Endpoint Security Trends 2023

AUTHOR

Krista Macomber
Research Director | The Futurum Group

Daniel Newman
CEO | The Futurum Group

MARCH 2024

IN PARTNERSHIP WITH

Dell Technologies

Executive Summary

Organizational cyber resiliency has become a board-level priority due to the growing incidence and severity of cyber-attacks and the increased risk this brings. As enterprises look to prevent attacks and mitigate their impact when they inevitably occur, the security of endpoint devices, IT systems, software, networks, cloud environments and associated supply chains is of particular concern. For greater insight into the level and types of threats that enterprises are encountering, The Futurum Group, in collaboration with Dell Technologies, executed a survey of 989 technology and security professionals that play a role in the planning implementation, management, or operations pertaining to device-level security. A follow-up to an initial iteration of this survey published in 2020, these findings demonstrate how the world adapted post-pandemic, as well as how measures, practices and policies for security are evolving,

Alarmingly, nearly 90% of respondents surveyed indicated that their organization has experienced an increase in security issues, citing **hardware-related attacks as a growing vector**. Against this backdrop, nearly all indicated that their organization has been challenged to maintain a strong security posture. Specifically, today's enterprises are challenged when it comes to recruiting and retaining the talent necessary to maintain a strong security posture (as noted by 95% of respondents). This is a particular challenge considering the pace at which malicious actors – including state-sponsored and other external threat actors, as well as those internal to the organization – are innovating. This is further compounded by employees bypassing standard security protocol to acquire and deploy technologies for remote or work-from-home use (as noted by 90% of respondents).

In an effort to keep pace with the growing number of threats, nearly all respondents also indicated that their organization has been changing and/or adapting corporate policies and business processes to maintain, and ideally improve, their security posture. Work remains, however, to ensure cyber resiliency across the hardware journey, which spans the supply chain, implementation of security tools and processes, and ongoing end-user operations. This research digs into modern attack techniques and how IT and security practitioners can most effectively respond and react, grounded in quantitative survey feedback.

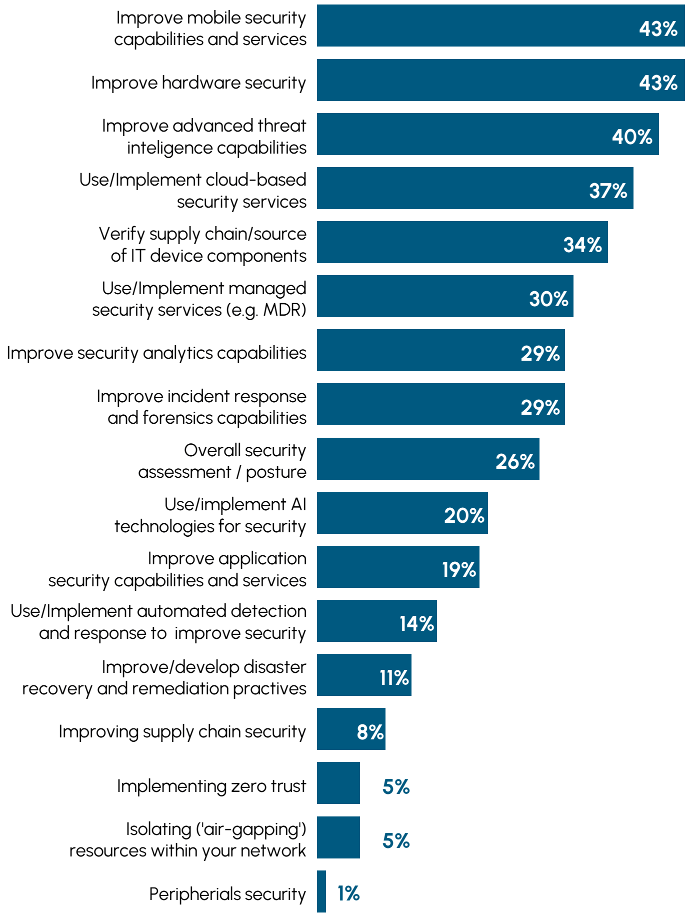
© 2024 The Futurum Group. All rights reserved.

Hardware-Based Attacks are on the Rise

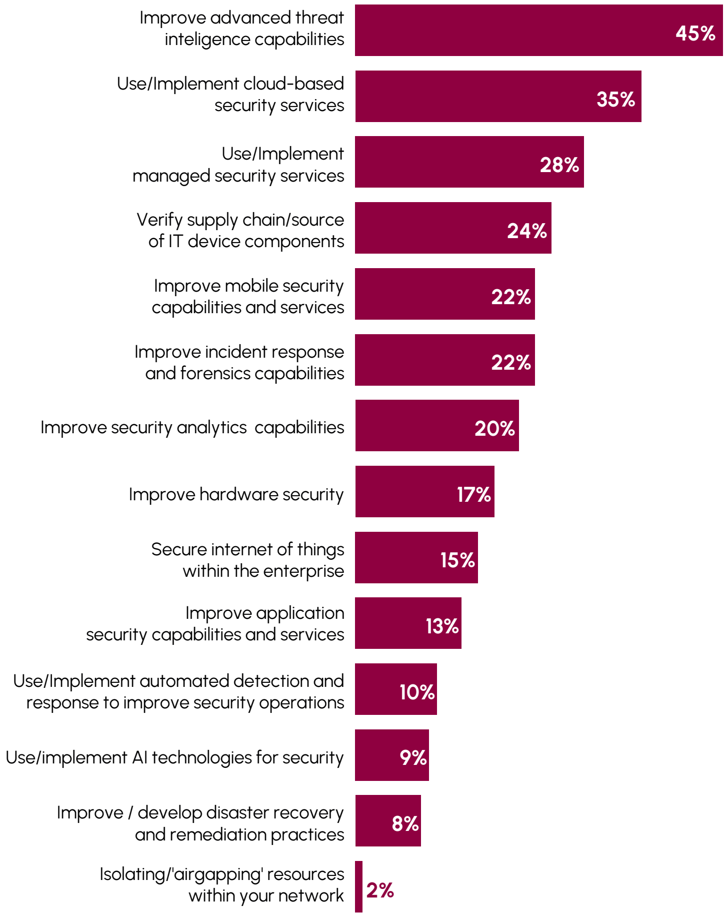
Since the initial iteration of this survey, security priorities have shifted, with an emphasis on shoring up vulnerabilities pertaining to end-user devices and IT hardware.

Specifically, the top 3 priorities in the 2020 iteration of the survey were:	**1.** Improve advanced threat intelligence capabilities **2.** Use/Implement cloud-based security services **3.** Use/Implement managed security services
Compared to the top 3 priorities in the current iteration of the survey:	**1.** Improve mobile security capabilities and services **2.** Improve hardware security **3.** "Improve advanced threat intelligence capabilities," which remained in the top three but dropped from its number one position.

2023 Please Select the TOP FIVE initiatives for IT security is your organization pursing over the coming 12 months?



2019 Please Select the TOP FIVE initiatives for IT security is your organization pursing over the coming 12 months?



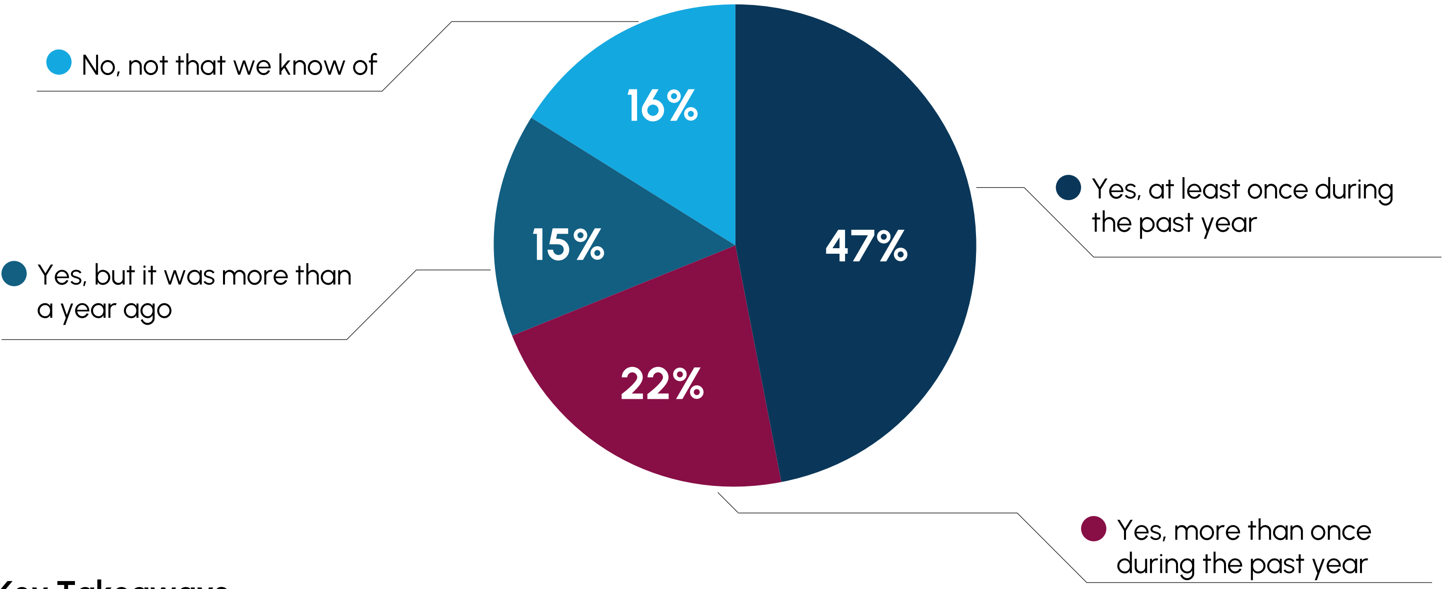
Note: Categories do no match exactly between years

© 2024 The Futurum Group. All rights reserved.

This makes sense given that a larger number of respondents noted hardware-based security threats and breaches targeting firmware/BIOS or silicon, when compared to 2020. The Futurum Group believes this indicates not only an increase in device-related attacks, but it also points to greater awareness and detection of these types of attacks.

- In the 2020 iteration of this study, 44% of respondents indicated having experienced at least one BIOS or hardware-level attack during the past year.
- **69% of organizations say they've had at least one hardware- / firmware-level attack during the past year, up 1.5X from 2020**

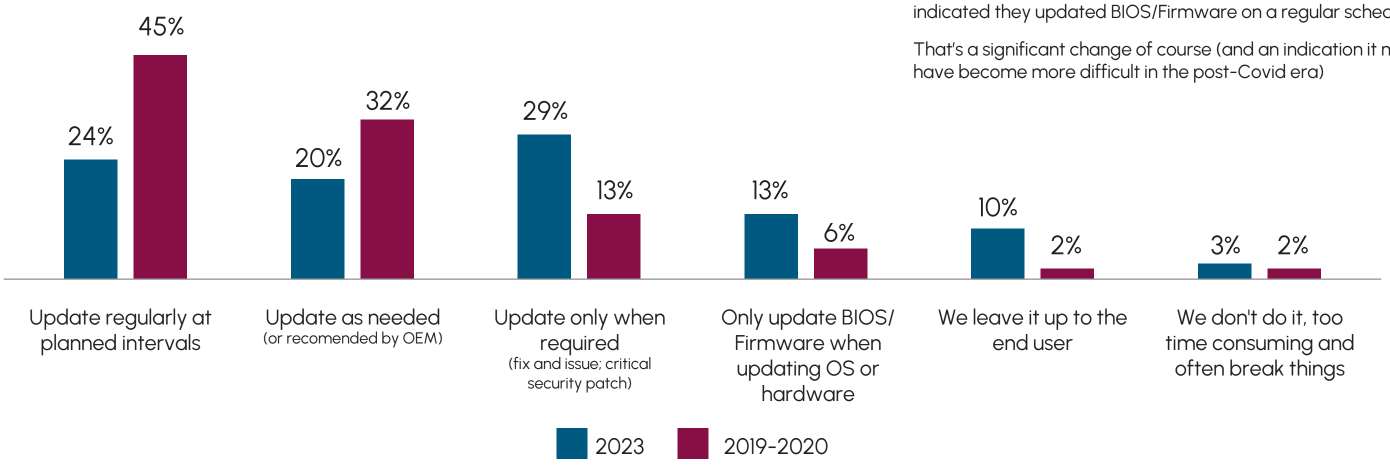
Percent citing previous hardware level breach



Key Takeaways

Hardware-related incidents can materially compromise sensitive data or degrade operational capacity. Organizations can mitigate the risk of a successful breach in a number of ways. Sourcing devices from legitimate vendors with strong security practices will help reduce the attack surface. Once secure devices are deployed, keeping the BIOS software up-to-date is important because BIOS updates often include important security patches and bug fixes. However, survey responses indicate that, most commonly, these updates are occurring at regularly planned intervals (24%) and when recommended by the device original equipment manufacturer (OEM) (20%) - indicating that the majority of organizations are not updating BIOS and that the percentage who are updating has decreased.

What is your primary approach to BIOS/Firmware updates? (Select one)



Note: Note that in 2019 – 2020 just over 45% of organizations indicated they updated BIOS/Firmware on a regular schedule

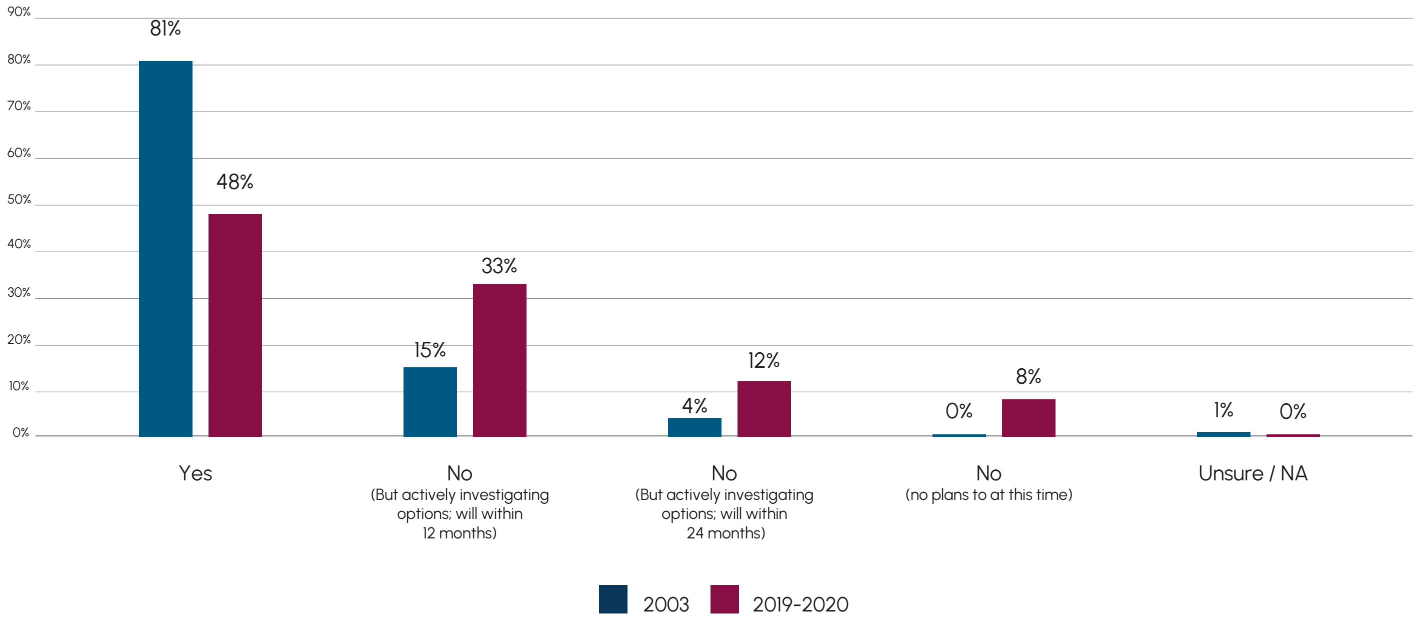
That's a significant change of course (and an indication it may have become more difficult in the post-Covid era)

To further protect the BIOS, respondents commonly indicated using manual password management on the device (50%), BIOS recovery options controlled by IT (58%), and password management through a Unified Endpoint Management (UEM) app (43%).

Based on the survey results, organizations are aware of several methods for maintaining stronger BIOS/firmware security. What is telling is the year-over-year shift in priority towards updating only when required, i.e., fixing a known issue, versus proactively updating at planned intervals or when recommended by the manufacturer. This approach is likely to leave organizations exposed as flaws in firmware may remain undetected for weeks.

This year, we also saw respondents turn increasingly towards software-based security to help protect against hardware-based threats, specifically endpoint detection and response (EDR) tools, which continuously monitor end-user devices including servers, desktops, laptops, and mobile devices for malicious activity. Year-to-year, the percentage of respondents currently using an EDR increased from 48% in the prior study to 81%.

Current Use of Endpoint Detection and Response



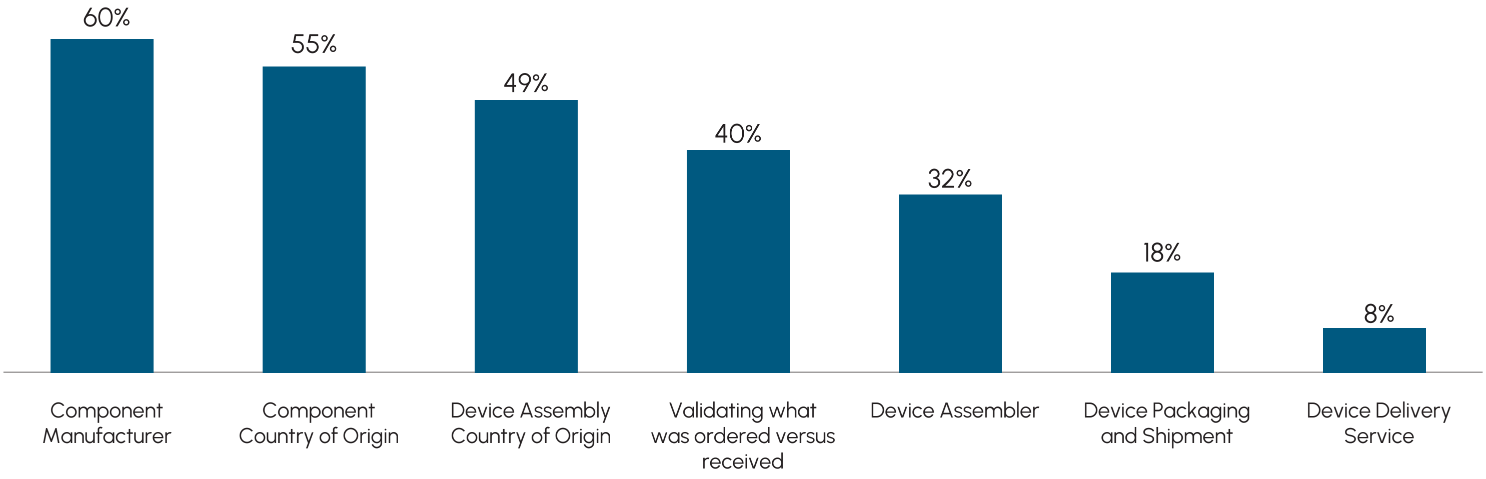
Global Supply Chains are a Critical Vulnerability to be Addressed

The supply chain is a growing area of vulnerability; nearly 90% of respondents indicated that their supply chain has been disrupted and introduced new security risks/challenges. The problem is that, as cyberattacks have grown more sophisticated in their ability to exploit vulnerabilities, the global economy has become more reliant on distributed supply chains spanning countries and regions across the world. Additionally, one in four respondents indicated that, while their organization requires end-users to purchase or use only authentic devices from approved suppliers, this policy is not completely enforced. What's more, where it is enforced, IT still may not be aware what shadow equipment was deployed post-COVID. Simply put, supply chain poses a growing concern given the massive attack surface it presents to adversaries.

Specifically, respondents indicated being most concerned about are:

- Component manufacturing
- Component country of origin
- Device assembly country of origin

Top supply chain threats



Key Takeaways

There are dozens of points across the supply chain and each one can present an opportunity for an attacker. Knowing the devastating impact of a successful supply chain breach, organizations cannot risk overlooking potential blind spots.

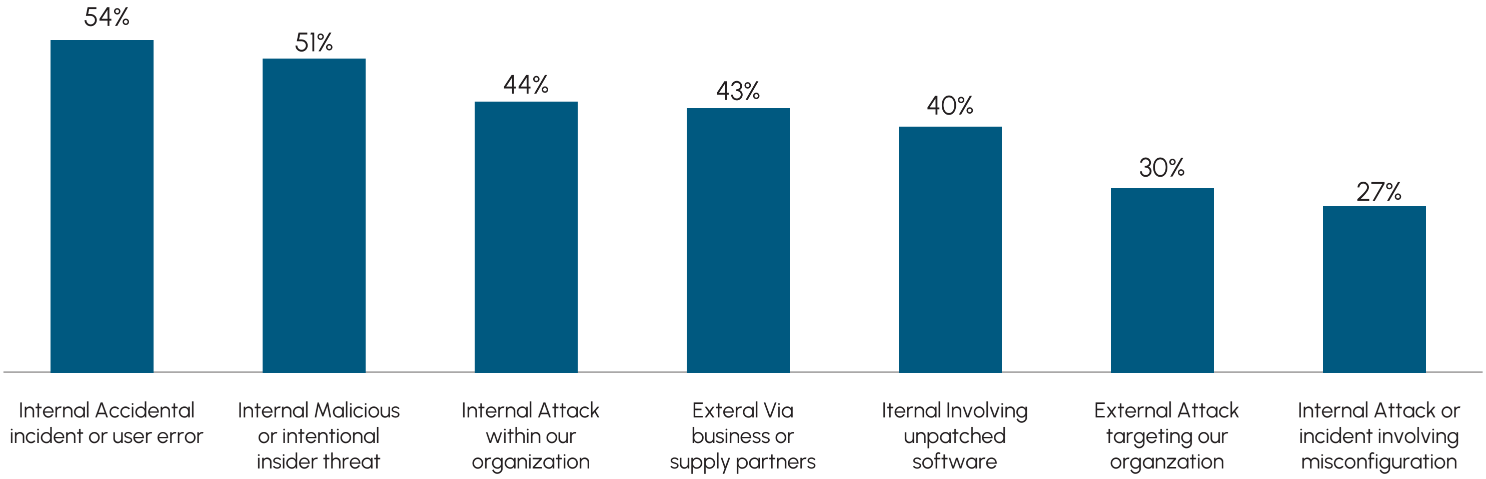
It's critical to maintain compliance with security policies and protocols that have been established. Equally as important is auditing those policies and protocols periodically to make sure they are adequately addressing emerging threats. That means extending scrutiny to vendors to ensure rigor of their supply chain controls as well.

Malicious and Negligent Insider-Related Issues Continue to Create Risk

While market buzz around ransomware and state-sponsored attacks remains high, it is clear based on survey feedback that issues pertaining to malicious insiders and accidental human error are rising. Nearly 70% of respondents indicated having experienced one or more software-related breach during the past 12 months, with the most common types of these breaches being:

- Internal attack within their organization
- Internal, accidental incident/user error
- Internal malicious/intentional insider threat
- Attack or incident involving their business partners/third-party suppliers
- Attack or incident involving unpatched software

Most common types (causes) of software breaches and attacks



Key Takeaways

No matter the type of attack, it is abundantly clear that threat detection simply needs to happen faster, in order to mitigate business downtime and data loss. This boils down to how quickly issues can be identified, escalated, investigated, and addressed. Again, while respondents reported growing adoption of EDR and continued use of Security Information and Event Management (SIEM) tools, as attackers become more and more sophisticated, organizations will need to take a hard look at how effective their legacy systems are against modern threats. With the move to hybrid work, adversaries seized the opportunity to not only exploit devices, but unsecured networks and cloud-based environments as well. As such, organizations have started to move towards extended threat detection and response (XDR), and we expect that trend to grow.

Recommendations

Attacks can happen across the entire lifetime of a device, from design to manufacture through to retirement – and every step in between. This makes maintaining device trust an ongoing challenge. The Futurum Group recommends adopting a multi-pronged approach to endpoint security that helps reduce the attack surface and promote long-term cyber resiliency. This includes, but is not limited to:

- **Sourcing hardware from secure suppliers that understand the implications of an evolving threat landscape.** The devices you procure should be built with security in mind. Working with suppliers that proactively consider security at the product design and development phases is critical to building and retaining a strong security posture. Secure suppliers, all too familiar with the risk of product tampering, will also be well-positioned to allay the growing concern around component integrity.
- **Deploying PCs with security built in.** Given the nature of attacks today, built-in security features are no longer an option. Devices should offer visibility into foundational attacks – and, importantly, give you the ability to take action against them quickly as time is of the essence when it comes to security. For example, devices should allow you to verify the integrity of the BIOS and other critical firmware as needed.
- **Further secure the fleet with software.** Phishing and other attacks that take advantage of user error continues to grow. Seeing the risk that malicious and negligent insiders pose, it is best to plan for the worst-case scenario: a successful breach. Shore up your defenses with solutions that enable prevention, detection and response, and remediation across endpoints, as well as into the network and cloud where so many attacks originate today. Work to ensure devices and software work together for the best possible defense.

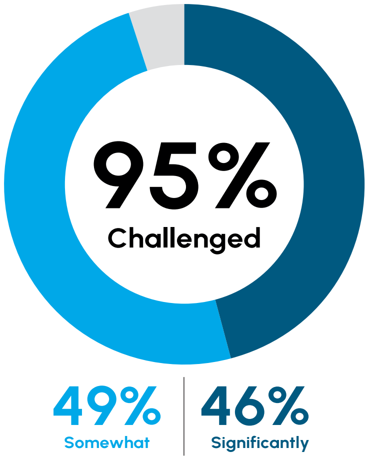
Appendix

2023 SECURITY DISRUPTORS

Please fill in the following statements (significantly; somewhat; not at all): Over the past 18 months…

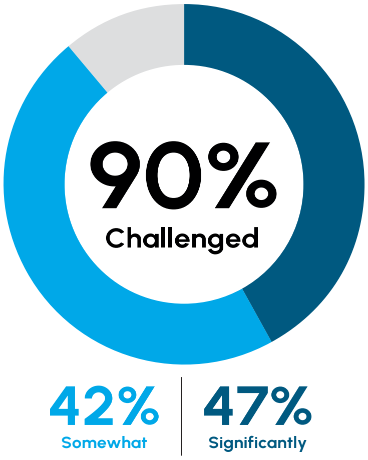
Talent

Our organization has been__________ challenged to **retain and/or recruit** the talent necessary to maintain a strong security posture



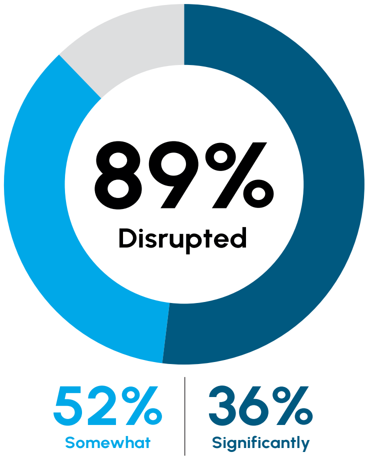
Remote Workers

Our organization has been __________ challenged (or impacted) by **employees bypassing our normal process to acquire and deploy technologies** for remote or work-from-home use



Supply Chain

Our organization has been __________ **disrupted and introduced new security risks** and challenges



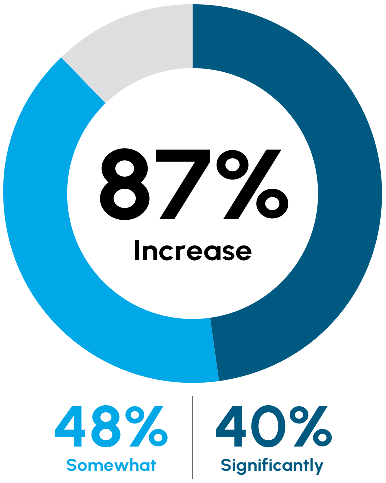
BY REGION		Been significantly	Been somewhat
Our organization has __________challenged to retain and/or recruit the talent necessary to maintain a strong security posture	AP	43%	52%
	EMEA	51%	48%
	NA	40%	52%
	SA	60%	37%
Our organization has __________challenged (or impacted) by employees bypassing our normal process to acquire and deploy technologies for remote or work-from-home use	AP	49%	44%
	EMEA	61%	35%
	NA	40%	43%
	SA	32%	57%
Our supply chain has __________disrupted and introduced new security risks and challenges	AP	43%	51%
	EMEA	37%	54%
	NA	31%	53%
	SA	41%	50%

2023 SECURITY CHALLENGES

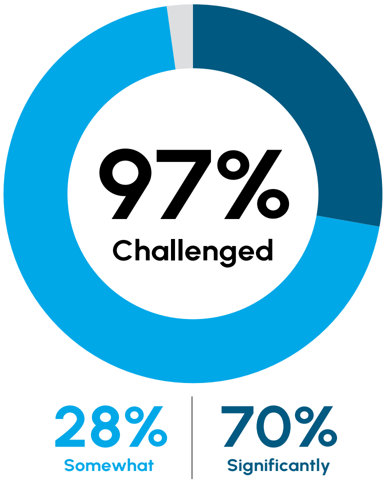
Please fill in the following statements (significantly; somewhat; not at all): Over the past 18 months...

Overall Security Issues

Our organization has been__________ **experincing an increase** in security issues

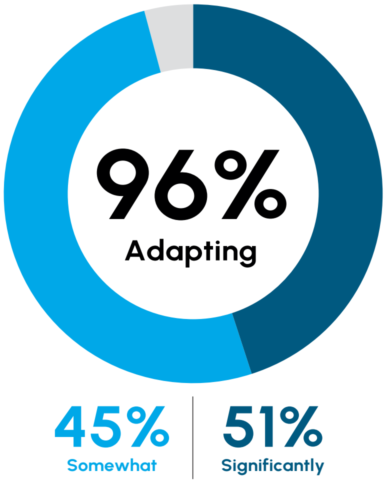


Our organization has been __________ challenged to **maintain a strong security posture**



Policies & Process

We've been __________ changing and/or adapting our **corporate policies and business processes** to maintain and/or improve our security posture given current/emerging business realities



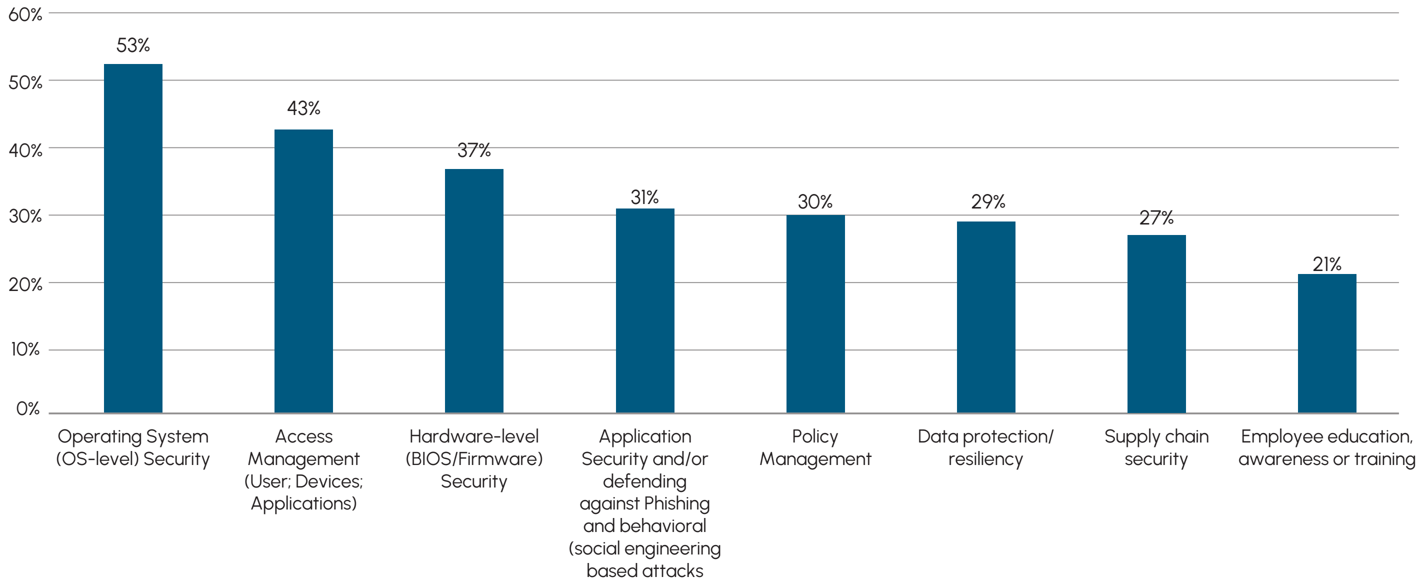
BY REGION		Been significantly	Been somewhat
Our organization has __________experiencing an increase in security issues	AP	45%	50%
	EMEA	44%	49%
	NA	31%	49%
	SA	51%	33%
Our organization has __________challenged to maintain a strong security posture	AP	67%	32%
	EMEA	82%	17%
	NA	59%	36%
	SA	81%	19%
We've __________changing and/or adapting our corporate policies and business processes to maintain and/or improve our security posture given current/ emerging business realities	AP	51%	44%
	EMEA	52%	48%
	NA	49%	45%
	SA	61%	37%

© 2024 The Futurum Group. All rights reserved.

2023 SECURITY NEEDS

Which of the following do you consider the top (most critical) needs in maintaining a strong security posture for your organization? (Select up to three)

Top (three) ranking of most critical needs in maintaining a strong security posture



Others (not included in chart):

7% Preventing device misconfigurations

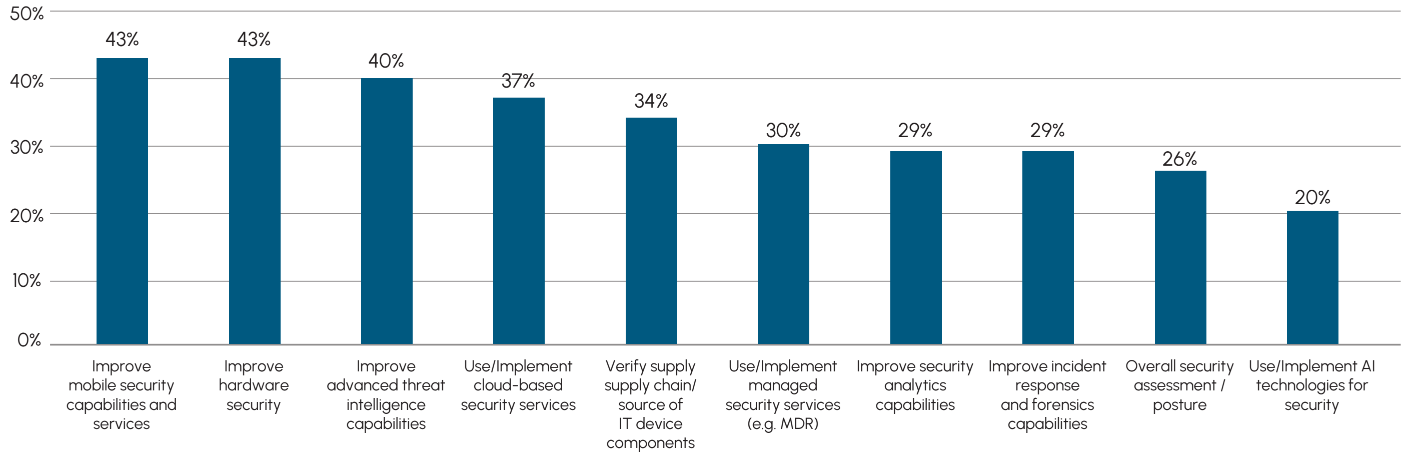
2% iguring out what we don't know (that we don't know)

BY REGION	AP	EMEA	NA	SA
Supply chain security	33%	18%	34%	15%
Hardware-level (BIOS/Firmware) Security	41%	44%	27%	46%
Operating System (OS-level) Security	52%	62%	47%	52%
Access Management (Users; Devices; Applications)	40%	50%	38%	46%
Policy Management	22%	44%	24%	28%
Application Security and/or defending against Phishing and behavioral (social engineering) based attacks	36%	25%	35%	26%
Employee education, awareness or training	21%	20%	23%	20%
Data protection/resiliency	26%	14%	42%	29%
Data protection/resiliency Preventing device misconfigurations	7%	4%	10%	7%
Figuring out what we don't know (that we don't know)	1%	1%	3%	4%

2023 SECURITY INITIATIVES

Which of the following initiatives for IT security would you consider your organization's top, most important focus or initiatives for the coming 12 months? (Select up to five)

Top (five) security needs for (focal points) for the coming 12 months



19% Improve application security capabilities and services

14% Use/Implement automated detection and response to improve security operations

11% Improve/develop disaster recovery and remediation practices

8% Improving supply chain security

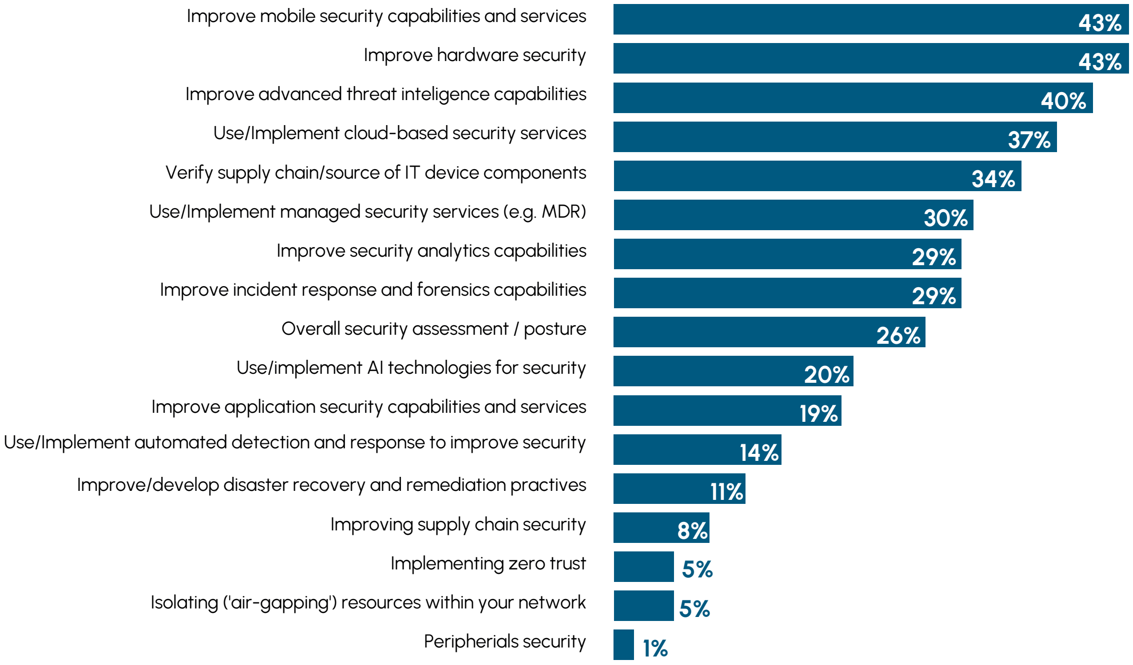
5% Implementing zero trust

5% Isolating ('air-gapping') resources within your network

1% Peripherals security

From the 2023 Study

2023 Please select the TOP FIVE initiatives for IT security is your organization pursing over the coming 12 months?

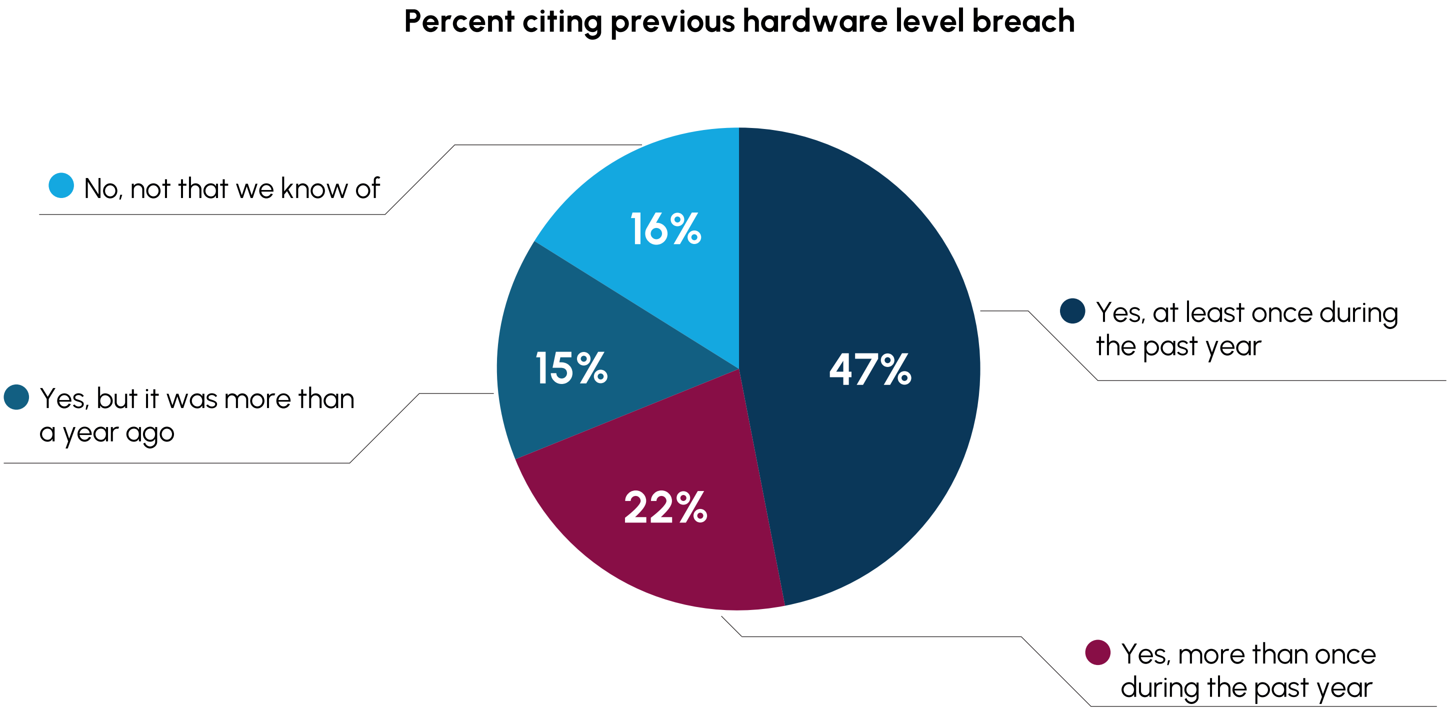


Note: Categories do not match exactly between years

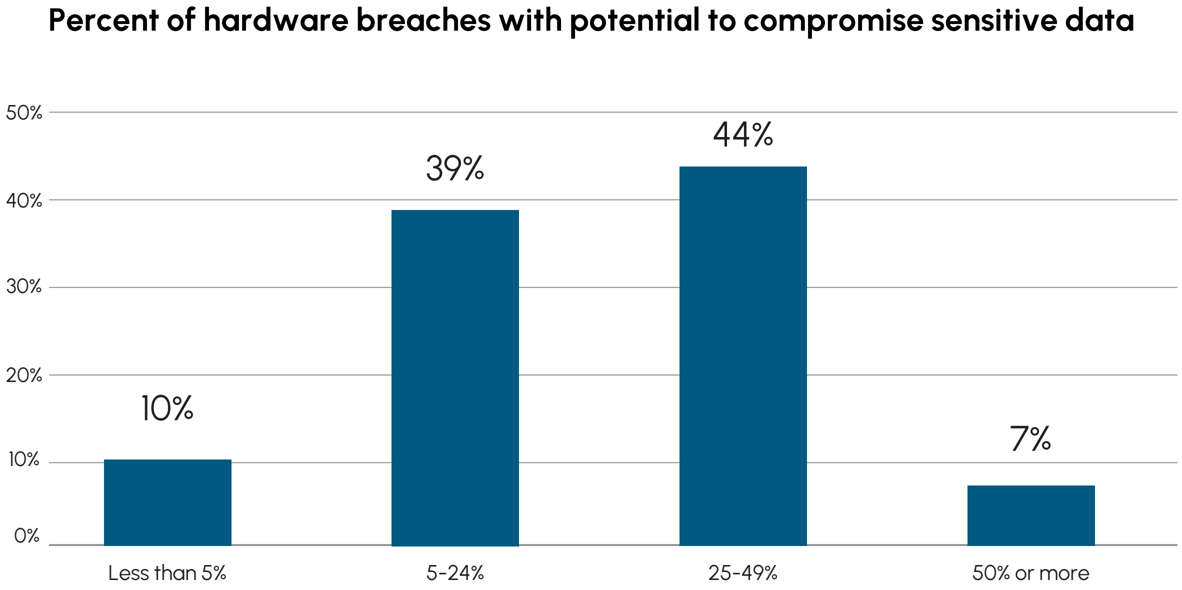
BY REGION	AP	EMEA	NA	SA
Overall security assessment / posture	17%	16%	38%	28%
Improve advanced threat intelligence capabilities	40%	39%	42%	39%
Use/Implement cloud-based security services	38%	37%	35%	41%
Improve mobile security capabilities and services	49%	46%	37%	39%
Improve hardware security	39%	49%	43%	31%
Use/Implement managed security services (e.g., MDR)	32%	39%	26%	23%
Improve incident response and forensics capabilities	30%	37%	22%	28%
Verify supply chain/source of IT device components	37%	29%	36%	34%
Improve security analytics capabilities	28%	31%	26%	36%
Improve application security capabilities and services	23%	18%	21%	11%
Use/Implement AI technologies for security	24%	11%	21%	34%
Use/Implement automated detection and response to improve security operations	16%	9%	16%	20%
Improve/develop disaster recovery and remediation practices	11%	9%	12%	16%
Isolating ('air-gapping') resources within your network	6%	1%	6%	7%
Implementing zero trust	4%	1%	10%	2%
Improving supply chain security	7%	2%	12%	10%
Peripherals security	0%	0%	1%	0%

2023 HARDWARE SECURITY BREACHES ARE AN ISSUE

Has your organization ever experienced a hardware-level breach (targeting firmware/BIOS or silicon)?

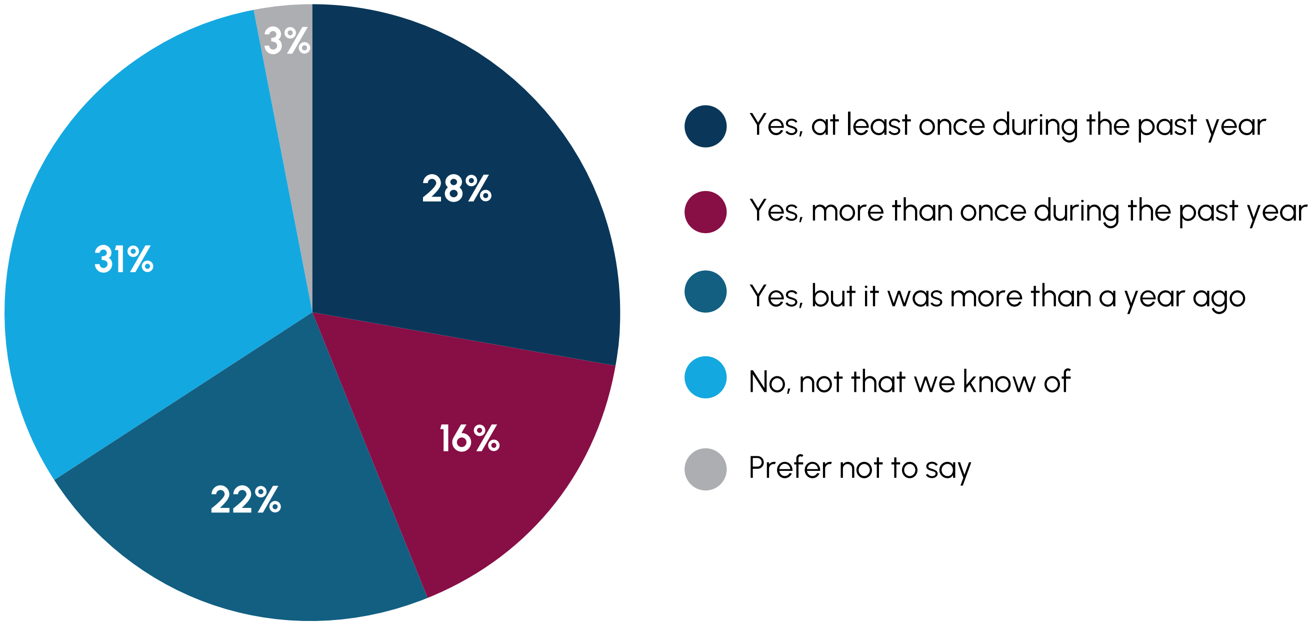


(If YES, during past 12 months) What percent of hardware breaches (during the past year) had the potential to compromise sensitive data or degrade operational capacity?



© 2024 The Futurum Group. All rights reserved.

Has your organization ever experienced a hardware-level or BIOS event (breach in hardware or silicon-level security) that had the potential to compromise sensitive data or degrade operational capacity?



Has your organization ever experienced a hardware-level or BIOS event (breach in hardware or silicon-level security) that had the potential to compromise sensitive data or degrade operational capacity?

BY REGION	AP	EMEA	NA	SA
Yes, at least once during the past year	53%	60%	31%	58%
Yes, more than once during the past year	34%	21%	18%	20%
Yes, but it was more than a year ago	10%	12%	23%	9%
No, not that we know of	4%	8%	29%	13%

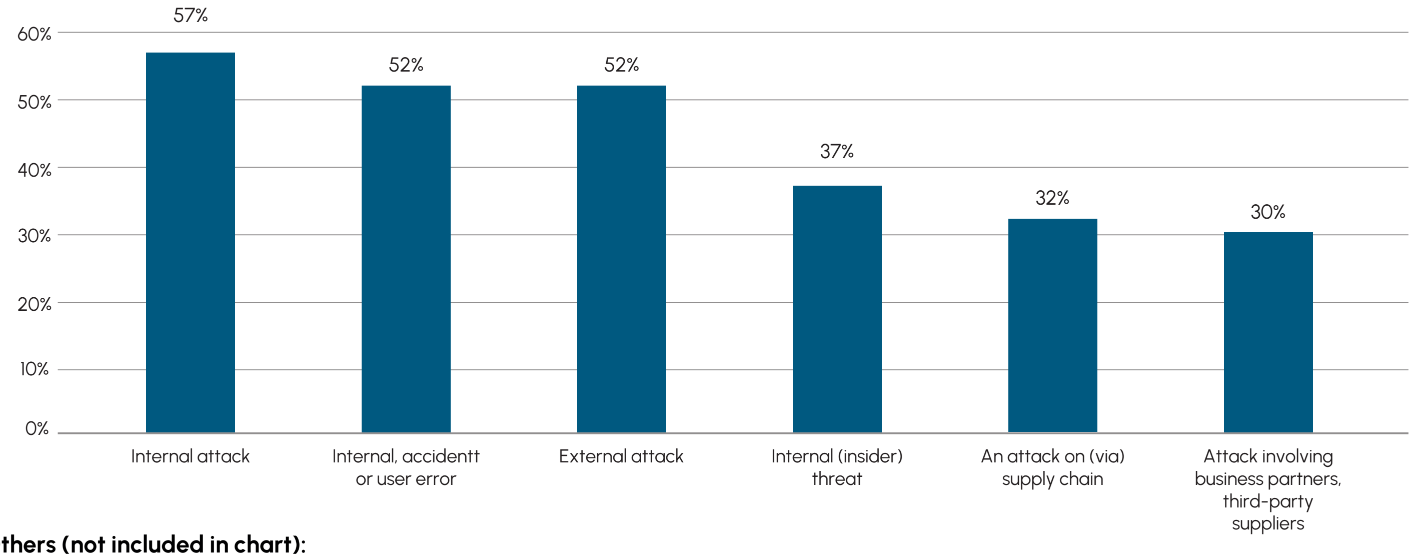
(If YES, during past 12 months) What percent of hardware breaches (during the past year) had the potential to compromise sensitive data or degrade operational capacity?

BY REGION	AP	EMEA	NA	SA
Less than 5%	12%	7%	14%	4%
5 – 24%	41%	38%	40%	35%
25 – 49%	41%	49%	39%	52%
50% or more	8%	6%	7%	9%

2023 HARDWARE ATTACK TYPES

Please identify the top-most common types of breaches experienced this past year: (Select up to five IF you've experienced a breach)

Most common types of HW security breaches (select up to 5)



Others (not included in chart):

21% Physical tampering of a device

17% Lost/stolen asset(s)

12% Rootkit or firmware exploit

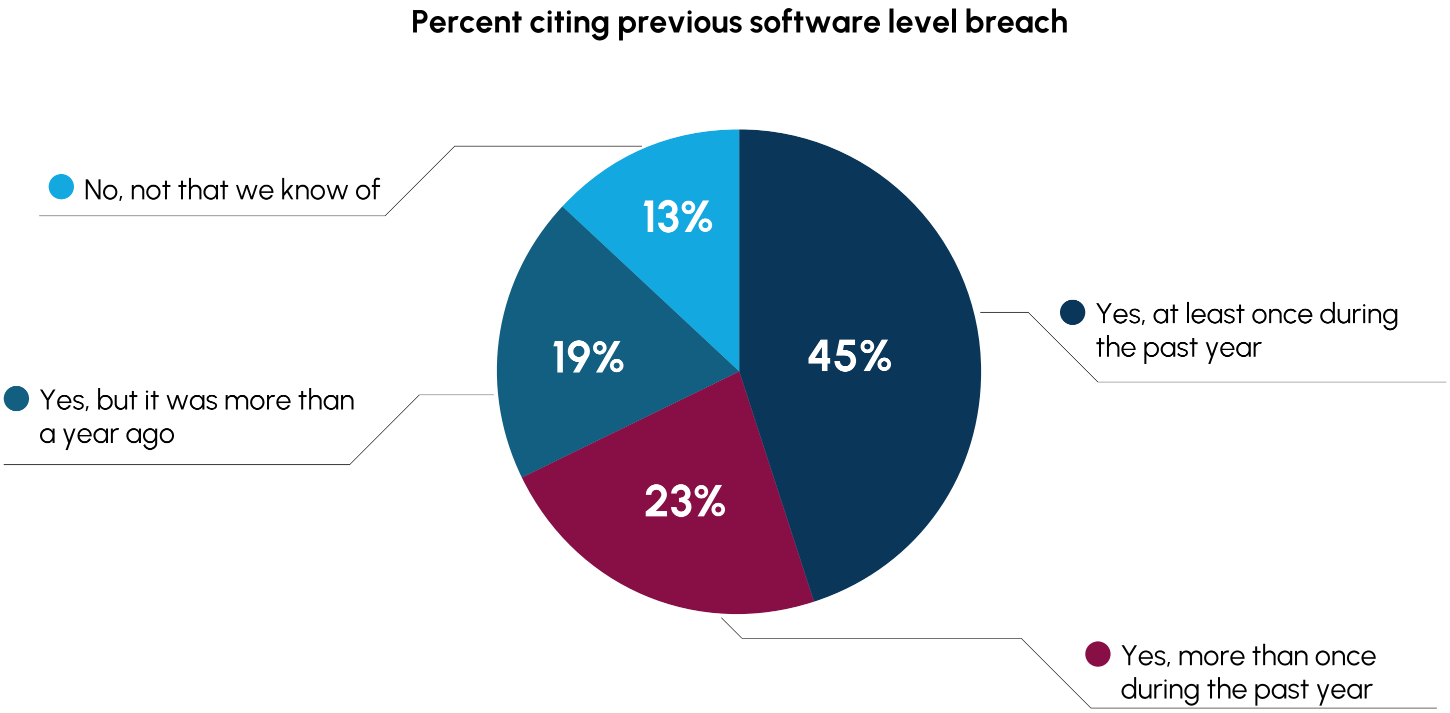
5% Chip-level exploit

BY REGION	AP	EMEA	NA	SA
Physical tampering of a device	17%	16%	27%	25%
An attack on (or through) our supply chain	38%	27%	34%	34%
External attack targeting our organization	48%	52%	54%	52%
Internal attack within our organization	58%	69%	42%	52%
Internal, accidental incident/user error	57%	58%	42%	49%
Internal malicious/intentional insider threat	41%	39%	34%	34%
Attack or incident involving our business partners/third-party suppliers	32%	24%	37%	29%
Lost/stolen asset(s)	18%	11%	22%	26%
Rootkit or firmware exploit	12%	3%	21%	12%
Chip-level exploit	5%	1%	10%	5%
Other	0%	0%	1%	1%

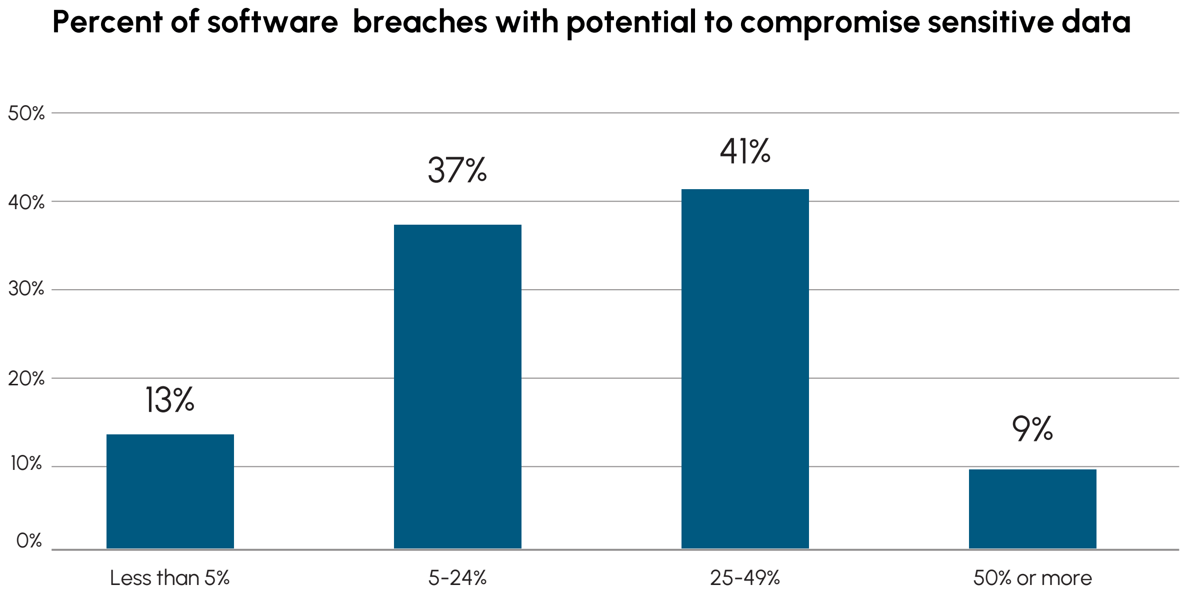
© 2024 The Futurum Group. All rights reserved.

2023 SOFTWARE SECURITY BREACHES ARE AN ISSUE

Has your organization ever experienced a software-level breach (in an application, operating system, service, or kernel-level security)?



(If YES, during past 12 months) What percent of software breaches (over the past year) had the potential to compromise sensitive data or degrade operational capacity?



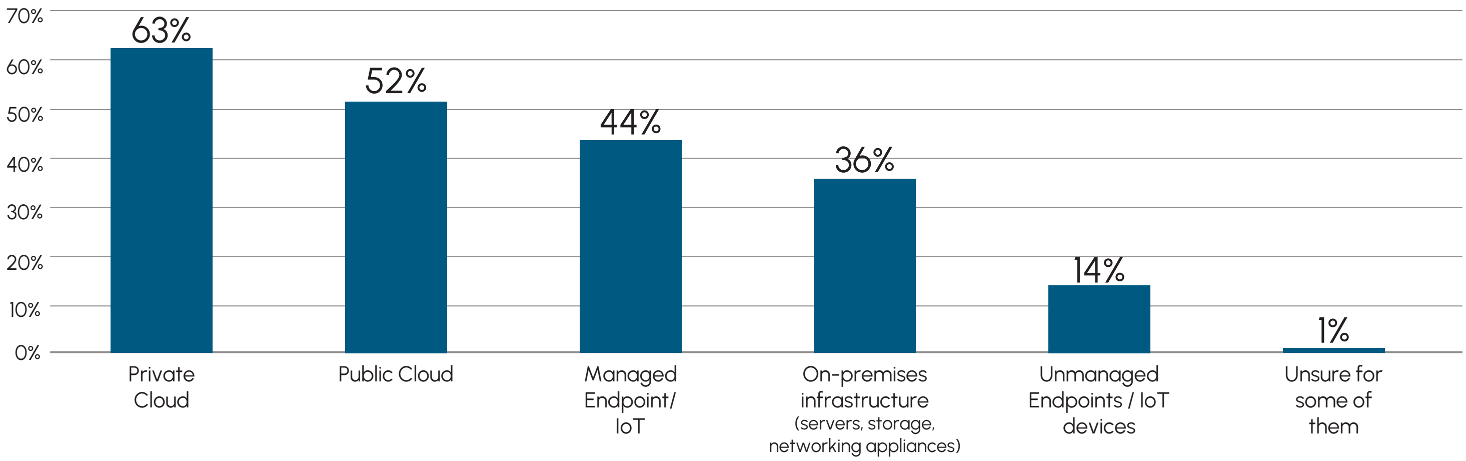
Has your organization ever experienced a software-level breach (in an application, operating system, service, or kernel-level security)?

BY REGION	AP	EMEA	NA	SA
Yes, at least once during the past year	49%	59%	31%	53%
Yes, more than once during the past year	39%	19%	18%	23%
Yes, but it was more than a year ago	11%	16%	26%	16%
No, not that we know of	2%	7%	25%	8%

(If YES, during past 12 months) What percent of software breaches (over the past year) had the potential to compromise sensitive data or degrade operational capacity?

BY REGION	AP	EMEA	NA	SA
Less than 5%	18%	10%	14%	7%
5 – 24%	37%	32%	43%	37%
25 – 49%	36%	52%	31%	45%
50% or more	10%	6%	12%	11%

Please indicate the area(s) where those breaches took place: (Select all that apply)



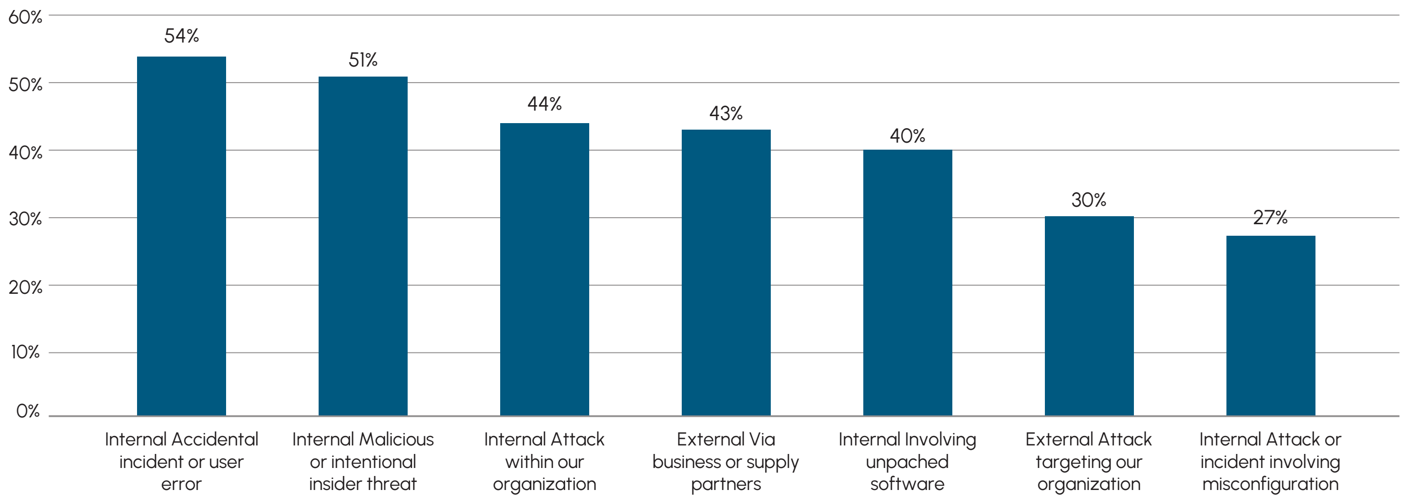
BY REGION	AP	EMEA	NA	SA
On-premises Infrastructure (servers, storage, networking appliances)	38%	27%	49%	25%
Private Cloud	63%	73%	50%	68%
Public Cloud	43%	55%	54%	56%
Managed Endpoints/IoT devices	51%	42%	43%	39%
Unmanaged Endpoints/IoT devices	18%	10%	19%	9%
Unsure for some of them	1%	0%	1%	3%

© 2024 The Futurum Group. All rights reserved.

2023 INTERNAL ISSUES TOP THE SECURITY RISKS

Please identify the top-most common types of software breaches you've experienced: (Select up to five)

Most common types (causes) of software breaches and attacks



Others (not included in chart):

18% External Social engineering (phishing)

4% Internal Lost/stolen asset(s)

BY REGION	AP	EMEA	NA	SA
External attack targeting our organization	26%	20%	46%	29%
Internal attack within our organization	54%	43%	37%	45%
Internal, accidental incident/user error	55%	61%	48%	44%
Internal malicious/intentional insider threat	63%	53%	35%	60%
Attack or incident involving our business partners/third-party suppliers	44%	47%	41%	39%
Attack or incident involving unpatched software	41%	36%	46%	35%
Attack or incident involving misconfiguration	25%	24%	32%	32%
Attack or incident involving social engineering (phishing)	15%	9%	28%	21%
Lost/stolen asset(s)	2%	0%	9%	4%

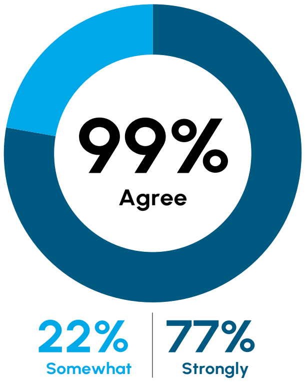
© 2024 The Futurum Group. All rights reserved.

2023 SUPPLY CHAIN DISRUPTIONS

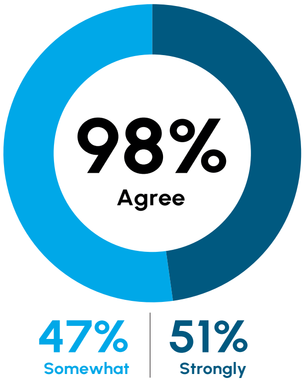
The next few questions deal with the Supply Chain (where and how products or components are supplied to your organization).

How much do you currently Agree/Disagree with the following statements? Over the past 18 months...

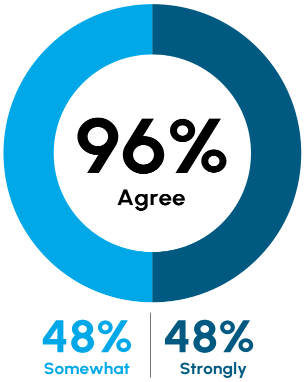
My organization is interested in supply chain security measurement and standards



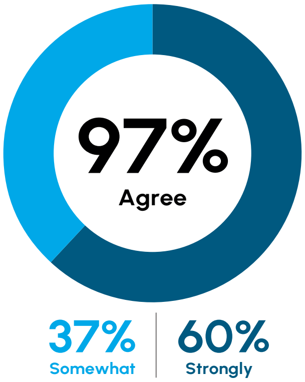
My organization would prioritize for supply chain security measurements and standars



Supply chain security measurements and standards are the responsibility of the manufacturer and should be icluded in the purchase price of equipment



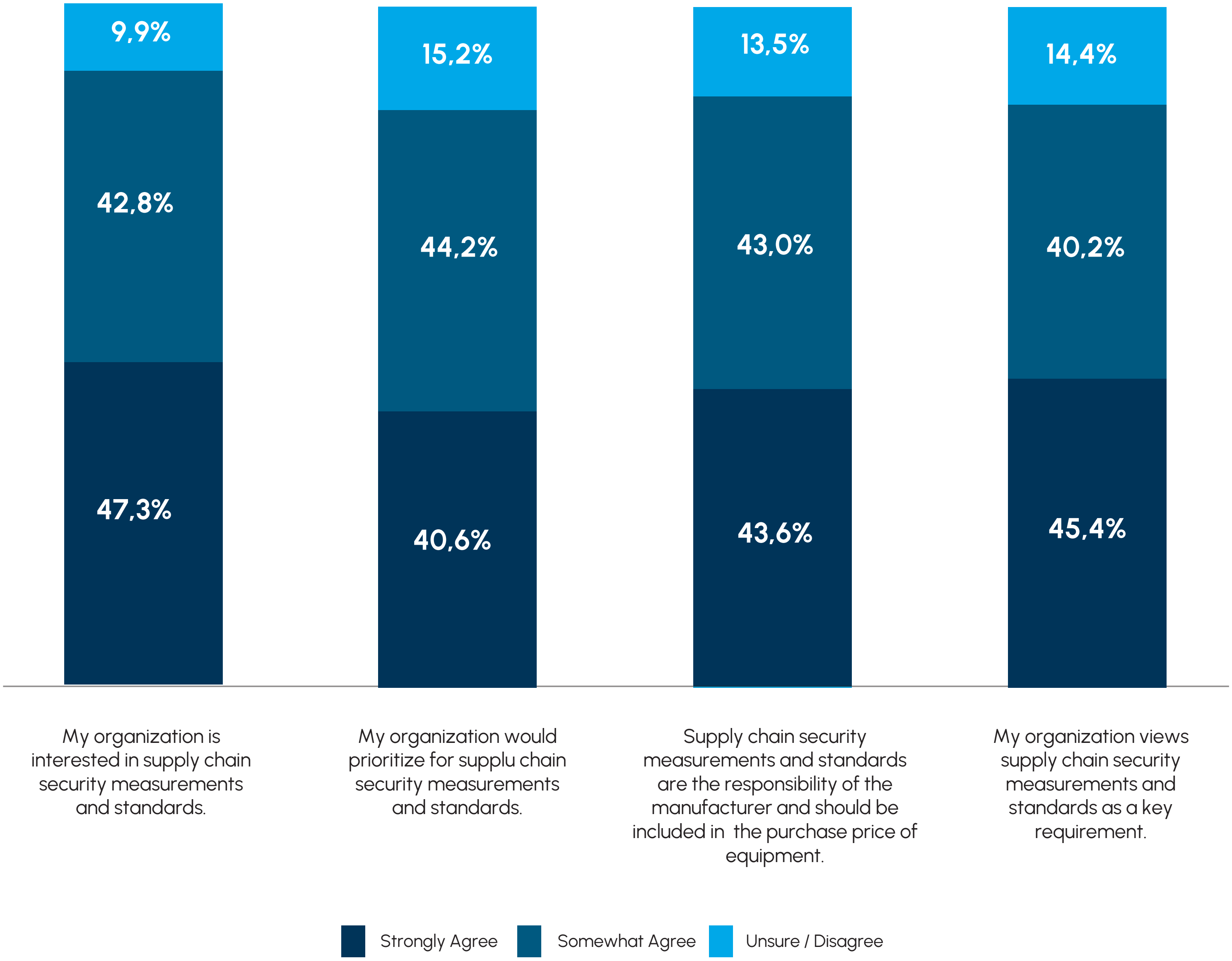
My organizaiton views supply chain security measurements and standards as a key requirement



BY REGION		Strongly Agree	Somewhat Agree
My organization is interested in supply chain security measurements and standards	AP	70%	30%
	EMEA	84%	16%
	NA	75%	24%
	SA	82%	18%
My organization would prioritize for supply chain security measurements and standards	AP	49%	50%
	EMEA	49%	52%
	NA	55%	42%
	SA	51%	49%
Supply chain security measurements and standards are the responsibility of the manufacturer and should be included in the purchase price of equipment	AP	49%	48%
	EMEA	55%	44%
	NA	42%	53%
	SA	51%	43%
My organization views supply chain security measurements and standards as a key requirement	AP	62%	35%
	EMEA	54%	46%
	NA	64%	31%
	SA	58%	40%

2023 SUPPLY CHAIN SECURITY

Please indicate if you agree/disagree with the following:

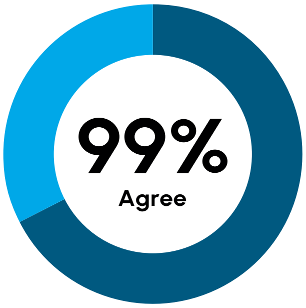


2023 SUPPLY CHAIN EXPECTATIONS

The next few questions deal with the Supply Chain (where and how products or components are supplied to your organization).

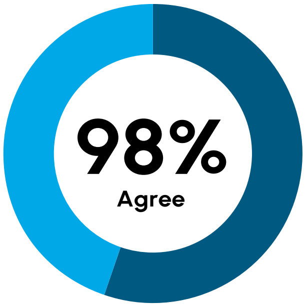
How much do you expect to Agree/Disagree in 18 – 36 months?

My organization is interested in supply chain security measurement and standards



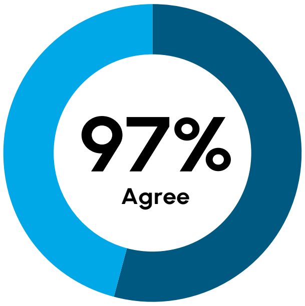
32% Somewhat | 66% Strongly

My organization would prioritize for supply chain security measurements and standars



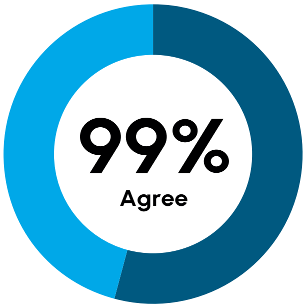
44% Somewhat | 54% Strongly

Supply chain security measurements and standards are the responsibility of the manufacturer and should be icluded in the purchase price of equipment



45% Somewhat | 53% Strongly

My organizaiton views supply chain security security measurements and standards as a key requirement

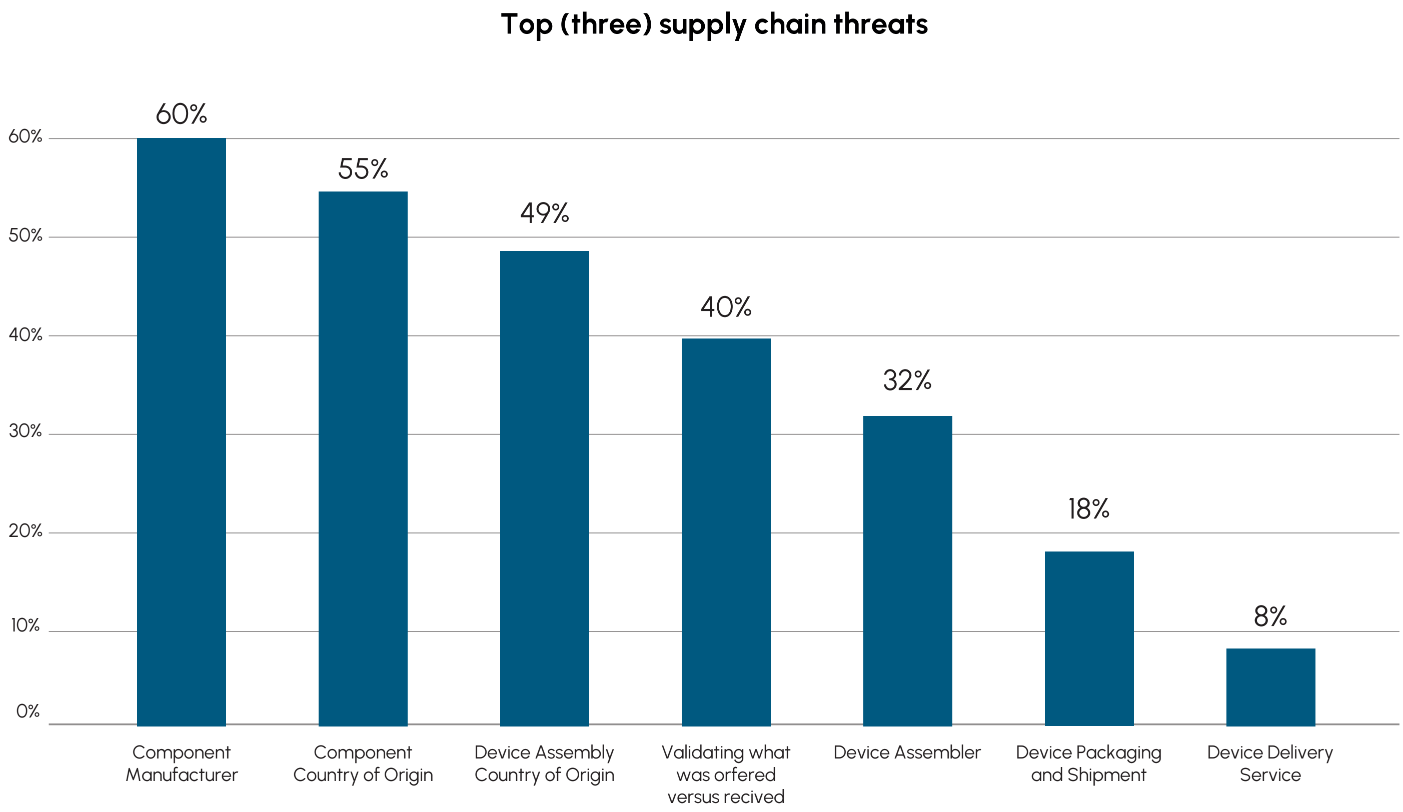


40% Somewhat | 58% Strongly

BY REGION		Strongly Agree	Somewhat Agree
My organization is interested in supply chain security measurements and standards	AP	65%	34%
	EMEA	70%	31%
	NA	62%	36%
	SA	78%	21%
My organization would prioritize for supply chain security measurements and standards	AP	48%	51%
	EMEA	54%	46%
	NA	55%	42%
	SA	62%	37%
Supply chain security measurements and standards are the responsibility of the manufacturer and should be included in the purchase price of equipment	AP	58%	40%
	EMEA	52%	49%
	NA	52%	43%
	SA	48%	48%

2023 SUPPLY CHAIN THREATS

Which of the following would you consider (or rank as) the top hardware supply chain threats to your organization today? (Select up to three)



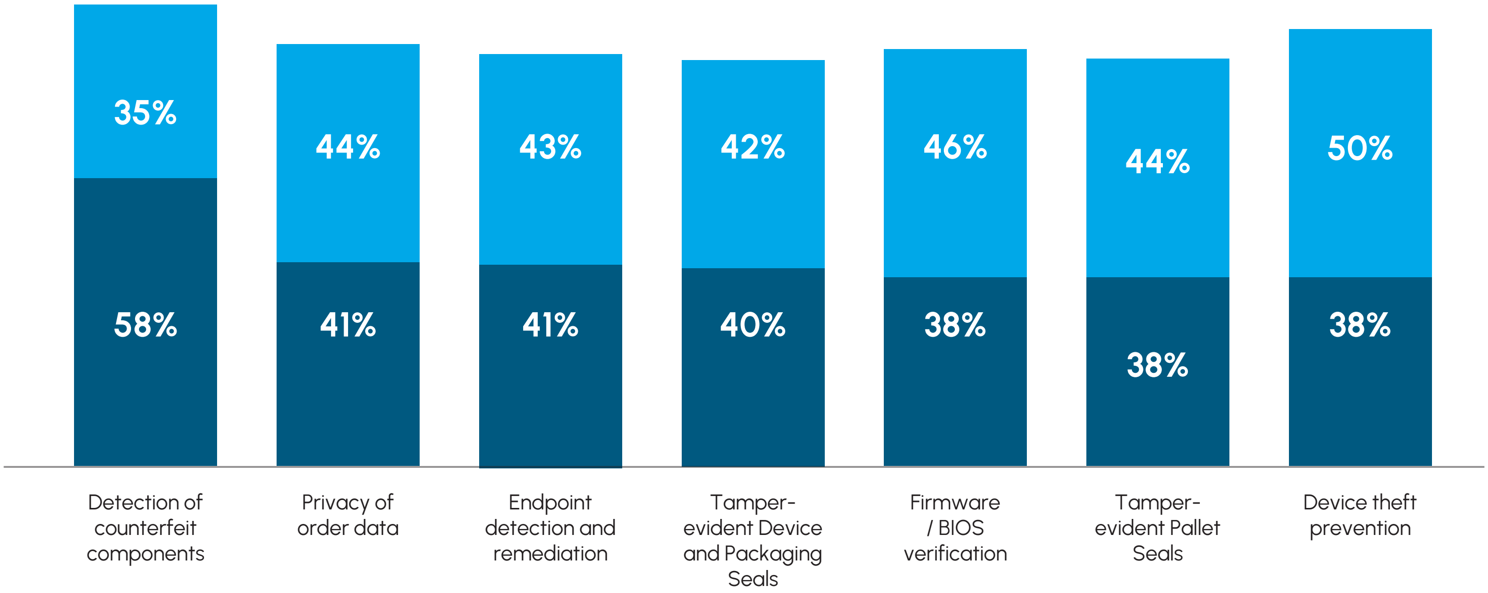
BY REGION	AP	EMEA	NA	SA
Validating what was ordered versus received	36%	39%	42%	40%
Component Country of Origin	57%	63%	48%	53%
Component Manufacturer	68%	66%	51%	60%
Device Assembly Country of Origin	53%	54%	47%	38%
Device Assembler	30%	27%	36%	36%
Device Packaging and Shipment	15%	7%	27%	15%
Device Delivery Service	4%	2%	13%	12%

© 2024 The Futurum Group. All rights reserved.

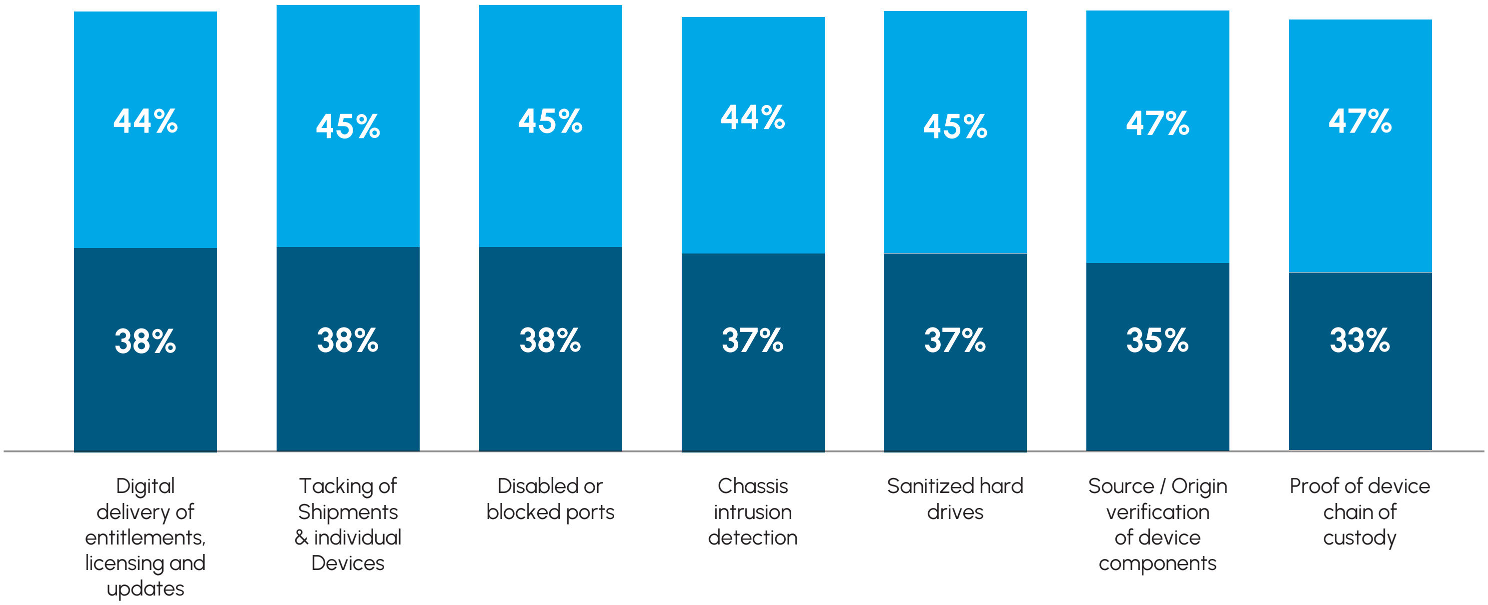
2023 SUPPLY CHAIN SECURITY MEASURES

How important are the following security measures to your organization's overall level of exposure to threats or risks in the hardware supply chain? (Please rate all)

Top critical security measures today (by Critical, Ranks 1 - 7)



Top critical security measures today (by Critical, Ranks 8 - 14)

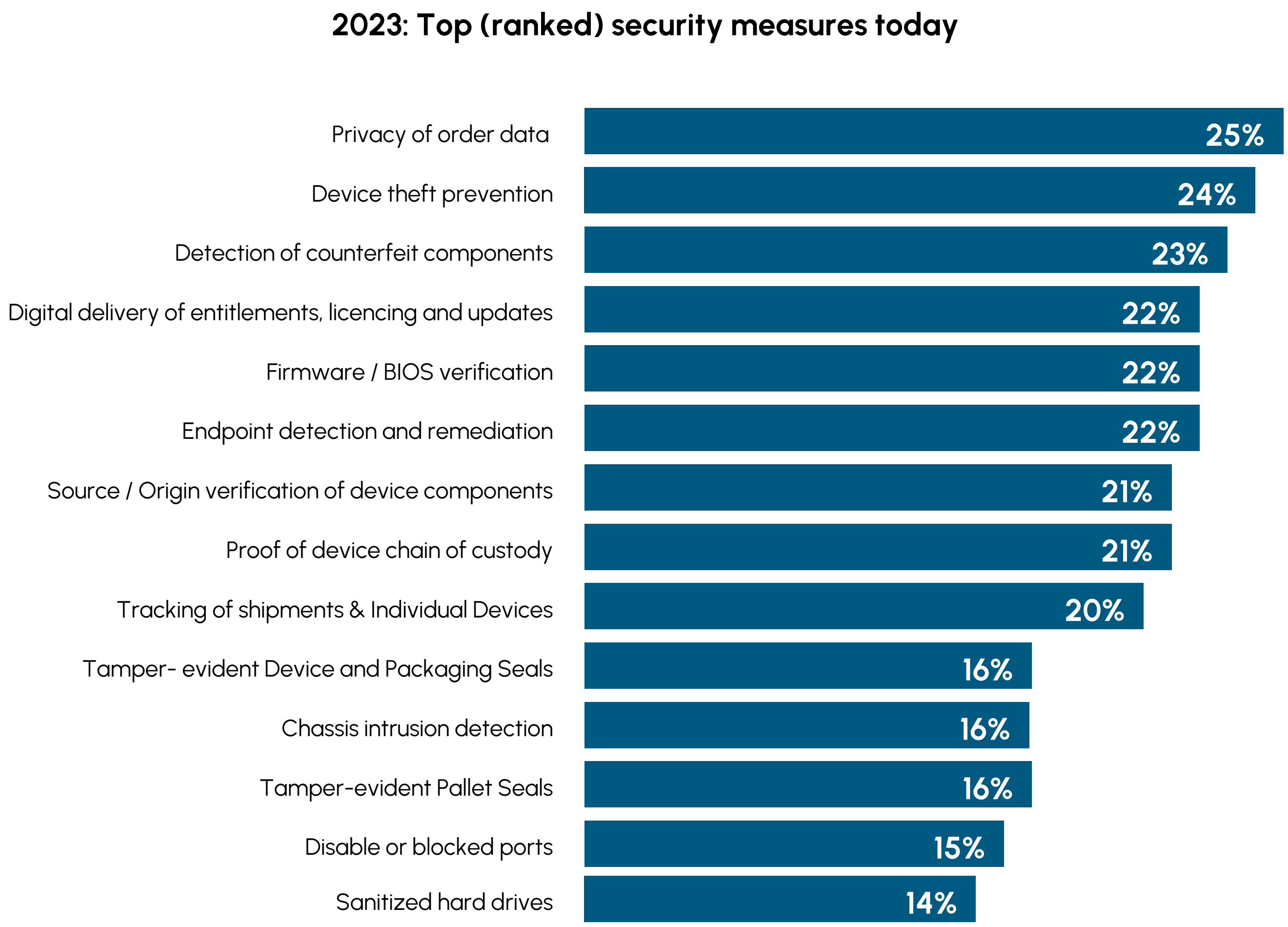


© 2024 The Futurum Group. All rights reserved.

How important are the following security measures to your organization's overall level of exposure to threats or risks in the hardware supply chain? (Please rate all)

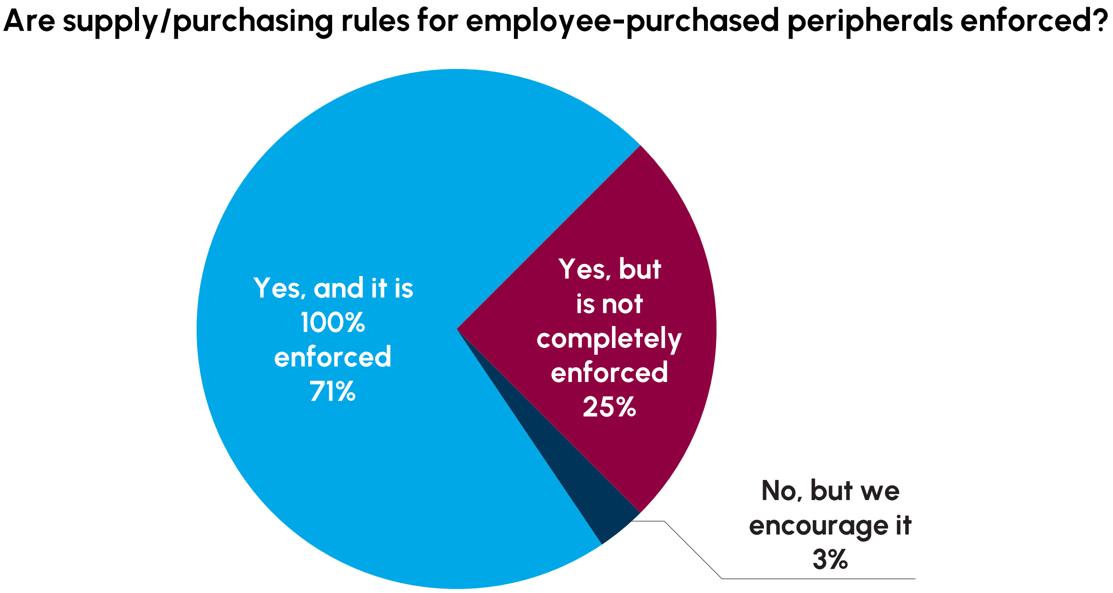
BY REGION		Critically	Moderately
Detection of counterfeit components	AP	49%	45%
	EMEA	69%	26%
	NA	53%	36%
	SA	65%	32%
Device theft prevention	AP	30%	50%
	EMEA	33%	60%
	NA	45%	41%
	SA	40%	55%
Firmware/BIOS verification	AP	27%	54%
	EMEA	38%	50%
	NA	42%	41%
	SA	47%	41%
Tamper-evident Device and Packaging Seals	AP	32%	41%
	EMEA	43%	41%
	NA	41%	41%
	SA	40%	48%
Endpoint detection and remediation	AP	32%	53%
	EMEA	43%	41%
	NA	46%	36%
	SA	34%	54%
Proof of device chain of custody	AP	31%	46%
	EMEA	38%	46%
	NA	31%	47%
	SA	32%	51%
Source/Origin verification of device components	AP	34%	50%
	EMEA	35%	50%
	NA	35%	43%
	SA	40%	49%
Digital delivery of entitlements, licensing and updates	AP	33%	44%
	EMEA	42%	41%
	NA	37%	44%
	SA	34%	49%
Tamper-evident Pallet Seals	AP	33%	46%
	EMEA	41%	46%
	NA	36%	41%
	SA	46%	39%
Sanitized hard drives	AP	29%	51%
	EMEA	38%	45%
	NA	40%	42%
	SA	37%	43%
Tracking of Shipments & Individual Devices	AP	30%	43%
	EMEA	40%	45%
	NA	41%	43%
	SA	33%	53%
Disabled or blocked ports	AP	29%	53%
	EMEA	44%	42%
	NA	35%	43%
	SA	43%	43%
Chassis intrusion detection	AP	35%	44%
	EMEA	42%	45%
	NA	35%	42%
	SA	35%	50%
Privacy of order data	AP	36%	46%
	EMEA	38%	48%
	NA	44%	39%
	SA	49%	43%

Please select your organizations top security measures (Select up to three)



2023 SUPPLY CHAIN PURCHASING RULES

Does your organization require end-users within your organization to purchase or use only authentic peripheral devices from suppliers that are approved by your IT department?



2023 SUPPLY CHAIN SECURITY MEASURES (PRIORITIZED)

Please select your organizations top security measures (Select up to three)

BY REGION	AP	EMEA	NA	SA
Detection of counterfeit components	36%	39%	42%	40%
Device theft prevention	57%	63%	48%	53%
Firmware/BIOS verification	68%	66%	51%	60%
Tamper-evident Device and Packaging Seals	53%	54%	47%	38%
Endpoint detection and remediation	30%	27%	36%	36%
Proof of device chain of custody	15%	7%	27%	15%
Source/Origin verification of device components	4%	2%	13%	12%
Digital delivery of entitlements, licensing and updates	4%	4%	4%	4%
Tamper-evident Pallet Seals	4%	4%	4%	4%
Sanitized hard drives	4%	4%	4%	4%
Tracking of Shipments & Individual Devices	4%	4%	4%	4%
Disabled or blocked ports	4%	4%	4%	4%
Chassis intrusion detection	4%	4%	4%	4%
Privacy of order data	4%	4%	4%	4%

Does your organization require end-users within your organization to purchase or use only authentic peripheral devices from suppliers that are approved by your IT department?measures (Select up to three)

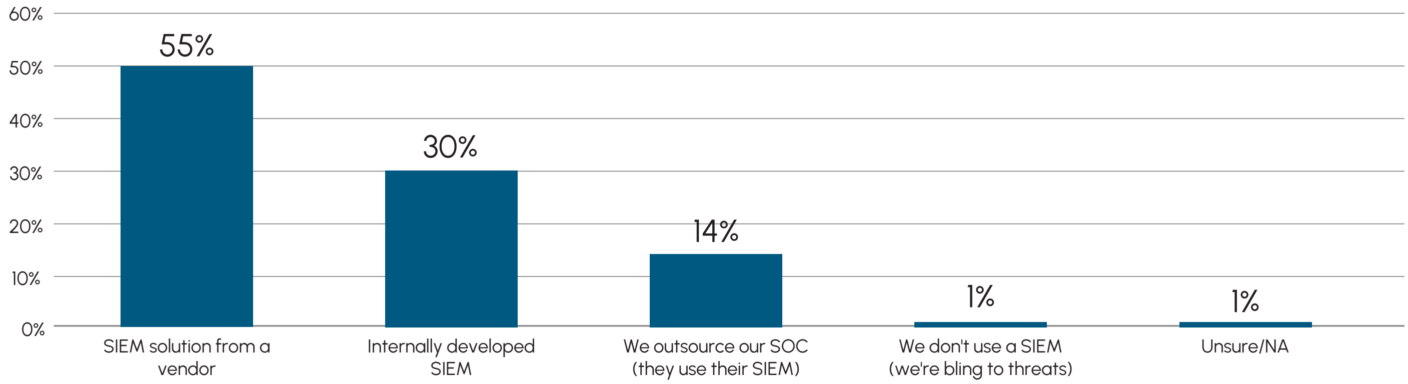
BY REGION	AP	EMEA	NA	SA
Yes, and it is 100% enforced	71%	79%	64%	74%
Yes, but it is not completely enforced	24%	20%	29%	25%
No, but we encourage it	5%	1%	6%	0%
No, end-users can purchase/use what they need	0%	0%	1%	1%

2023 HOME-GROWN SIEM SOLUTIONS ARE POPULAR

We're going to ask you about two types of Security Monitoring solutions starting with SIEM (Security Info & Event Management) tools followed by EDR (Endpoint Detection & Response) tools.

What are you (primarily) using for monitoring your security environment (SIEM)?

Primary approach to security monitoring today (select only one)

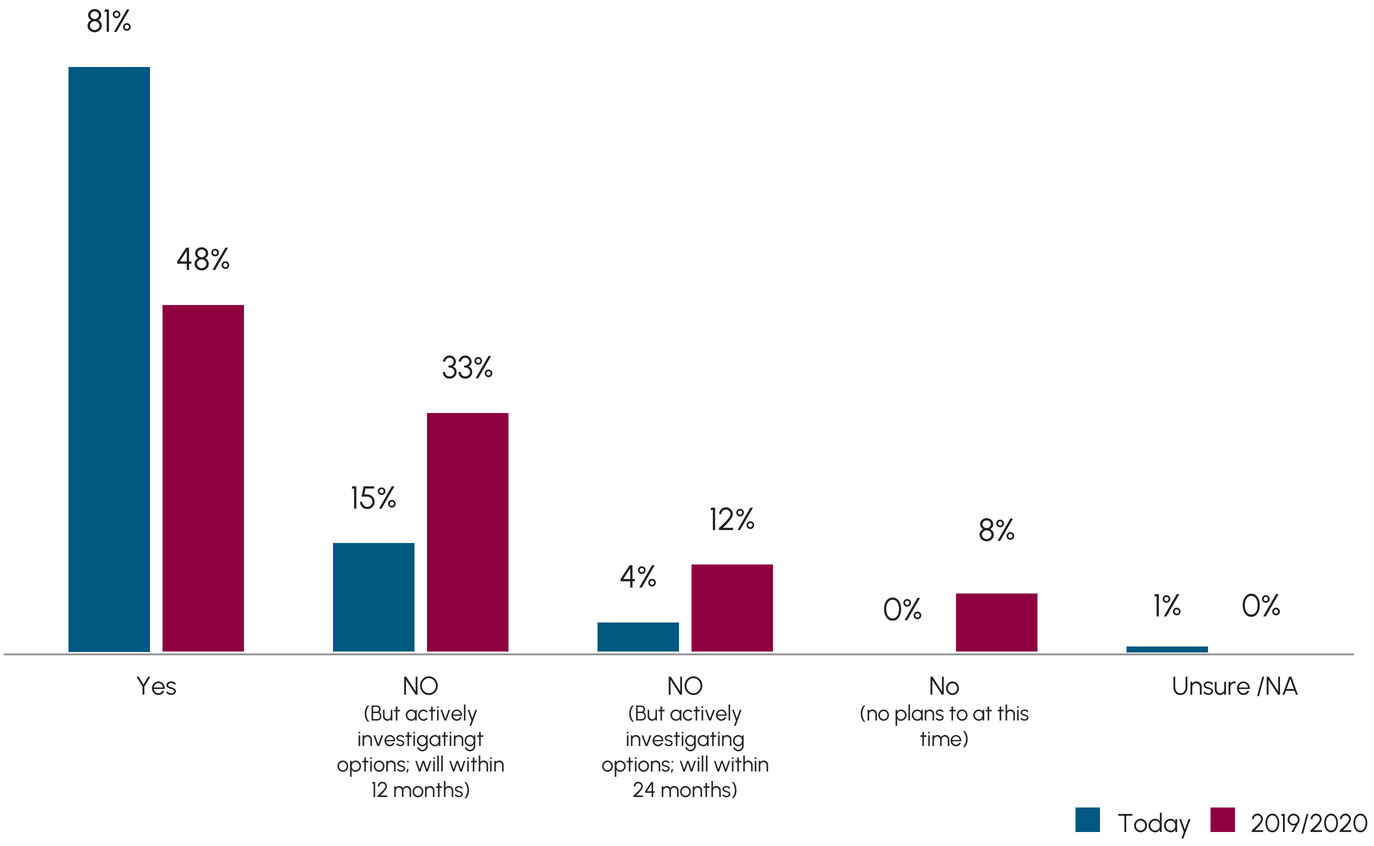


BY REGION	AP	EMEA	NA	SA
We purchased a Security Information and Event Management (SIEM) solution from a vendor	60%	49%	55%	64%
We use a SIEM we developed in house	26%	37%	26%	28%
We outsource our SOC, they use their SIEM	13%	14%	16%	8%
We don't use a SIEM (we're blind to threats)	1%	0%	1%	0%

© 2024 The Futurum Group. All rights reserved.

2023 ORGANIZATIONS UNDERSTAND THE VALUE OF EDR SOLUTIONS

Do you currently use an EDR (Endpoint Detection and Response) security solution?



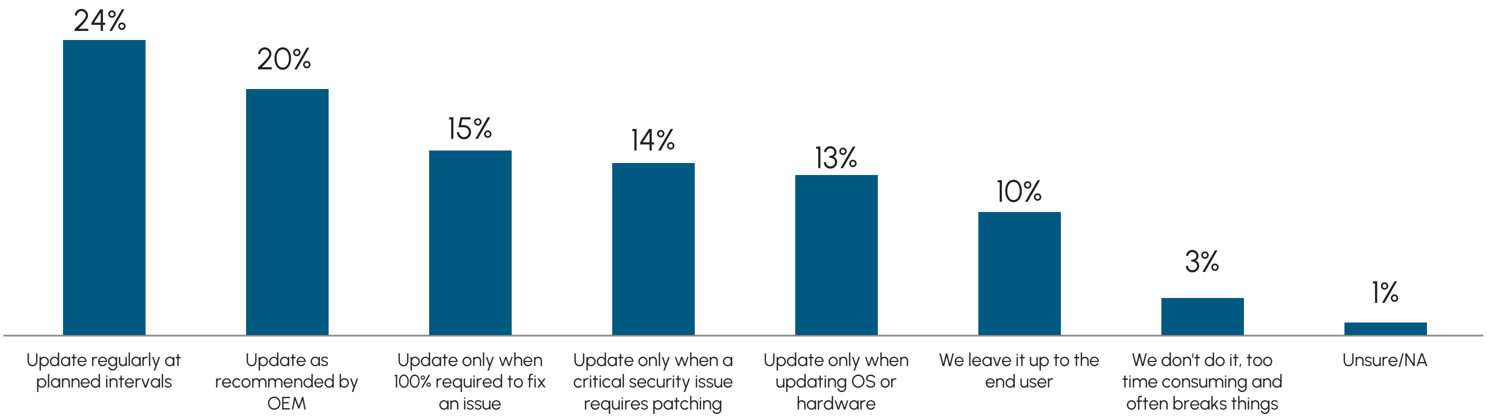
BY REGION	AP	EMEA	NA	SA
Yes	88%	84%	73%	85%
No (but actively investigating options; will within 12 months)	6%	14%	20%	13%
No (but actively investigating options; will within 24 months)	7%	1%	5%	2%
No (no plans to at this time)	0%	0%	1%	0%

© 2024 The Futurum Group. All rights reserved.

2023 PREFERENCES FOR BIOS HAVE EVOLVED

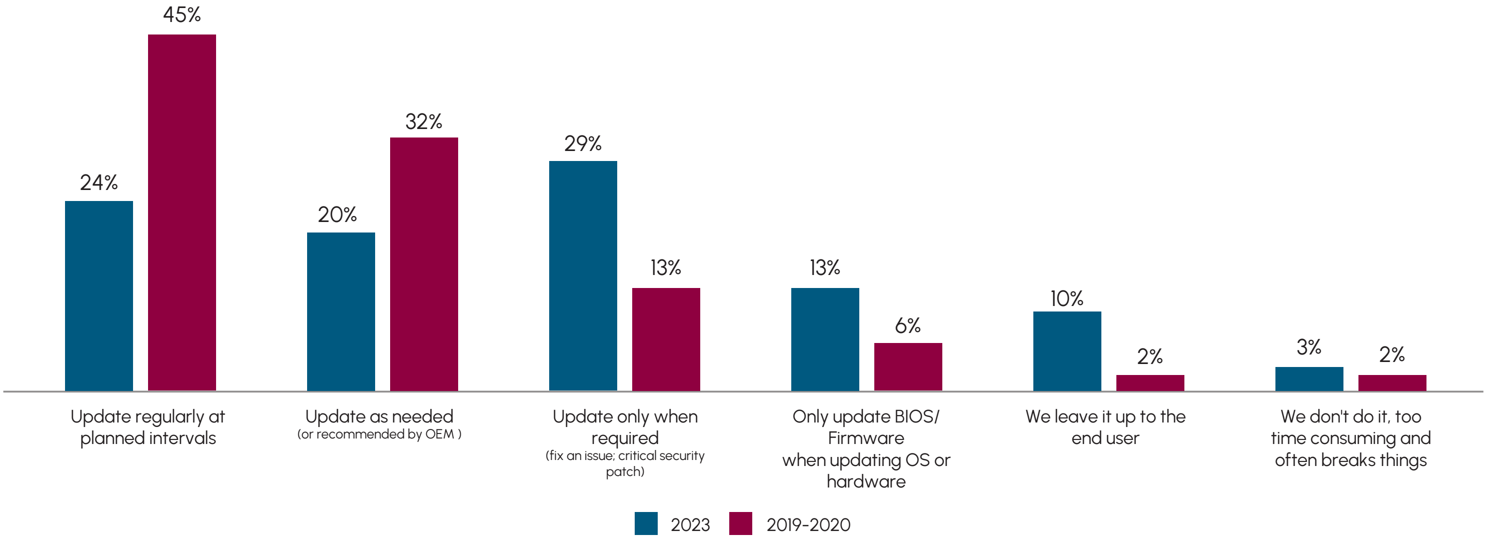
What is your primary approach to BIOS/Firmware updates? (Select one)

Primary approach to BIOS/Firmware updates



BIOS UPDATES: Y/Y COMPARISON

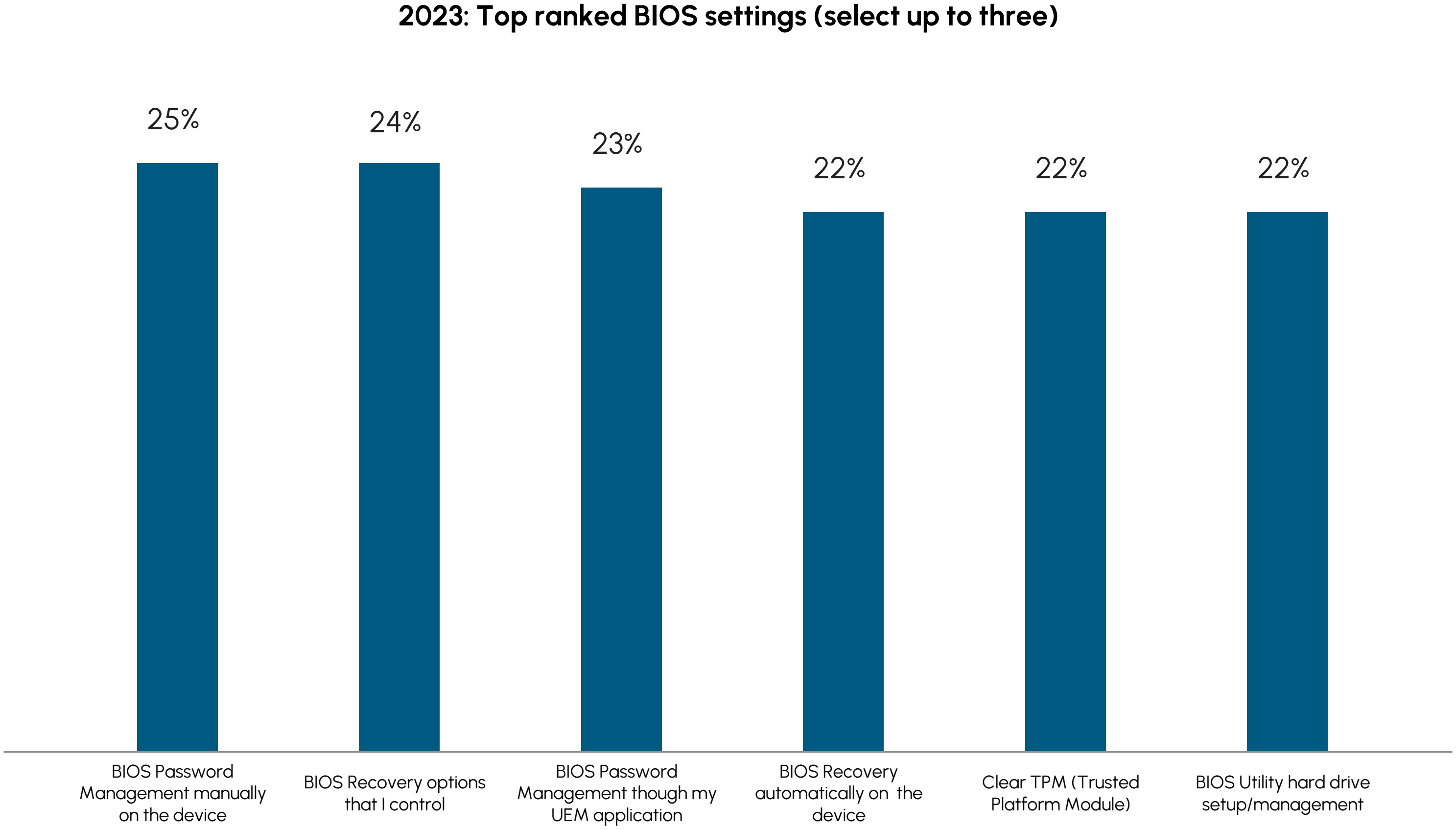
What is your primary approach to BIOS/Firmware updates? (Select one)



BY REGION	AP	EMEA	NA	SA
We update regularly at planned intervals	21%	21%	28%	28%
We only update BIOS/Firmware when 100% required to fix an issue	16%	18%	13%	14%
We only update BIOS/Firmware when updating OS or hardware	16%	13%	14%	8%
We only update BIOS/Firmware when a critical security issue requires patching	17%	16%	11%	11%
We don't do it, updating BIOS/Firmware is time consuming and often breaks things	1%	2%	3%	6%
We leave it up to the end user to keep BIOS/Firmware updated on their devices	15%	9%	9%	7%
We update BIOS/Firmware based upon the OEM's advice (update as recommended).	16%	20%	22%	24%

2023 PREFERENCES FOR BIOS SETTINGS

Which of the following BIOS settings would you consider the top ranked or most important to your organization's security strategy? (Select up to three)



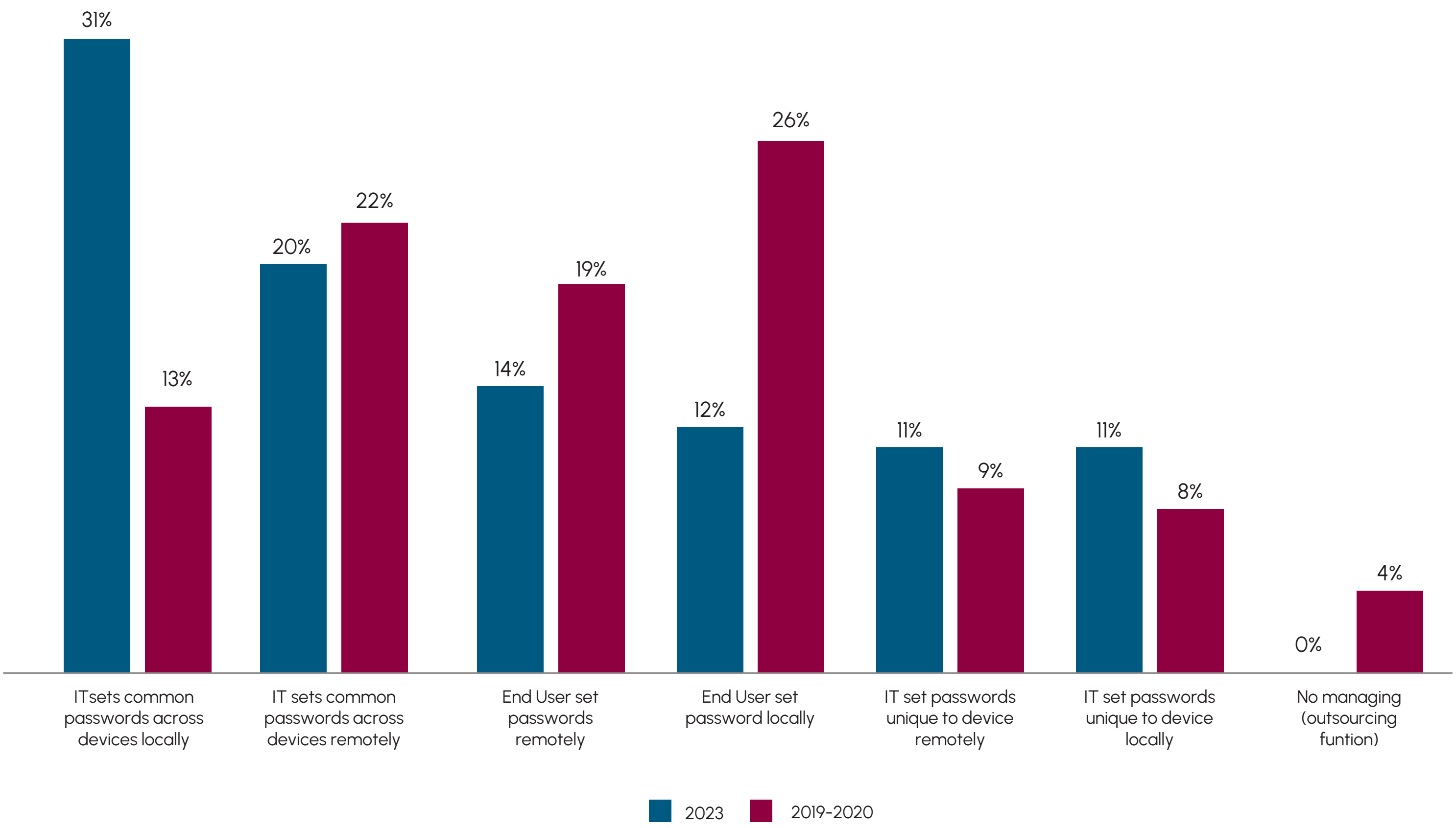
BY REGION	AP	EMEA	NA	SA
BIOS Recovery automatically on the device	37%	44%	42%	41%
BIOS Recovery options that I control	59%	67%	51%	55%
BIOS Password Management manually on the device	70%	68%	47%	57%
BIOS Password Management though my UEM application	44%	37%	47%	43%
Clear TPM (Trusted Platform Module)	23%	9%	26%	21%
BIOS Utility hard drive setup/management	11%	3%	23%	20%

© 2024 The Futurum Group. All rights reserved.

PREFERENCES FOR BIOS SETTINGS (IN 12 – 18 MONTHS)

Which of the following BIOS settings would you consider the top ranked or most important to your organization's security strategy? (Select up to three)

BIOS Password Preferences (Y/Y Comparison, select only one)



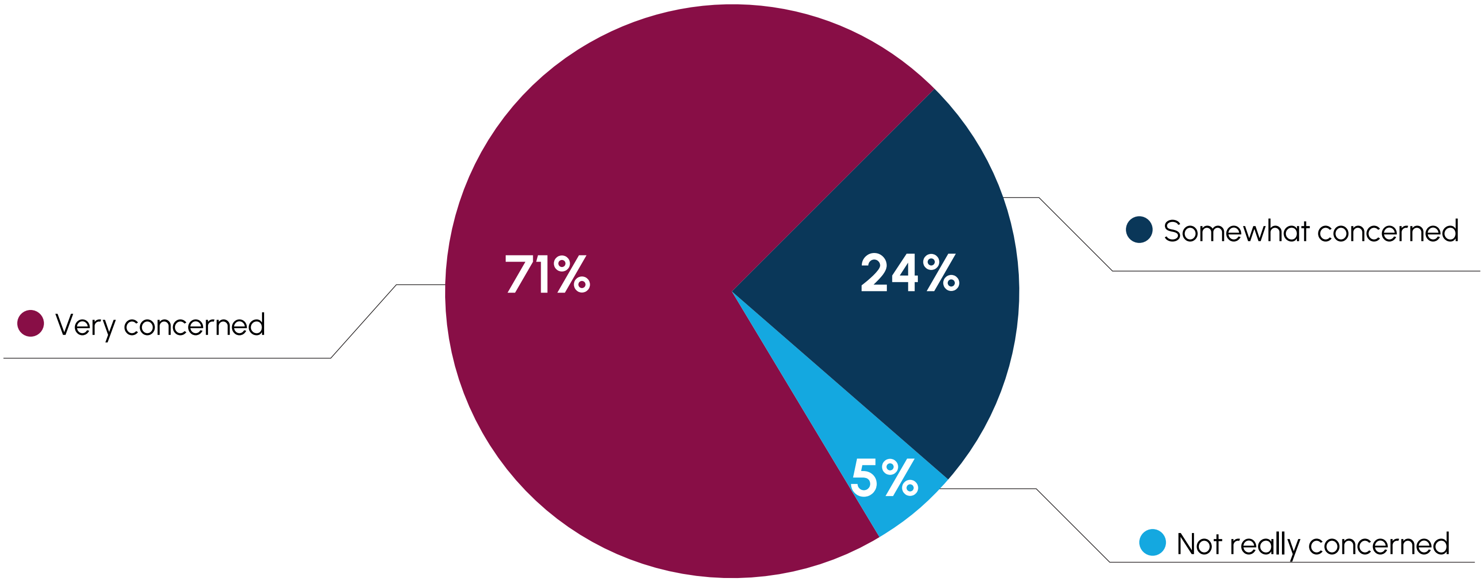
BY REGION	AP	EMEA	NA	SA
End Users set passwords locally	10%	12%	14%	13%
End Users set passwords remotely	9%	17%	14%	18%
IT sets common passwords across devices locally	36%	38%	26%	20%
IT sets common passwords across devices remotely	22%	21%	18%	19%
IT sets passwords unique to device locally	13%	5%	12%	15%
IT sets passwords unique to device remotely	11%	6%	14%	13%
Not managing (outsourcing function)	0%	0%	1%	1%

© 2024 The Futurum Group. All rights reserved.

2023 PERIPHERAL RISKS

How concerned are you that your organization's sensitive data could be potentially compromised (or at risk) due to a peripheral device security breach?

Concern over sensitive data being at risk due to a peripheral breach

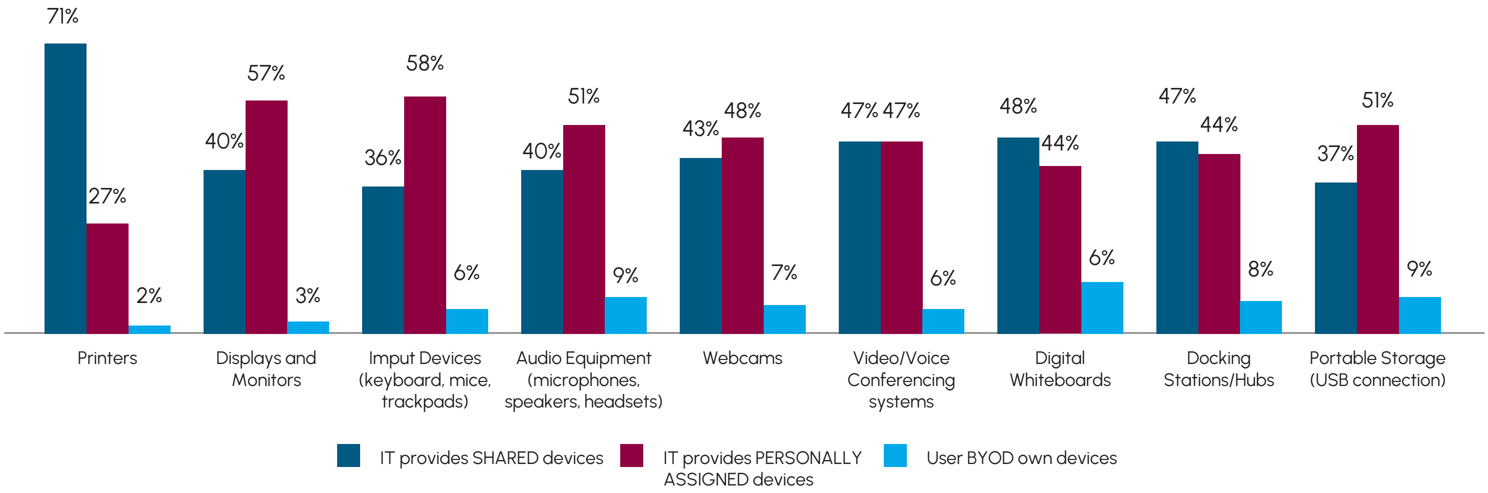


BY REGION	AP	EMEA	NA	SA
Very concerned	84%	82%	56%	70%
Somewhat concerned	15%	15%	36%	22%
Not really concerned	1%	3%	8%	8%

2023 PERIPHERAL DEPLOYMENTS (WIRED)

Please select the primary (most common) way each of the following WIRED peripheral devices are used (provided)

How are WIRED peripheral devices provided?



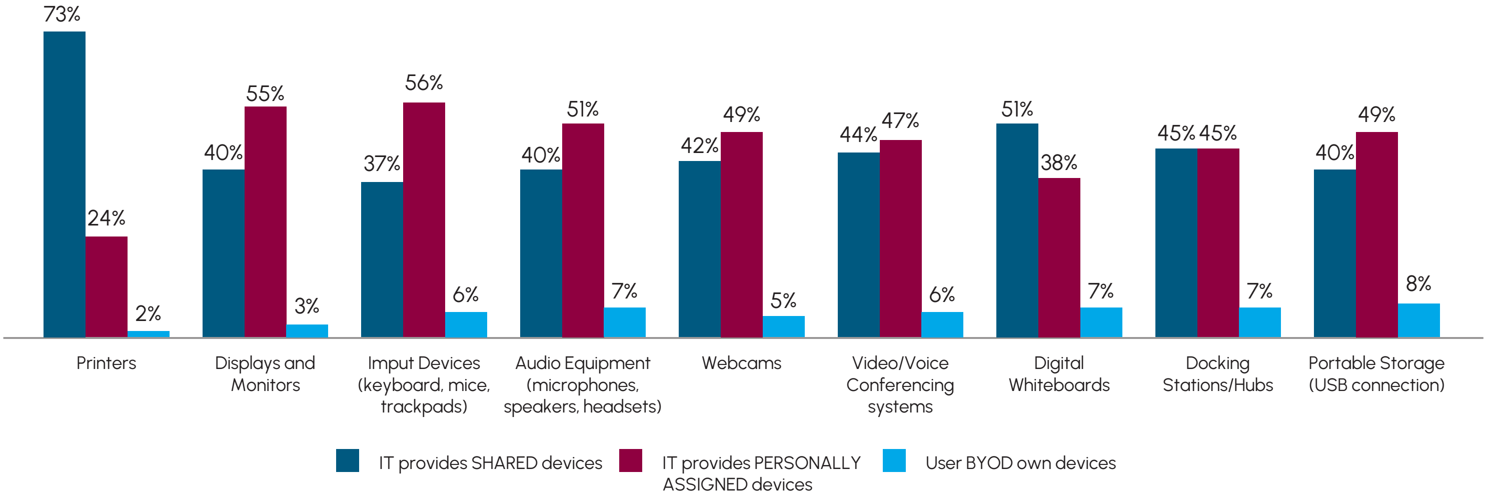
BY REGION		IT provides shared devices)	IT provides personal device	Users bring their own
Printers	AP	58%	39%	3%
	EMEA	79%	20%	1%
	NA	69%	28%	3%
	SA	77%	23%	0%
Displays and Monitors	AP	40%	57%	3%
	EMEA	46%	52%	2%
	NA	36%	60%	4%
	SA	36%	63%	1%
Imput Devices (keyboard, mice, trackpads)	AP	37%	54%	9%
	EMEA	44%	52%	4%
	NA	29%	65%	6%
	SA	33%	57%	10%
Audio Equipment (microphones, speakers, headsets)	AP	46%	41%	13%
	EMEA	43%	52%	6%
	NA	38%	51%	10%
	SA	27%	64%	8%
Webcams	AP	36%	54%	10%
	EMEA	50%	45%	4%
	NA	44%	45%	8%
	SA	35%	59%	6%
Video/Voice Conferencing systems	AP	44%	50%	6%
	EMEA	48%	48%	4%
	NA	49%	44%	6%
	SA	44%	50%	6%
Digital Whiteboards	AP	44%	48%	8%
	EMEA	54%	39%	5%
	NA	46%	45%	6%
	SA	48%	43%	5%
Docking Stations/Hubs	AP	47%	46%	8%
	EMEA	52%	41%	8%
	NA	43%	46%	9%
	SA	47%	43%	6%
Portable Storage (USB connection)	AP	44%	48%	8%
	EMEA	35%	59%	6%
	NA	36%	46%	12%
	SA	37%	54%	6%

© 2024 The Futurum Group. All rights reserved.

2023 PERIPHERAL DEPLOYMENTS (WIRELESS)

Please select the primary (most common) way each of the following WIRELESS peripheral devices are used (provided)

How are WIRELESS peripheral devices provided?

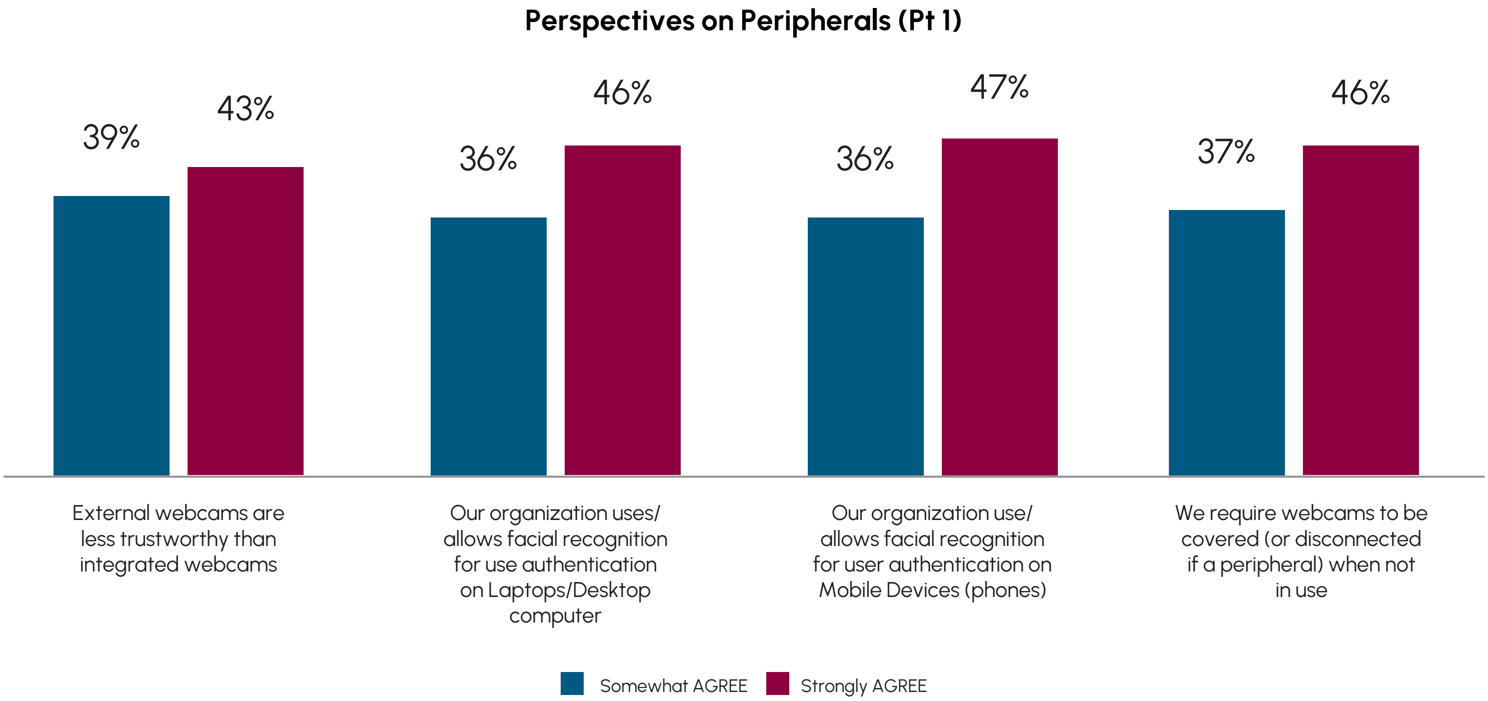


BY REGION		IT provides shared devices)	IT provides personal device	Users bring their own
Printers	AP	70%	28%	2%
	EMEA	79%	20%	1%
	NA	68%	26%	4%
	SA	79%	18%	3%
Displays and Monitors	AP	39%	55%	5%
	EMEA	45%	53%	1%
	NA	36%	56%	4%
	SA	44%	53%	1%
Imput Devices (keyboard, mice, trackpads)	AP	36%	53%	11%
	EMEA	42%	53%	5%
	NA	35%	57%	6%
	SA	32%	62%	4%
Audio Equipment (microphones, speakers, headsets)	AP	42%	51%	7%
	EMEA	47%	50%	3%
	NA	36%	51%	11%
	SA	32%	60%	6%
Webcams	AP	40%	55%	4%
	EMEA	48%	47%	4%
	NA	41%	45%	7%
	SA	32%	59%	6%
Video/Voice Conferencing systems	AP	44%	44%	12%
	EMEA	42%	53%	5%
	NA	46%	45%	5%
	SA	48%	47%	4%
Digital Whiteboards	AP	55%	38%	8%
	EMEA	52%	37%	9%
	NA	50%	37%	7%
	SA	46%	46%	4%
Docking Stations/Hubs	AP	39%	53%	7%
	EMEA	53%	41%	6%
	NA	45%	42%	8%
	SA	39%	51%	4%
Portable Storage (USB connection)	AP	43%	47%	9%
	EMEA	42%	51%	6%
	NA	37%	47%	8%
	SA	38%	49%	10%

© 2024 The Futurum Group. All rights reserved.

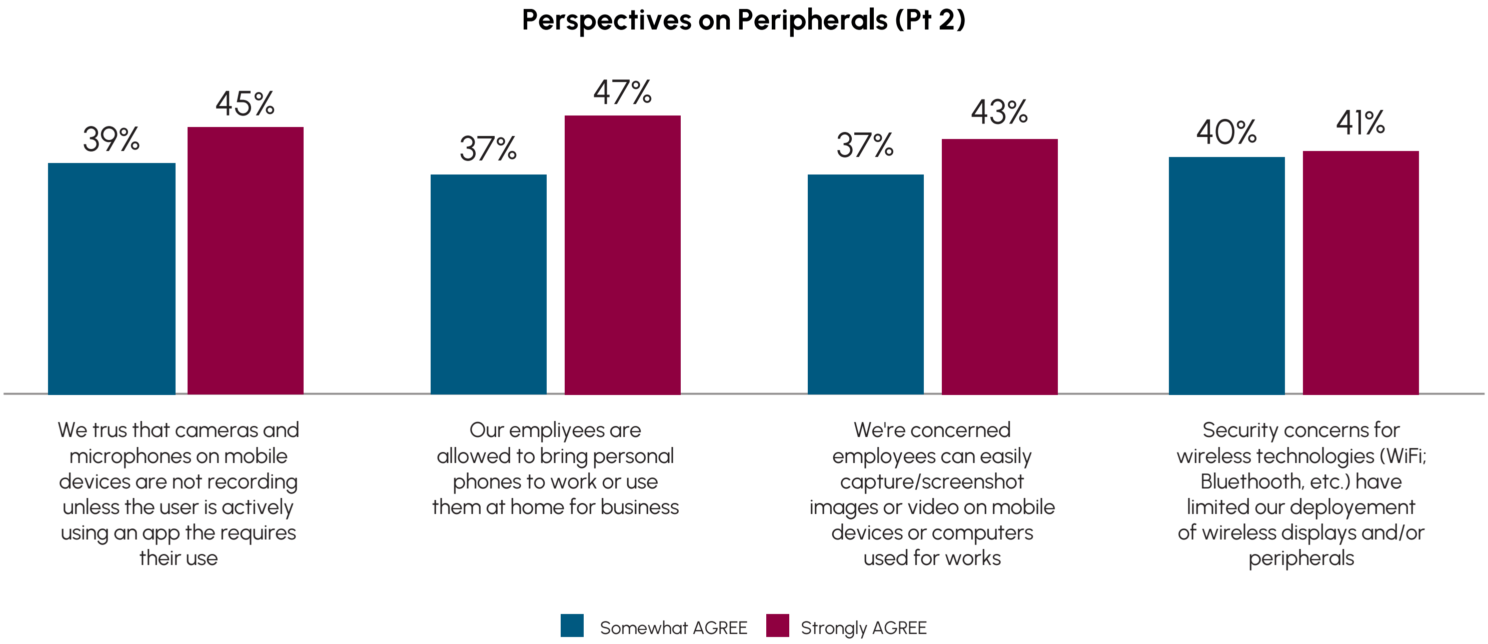
2023 PERIPHERAL PERSPECTIVES, 1

Would you agree or disagree with the following statements:



PERIPHERAL PERSPECTIVES, 2

Would you agree or disagree with the following statements:



© 2024 The Futurum Group. All rights reserved.

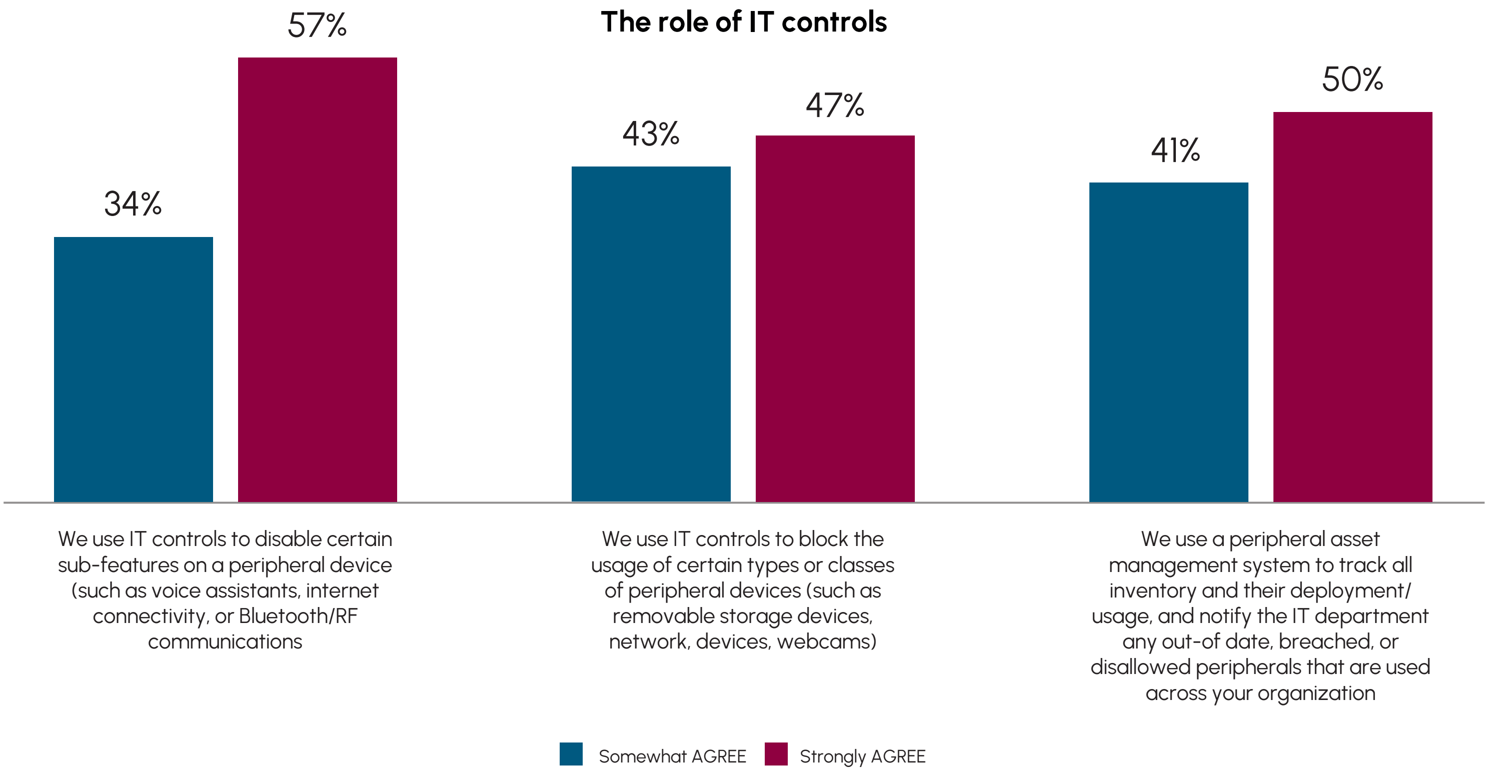
PERIPHERAL PERSPECTIVES, 2

Would you agree or disagree with the following statements:

BY REGION		Agree Overall	Strongly Agree	Somewhat Agree
External webcams are less trustworthy than integrated webcams	AP	83%	46%	37%
	EMEA	94%	48%	45%
	NA	74%	38%	36%
	SA	76%	37%	38%
Our organization uses/allows facial recognition for user authentication on Laptops/Desktop computers	AP	89%	49%	40%
	EMEA	93%	52%	41%
	NA	71%	39%	32%
	SA	79%	48%	31%
Our organization uses/allows facial recognition for user authentication on Mobile Devices (phones)	AP	89%	46%	43%
	EMEA	92%	51%	41%
	NA	75%	47%	29%
	SA	82%	46%	36%
We require webcams to be covered (or disconnected if a peripheral) when not in use	AP	87%	46%	41%
	EMEA	93%	51%	42%
	NA	75%	45%	30%
	SA	74%	32%	41%
We trust that cameras and microphones on mobile devices are not recording (unless app that requires use)	AP	86%	43%	43%
	EMEA	92%	54%	38%
	NA	79%	40%	39%
	SA	81%	41%	39%
Our employees are allowed to bring personal phones to work or use them at home for business	AP	79%	43%	37%
	EMEA	92%	54%	38%
	NA	80%	43%	37%
	SA	82%	48%	34%
We're concerned employees can easily capture/screenshot images or video on mobile devices or computers used for work	AP	81%	46%	35%
	EMEA	91%	51%	41%
	NA	74%	37%	37%
	SA	72%	42%	29%
DSecurity concerns for wireless technologies have limited our deployment of wireless displays and/or peripherals	AP	82%	44%	38%
	EMEA	92%	49%	43%
	NA	74%	36%	38%
	SA	74%	34%	39%

2023 THE ROLE OF IT CONTROLS FOR PERIPHERALS

Would you agree or disagree with the following statements:



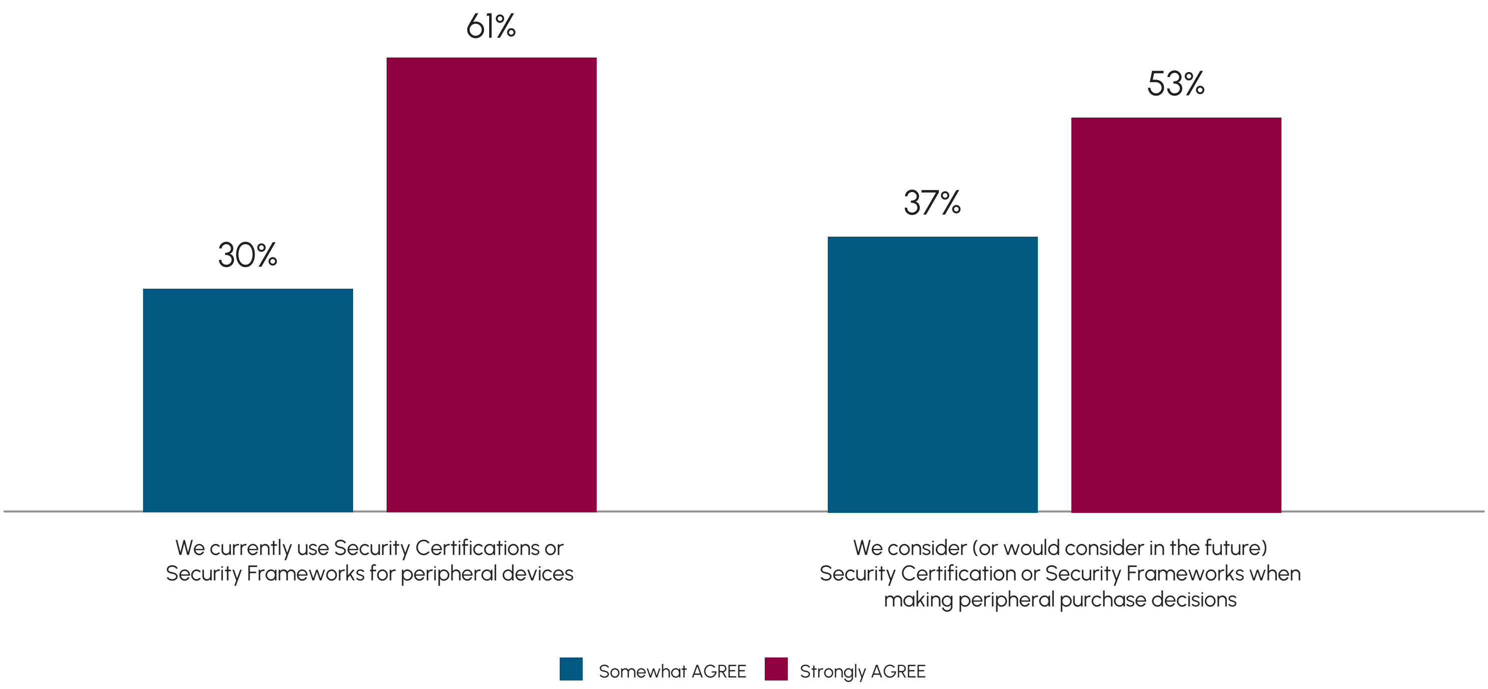
BY REGION		Agree Overall	Strongly Agree	Somewhat Agree
We use IT controls to disable certain sub-features on a peripheral device (such as voice assistants, internet connectivity, or Bluetooth/RF communications)	AP	90%	56%	33%
	EMEA	97%	61%	36%
	NA	87%	56%	32%
	SA	86%	52%	34%
We use IT controls to block the usage of certain types or classes of peripheral devices (such as removable storage devices, network devices, webcams)	AP	89%	42%	47%
	EMEA	96%	50%	46%
	NA	85%	47%	39%
	SA	88%	48%	40%
We use a peripheral asset management system to track all inventory and their deployment/usage, and notify the IT department any out-of-date, breached, or disallowed peripherals that are used across your organization	AP	89%	49%	40%
	EMEA	95%	51%	45%
	NA	88%	49%	38%
	SA	86%	49%	37%

© 2024 The Futurum Group. All rights reserved.

2023 THE ROLE OF FRAMEWORKS FOR PERIPHERALS

Would you agree or disagree with the following statements:

The role of Security Frameworks and Certifications for Peripherals

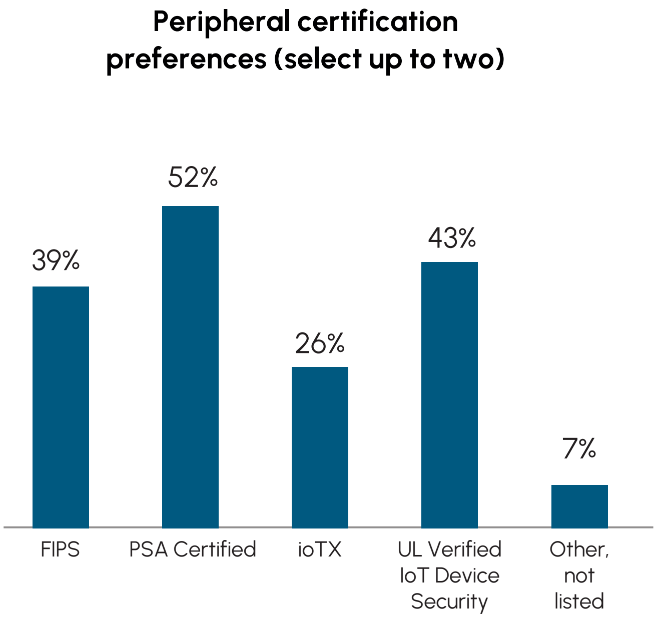


BY REGION		Agree Overall	Strongly Agree	Somewhat Agree
We currently use Security Certifications or Security Frameworks for peripheral devices	AP	94%	59%	35%
	EMEA	97%	65%	32%
	NA	87%	60%	27%
	SA	86%	59%	27%
We consider (or would consider in the future) Security Certifications or Security Frameworks when making peripheral purchase decisions	AP	89%	53%	36%
	EMEA	96%	54%	42%
	NA	89%	52%	37%
	SA	87%	58%	29%

2023 INTEREST IN CERTIFICATION AND FRAMEWORKS

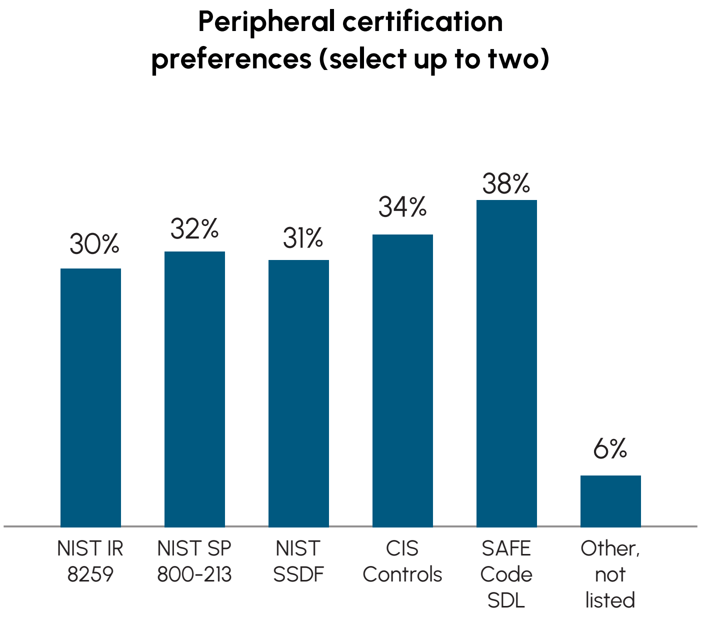
If AGREE with Q42 (use or would consider using security frameworks or security certifications):

We're most interested in the following **security certifications** for peripheral devices: (Select up to two)



BY REGION	AP	EMEA	NA	SA
FIPS	41%	39%	38%	36%
PSA Certified	48%	52%	55%	51%
ioTX	25%	27%	24%	29%
Ul Verified IoT Device Security	48%	40%	42%	44%
Other, not Listed	8%	9%	4%	10%

We're most interested in the following **security frameworks** for peripheral devices: (Select up to two)



BY REGION	AP	EMEA	NA	SA
NIST IR 8259	32%	31%	28%	31%
NIST SP 800-213	30%	34%	30%	33%
NIST SSDF	33%	33%	30%	21%
CIS Controls	31%	31%	36%	38%
SAFECode SDL	40%	36%	36%	48%
Other, not listed	7%	6%	6%	7%

© 2024 The Futurum Group. All rights reserved.

Important Information About this Report

CONTRIBUTORS

Krista Macomber
Research Director | The Futurum Group

PUBLISHER

Daniel Newman
CEO | The Futurum Group

INQUIRIES

Contact us if you would like to discuss this report and The Futurum Group will respond promptly.

CITATIONS

This paper can be cited by accredited press and analysts, but must be cited in-context, displaying author's name, author's title, and "The Futurum Group." Non-press and non-analysts must receive prior written permission by The Futurum Group for any citations.

LICENSING

This document, including any supporting materials, is owned by The Futurum Group. This publication may not be reproduced, distributed, or shared in any form without the prior written permission of The Futurum Group.

DISCLOSURES

The Futurum Group provides research, analysis, advising, and consulting to many high-tech companies, including those mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

ABOUT DELL TECHNOLOGIES INC

Dell Technologies Inc engages in designing, developing, manufacturing, marketing, selling, and providing support for information technology infrastructure such as laptops, desktops, mobile devices, workstations, storage devices, software, cloud solutions, and notebooks.

ABOUT THE FUTURUM GROUP

The Futurum Group is an independent research, analysis, and advisory firm, focused on digital innovation and market-disrupting technologies and trends. Every day our analysts, researchers, and advisors help business leaders from around the world anticipate tectonic shifts in their industries and leverage disruptive innovation to either gain or maintain a competitive advantage in their markets.

CONTACT INFORMATION

The Futurum Group LLC I futurumgroup.com I (833) 722-5337 I

© 2024 The Futurum Group. All rights reserved.