What's Next in Cyber

A Global Executive Pulse Check

2022 GLOBAL SURVEY

paloalto® NETWORKS

If "disruption" is defined as radical change, then security professionals are certainly no strangers to it.

Even before the pandemic, remote work was growing in popularity, digital transformation was driving companies to the cloud, the proliferation of IoT devices was exposing new security vulnerabilities, and increasingly sophisticated cybercriminals were regularly exploiting new attack vectors.

The pandemic just shifted the need to address these challenges into overdrive.

In the blink of an eye, hybrid work became the status quo. Unsecured third-party devices were being used everywhere. And a massive shift to multicloud environments left cybersecurity teams scrambling to secure more than ever against more cyberthreats than ever. To boot, talent shortages made doing so all the more difficult.

At Palo Alto Networks, our vision is to make each day safer than the one before. As a means of making sure we continue to do so, it's important for us to know the concerns, priorities, and observations of the world's executives in regard to securing their organizations. To find out, we asked 1,300 C-suite leaders (CISOs, CIOs, CSOs, CTOs, and COOs) from around the globe and across different industries to share their thoughts and their wisdom. Their answers can be found in the 2022 Global What's Next in Cyber survey. **In the pages ahead, we've pulled out some of the key data from the survey to help inform your own cyber transformation.**

Here are some of our observations based on the results.

On the one hand, organizations are racing toward modernizing their infrastructure, with software smart and fast enough to respond to current and future threats, and to achieve cyber resilience. On the other hand, not everybody is where they need to be. We understand that it can be difficult to know where to start or what to prioritize, but there are some critical areas where organizations need to move the dial. Leaders will need to make tough decisions and bold moves.

Cyber transformation is only possible when CIOs and CISOs free themselves from the legacy security architectures of today and reimagine them for the future — one where the most complex and evasive threats are stopped in real time, at any scale.

In the secure future, hybrid work is protected by secure access service edge (SASE), with continuous security delivered at scale. Artificial intelligence and machine learning automate anomaly detection, improve visibility and control, and counter zero-day attacks. And defending our digital way of life is simplified by integrated security platforms designed to protect the most critical areas of modern organizations.

At Palo Alto Networks, our goal is to help organizations leverage security as a strategic enabler of the business outcomes they desire. We want to be your partner in securing the way forward. **We hope these survey results will shine a light on the path ahead so you can walk it with confidence and optimism.**

For details on the methodology used in this survey, please see the Appendix.

The Growing Threat

These days, every organization is in the crosshairs of cybercriminals. Every new device, user, or piece of sensitive data expands the attack surface, giving threat actors more opportunities to compromise environments. And they're doing so with astonishing speed. Ransomware and business email compromise (BEC) are among the top attacks organizations will continue to face, with phishing and software vulnerabilities likely to remain the top means of access.

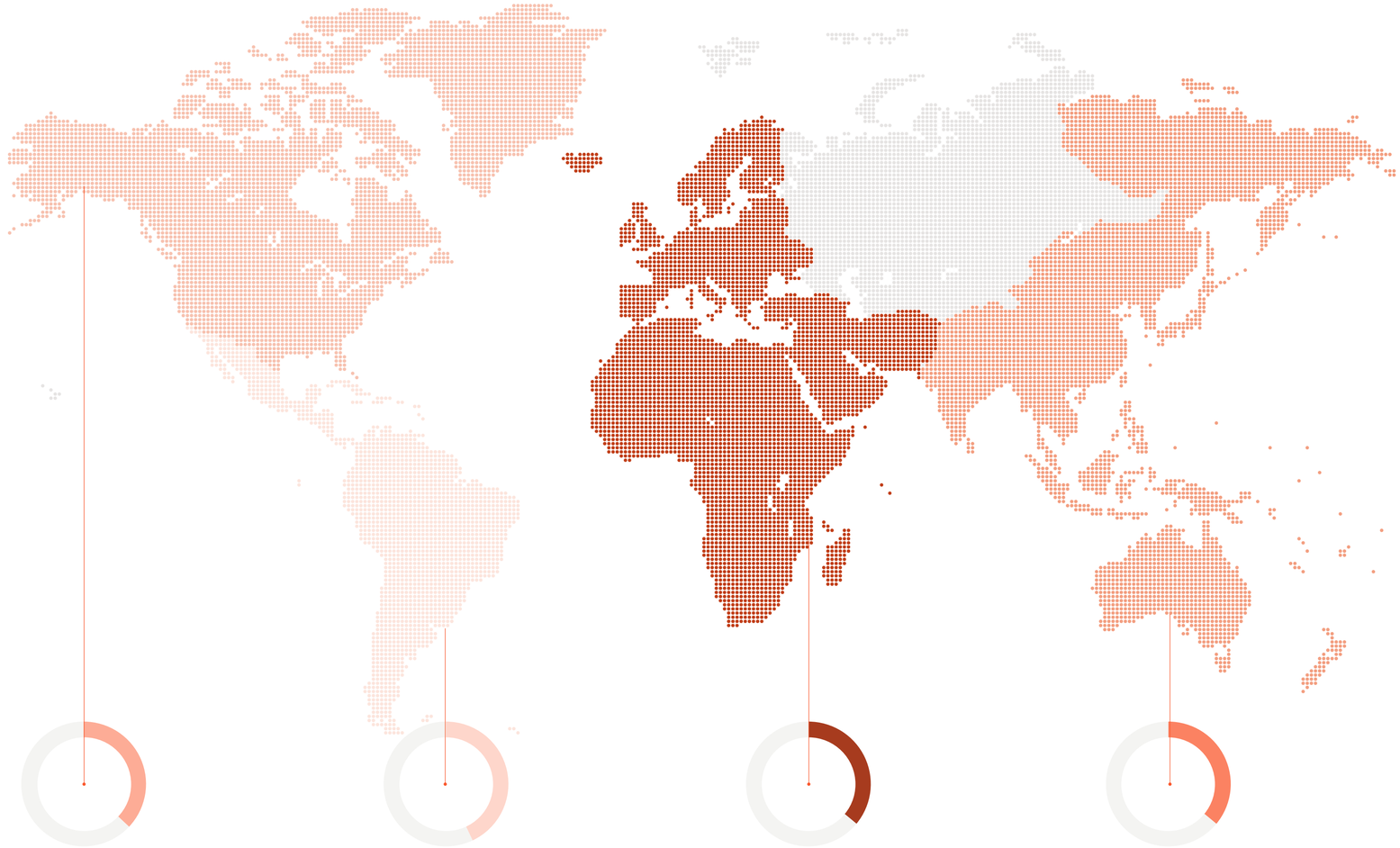
IN THE LAST 12 MONTHS

96%
of all respondents experienced at least one breach

57%
experienced three or more breaches

33%
of CXOs said they experienced an operational disruption as a result of a breach

84%
agree (to varying levels) that they have seen more security incidents due to hybrid work



THE TOP REASON CXOs CITE FOR SUCCESSFUL BREACHES, BY REGION

NAM
Increase in hybrid/remote work

LATAM
Insufficient threat detection and response capabilities

EMEA
Improving capabilities of cybersecurity adversaries

JAPAC
Insufficient threat detection and response capabilities

What Keeps Executives Up at Night?

According to the survey, **only 25% of executives believe their organizations' cybersecurity readiness and resilience is high**. We asked them to select their top three cybersecurity business priorities and the top three challenges for managing security across their organizations.

It isn't surprising to see executives prioritizing automation and improved security operations, as **96% of those surveyed report a lack of skilled cyber professionals as one of their biggest challenges.**

The Top Three:

TYPES OF THREATS ORGANIZATIONS ARE CONCERNED ABOUT, BY REGION

	NAM	JAPAC	EMEA	LATAM
1	Ransomware	Supply chain threats	Supply chain threats	Unknown zero-day threats
2	Malicious insiders	Malicious insiders	Business email compromise	Ransomware
3	DDoS Attacks	DDoS Attacks	DDoS Attacks	Supply chain threats

CYBERSECURITY CHALLENGES

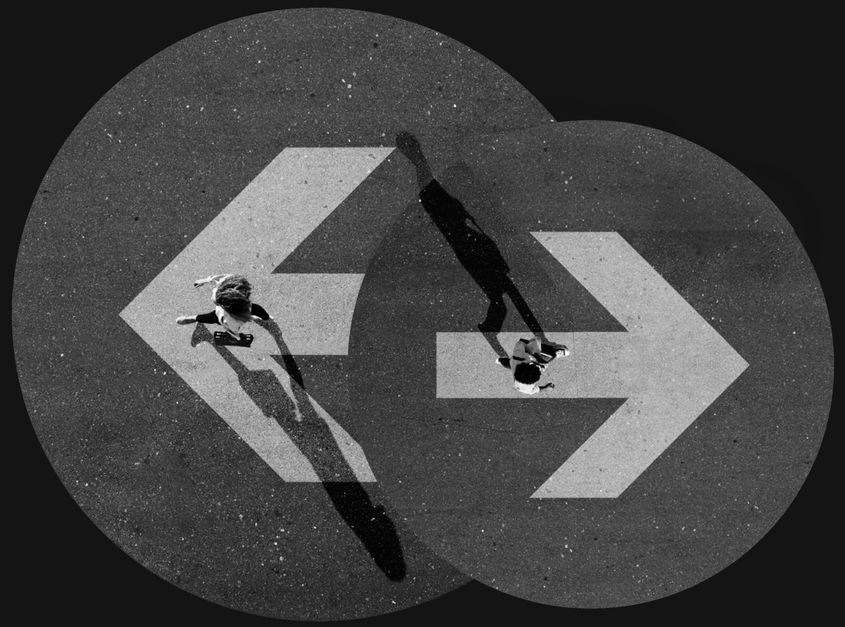
1. Increase in data management / perimeter complexities
2. Lack of skilled cyber professionals
3. Security is not keeping up with changes in the tech stack

CYBERSECURITY PRIORITIES

1. Data protection and privacy
2. Improving security operations/efficiency
3. Automation of threat detection and response

Executive Alignment Is Still an Issue

Eighty-nine percent of respondents say cybersecurity is on their boards' agenda at least once a quarter. However, lack of executive and board alignment and inadequate security governance across the organization must be addressed in order to truly manage cyber risk.



62%

of executives believe their boards' recognition of cyber risk has only marginally increased alongside the acceleration of digital transformation initiatives

37%

of respondents say lack of executive alignment on prioritizing cybersecurity is one of the top three challenges across their organization; surprisingly, banking and healthcare industry respondents selected this far more than any other answer

33%

of executives say inadequate governance across the organization is one of their greatest challenges; NAM leaders (37%) selected this more often than respondents from other regions

Vendors and Tools: Consolidation Is Coming

As organizations face a constant onslaught of cyberattacks, the complexity of managing vendors and point solutions creates security gaps. That explains why globally **77% of respondents said they are highly likely to reduce the number of security solutions and services they rely on.** Going forward, we anticipate that cybersecurity teams will consolidate their vendor environments and pursue platforms that are comprehensive and scalable.

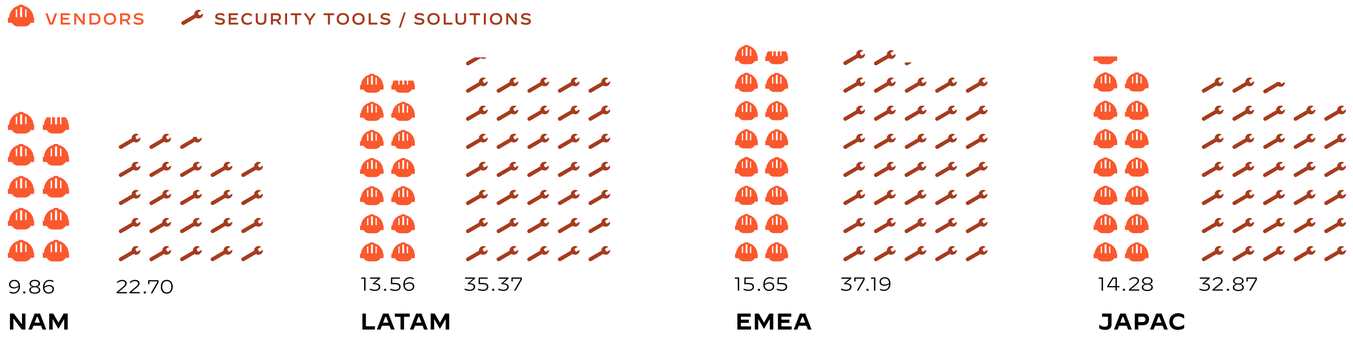
GLOBALLY

41% of organizations work with 10 or more cybersecurity vendors

NUMBER OF SECURITY VENDORS / TOOLS USED BY ORGANIZATIONS TODAY

13.39 **VENDORS** (TOTAL AVERAGE)

31.58 **SECURITY TOOLS / SOLUTIONS** (TOTAL AVERAGE)



Investing in What's Next: Budgets and Resources

Globally, cybersecurity will continue to be a high-priority investment. **But where will the dollars go?** As enterprises continue to rethink connectivity, we see them investing to protect 5G networks and the Internet of Things, while turning to automation to improve productivity and operational efficiency.

WHAT IS GOING TO HAPPEN TO CYBERSECURITY BUDGETS IN 2023?

0% (NO ONE)
thinks budgets will decrease

10%
expect budgets to remain flat

68%
expect a budget increase this year of up to 10%

22%
say budgets will increase more than 10%

AREAS OF CYBERSECURITY RECEIVING THE MOST FUNDING

1. Data Security
2. Cloud Security
3. Internet of Things (IoT) Security

Nearly 25%
of executives surveyed say at least half their cybersecurity budgets are allocated to hybrid workforce security requirements

THE TOP WAY REGIONS ARE COPING WITH THE CYBER SKILLS SHORTAGE

NAM
Automating more security operations; switching to managed services (tie)

EMEA
Automating more security operations

JAPAC
Offering better benefits than other companies

LATAM
Offering higher wages than other companies

Who is investing in
5G
NEXT YEAR?

51%	78%	73%	68%
NAM	EMEA	LATAM	JAPAC

While **88%** of global executives surveyed say they understand the security challenges of 5G, **few (21%) have a plan yet to address them**.

In Zero Trust We Trust

Zero Trust has quickly moved from a cybersecurity concept to an operational imperative for organizations.

Top Reasons for Adopting a Zero Trust Framework

Growing supply chain / vendor ecosystem **52%**

Sophistication and frequency of attacks **49%**

Hybrid workforce **47%**

98%

of CXOs surveyed say implementing Zero Trust is challenging

Top 3 Challenges to Implementing Zero Trust

1. Lack of internal expertise
2. Not knowing where to start and how to prioritize
3. Lack of qualified vendors with a complete and integrated solution

TOP CHALLENGE TO IMPLEMENTING ZERO TRUST, BY REGION

NAM

Not knowing where to start and how to prioritize

EMEA

Lack of qualified vendors with a complete and integrated solution

LATAM

Lack of tools to truly implement Zero Trust

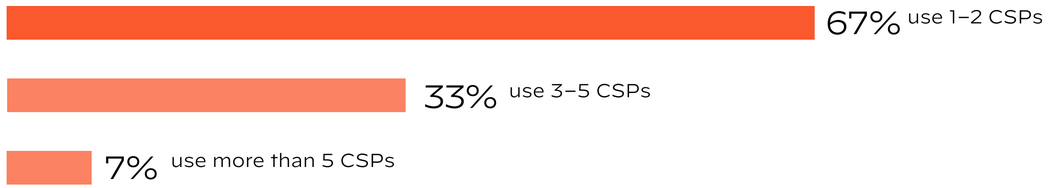
JAPAC

Lack of internal expertise

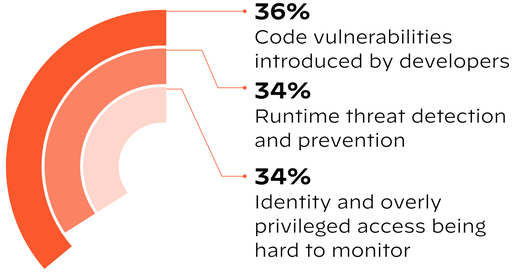
Security in the Clouds

As the place where business builds, works, and plays, the public cloud now hosts countless applications, and that trend will accelerate. But securing today's future-forward, cloud-powered businesses is easier said than done, particularly amid the proliferation of multicloud environments.

HOW MANY CLOUD SERVICE PROVIDERS (CSPs) ORGANIZATIONS USE



TOP CYBERSECURITY CONCERNS FOR PUBLIC CLOUD ADOPTION



36%
Code vulnerabilities introduced by developers

34%
Runtime threat detection and prevention

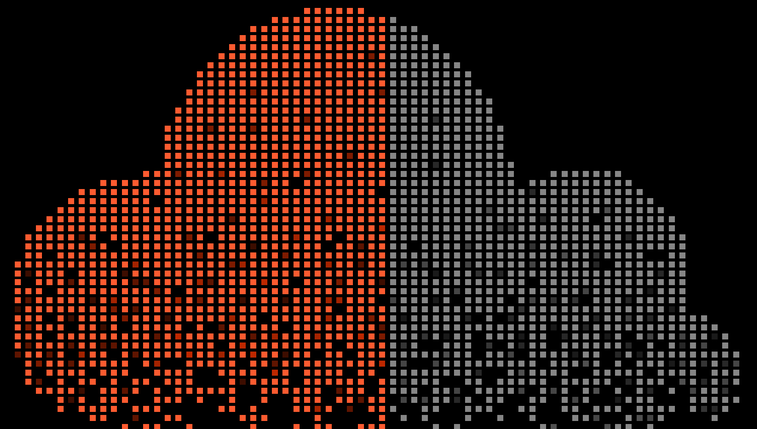
34%
Identity and overly privileged access being hard to monitor

PRIMARY WAYS ORGANIZATIONS ARE ADDRESSING CLOUD SECURITY REQUIREMENTS

37%
Deploying Web Application and API Security

35%
Requiring developers to use code security and scanning tools

35%
Deploying virtual firewalls to protect cloud application perimeter



50% of organizations plan to increase investments in software firewalls on both public and private clouds.

DevSecOps

Given the ever-growing number of applications being hosted in the public cloud, DevOps teams now need to move with greater speed. With survey respondents admitting to multiple cyber incidents, it suggests that vulnerabilities may not be getting identified in DevOps production environments.

To stop managing security incidents and start preventing them, organizations must take a holistic approach to cloud security. Those that integrate security into application development and deployment from the get-go will be the most successful at balancing security and speed.

74% of respondents agree that security slows down DevOps

366 unique applications used by organizations on average

#1 application security concern for leaders is securing data

AI and Automation for the Win

The security operations center (SOC) is ground zero for effective deployment of AI/ML. Security teams will need to shift their thinking on SOCs to an automation-first mindset, whereby AI and automation both accelerate detection and equip the detectors, ultimately leading to more effective security outcomes. Automation and AI will also be important in creating greater operational efficiency as organizations combat a severe shortage of cyber talent.

49%

of respondents think that AI has the highest impact on security in the realm of more effective threat detection

39%

of global executives think that threat detection, alert triage and incident response can be almost completely automated in the SOC

Securing the Way Forward

As companies accelerate their digital transformation journeys, they need to make cybersecurity the first step, rather than the last mile. As they race to keep pace with an ever-evolving and expanding threat landscape, the time for reimagining the cybersecurity architectures designed to protect their people, their data, and their infrastructures is now. Cyberattackers don't rest with macroeconomic challenges, they double down on them. The cybersecurity imperative has never been more pronounced.

Cybersecurity has been elevated from a compliance function to a strategic imperative. It's a new vision of the digital world. Increasingly, that vision challenges our approach to digital defense, requiring that we move from a single solution for every problem to a platform approach designed to deliver best-of-breed security across the board.

Be bold. Change with purpose.
Embrace the technologies that enable you to secure the way forward.

Appendix

METHODOLOGY

The Palo Alto Networks 2022 Global What's Next in Cyber Survey, conducted by Wakefield Research between July 26 and August 16, 2022, polled 1,300 C-suite leaders who are responsible for cyber at large companies (those with $250+ million in revenue) around the globe (NAM: US, Canada; EMEA: U.K, France, Germany, Netherlands, Italy, Spain; LATAM: Brazil, Mexico; JAPAC: Japan, Singapore, India, Australia, and New Zealand), and asked them to share their priorities, concerns, and opinions on the industry that is shaping every other.

CITATION

THE GROWING THREAT | 02

In the last 12 months, how many cybersecurity incidents or breaches are you aware of that your organization experienced?

In which of the following ways, if any, has your organization been negatively impacted by cybersecurity incidents or breaches? Please select all that apply.

Which of the following best reflects your belief on why there are still so many successful cybersecurity incidents and breaches on organizations today?

How strongly do you agree or disagree with the following statement: "My organization has seen an increased number of security incidents from unsecured devices due to a hybrid work environment"?

WHAT KEEPS EXECUTIVES UP AT NIGHT | 03

Which of the following types of threats is your organization most concerned about protecting itself against in 2023?

Which of the following business issues related to cybersecurity, if any, is your organization most focused on? Please select the top three.

Which of the following, if any, is the biggest challenge in managing cybersecurity across your organization? Please select the top three.

EXECUTIVE ALIGNMENT IS STILL AN ISSUE | 04

Approximately how often, if ever, is cybersecurity on your board's agenda?

How much has board-level recognition of cyber risk increased alongside accelerated digitalization strategies?

Which of the following, if any, is the biggest challenge in managing cybersecurity across your organization? Please select the top three.

VENDORS AND TOOLS: CONSOLIDATION IS COMING | 05

How important is it to your organization to reduce the number of possible security solutions or services used?

Approximately how many security vendors does your organization currently work with?

INVESTING IN WHAT'S NEXT: BUDGETS AND RESOURCES | 06

Which of the following emerging technologies, if any, is your organization most likely to invest in over the next year? Please select all that apply.

Which of the following areas of cybersecurity, if any, receive the most funding in your organization? Please select the top three.

How will your organization's cybersecurity budget change in 2023?

What percent of your cybersecurity budget is allocated to the following? (Hybrid workforce security requirements)

Which of the following measures, if any, is your organization taking to resolve this shortage of cybersecurity skills? Please select all that apply.

IN ZERO TRUST WE TRUST | 07

What is driving your organization's adoption of a Zero Trust framework? Please select all that apply.

Which of the following, if any, do you feel is the top challenge to a Zero Trust framework implementation?

SECURITY IN THE CLOUDS | 08

How many public cloud providers (i.e., Amazon Web Services, Microsoft Azure, Google Cloud Platform) do you use at your organization?

Does your organization plan to increase investment in software firewalls in any of the following? Please select all that apply.

What are your greatest security concerns for your public cloud environments? Please select all that apply.

Which of the following, if any, are primary ways that your organization addresses cloud security requirements? Please select up to three.

DEVSECOPS | 09

Does security slow down continuous development methods like development operations (DevOps) at your organization?

Approximately how many unique applications are in your environment?

AI AND AUTOMATION FOR THE WIN | 10

Which of the following areas, if any, do you feel artificial intelligence (AI) has the greatest impact on your organization's cybersecurity? Please select all that apply.

In which of the following areas, if any, do you believe can be completely or almost completely automated in your security operations center (SOC)? Please select all that apply.