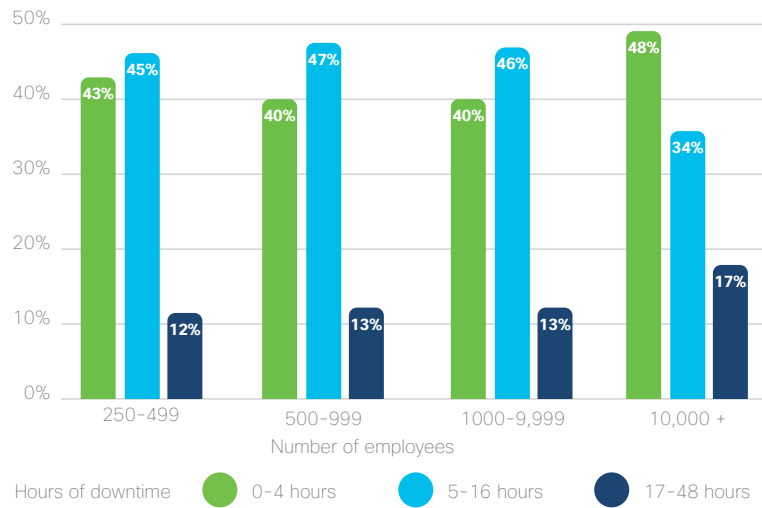
Source: Cisco 2020 CISO Benchmark Survey

Organizations having more than 100,000 records impacted from their most severe data breach rose from 15% last year to beyond 19% this year.

In addition, as Figure 5 shows, a major breach can impact nine critical areas of an organization. **The most impacted business areas were operations and brand reputation,** followed by finances, intellectual property, and customer retention.

Figure 5: Percentages of respondents claiming business areas that were negatively impacted by a breach. (N=2121). Percentages are rounded.

Source: Cisco 2020 CISO Benchmark Survey
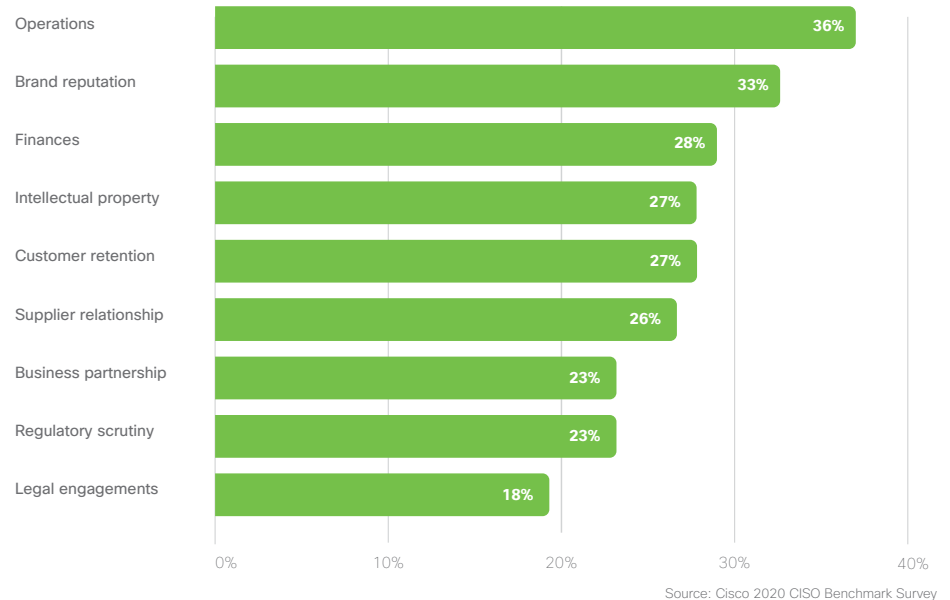
Looking at previous years, we see that the number of respondents experiencing a hit to **brand reputation from major breaches has risen from 26% to 33% in three years.** Those experiencing an impact to operations has remained steady between 36–38% of respondents. And those experiencing an impact to finances has decreased just one percentage point per year for the last three years – so also remaining relatively steady. With the impact to the overall brand on the rise, **it's crucial to include crisis communications planning into your overall incidence response plan.**

6. Why is voluntary breach disclosure at an all-time high?

At 61%, the percentage of survey respondents reporting that they voluntarily disclosed a breach last year is at the highest level in the previous four years. This shows that, overall, organizations are proactively reporting breaches, perhaps as a result of new legislation – or maybe from increased social consciousness and a desire to maintain customer trust.

The upside to this is that more than double the number of organizations that experienced a breach that lasted over 17 hours disclosed the breach voluntarily versus those that disclosed the breach involuntarily or due to reporting requirements.

More than half of all breaches (51%) put organizations on the defensive, having to manage the public scrutiny that comes with a breach. But while governmental reporting requirements have increased, involuntary disclosure remains largely the same at just over a quarter (27%) of breaches. **And 61% of respondents are now finding that their credibility rises when they voluntarily disclose a major breach, thus preserving their brand reputation.**

7. Can you quantify collaboration benefits between networking and security?

Collaboration between **network and security teams remains high** with more than 91% of respondents reporting that they're very or extremely collaborative in this year's survey. Collaboration between **endpoint and security teams also remains high at 87%**. Despite dropping a couple of percentage points in these areas, the overall trend is that you're less likely to work in silos.

8. What reasons do you observe other than cost reduction for outsourcing?

Compared to last year's report, outsourcing has increased significantly, possibly indicating a historical trend as vendor landscapes become so complex to manage in-house. Interestingly, organizations reported that they're expecting their outsourcing to decrease in the future.

Our respondents are outsourcing for a variety of core reasons, and it's not only cost. Cost efficiency is marginally ahead as the number one reason at 55%. However, it's quickly followed by security teams that want more timely responses to incidents (53%).

I see an increase in response exercises to data breaches, including playbooks that lay out the process and who needs to be able to talk to the press, what they should be saying. It inevitably starts at the highest of levels, but it's about the role that everybody in the enterprise can play post-breach, at the most dangerous time when everybody is looking for answers. That's a time for very cool heads to revert to well-practiced responses.

Steve Durbin, Managing Director, Information Security Forum
https://newsroom.cisco.com

9. Does preparation pay off for you?

When asked which security practices or policies apply to their organizations, we found that **those respondents who practiced the items listed below more frequently had lower major breach costs.** In other words, if the following six practices align with your security program, your breaches are more likely to stay below $100K.

· We review and improve our security practices regularly, formally, and strategically over time
· We regularly review connection activity on the network to ensure that security measures are working as intended
· Security is well integrated into our organization's goals and business capabilities
· We routinely and systematically investigate security incidents
· Our security technologies are well integrated to work effectively together
· Our threat detection and blocking capabilities are kept up to date

10. How critical is patching in breach defense?

A key concern for 2020 is that 46% of organizations (up from 30% in last year's report) had an incident caused by an unpatched vulnerability. In addition, **those that had a major breach due to an unpatched vulnerability last year experienced higher levels of data loss** (Figure 6). For example, 68% of organizations breached from an unpatched vulnerability suffered losses of 10,000 data records or more last year. For those who said they suffered a breach from other causes, only 41% lost 10,000 or more records in the same timeframe.

Figure 6: Respondents were asked if they experienced a security incident that resulted from an unpatched vulnerability in the last year, or from other causes, correlated with the number of data records lost (N=2053). Percentages are rounded.

Source: Cisco 2020 CISO Benchmark Survey
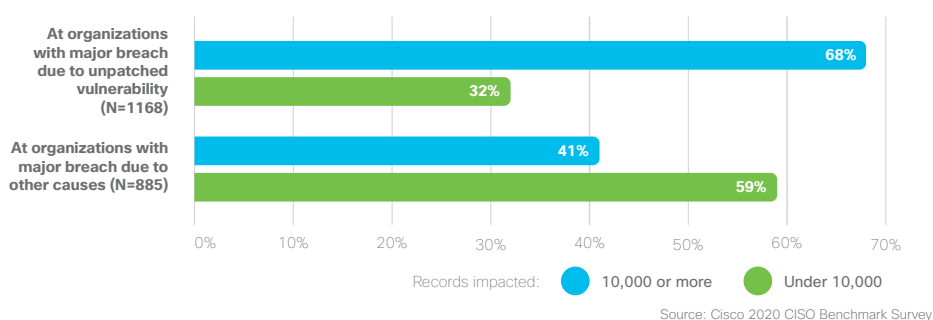
It's well known that patching can be difficult and cause disruptions. However, these results show that there is a tangible ROI in implementing a minimum baseline policy for the most recently released patches. **Organizations should maintain an up-to-date inventory of all devices in their environment and perform a risk analysis for any missing patches. Then, create a change management process to enforce version control and documentation.**

11. What causes downtime?

As shown earlier, respondents reported a range in hours of downtime. When asked for the most common cause of downtime, malware and malicious spam come in as the first and second most common. Interestingly, the third cause diverges depending on the length of downtime. For breaches with downtime between 0-4 hours, phishing is the third most common cause. For downtime between 4-24 hours, it's spyware. For anything over 24 hours, it's ransomware.

Significantly, ransomware doesn't discriminate; it was the most destructive threat for both small and enterprise organizations in terms of downtime. The large amounts of resultant downtime may be due to the depth of investigation needed to assess the damage, attempt to restore backups, and fix the entry vectors.

For more insights into how to deal with various types of attacks, subscribe to our Talos Threat Intelligence blog.

12. How challenging is it to protect the mobile workforce?

We asked our survey respondents to tell us how difficult it is to protect various aspects of their infrastructure. **More than half (52%) told us that mobile devices are now very or extremely challenging to defend.** They've overtaken user behavior, which was the biggest challenge from last year's report.

With a zero-trust framework, you can identify and verify every person and device trying to access your infrastructure. Zero trust is a pragmatic and future-proof framework that can help bring effective security across your architecture – spanning the workforce, workload, and workplace.

A zero-trust framework achieves these three success metrics, among others:

· The user is known and authenticated
· The device is checked and found to be adequate
· The user is limited to where they can go within your environment
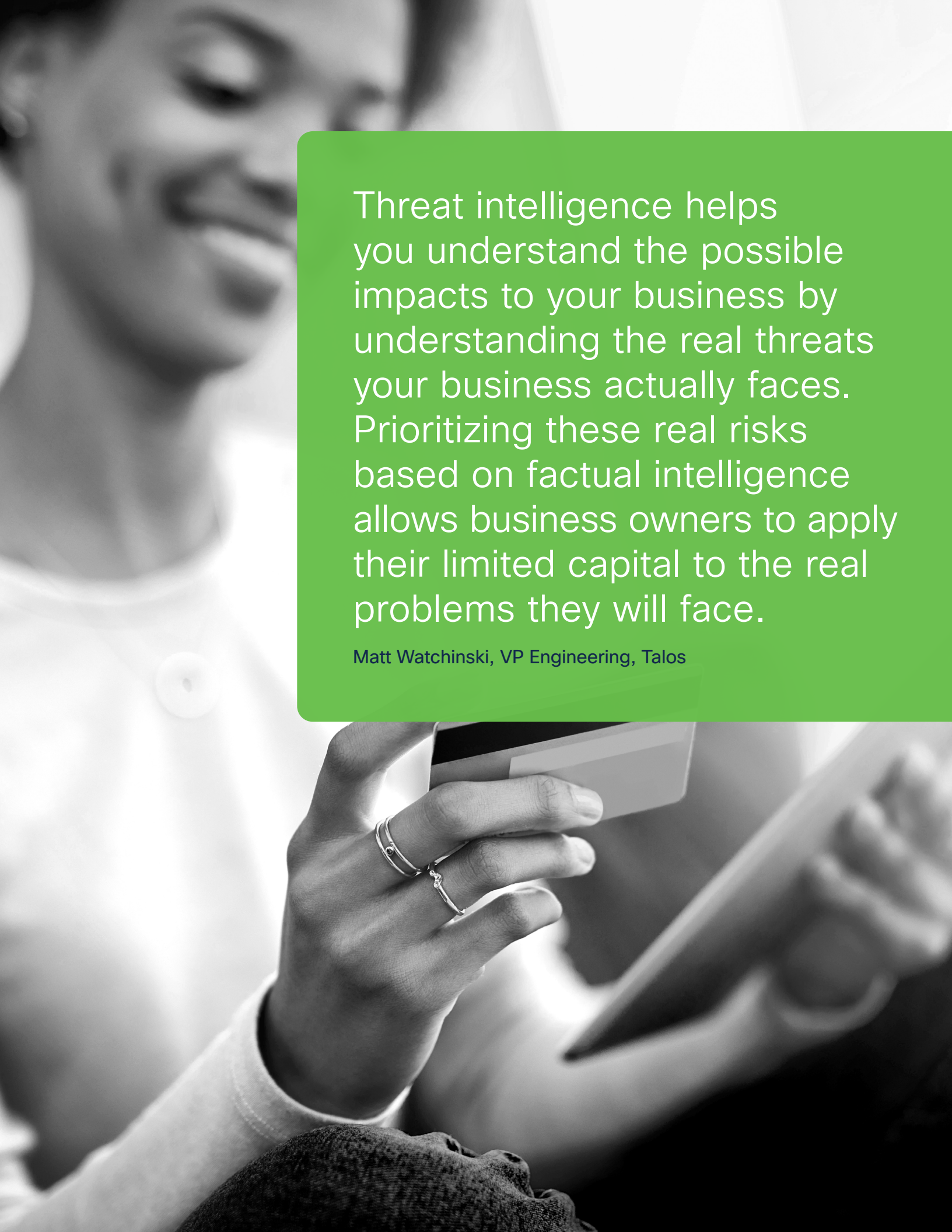
Having zero trust in place removes much of the guesswork in protecting your infrastructure from all potential threats, including mobile devices.

13. How might you extend zero trust to secure applications?

Workload security is about securing all user and device connections across your network. A zero-trust framework can identify the dependencies within and around databases and applications to apply micro-segmentation and contain lateral movement.

Forty-one percent of our surveyed organizations find data centers very or extremely difficult to defend, and 39% say they are really struggling to secure applications. The most troublesome aspect is data stored in the public cloud, with 52% finding it very or extremely challenging to secure.

A zero-trust framework provides you visibility into what's running – and what's critical – by identifying and enforcing policies throughout your network. It also alerts you in the case of a policy violation through continuous monitoring and response to indicators of compromise.

Threat intelligence helps you understand the possible impacts to your business by understanding the real threats your business actually faces. Prioritizing these real risks based on factual intelligence allows business owners to apply their limited capital to the real problems they will face.

Matt Watchinski, VP Engineering, Talos

14. Is defending the network infrastructure still challenging?

Private cloud infrastructure is a top security challenge for organizations. (Fifty percent of organizations find it very or extremely difficult to defend.) With regards to network infrastructure, 41% of organizations find this very or extremely challenging to defend.

Here is where a zero-trust framework delivers value. It includes maintaining software-defined access control over all the connections within your apps and across a multi-cloud environment based on user, device, and application context, not location. This model allows you to mitigate, detect, and respond to risks across your infrastructure – regardless of distribution or location. Shown below are defined framework stages to develop zero-trust security maturity.

Developing a Zero-Trust Security Maturity Model

At Cisco, we employ five transformational steps for our customers to adopt as a structure to implement a **zero-trust framework** for their organization:

Stage 1: Do you have a clear identity and access management (IAM) strategy aligned with your business needs that has resulted in a full implementation and integration of a multi-factor authentication (MFA) solution supported by risk-based policies?

Stage 2: Do you have an up-to-date asset inventory that distinguishes between managed and unmanaged devices, providing a hygienic check on them as part of an integrated IT and security function?

Stage 3: Do you have a trusted device policy that prompts users to update their devices against measured vulnerabilities — within a managed process — and reports on out-of-policy devices?

Stage 4: Do you control user access through a centrally managed policy that identifies and acts upon exceptions?

Stage 5: Do you have a business-aligned zero-trust strategy supported by an architecture and set of processes that enables users to seamlessly access both on-premise and cloud applications?

15. Can you measure the impact of vendor consolidation?

The trend to reduce complexity through vendor consolidation continues, holding steady with **86% of organizations using between 1 and 20 vendors, and only 13% using over 20** (Figure 7).

Figure 7: The number of different security vendors (i.e. brands, manufacturers) used within respondents' security environments (N=2800). Percentages are rounded.

Source: Cisco 2020 CISO Benchmark Survey
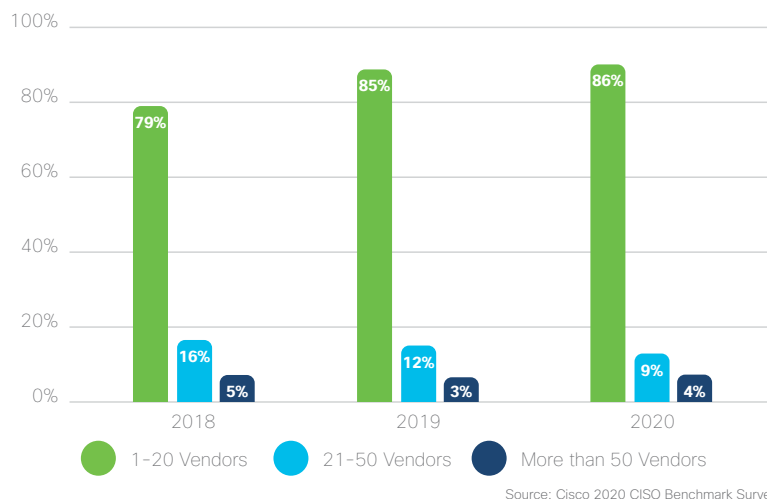
Since 2017, there have been some changes in how organizations feel they're coping with a multi-vendor strategy. **Twenty-eight percent now feel that managing a multi-vendor environment is very challenging, which has increased by 8% since 2017. Fifty-three percent now find that it's somewhat challenging.** Fewer organizations (down from 26% to 17%) find it easy to manage a multi-vendor environment. Most organizations are now in the 'finding it challenging' categories (81%). This might mean that you have fewer vendors to manage or that you have started to use tools such as analytics engines to improve results from multiple, disparate tools.

We also looked at trends between alerts within a multi-vendor environment and the impact they have on cybersecurity fatigue (which we explore a little further in the next topic). **Defined as virtually giving up on proactively defending against malicious actors, 42% of respondents are suffering from cybersecurity fatigue.**

Our data showed that, for the organizations who are suffering from cyber fatigue, they are far more likely to find a multi-vendor environment challenging. Alongside having to respond to too many alerts and struggling with vendor complexity, we found that having a more impactful breach (in terms of the number of hours of downtime) also increases cyber fatigue. But with over 96% of fatigue sufferers saying that managing a multi-vendor environment is challenging, **complexity appears to be one of the main causes of burnout.**

I don't want to spend my time integrating security products. I just want to do security.
I tell my team I want to see three things when it comes to a new product:

· Make sure it works
· Make sure it gives me full visibility
  No black holes
· Make sure it's integrated with the
 rest of our security ecosystem

Steve Martino, SVP, Chief Information and Security Officer, Cisco

16. What are the causes of your cybersecurity fatigue and burnout?

In the previous section, we began to see a relationship between multi-vendor environments and growing cyber fatigue. Now, we'll take a look into the average volume of daily security alerts an organization receives.

The overall number of daily alerts you are dealing with has increased over previous years. In 2017, 50% of organizations were receiving 5,000 or fewer daily alerts; now only 36% are in this category. And the amount of organizations who receive 100,000 or more daily alerts has grown from 11% in 2017 to 17% in 2020 (Figure 8).

Figure 8:   Reported number of alerts received (N=2800). Percentages are rounded.
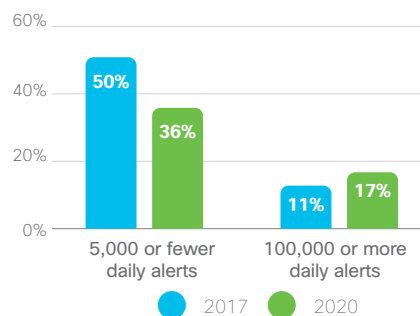
Source: Cisco 2020 CISO Benchmark Survey

Perhaps because of this increase in volume and the processing resources needed, alert investigation is at its lowest level in over four years at just under 48%. (The number was 56% in 2017, and it's been decreasing every year since.) The rate of legitimate incidents at 26% is consistent year-over-year and suggests that many investigations are turning up false positives.

On a positive note, the number of legitimate threats that are remediated has improved since last year's report, and we're now back to 2017 levels at 50%. However, this still means that half of all real incidents are being left unattended.

Notably, the overwhelming number of alerts is having an impact on cybersecurity fatigue. **Of those who say they are suffering from cyber fatigue, 93% of them receive more than 5,000 alerts every day.**

To deal with the increasing noise and volume of alerts, we advocate for an approach that has automation at its heart. Automation enables policies to be enforced more consistently, quickly, and efficiently. When a device is determined to be infected or vulnerable, it's automatically quarantined or denied access with no action required from an administrator.

17. What security benefits are associated with hosting infrastructure in the cloud?

Through our research, we've found that increased effectiveness, efficiency, and visibility are some of the main drivers for organizations to move their security (88%) and infrastructure (89%) to the cloud. And it's not surprising to see that **86% say utilizing cloud security has increased visibility into their networks.** In 2020, we continued to see more than 83% of organizations managing more than 20% of their IT infrastructure in the cloud (whether internally or externally).

Clients increasingly depend on vendors to dig deeper into incidents, providing advanced analytics and detailed forensics reporting. This requires IR providers to bring highly specialized combinations of products and processes to reduce the mean time to contain (MTTC) and mean time to remediate (MTTR) an active incident.

Market Guide for Digital Forensics and Incident Response Services, Gartner, December 2019[4]

---

[4] Brian Reed, Toby Bussa, Market Guide for Digital Forensics and Incident Response Services, Gartner, Dec 11, 2019

18. What challenges do you think the future holds?

Although presenting a tsunami of infrastructure change that can be challenging to implement, digital transformation continues to present itself as an opportunity for IT and security leaders to innovate and gain competitive advantage.

Security practitioners are embracing advanced technologies and approaches, from artificial intelligence and machine learning, to securely implementing DevOps and micro-segmentation. And as we all know, multi-cloud environments continue to be prevalent.

Given the dynamic nature of this environment, security professionals need to not only master the basics, but also stay current with the newer technologies available to them. Arguably, some of these newer technologies should become a staple in your security ecosystem — even if they aren't currently.

For example, we see that in this age of digital ubiquity, **only 27% of organizations are currently using multi-factor authentication (MFA).** This number is low for such a valuable zero-trust technology. Survey respondents from the following countries showed the highest adoption rates of MFA in this order: USA, China, Italy, India, Germany, and the UK. The industries with the highest adoption rates (in this order) are software development, financial services, government, retail, manufacturing, and telecommunications.

With regards to digital transformation, in addition to cloud adoption, automation is the big winner here. Many security practitioners are realizing the benefits of automation for solving their skills shortage problem as they adopt solutions with greater machine learning and artificial intelligence capabilities.

As Figure 9 illustrates, **a majority (77%) of our survey respondents are planning to increase automation to simplify and speed up response times in their security ecosystems.** When planning to automate, you should strategically define where automation will be most effective and provide the highest ROI within your organization.

Figure 9:   Those with plans to increase the use of automation across their organization's security ecosystem over the next year (N=2800). Percentages are rounded.

77%	Yes
18%	No
5%	Don't know

Source: Cisco 2020 CISO Benchmark Survey

19. How much focus should you place on incident response?

The threat landscape has evolved into a complex, challenging environment for organizations everywhere. A talent shortage, combined with increased incidents, has led to a generally weak security posture among most organizations. Sitting back and waiting for an alert to fire can bring stiff fines, increased scrutiny, lost intellectual property, data privacy concerns, and lost business. Prevention by gaining visibility, performing threat hunting, and establishing a zero-trust framework is now critical for protecting your infrastructure.

In our survey of IT decision-makers, **76% considered themselves to be very knowledgeable about incident response, and 23% said they were somewhat knowledgeable – together totaling 99%.** That's the good news. But as our survey found, the complexity of security is creating cybersecurity fatigue – and that could be straining your hard-to-gain resources. This is where outsourcing can help.

Figure 10: Percentages of survey respondents who are very and somewhat knowledgeable about incident response totaling 99%. N=2800. Percentages are rounded.

76%	Very knowledgeable
23%	Somewhat knowledgeable

Source: Cisco 2020 CISO Benchmark Survey

We found that 34% of you are outsourcing incident response services, and 36% are using external/third-party services to analyze compromised systems, which has risen from last year. Using an incident response service has become an efficient approach for protecting assets, mitigating risk, and maintaining compliance. It can help your organization protect against the unknown by having proactive planning and expertise to coordinate and carry out a response.

Want to learn how to grow careers in cybersecurity for you or your staff?

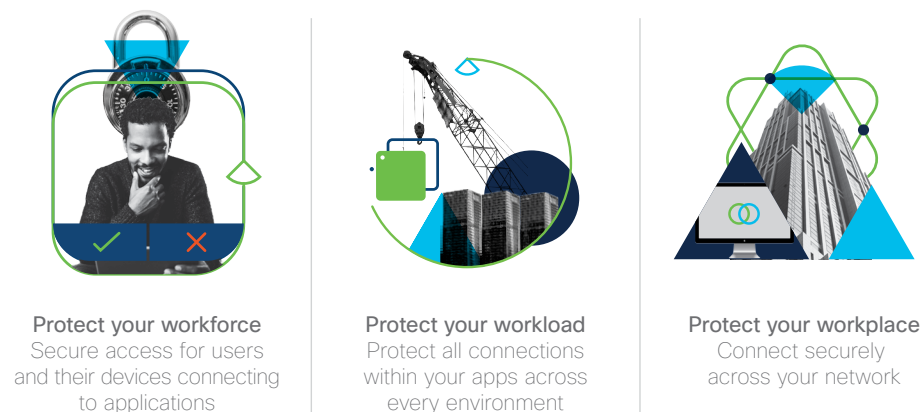Visit: Cisco Security Certifications.

20. What can you do now to drive improvements in your security posture?

You're up against active adversaries who are well-funded and endlessly patient. You're also dealing with perennial challenges that never seem to go away, like keeping an accurate inventory of users, applications, and devices. You're juggling business risk alongside security risk while empowering teams to move fast. Yet business decisions continue to be made without security in mind. And when you throw in new regulations, board mandates, tight budgets, risk management, and a revolving door of security talent, the grind never stops.

The challenges in defending your organization are accelerating, and they're not going to let up. It's time to work smarter, streamline defense, and focus on prevention as well as detecting and remediating threats. In this report, we've provided 20 areas you can consider to help you run your organization more securely. With them, we've provided recommendations that can be summarized as:

- Employ a layered defense, which should include MFA, network segmentation, and endpoint protection

- Gain the highest levels of visibility to bolster data governance, lower risk, and increase compliance

- Shore up defenses, update and patch your devices, and focus on cyber hygiene through drills and training

- Improve your security maturity by building a zero-trust framework (Figure 11).

Figure 11: A zero-trust strategy can secure workforce, workload, and workplace.

Protect your workforce
Secure access for users and their devices connecting to applications

Protect your workload
Protect all connections within your apps across every environment

Protect your workplace
Connect securely across your network

At Cisco, we believe it's time for the security industry to evolve. Security solutions should work like a team. Teams communicate in real time, learn from each other, and respond as a coordinated unit. Your endpoint security must work with your network security and cloud security, and you need MFA that covers identity and access. **We believe that truly securing your business is best accomplished through a platform approach to ensure all gaps have security coverage.**

Securing What's Now and What's Next

Our vision is to protect our customers from the threats of today and tomorrow so that they can focus on their core mission and leave the security to us.

Introducing the Cisco Security Platform – SecureX – created by the strongest security team on the planet, offering the protection you need for the way your business works.

- We start with **best of breed solutions,** protecting the network, endpoint, applications, and cloud
- We use **trust verification** to ensure that only the right people gain access to your network
- We back each product with industry-leading Talos **threat intelligence** to block more threats and keep organizations safer
- We provide **automated responses to advanced threats** and **streamline operations with integrated threat and security management** throughout our portfolio
- **We build our solutions to work with the other technologies you have in place –** even outside of Cisco – for integrated security responses

SecureX delivers visibility, automated actions, and improved security posture. Tailored, cloud-delivered applications have also been built on top of the **SecureX platform** to drive the complexity out of security. We connect Cisco's integrated security portfolio and third-party products from the customer's environment to a consistent interface. And platform-level innovation from Cisco offers the most integrated analytics on the planet. All working together:

- SecureX unites security, network, and IT operations teams with collaborative workflows to improve productivity
- Cisco Threat Response simplifies threat investigations and remediation to improve SecOps efficiency
- Analytics simplify the detection of unknown threats to improve policy decisions, response times, and threat response efficacy

With our integrated portfolio and industry-leading threat intelligence, Cisco gives you the scope, scale, and capabilities to keep up with the complexity and volume of threats. Putting security above everything helps you innovate while keeping your assets safe. Cisco prioritizes security in all that we do. Only with Cisco can you attain effective network security to face tomorrow's evolving threats. Find out more about our platform approach at cisco.com/go/security.

About the Cisco Cybersecurity Report Series

Throughout the past decade, Cisco has published a wealth of definitive security and threat intelligence information for security professionals interested in the state of global cybersecurity. These comprehensive reports have provided detailed accounts of threat landscapes and their organizational implications, as well as best practices to defend against the adverse impacts of data breaches.

Cisco Security now publishes a series of research-based, data-driven publications under the banner Cisco Cybersecurity Series. We've expanded the number of titles to include different reports for security professionals with different interests. Calling on the depth and breadth of expertise of threat researchers and innovators in the security industry, the reports in each year's series include the Data Privacy Benchmark Study, the Threat Report, and the CISO Benchmark Study, with others published throughout the year.

For more information, and to access all the reports and archived copies, visit www.cisco.com/go/securityreports.

2019 Data Privacy	2019 Threat Report	2019 CISO Benchmark	Email: Click with Caution
Security Bottom Line	Threat Hunting	Consumer Privacy Survey	2019 Threats of the Year
2020 Data Privacy	2020 CISO Benchmark		

Published February 2020

CISO_02_0220