DARK
Reading
REPORTS
February 2022

Next

How Enterprises Plan to Address Endpoint Security Threats in a Post-Pandemic World

Many enterprises are building on the changes they made to their endpoint security strategies when the COVID-19 pandemic first forced a shift to remote work. Zero-trust network access, MFA, and EDR have emerged as major focus areas.

Sponsored by FORTINET

informa
tech

TABLE OF CONTENTS

Figures

About the Author

Jai Vijayan

Dark Reading

Jai Vijayan is a seasoned technology reporter with over 20 years of experience in IT trade journalism. He specializes in writing on information security and data privacy topics. He was most recently a Senior Editor at Computerworld. He is a regular contributor to Dark Reading, CSO Online, and TechBeacon.

EXECUTIVE SUMMARY

Zero-trust network access and multifactor authentication have emerged as top focus areas for organizations that want to bolster endpoint security defenses in a world that has been transformed by the COVID-19 pandemic. The shift to a more distributed work environment and the accelerated adoption of cloud services and digital transformation initiatives since the pandemic began has also driven substantially greater interest in endpoint detection and response (EDR) technologies and end-user awareness training.

Dark Reading's 2022 Endpoint Security Survey polled 190 IT and cybersecurity professionals on the impact of pandemic-related changes — such as the shift to a remote and hybrid work model — on endpoint security strategies. The goal was to understand how organizations are responding to the changes and the challenges they are encountering along the way. Survey respondents included individuals who identified themselves as the CIO, CTO, COO, CSO, IT director, and network system administrator from organizations ranging in size from fewer than 50 employees to 10,000 or more.

The data shows that two years into the pandemic, many organizations have settled into a "new normal" where enterprise workers, data, and endpoint systems are more scattered than before and must be protected across on-premises, remote/home, and hybrid environments. A substantial number of organizations have made changes to their endpoint strategies that they now have no intention of rolling back once the pandemic passes. Instead, many are doubling down on efforts around zero trust, multifactor authentication (MFA), identity and access management, and other endpoint security initiatives. End users continue to be a major source of worry for IT and security decision-makers, and many of them have ramped up efforts around end-user security awareness training at their organizations. Phishing, malware, and ransomware continue to pose major problems, as do attacks involving credential theft.

Most enterprises expect endpoint security budgets to increase this year. But the priorities for increased spending continue to be antivirus tools, VPN, and anti-spam products and less so some of the other areas such as MFA and zero-trust access. Endpoint visibility issues and challenges associated with zero trust have emerged as new endpoint security challenges.

The following are some key data points from the survey:

- 54% of respondents say the changes they made to endpoint security because of the pandemic are now permanent.
- 46% of organizations plan to make major changes to their MFA strategies in 2022; 46% plan the same with end-user awareness training.
- 46% of IT and security decision-makers expect that most of the end users will split time evenly between home and office in a post-pandemic world.
- 73% of respondents see phishing as the biggest end-user security challenge at their organization; for 47%, it's targeted malware.
- 21% of organizations have already implemented a zero-trust initiative internally; 52% are working on it.
- 62% of organizations will spend more on endpoint security in 2022 than last year.
- 54% of organizations have deployed EDR as a defense against attacks involving the use of stolen credentials.

RESEARCH SYNOPSIS

Survey Name: Dark Reading 2022 Endpoint Security Survey

Survey Date: December 2021

Number of Respondents: 190 technology and cybersecurity professionals at companies of all sizes from a variety of industries. The margin of error for the total respondent base is +/-7.1 percentage points.

Methodology: The survey queried technology decision-makers with IT or cybersecurity job titles at organizations of all sizes from more than 19 industry sectors. Forty percent of respondents hold high-level positions within IT or cybersecurity, such as IT director/head, cybersecurity director/head, CIO, CTO, or CSO. The survey was conducted online. Respondents were recruited via email invitations containing an embedded link to the survey. The emails were sent to a select group of Informa Tech's qualified database; Informa is the parent company of Dark Reading. Informa Tech was responsible for all survey administration, data collection, and data analysis. These procedures were carried out in strict accordance with standard market research practices and existing US privacy laws.

ABOUT US

Dark Reading Reports offer original data and insights on the latest trends and practices in IT security. Compiled and written by experts, Dark Reading Reports illustrate the plans and directions of the cybersecurity community and provide advice on the steps enterprises can take to protect their most critical data.

Dark Reading Reports

Previous Next

Table of Contents

Enterprises Make Significant Changes to Endpoint Security Strategies

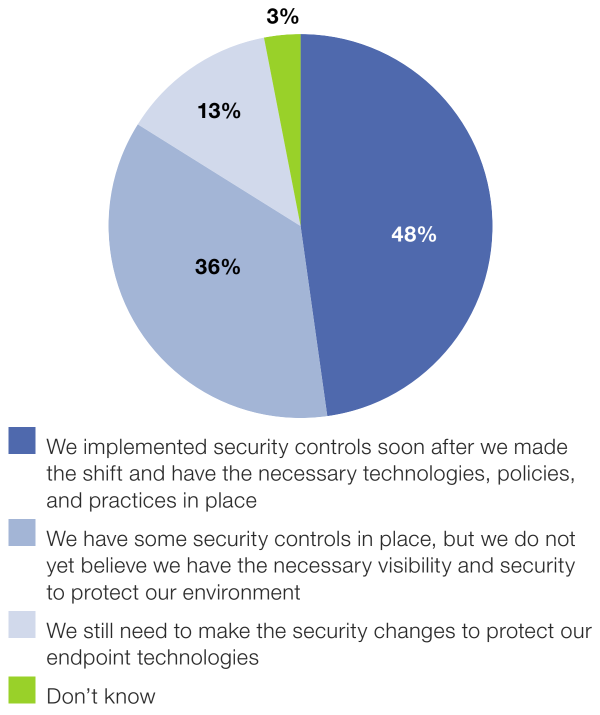
Nearly half (48%) of organizations in Dark Reading's 2022 Endpoint Security Survey made changes to their endpoint security strategy when the COVID-19 pandemic first forced a shift to a work-from-home mode in early 2020 **(Figure 1)**. This included implementing controls such as multifactor authentication (MFA), zero-trust access, endpoint detection and response (EDR), and VPNs. Our survey last year showed that organizations also increased their focus on security awareness training to mitigate risky behaviors by remote workers and started putting more effort into securing remote home network connections and on identity and access management.

Most organizations (54%) that made these changes to their endpoint security strategy have no intention of rolling them back once the pandemic passes **(Figure 2)**. In fact, our survey shows that organizations plan to double down on their efforts around these areas this year as they prepare for a post-pandemic world where workers, data, and applications are more scattered than ever before.

Figure 1.

Effects of Home Workers on Endpoint Computing Strategy

Enterprises were forced to pick speed over security when shifting to a work-from-home mode. How has that trade-off affected your endpoint computing strategy?

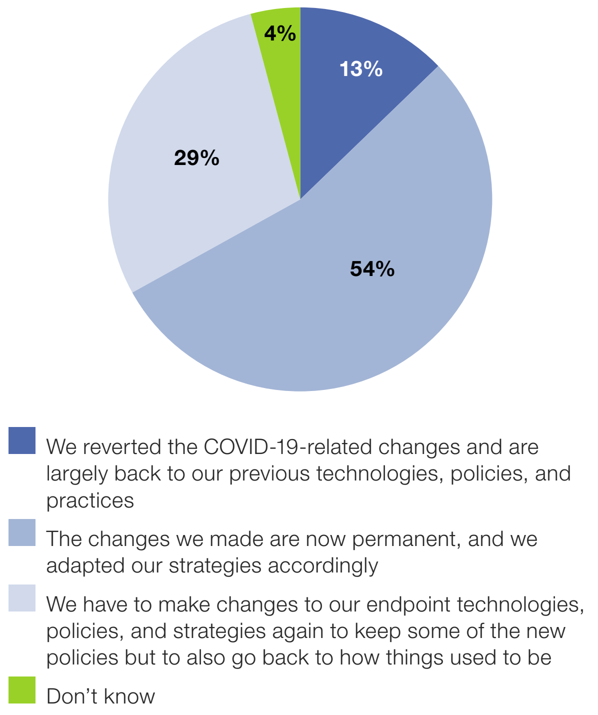


Data: Dark Reading survey of 190 IT and cybersecurity professionals, December 2021

Figure 2.

Current Endpoint Computing Strategy

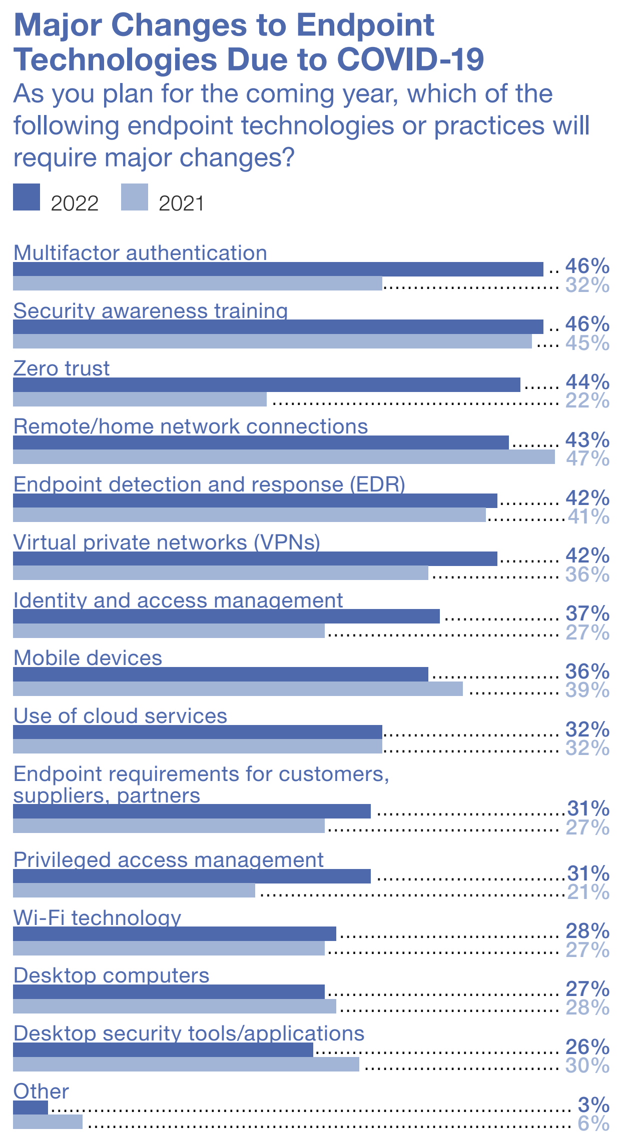
The COVID-19 pandemic forced enterprises to make a rapid change to employees working from home. With this in mind, what does your current endpoint computing strategy look like?



Data: Dark Reading survey of 190 IT and cybersecurity professionals, December 2021

Interest in zero-trust network access, in particular, appears to have soared, with 44% of respondents identifying it as a major area for change this year, up from just 22% in 2021 **(Figure 3)**. Twenty-one percent of organizations have already implemented a

Figure 3.

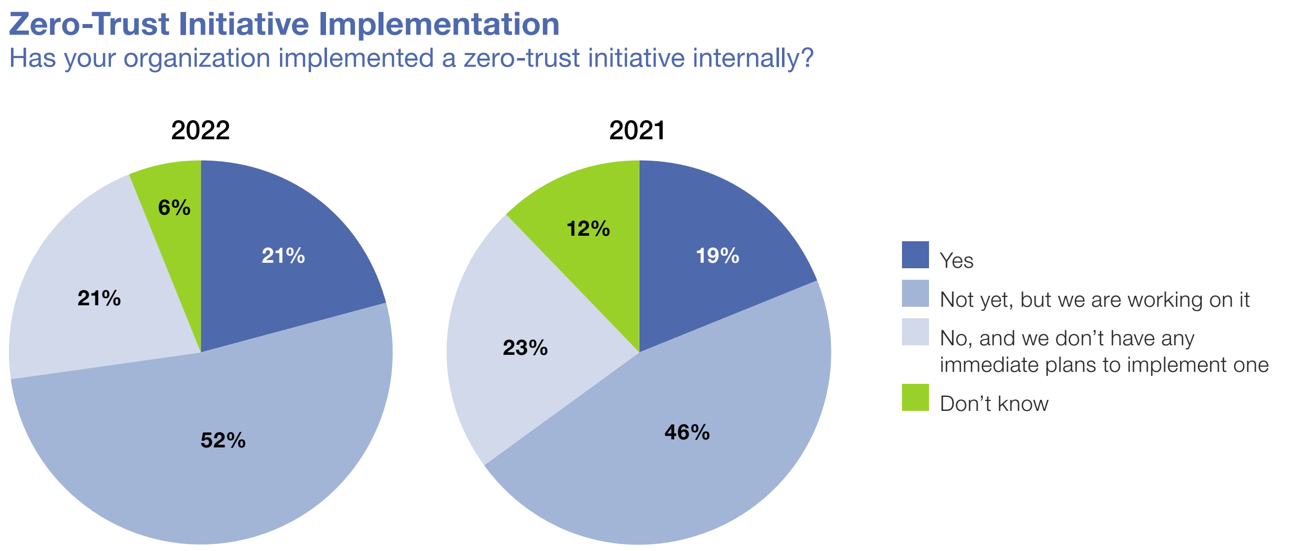


Note: Multiple responses allowed
Data: Dark Reading survey of 190 IT and cybersecurity professionals in December 2021 and 164 in December 2020

zero-trust initiative internally, and 52% are working on one **(Figure 4)**. The total 73% of organizations in our survey this year that either have implemented a zero-trust initiative or are deploying one is higher than the 65% that said the same thing last year and the 55% in our 2020 survey. “The most important change I would want to have is a proper network access control solution in place along with a zero trust solution,” one survey respondent says. “Allow users to access the applications they need to access, and the rest all should be restricted and blocked.”

Many experts consider zero-trust access models — where every access request to enterprise assets from inside or outside the network is vetted and authenticated using contextual, real-time user and device data — as being essential to security in a distributed world. A survey that Microsoft conducted last year of more than 1,200 security decision-makers showed 96% of the respondents identifying zero trust as a top priority. The report identified the shift to remote work because of COVID-19 as one of the primary drivers of the trend.

Figure 4.



Data: Dark Reading survey of 190 IT and cybersecurity professionals in December 2021 and 164 in December 2020

Multifactor authentication (MFA) — another measure that security experts have said is critical to supporting anytime, anywhere access to enterprise data and assets — continues to be a big focus area for enterprise organizations. Forty-six percent of respondents, compared with 32% last year, say they plan to make major changes to their MFA strategy in 2022 to bolster endpoint security. MFA combines the use of passwords with a second form of authentication, such as a PIN, security token, one-time password, or biometric identifier. Many believe a multilayered identity verification process is critical to protecting against breaches at a time when attackers have increasingly begun using stolen account credentials to breach enterprise networks, escalate privileges, and move laterally on them. Allied Market Research recently predicted that global demand for MFA technologies will top $40 billion by 2030, up from $10.3 billion in 2020, driven largely by an increase in cyberattacks during the COVID-19 pandemic, regulations, and other factors.

Enterprises are continuing to make a slew of other significant changes to support new business and workplace requirements triggered by the pandemic. Forty-six percent of organizations, for example, plan to boost end-user security awareness training — almost certainly because of the increased threat to their environments from remote home workers. As one survey respondent notes: “End users often forget to practice what they are taught or don’t take the material as seriously as they should. The weakest point in any security scheme is the end user.”

Forty-three percent plan to make changes to their controls for securing remote and home networks, and 42% will ramp up efforts around EDR technologies. Other endpoint areas that security decision-makers plan to focus on this year include VPNs (42%), identity and access management (37%), and mobile devices (36%).

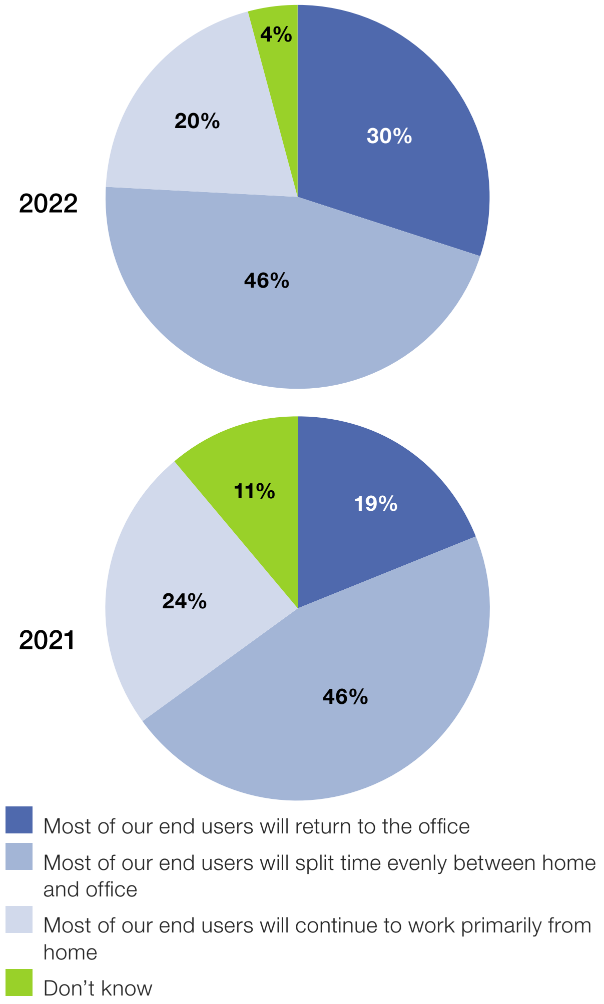
The data suggests that many IT and security decision-makers have accepted the changes triggered by the pandemic as the “new normal” and are adjusting their endpoint strategies to support those changes. Indeed, 20% of organizations expect most of their workers will continue to work from home once the pandemic passes, and 46% expect that most workers will split time evenly between home and office **(Figure 5)**. In other words, 66% of organizations expect most end users will continue to work from home to some extent after the pandemic passes. Our data supports what some analyst firms — such as Gartner — predicted early in the pandemic about the shift to distributed work and operational environments becoming the new normal.

Importantly, not all the changes that security organizations have made — or are making — to their endpoint security controls are about enabling secure anywhere, anytime access for remote workers. As the pandemic has continued, many organizations have found themselves having to make endpoint changes for a variety of other reasons as well. The accelerated shift to cloud services is one example. A survey that analyst firm 451 Group conducted last year found 40% of organizations had increased use of public cloud services because of the pandemic. Eighty-five percent expected the shift to the cloud to be permanent.

Figure 5.

Changes to End-User Computing Model as COVID-19 Threat Decreases

As the threat of COVID-19 decreases, how do you expect the end-user computing model in your enterprise to change?



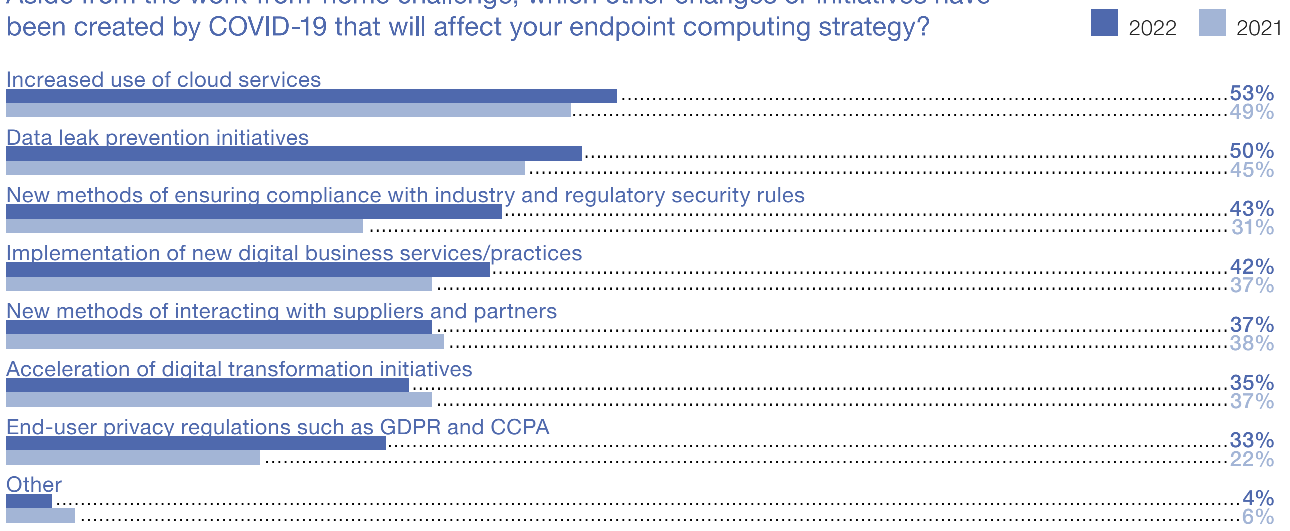
Data: Dark Reading survey of 190 IT and cybersecurity professionals in December 2021 and 164 in December 2020

So, it's not surprising that more than half (53%) of organizations in Dark Reading's 2022 Endpoint Security Survey have had to tweak their endpoint security controls to accommodate increased use of cloud services since the pandemic began **(Figure 6)**. Data leak concerns — likely tied to increased cloud use — triggered endpoint security changes at 50% of organizations, and 43% made changes because of compliance and regulatory requirements. Digital transformation initiatives were another factor. Forty-two percent say the ongoing shift to a digital-first business model at the organization has necessitated changes to their endpoint security.

Figure 6.

Changes or Initiatives Created by COVID-19 Affecting Endpoint Computing Strategy

Aside from the work-from-home challenge, which other changes or initiatives have been created by COVID-19 that will affect your endpoint computing strategy?



Note: Multiple responses allowed
Data: Dark Reading survey of 190 IT and cybersecurity professionals in December 2021 and 164 in December 2020

Previous Next

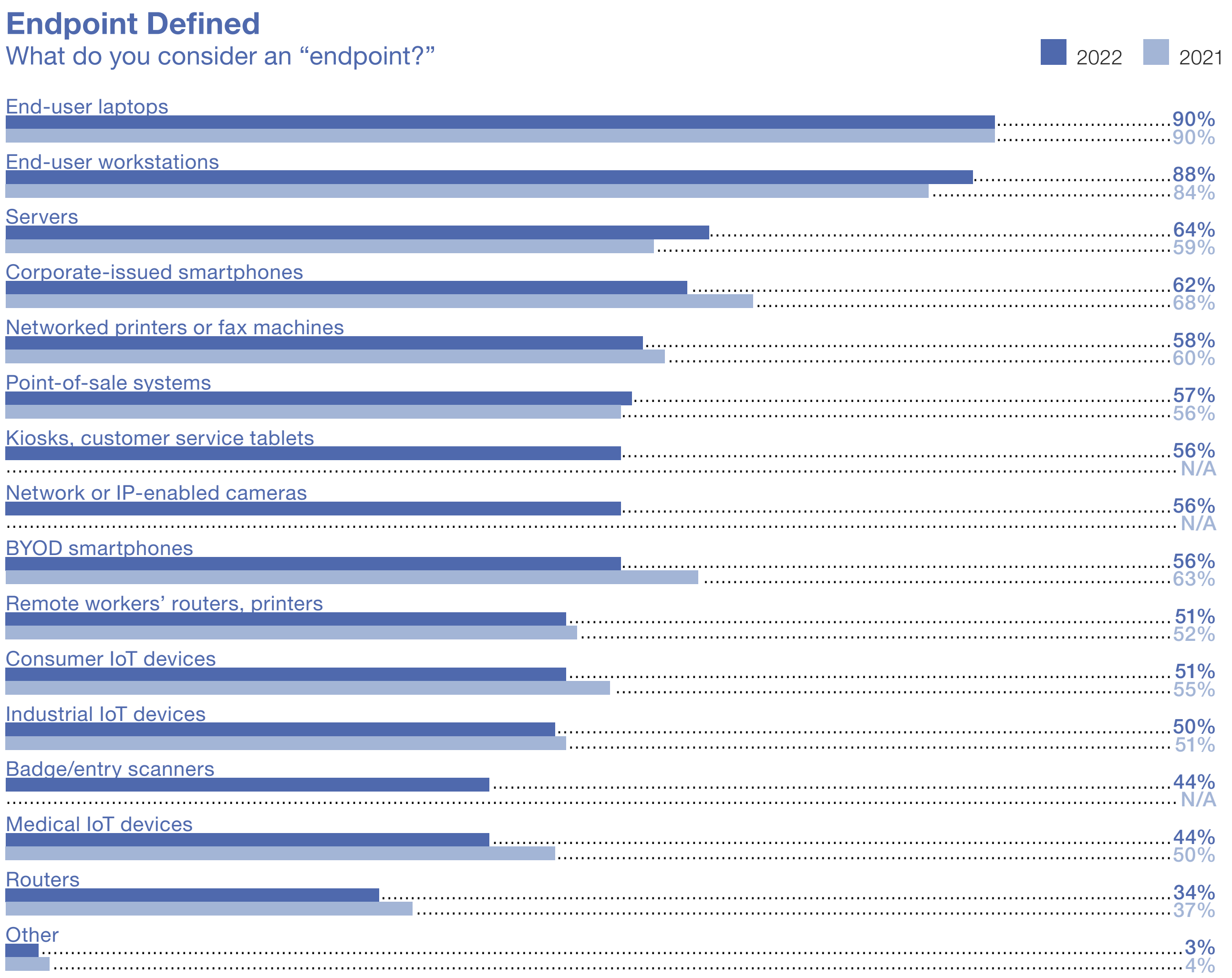
Table of Contents

Rapidly Changing Threat Landscape

Threats to enterprise endpoints extend well beyond end-user laptops and workstations. Our survey shows that when security leaders talk about protecting endpoint devices, they also include servers, corporate-issued and personally owned mobile devices, network printers, point-of-sale systems, kiosks and tablets used for customer service, routers used by remote workers, and consumer Internet of Things and Industrial IoT devices. As might be expected, most organizations (90%) consider end-user laptops and end-user workstations (88%) as endpoint devices **(Figure 7)**. At 64% of organizations, servers are an endpoint technology. Fifty-eight percent extend the definition to network-connected printers, 57% to point-of-sale systems, and 56% to kiosks and tablets used for customer service. Some organizations (34%) include network routers in their endpoint protection strategy.

End users continue to represent one of the biggest threats to this broad endpoint environment. A startling 87% of IT and security decision-makers expect that if attackers want to steal their organization's most sensitive data, they would likely begin by

Figure 7.



Endpoint Defined

What do you consider an "endpoint?"

Note: Multiple responses allowed

Data: Dark Reading survey of 190 IT and cybersecurity professionals in December 2021 and 164 in December 2020

Previous Next

Table of Contents

targeting a single end user **(Figure 8)**. Multiple factors appear to be contributing to that pessimistic outlook. Seventy-three percent of survey respondents express concern about threat actors using phishing and social engineering scams to trick users into dropping malware on their network or stealing data from it **(Figure 9)**. Forty-five percent say their biggest endpoint concern is end users who fail to comply with policies such as those related to VPN use and downloading unauthorized applications on their devices. Eighteen percent are worried about malicious users that might want to sabotage, steal, or leak sensitive assets, and 30% about employees using devices on public Wi-Fi and other public networks.

“Phishing and social engineering attacks are constant,” one survey taker notes. “Despite a significant increase in training and awareness, the workforce shortage seems to have some of our users not caring about getting in trouble and slacking off on the required training.”

Figure 8.

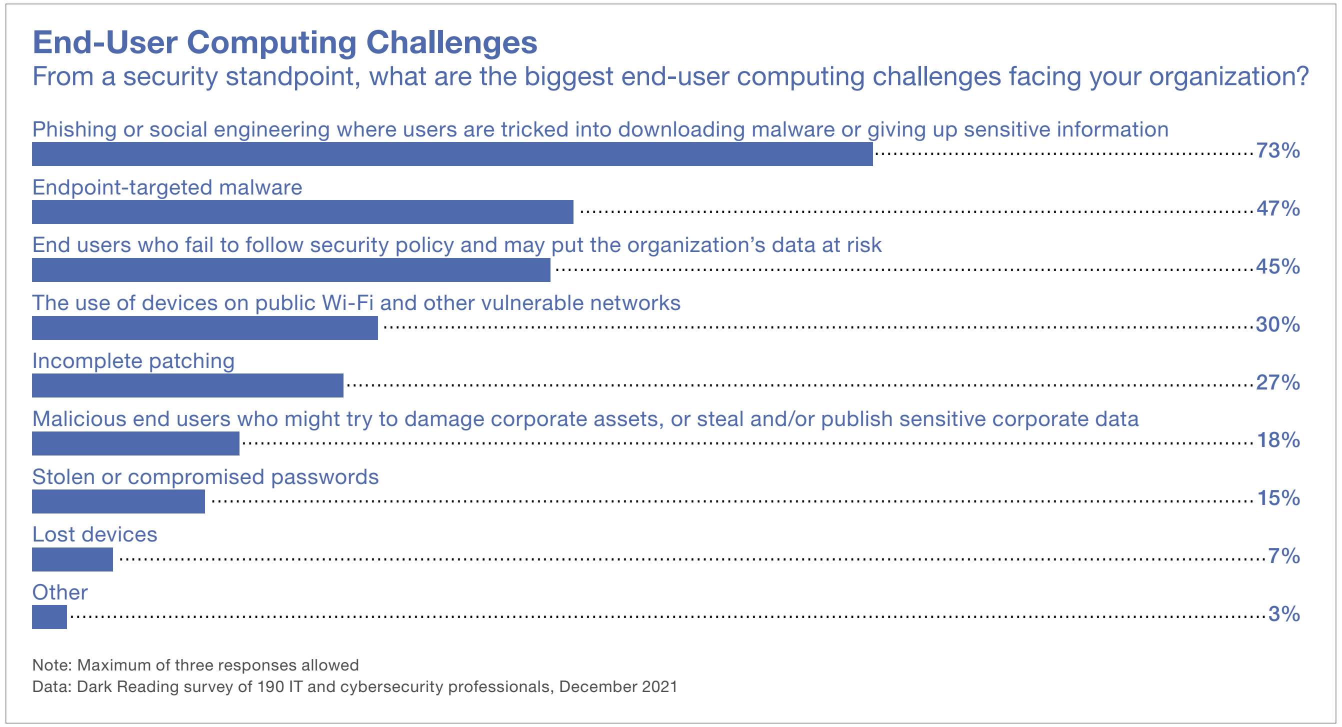
Endpoint Security Belief Statements

Please indicate below whether you agree or disagree with the following statements.

	Strongly agree	Agree	Disagree	Strongly disagree
The general increase in ransomware attacks has caused us to increase investments in endpoint security	36%	57%	7%	0%
I believe that if an attacker wanted to crack my organization’s most sensitive data, they would likely begin by attacking a single end user	33%	54%	12%	1%
I am confident in my organization’s ability to manage end-user access privileges	20%	65%	15%	0%
The increase in attacks using end-user credentials has caused us to increase investments in endpoint security	28%	55%	16%	1%
I am confident that my organization’s current approach to authentication/passwords is effective	16%	63%	19%	2%
I am confident that my organization’s current approach to security awareness training is effective	16%	61%	20%	3%
I believe that the endpoint security changes necessitated in my organization due to COVID-19 have significantly increased our risk of a major data breach in 2022	14%	43%	36%	7%
I believe my team would know immediately if an end user was trying to steal or exfiltrate corporate data	13%	43%	38%	6%

Data: Dark Reading survey of 190 IT and cybersecurity professionals, December 2021

Figure 9.


End-User Computing Challenges
From a security standpoint, what are the biggest end-user computing challenges facing your organization?

Note: Maximum of three responses allowed
Data: Dark Reading survey of 190 IT and cybersecurity professionals, December 2021

None of these issues are new. But the fact that a relatively high percentage of security and IT decision-makers still consider such factors a major concern shows how challenging it has been for organizations to get a grip on the end-user problem. Verizon's seminal "Data Breach Investigations Report" (DBIR) for 2021 showed that a staggering 85% of the breaches that it investigated the previous year involved the human element. According to the DBIR, 50% of breaches involved a mistake by systems administrators with elevated access privileges, and 61% were tied to stolen end-user account credentials. In our research, targeted malware (47%) and incomplete patching (27%) were two issues, not directly related to end-user behavior, that survey respondents identify as major endpoint security threats.

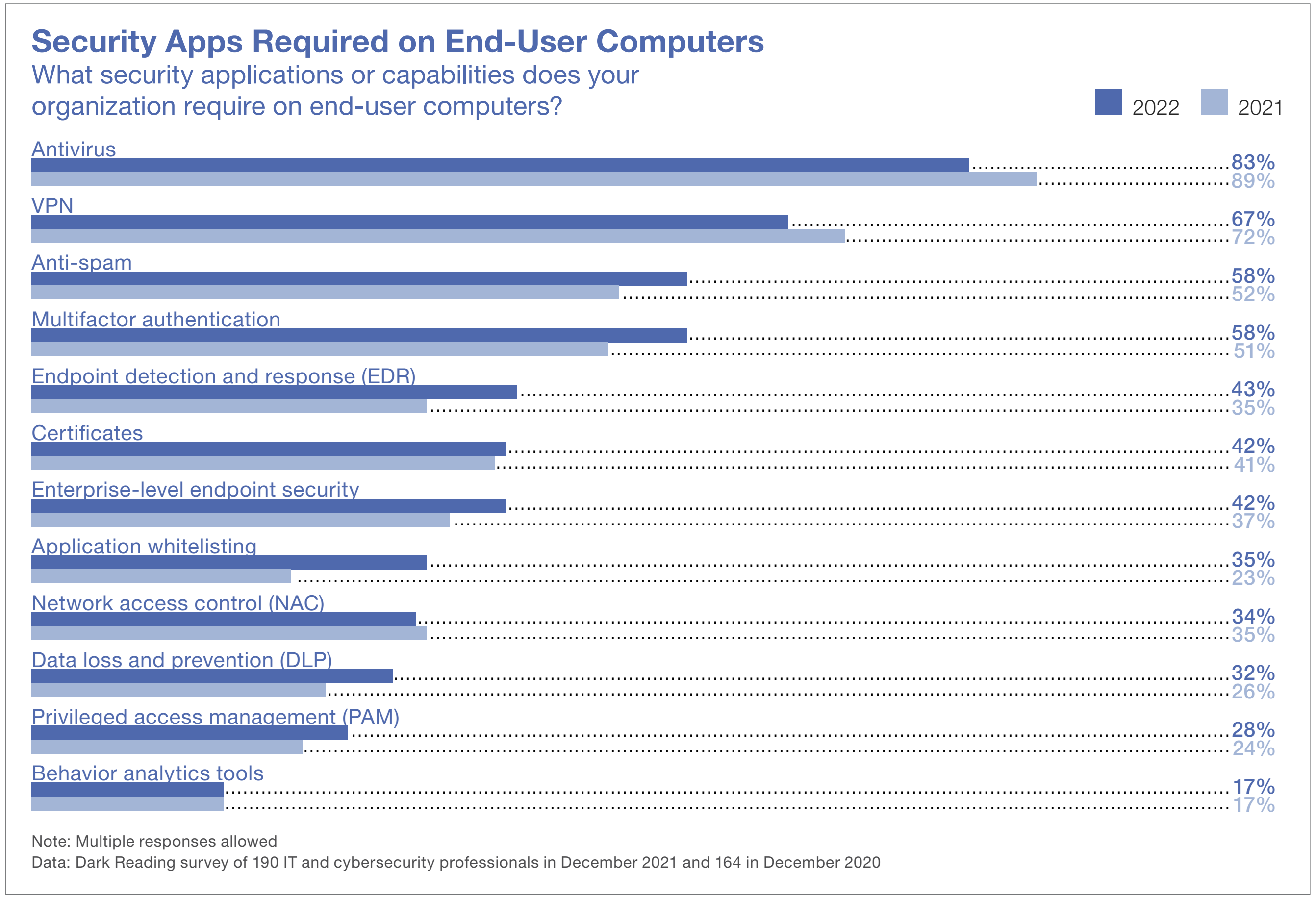
What measures have security organizations implemented to address these challenges, and what are the endpoint spending priorities for 2022?

Antivirus, VPN, and anti-spam tools continue to be primary endpoint requirements at most organizations. Eighty-three percent of organizations in our survey require endpoint devices to have software for detecting and blocking viruses and other malware; 67% require VPN software and 58% anti-spam tools. Our 2022 survey marked the third year in a row where the percentage of organizations that require an antivirus tool on endpoint devices has decreased. Last year, antivirus software was an endpoint requirement at 89% of organizations, and in 2020, 92% of organizations required it. The decline in standalone antivirus software usage reflects a trend toward the growing integration of malware-detection functions in other technologies, such as endpoint detection and response products, operating systems, and cloud technologies. One apparent indication of the trend was the notable increase in the percentage of respondents who identify EDR as an endpoint requirement in our survey this year — 43% compared with 35% in 2021 **(Figure 10)**.

Previous Next

Table of Contents

Figure 10.



Note: Multiple responses allowed
Data: Dark Reading survey of 190 IT and cybersecurity professionals in December 2021 and 164 in December 2020

Other endpoint security requirements include MFA (58%); digital certificates (42%); enterprise-specific endpoint management tools from companies like CrowdStrike and Tanium (42%); application whitelisting (35%); network access control (34%); and data loss prevention (DLP) tools (32%).

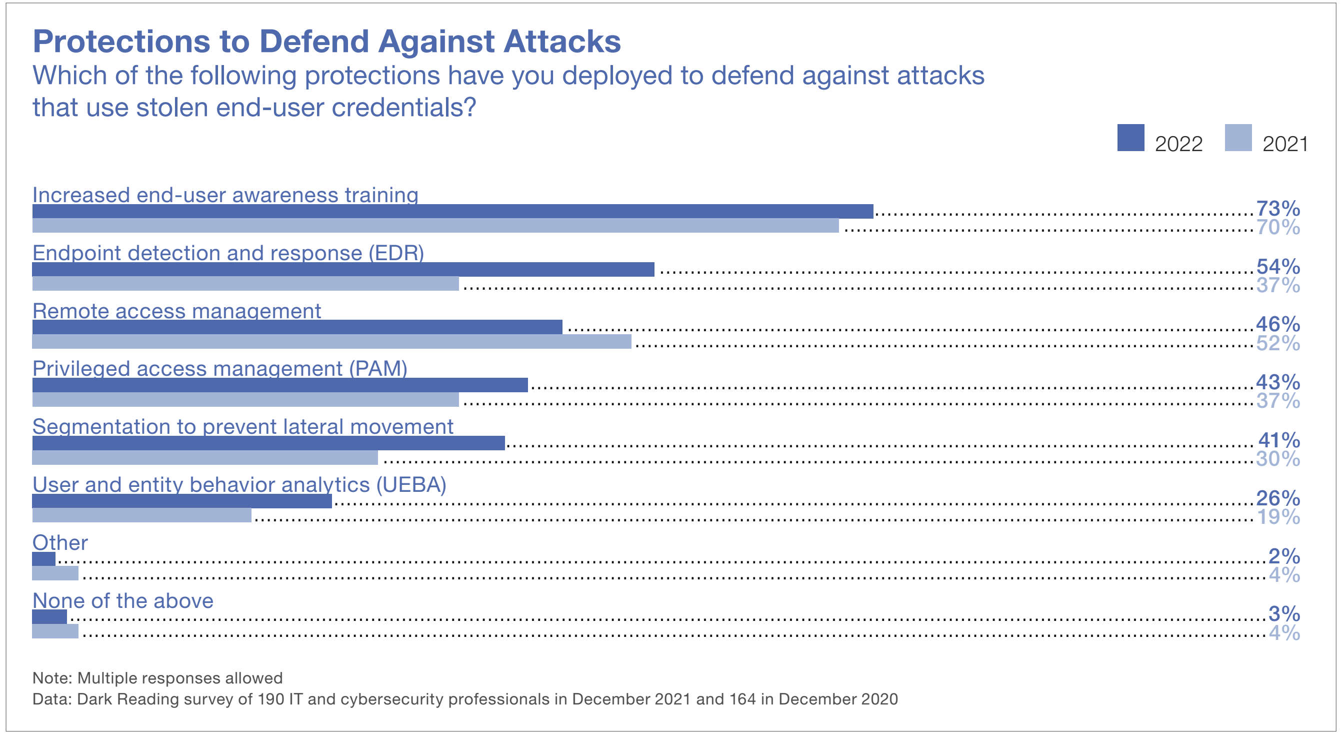
The broad array of controls that enterprise organizations require on endpoint devices these days — especially things such as app whitelisting and DLP — reflects heightened concerns over the vulnerability of the endpoint environment to targeted and opportunistic attacks. Numerous reports in recent years have chronicled a sharp increase in attacks against endpoint devices from threat actors trying to find an entry point into enterprise networks or deploy ransomware botnet software and other malware, or to steal data. Most attacks have involved phishing and other social engineering scams. But threat actors have continued to exploit vulnerabilities and other infection vectors such as exposed RDP services, fileless malware, and stolen account credentials to infiltrate end-user systems and cause all kinds of mayhem.

Ransomware and credential theft have become especially big endpoint security concerns. In its 2021 DBIR, Verizon observed how credentials were the most sought-after data type among criminals and figuring in 61% of the breaches that it investigated. Dark Reading's survey shows that 93% of organizations plan to increase endpoint security spending because of the general increase in ransomware attacks over the past two years, and 83% plan to do so because of the increase in attacks involving the use of stolen account credentials.

A substantial number of organizations, in fact, have deployed multiple protections to mitigate exposure to endpoint attacks involving the use of stolen credentials. Because many credential compromises result from end-user mistakes — such as entering login information into a phishing page — many organizations (73%) have made increased end-user awareness training a top priority. Fifty-four percent (compared with 37% in 2021) have deployed EDR tools to detect and respond to endpoint threats, and 46% have put a bigger emphasis on remote access management.

Privileged access management (PAM) appears to be a major focus area, with 43% of respondents — compared with 37% last year — describing it as a protection they have implemented against credential misuse **(Figure 11)**. Forty-one percent say they have segmented their networks, apparently to limit lateral movement by an attacker with privileged credentials. The heightened focus on PAM is likely tied to the growing volume of attacks targeting login credentials belonging to IT administrators and other users with privileged access to critical systems and data. A CensusWide survey on behalf of ThycoticCentrify (now Delinea) last year showed 53% of the 150 responding organizations in the survey had experienced an attack targeting privileged credentials. In 85% of the instances where attackers managed to steal privileged credentials, they accessed critical systems and data.

Figure 11.



Protections to Defend Against Attacks

Which of the following protections have you deployed to defend against attacks that use stolen end-user credentials?

Note: Multiple responses allowed

Data: Dark Reading survey of 190 IT and cybersecurity professionals in December 2021 and 164 in December 2020

A high percentage of enterprises plan to increase budgets for endpoint security to address the rapidly evolving threat landscape. Forty-nine percent expect their endpoint security budget for 2022 will be slightly higher than 2021, and 13% expect it will be much higher **(Figure 12)**. The major focus areas for increased spending are endpoint security tools, MFA, and security awareness training. More respondents — 52%, 45%, and 43%, respectively — identify these three areas as a primary focus of their security spending this year, compared with other endpoint security controls **(Figure 13)**. Thirty-nine percent of organizations expect they'll be spending

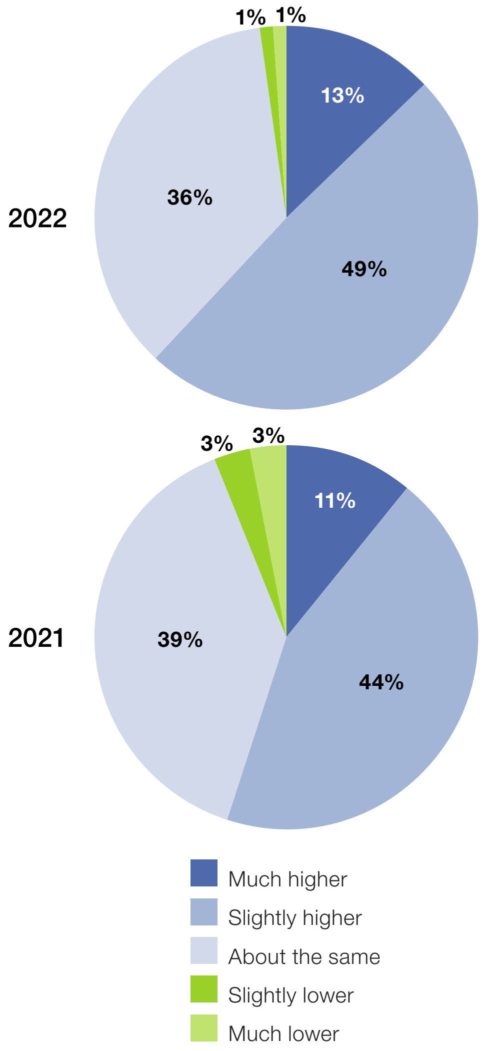
Previous Next

Table of Contents

Figure 12.

Endpoint Spending

How do you estimate your endpoint security spending next year will compare with this year?

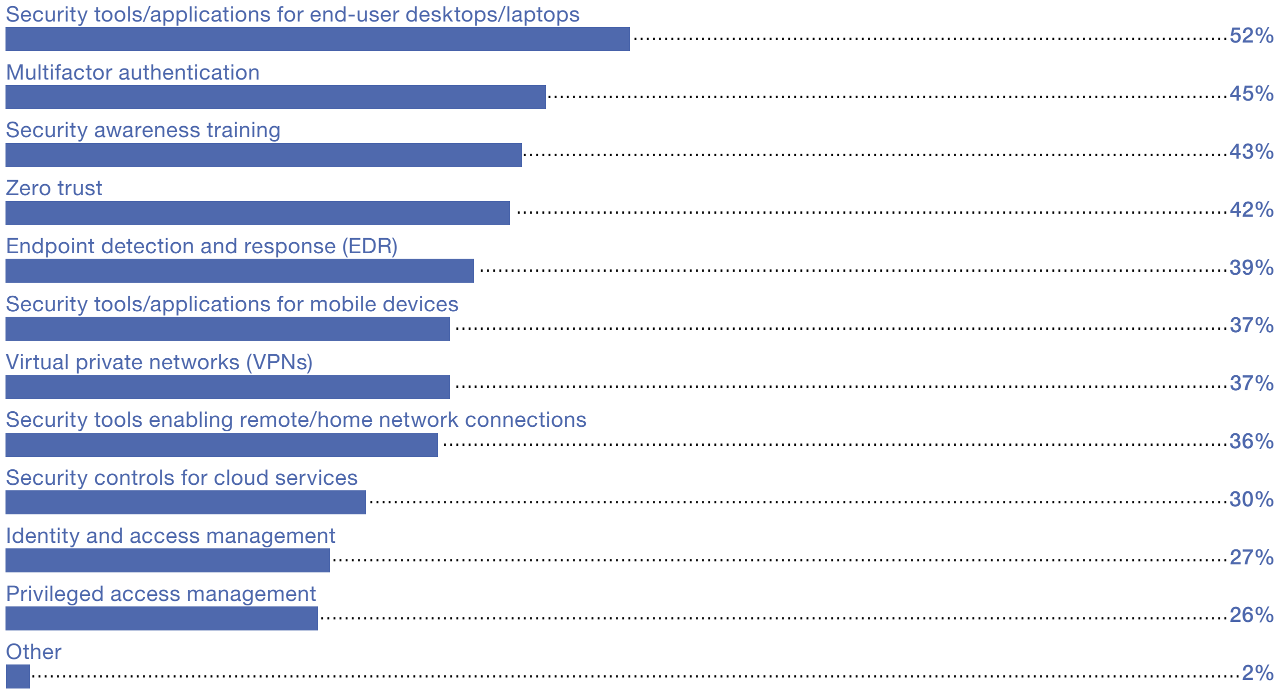


Data: Dark Reading survey of 190 IT and cybersecurity professionals in December 2021 and 164 in December 2020

Figure 13.

Focus of Security Spending in Next Year

Which of the following will you focus on for your 2022 endpoint security strategy spending?



Note: Multiple responses allowed
Data: Dark Reading survey of 190 IT and cybersecurity professionals, December 2021

more of their security dollars on EDR; 37% expect mobile device security to be a focus of increased spending; and 37% will use at least some of their endpoint budgets to ramp up VPN protections.

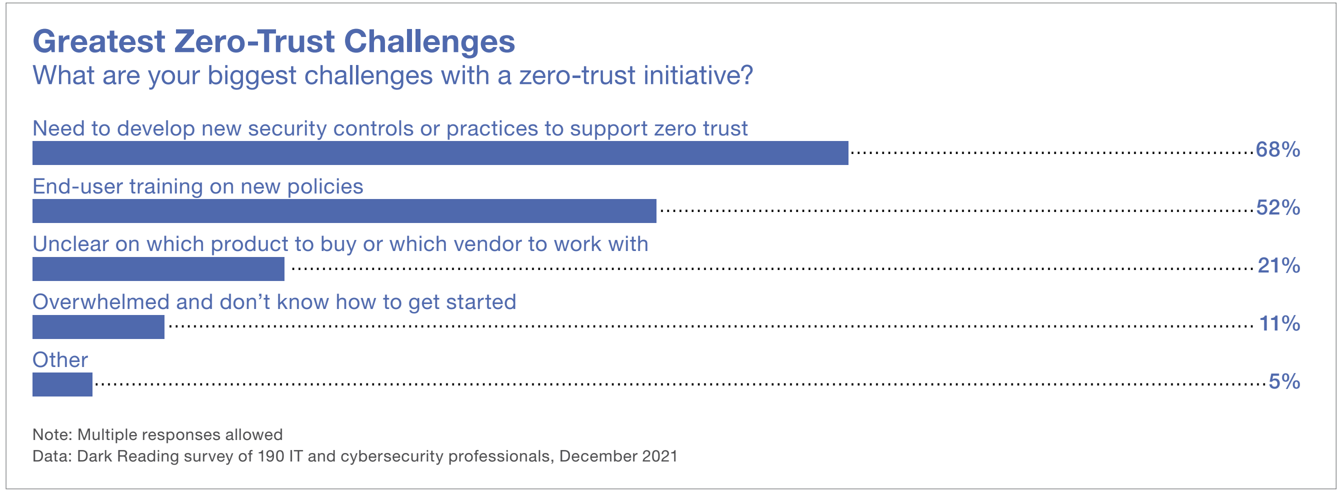
Many IT and security decision-makers appear confident in the measures they have implemented — or plan to implement — to bolster endpoint security. Despite the high concerns over end-user caused mishaps, 85% are confident their organizations can manage end-user access privileges. Similarly, while many perceive MFA as a critical requirement for endpoint security, 79% believe their organization's current approach to passwords and authentication is effective. More than half (56%) think the endpoint controls they have in place currently will help them immediately detect any attempts by an end user to steal or exfiltrate sensitive corporate data.

Endpoint Challenges and Concerns

Concerns over heightened threats to end-user devices have fueled big changes to endpoint security strategies at many organizations. However, our data shows a few potential trouble spots as well.

Take zero-trust initiatives. Though many organizations want to implement zero-trust network access, they face challenges on multiple fronts. Sixty-eight percent say they've had to develop new security controls or practices to support zero trust; 52% need to train users on new zero-trust policies, and 21% organizations have no idea which product to buy or which vendor to work with **(Figure 14)**.

Figure 14.



Note: Multiple responses allowed
Data: Dark Reading survey of 190 IT and cybersecurity professionals, December 2021

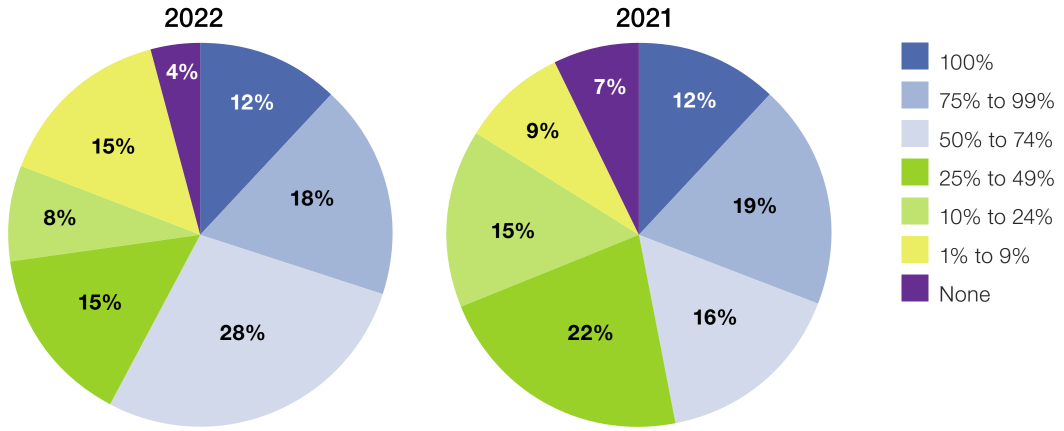
MFA is another example. Though many organizations have implemented multifactor authentication for accessing corporate systems and data, the extent to which it is required varies significantly by organization. While a few (12%) have implemented MFA across 100% of their application stack, 42% have MFA across less than 50% of the environment **(Figure 15)**.

Similarly, 67% of organizations have made changes to their endpoint security strategies to support the new work and business environment created by the COVID-19 pandemic. But a troubling 29% of organizations have yet to make changes to endpoint technologies and policies to keep up with the changed threat environment. These companies are likely at heightened risk of attack and compromise. Some of those that have deployed security controls to support the shift to a new distributed work environment appear to be having problems. Thirty-six percent of organizations that have some controls in place, for example, say they do not have the necessary visibility to effectively protect their endpoint footprint in new work-from-home and hybrid work environments. One survey respondent identifies the issue as having to do with the "persistent use of

Figure 15.

Percentage of Corporate Systems Requiring Multifactor Authentication

What percentage of your corporate systems or applications currently require multifactor authentication in order to be accessed?



Data: Dark Reading survey of 190 IT and cybersecurity professionals in December 2021 and 164 in December 2020

corporate assets on insecure home networks [that expose] assets to constant attacks that we have little to no visibility into."

Our data also suggests a slight disconnect between what security and IT decision-makers consider top endpoint priorities and where they are focusing their efforts and dollars. Many survey respondents identify zero trust, MFA, and EDR as top endpoint priorities. But antivirus tools, VPN, and anti-spam tools continue to be the top endpoint security requirements for most organizations. While 83% of organizations say they require AV software on endpoint devices, just 58% identify MFA as a requirement, and an even smaller 43% perceive EDR as a needed control on end-user devices.

The same pattern is evident in the data around enterprise spending plans for endpoint security. While MFA and zero trust are top priorities, more respondents (53%) identify security tools and applications for laptops and desktops as the primary focus for increased endpoint spending this year, compared with MFA (45%), zero trust (42%), and EDR (39%). Troublingly, while 62% expect endpoint security budgets to increase in 2022, a startling 36% expect to have the same budget as last year.

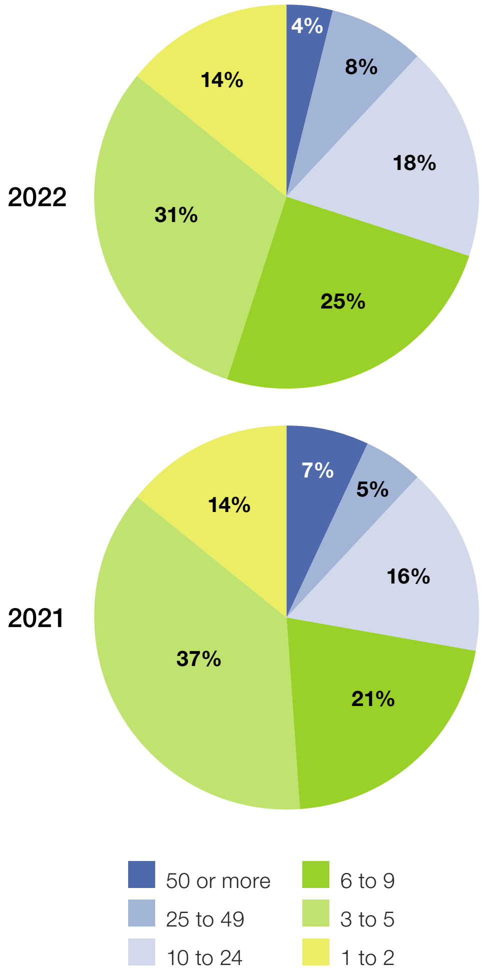
Conclusion

Many enterprise organizations are building on the changes they made to their endpoint security strategies when the COVID-19 pandemic first forced a shift to remote work. Zero-trust network access, MFA, and EDR have emerged as major focus areas for security and IT decision-makers. So, too, has end-user awareness training. Organizations concerned about the potent threat posed by end users have ramped up training efforts and expect to spend more on it in 2022. Even so, many remain very concerned about phishing and social engineering threats and expect that end users will be the primary target for attackers who want to steal sensitive data. Many organizations expect to spend more on endpoint security in 2022 compared with 2021. The major focus areas for spending, however, continue to be antivirus, anti-spam, and VPN tools and less so on more critical areas, such as zero-trust and MFA.

Figure 16.

Number of Security Vendors' Tools to Secure Devices

Approximately how many security vendors' tools does your enterprise employ to secure end-user devices?

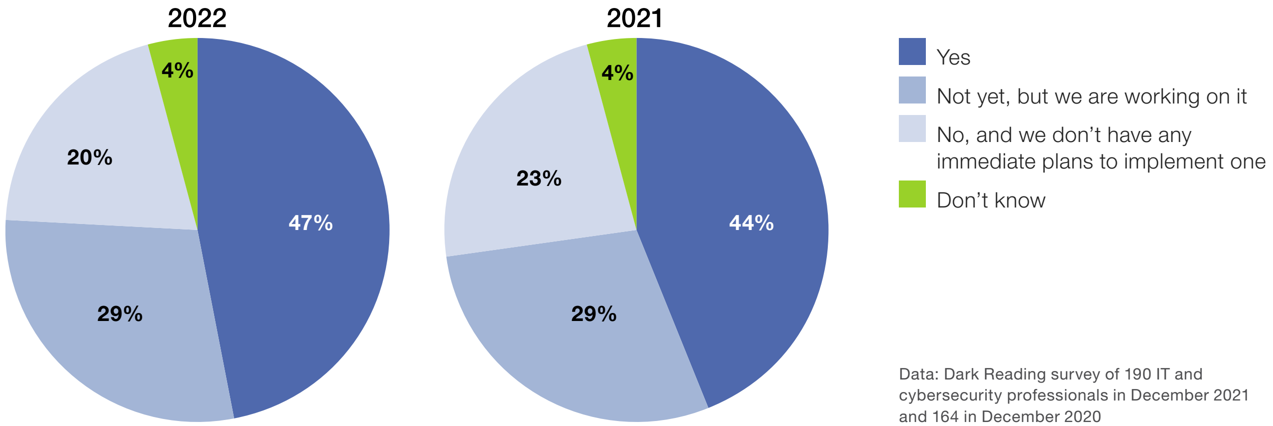


Data: Dark Reading survey of 190 IT and cybersecurity professionals in December 2021 and 164 in December 2020

Figure 17.

Use of Single Login

Does your organization have a "single login" initiative that enables end users to access most corporate applications using a single method of authentication?

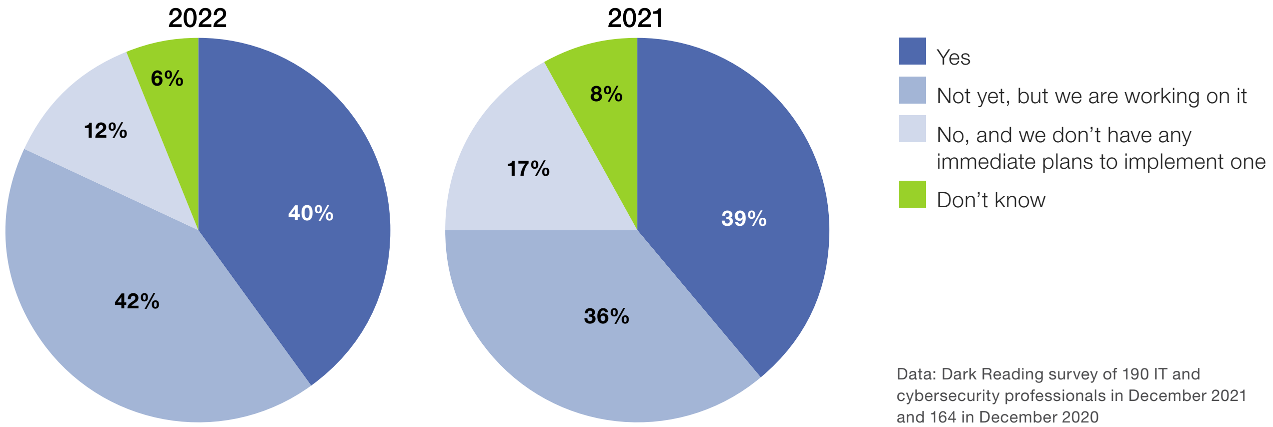


Data: Dark Reading survey of 190 IT and cybersecurity professionals in December 2021 and 164 in December 2020

Figure 18.

Identity Management for End-User Access

Has your organization implemented a common scheme for identity management that allows you to manage end-user access regardless of a user's location or device used?

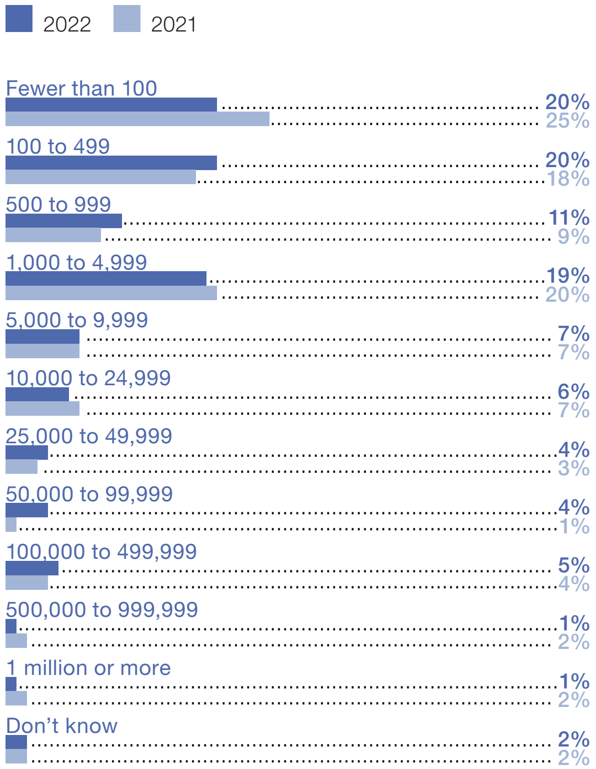


Data: Dark Reading survey of 190 IT and cybersecurity professionals in December 2021 and 164 in December 2020

Figure 19.

Total Number of Endpoint Devices Under Management

What is the total number of endpoint devices that your IT organization is responsible for managing?

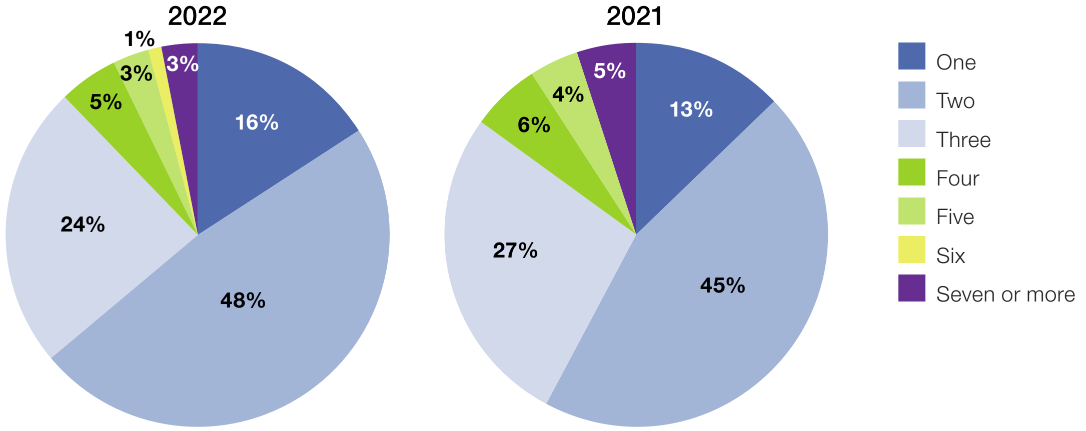


Data: Dark Reading survey of 190 IT and cybersecurity professionals in December 2021 and 164 in December 2020

Figure 20.

Number of Devices Used by Employees

On average, how many devices does each of your employees use to interact with corporate data?

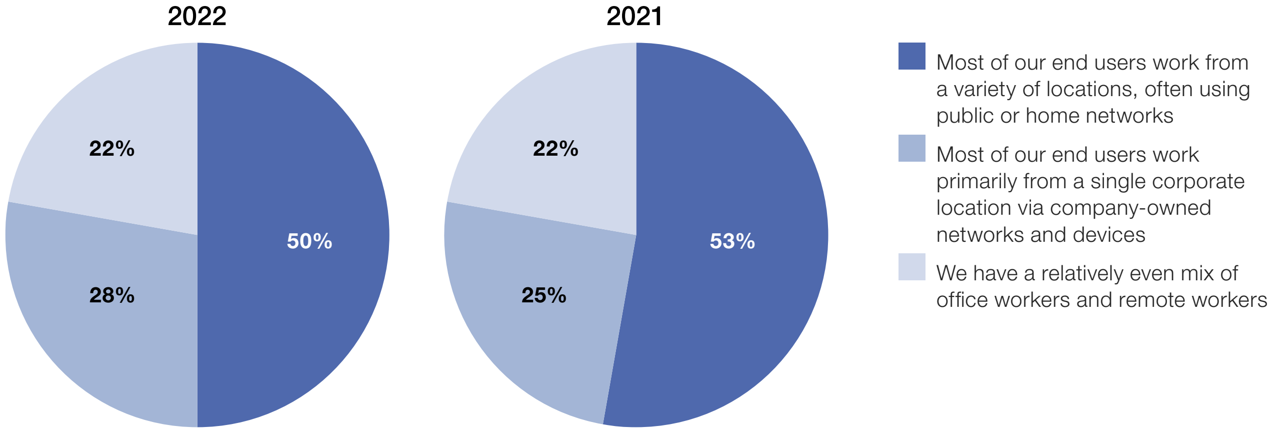


Data: Dark Reading survey of 190 IT and cybersecurity professionals in December 2021 and 164 in December 2020

Figure 21.

End-User Mobility

On average, how mobile are your end users?



Data: Dark Reading survey of 190 IT and cybersecurity professionals in December 2021 and 164 in December 2020

Like this report?

Share it!

Tweet Follow

Share

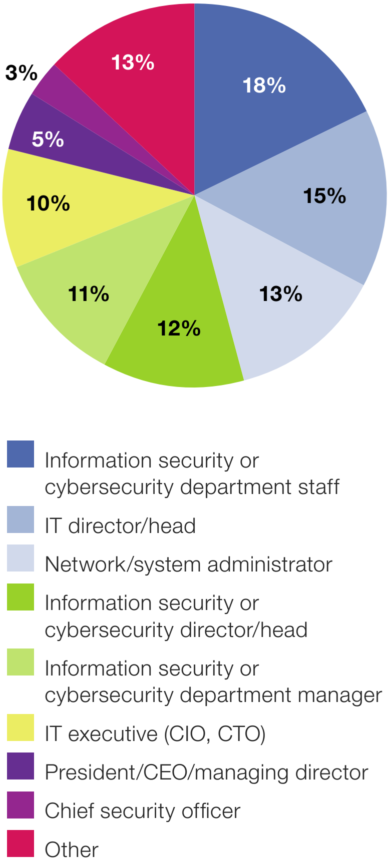
Previous Next

Table of Contents

Figure 22.

Respondent Job Title

Which of the following best describes your job title?

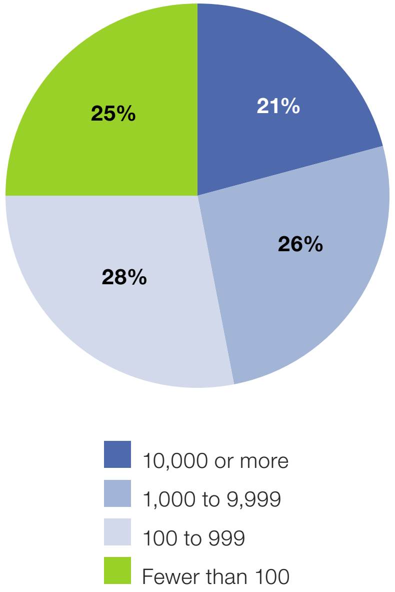


Data: Dark Reading survey of 190 IT and cybersecurity professionals, December 2021

Figure 23.

Respondent Company Size

Approximately how many employees are in your organization?

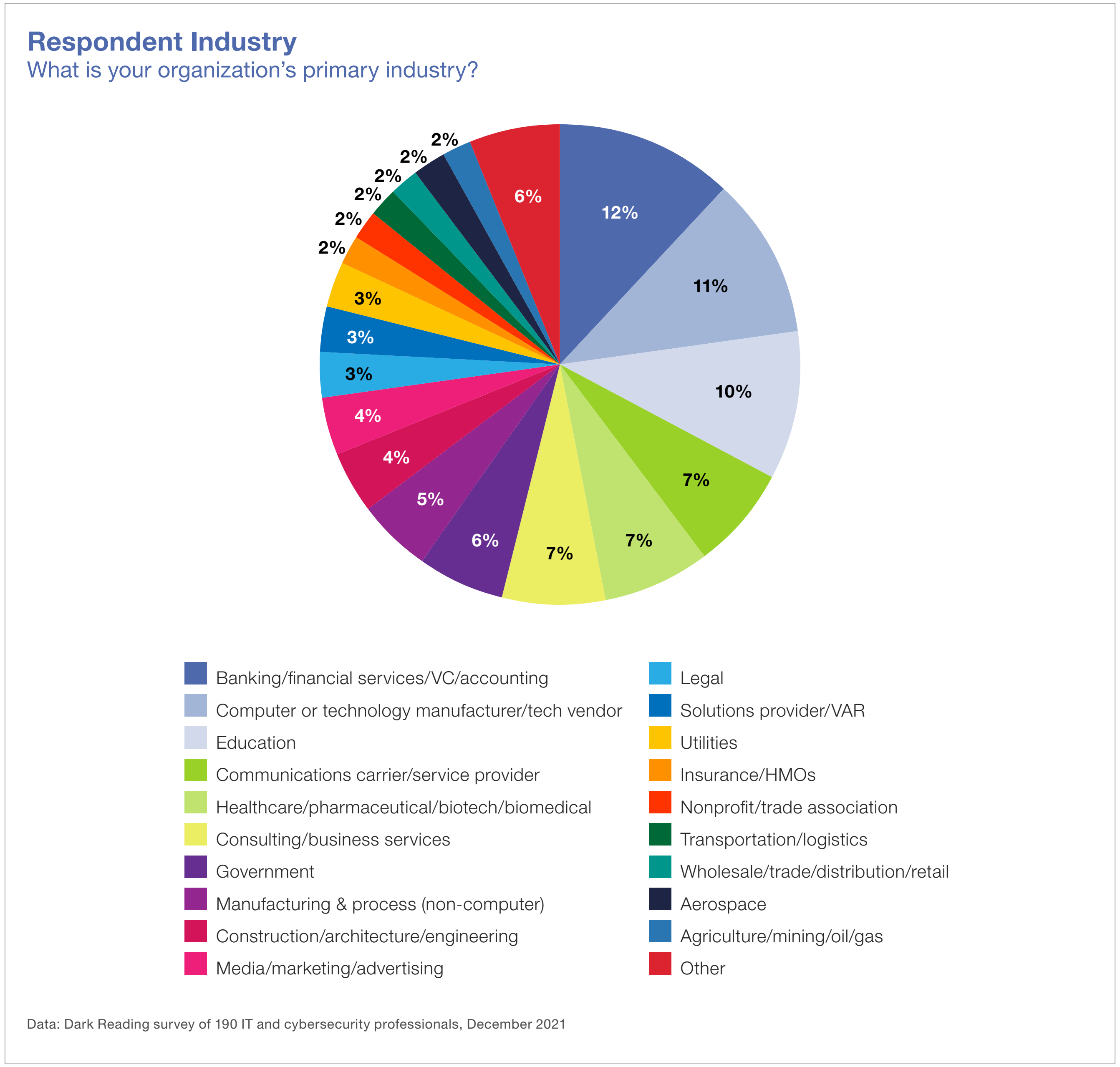


Data: Dark Reading survey of 190 IT and cybersecurity professionals, December 2021

Previous

Table of Contents

Figure 24.



Respondent Industry

What is your organization's primary industry?

Data: Dark Reading survey of 190 IT and cybersecurity professionals, December 2021