DARKReading

REPORTS

April 2020

How Enterprises Are Managing Endpoint Security Threats

Enterprise organizations have deployed a wide array of tools and processes for protecting against endpoint threats. But many remain dangerously vulnerable to security lapses caused by end users.

Sponsored by DUO

informa tech

TABLE OF CONTENTS

Table of Contents

Figures

Jai Vijayan
Dark Reading Reports

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 Christian Science Monitor Passcode, Dark Reading, CSO Online, TechTarget, and several other publications.

EXECUTIVE SUMMARY

Enterprise organizations have deployed a wide array of tools and processes for protecting against endpoint threats. But many remain dangerously vulnerable to security lapses caused by end users.

Dark Reading surveyed 120 IT and cybersecurity professionals on their biggest endpoint security concerns and their preparedness to deal with them. The CIOs, CTOs, CISOs, directors, and other IT professionals who participated in the survey represent organizations from more than 18 sectors, including banking, healthcare, government, communications, retail, manufacturing, and consulting services.

The results of the survey reflect near ubiquitous concern among enterprise organizations over the threat to security posed by end users who are careless, negligent, or malicious, and those who refuse to follow security policies. A high percentage believe that an attacker who wants to crack their most sensitive data would likely begin by attacking a single user.

Half of the organizations represented in our survey have revised their security policy in the past year to keep pace with the rapidly evolving endpoint threat landscape. Most survey respondents include bring-your-own-device smartphones in their definition of "endpoint," and half count remote users' networked devices (including home printers and routers) in that category, too. Nevertheless, even the most up-to-date policies might not be prepared for organizations' current needs to support growing numbers of work-from-home staff.

Dark Reading's survey found that antivirus software — once the only endpoint defense for many organizations — is now just one of many required tools on client systems. End-user awareness training and practices such as strong authentication and access control appear now to be high-focus areas at a majority of companies. Many are implementing a "zero-trust" approach to mitigate the risk of attackers abusing illegitimately obtained user credentials to create havoc on their networks.

The data shows that a substantial percentage of organizations plan to increase endpoint security spending over the next 12 months in response to the rapidly changing threat landscape.

EXECUTIVE SUMMARY

Here are some of the top takeaways from the survey:

- 51% of respondents say that at least some of their endpoint devices are running unsupported (end-of-support or end-of-life) operating systems.
- 46% expect their endpoint security spending will be "slightly higher" or "much higher" next year.
- 80% say that ransomware attacks have driven them to spend more on endpoint security protections.
- 71% identify phishing/social engineering as their biggest endpoint security concern.
- 47% say the endpoint issue they encounter on a daily basis is users sharing credentials or downloading malware.
- 40% of organizations have deployed an endpoint detection and response product.
- 29% require the use of VPNs on smartphones used for business purposes.
- 50% of organizations updated their endpoint security policy in the last year.
- 58% say they have a "liberal BYOD policy and will find a way to securely connect almost any device to the network."

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

SYNOPSIS

RESEARCH

Survey Name Dark Reading 2020 Endpoint Security Survey

Survey Date March 2020

Primary Region North America

Number of Respondents 120 cybersecurity and IT professionals at companies of all sizes. The margin of error for the total respondent base (N=120) is +/-8.8 percentage points.

Purpose Dark Reading surveyed cybersecurity and IT professionals to uncover organizations' policies, spending plans, successes, and challenges related to endpoint device security. The survey also delved into the nature of the definition of an endpoint. With smartphones, laptops, point-of-sale systems, and Internet of Things devices making their way into the enterprise, the definition is wide open.

Methodology The survey queried technology professionals with cybersecurity, IT, and other corporate job titles at predominantly North American organizations. Questions centered on defining an endpoint, organizations' policies, and the challenges they face regarding endpoint security. The survey was conducted online. Respondents were recruited via an email invitation containing an embedded link to the survey. The email was sent to a select group of Informa Tech's qualified database; Informa is the parent company of Dark Reading. Informa Tech research was responsible for all programming and data analysis. These procedures were carried out in strict accordance with standard market research practices.

Mushrooming Endpoint Security Concerns

Endpoint devices have become a critical front in the battle to protect sensitive enterprise data from cyberattacks. In recent years, adversaries have heavily targeted end users and their devices via phishing and other social engineering campaigns designed to steal data and credentials, to deploy malware, and to gain broad access to the enterprise network.

A Verizon analysis of more than 41,600 security incidents and 2,013 actual data breaches in 2019 found that a startling 94% of all malware that ended up on end-user computers was delivered via email. Thirty-two percent of the breaches and 78% of all cyber-espionage incidents that Verizon investigated in 2019 involved phishing. Verizon found that adversaries regularly used phishing email to trick users into sharing their email credentials, which were then used to deliver malware and to carry out other malicious activity.

The results of Dark Reading's 2020 Endpoint Security Survey reflect a high level of concern among security and technology leaders over such issues. Seventy-one percent of respondents identify phishing and other social engineering scams as their greatest endpoint security concern (**Figure 1**). Half express the same sentiment over end users putting the organization's data at risk by failing to follow security policy. Concerns over end-user failings are so high that 87% expect that an attacker trying to steal the organization's most sensitive data would likely begin by attacking a single user (**Figure 2**).

"[The] insider threat, whether purposeful or accidental, is always the biggest risk," one survey taker says in response to an open-ended question asking respondents to identify their biggest endpoint security concerns. "If my security team needs tools to identify bad emails, my users don't stand a chance," the respondent says. Another respondent says that while users may not always be the weakest link, "they are the primary attack vector."

For many organizations, the concerns are not merely theoretical. We asked survey

Figure 1

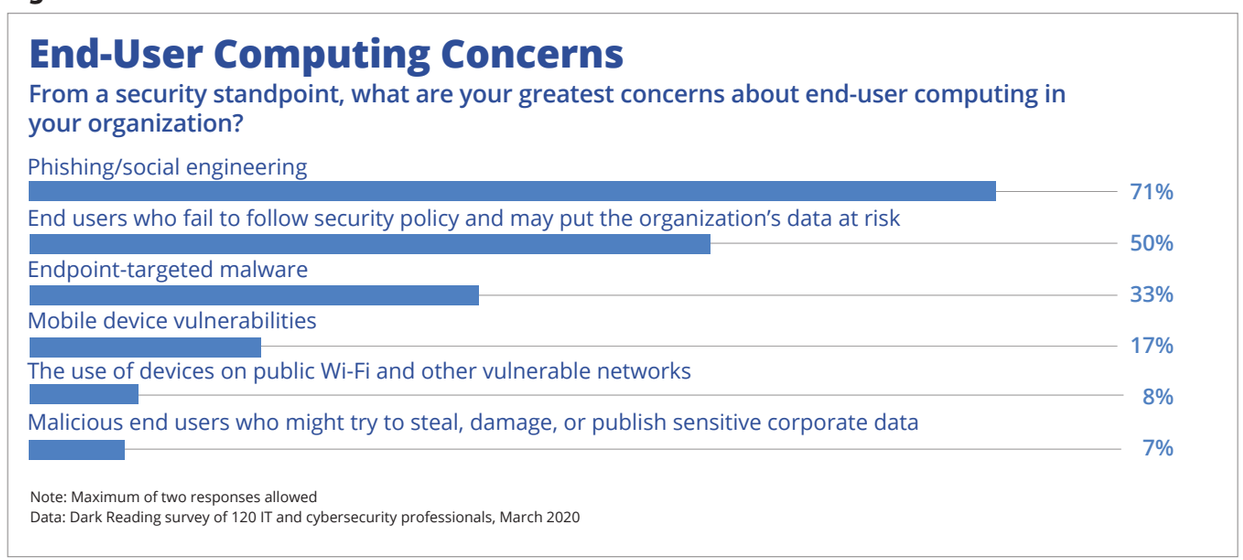


Figure 2

Agree or Disagree Statements

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

	Strongly agree	Agree	Neutral	Disagree
I believe that if attackers wanted to crack my organization's most sensitive data, they would likely begin by attacking a single end user	35%	52%	12%	1%
The general increase in ransomware attacks has caused us to increase investments in endpoint security	24%	56%	16%	4%
I believe that end-user security is more an issue of corporate culture than of technology	23%	56%	21%	0%
The increase in attacks using end-user credentials has caused us to increase investments in endpoint security	16%	57%	23%	4%
I am confident that my organization's current approach to authentication/passwords is effective	16%	61%	20%	3%
I am confident in my organization's ability to manage end-user access privileges	15%	70%	12%	3%
I am confident that my organization's current approach to security awareness training is effective	14%	55%	28%	3%
I believe my team would know immediately if an end user was trying to steal or exfiltrate corporate data	11%	35%	46%	8%

Data: Dark Reading survey of 120 IT and cybersecurity professionals, March 2020

takers to identify the two most common endpoint security issues their teams grapple with every day. Forty-seven percent believe their biggest challenge has to do with users being tricked into downloading malware on their systems or giving up their credentials to an attacker (**Figure 3**). Forty-two percent say they grapple daily with the consequences of end users breaking policy around issues such as VPN and public Wi-Fi use and around the downloading of unauthorized applications onto their devices.

"You can lock down the system, to some extent, but it seems like it is human nature to try and circumvent the system," says Kenneth Stephenson, director of information systems at Thinkpath Engineering Services and a survey respondent. "Everyone's looking for the easy way to accomplish the task at hand."

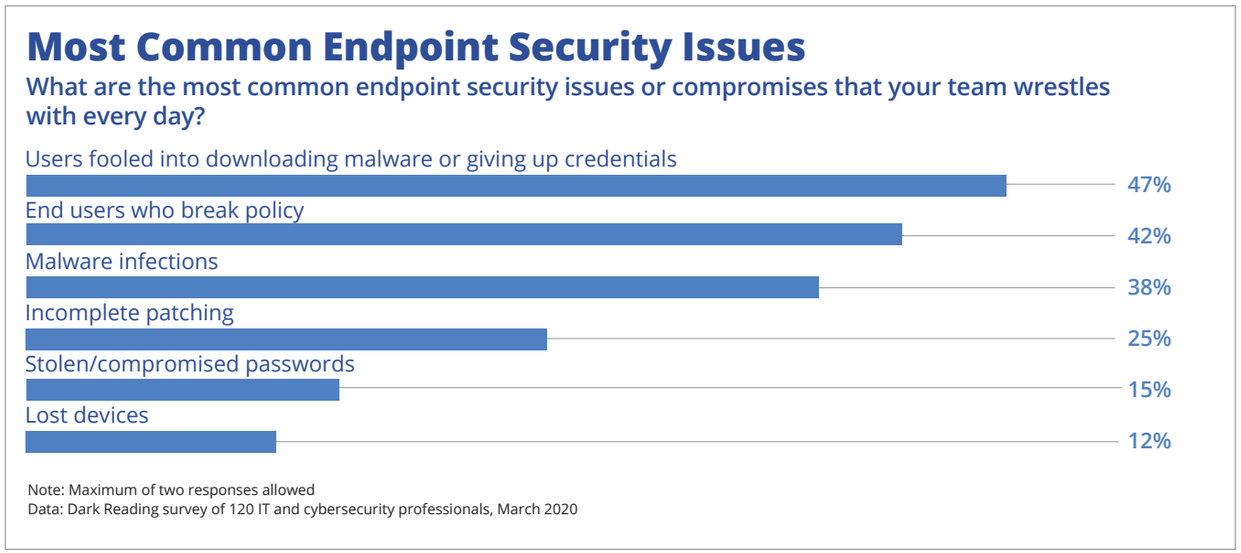
While a vast majority of the problems that organizations are encountering at the endpoint are user-related, there are a handful of other issues as well. Twenty-five percent of our survey respondents cite problems related to incomplete patching. Issues related to stolen or compromised passwords (15%) and lost devices (12%) are two other concerns that some organizations deal with on a daily basis.

The Increasingly Mobile Endpoint

Defining the term "endpoint device" is itself a daunting challenge.

While respondents to Dark Reading's 2020 Endpoint Security Survey are generally in agreement that end-user workstations (92%) and end-user laptops (92%) should be included, a long list of other network-connected devices also passed the test (**Figure 4**). Most respondents include

Figure 3



corporate-issued smartphones (75%) and employee-owned bring-your-own-device (BYOD) smartphones (66%) in their endpoint definition, and 53% also include consumer Internet of Things (IoT) devices.

Respondents also extend the word "endpoint" beyond the end user. Point-of-sale systems (65%), corporate networked printers (63%), corporate servers (59%), industrial IoT devices (55%), medical IoT devices (49%), and routers (34%) made the cut. Nearly half (49%) also count remote workers' networked devices (printers/ routers). Using these broad definitions, most respondents (56%) still say they manage fewer than 1,000 endpoints, but 5% of organizations estimate that they have 100 or even 1,000 times as many (**Figure 5**).

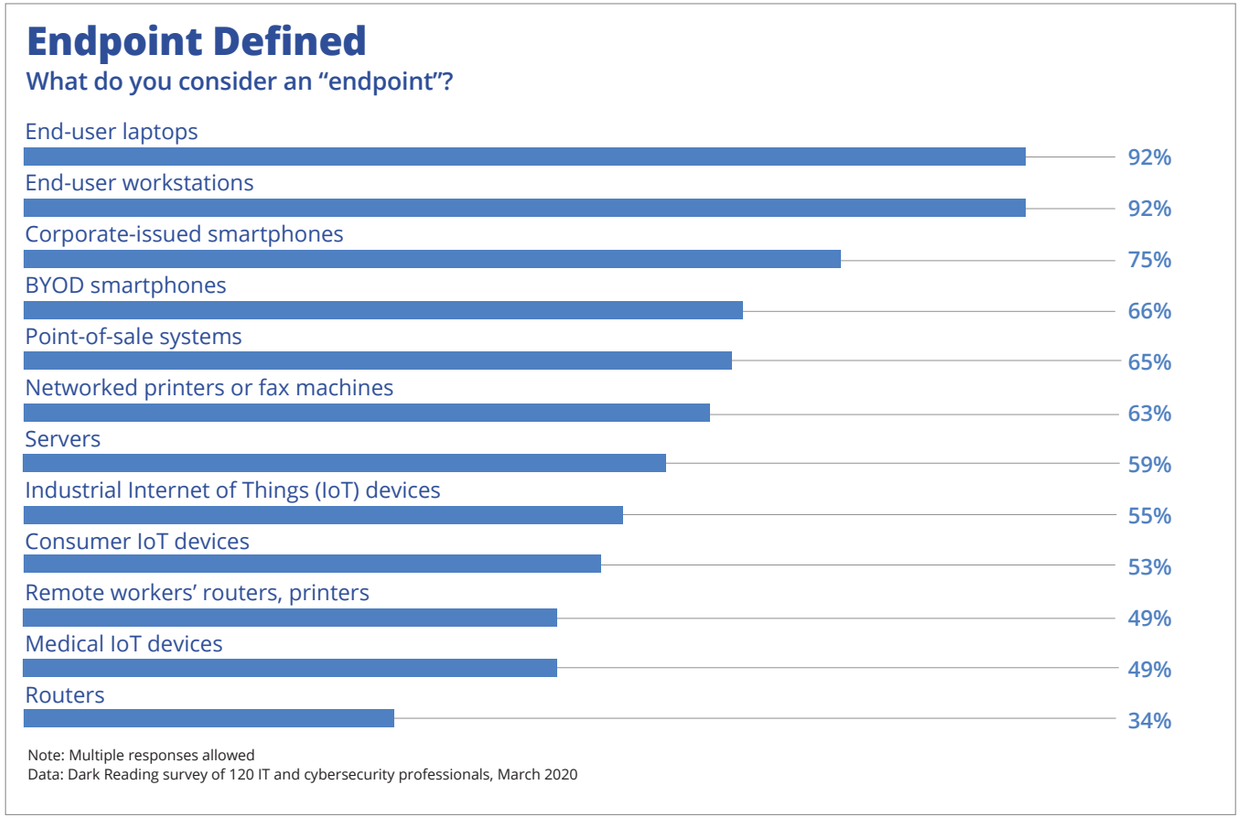
The figures about BYOD smartphones and remote workers' networked devices are particularly significant right now. As IT teams try to support quarantined home workers during the COVID-19 pandemic, security teams must both support and defend new technologies and business processes.

Despite the near ubiquitous use of smartphones these days, relatively few respondents list mobile devices high among their concerns. Only 17% of the respondents in our survey name mobile device vulnerabilities among their top two end-user computing worries. Fifty-eight percent describe their organizations as having a liberal BYOD policy and say they have ways to securely connect just about any device that an end user might want to connect to the network (**Figure 6**).

Survey respondent Eugene Ching, managing director at Qavar, a Singapore-based firm that builds AI-powered custom apps, represents one such organization. Ching says his company allows users to use personally owned and unmanaged mobile devices to access enterprise apps. "We do so to allow employees freedom," Ching says. "We believe we have educated our team to be very aware of the risks that surround this freedom."

One reason for the relatively low level of concern around mobile device usage could be that a substantial number of organizations in our survey support only a small number of remote employees. At 44% of the organizations surveyed, most end users work primarily from a single corporate location

Figure 4



using company-owned devices and networks (**Figure 7**). The remaining respondents are evenly split: 28% say that most of their organization's employees worked remotely from a variety of locations, connecting from a variety of public and home networks, and 28% say their organization's employees are a relatively even mix of office and remote workers.

Another more broadly applicable reason is that mobile devices do not yet present the same risks to enterprise data as Windows desktop and notebook computers. Mobile devices are much harder targets for attackers than the typical Windows systems that are deployed at most organizations, says John Pescatore, director of emerging security trends at the SANS Institute.

"Android and iOS devices were largely built with full-time connectivity in mind," Pescatore says. The platforms support key protections such as mobile device management, encryption, sandboxing, and application whitelisting that make them harder to compromise than typical Windows-based systems. Both Google and Apple have also gotten better over the years at preventing malicious apps from invading their official application stores. "Mobile attacks are hard to pull off," Pescatore says. "There's certainly malware that impacts mobile devices but [is] typically less damaging" to enterprise data security than malware that targets PCs.

Mitigating Endpoint Risks

What approaches have organizations taken to mitigate endpoint security risk? Dark Reading's 2020 Endpoint Security Survey shows that a majority of businesses and

Figure 5

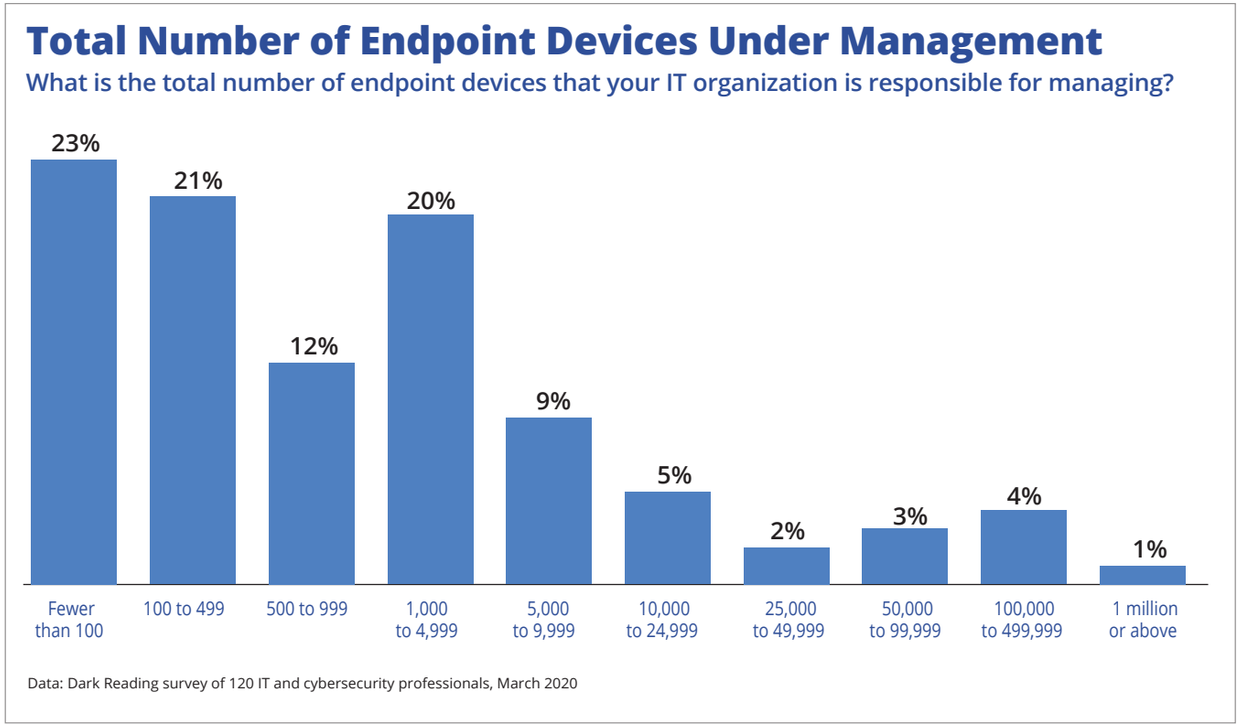
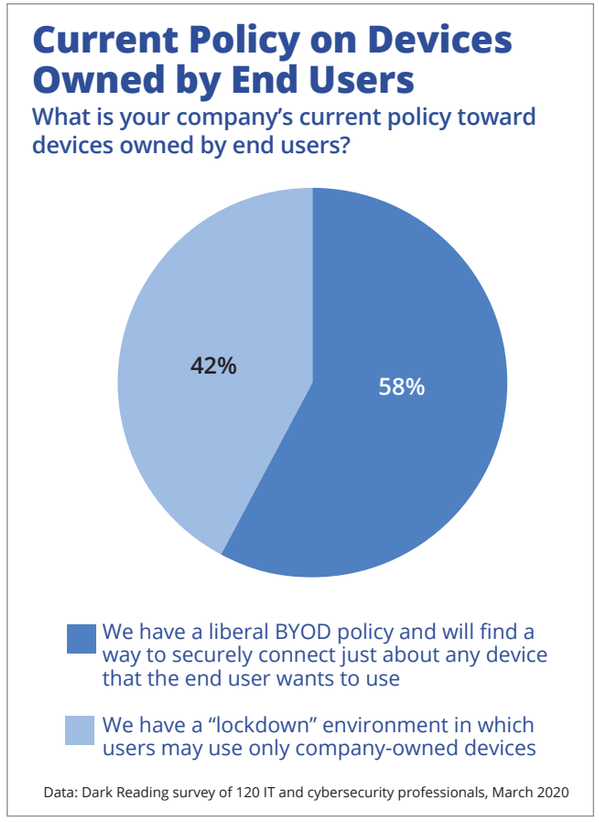


Figure 6



enterprises have deployed a variety of tools and processes to mitigate end-user and client-device risks.

Signature-based antivirus tools continue to be widely deployed. Ninety-two percent of organizations have an antivirus product in place — evidence that many still consider these products to be effective in blocking known threats (**Figure 8**). But unlike in the past, when an AV product pretty much constituted an organization's entire endpoint defense, now it's just one of many tools deployed for client security.

Two-thirds of the organizations in our survey have a VPN client on end-user systems; 57% require anti-spam controls; 47% have implemented certificate-based authentication for endpoints; and 32% use

Figure 7

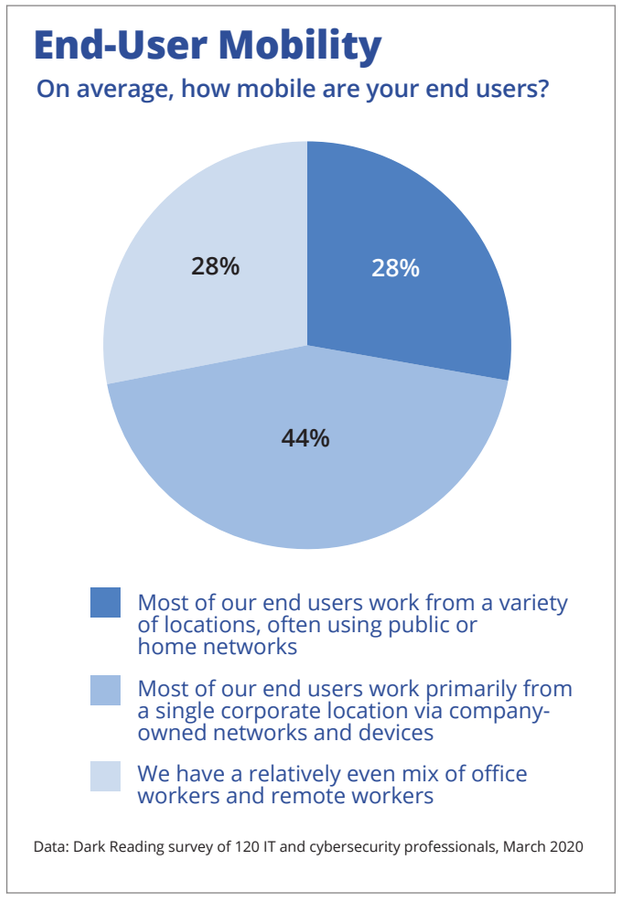
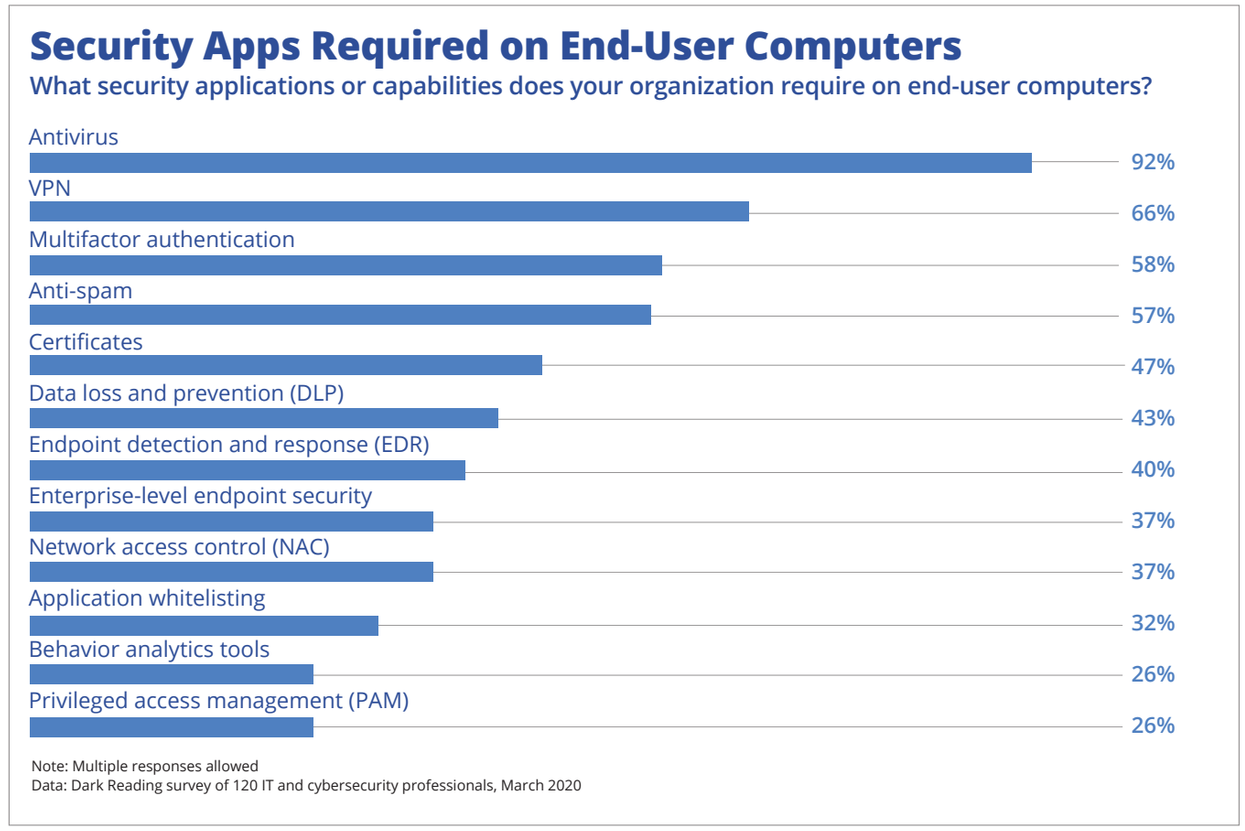


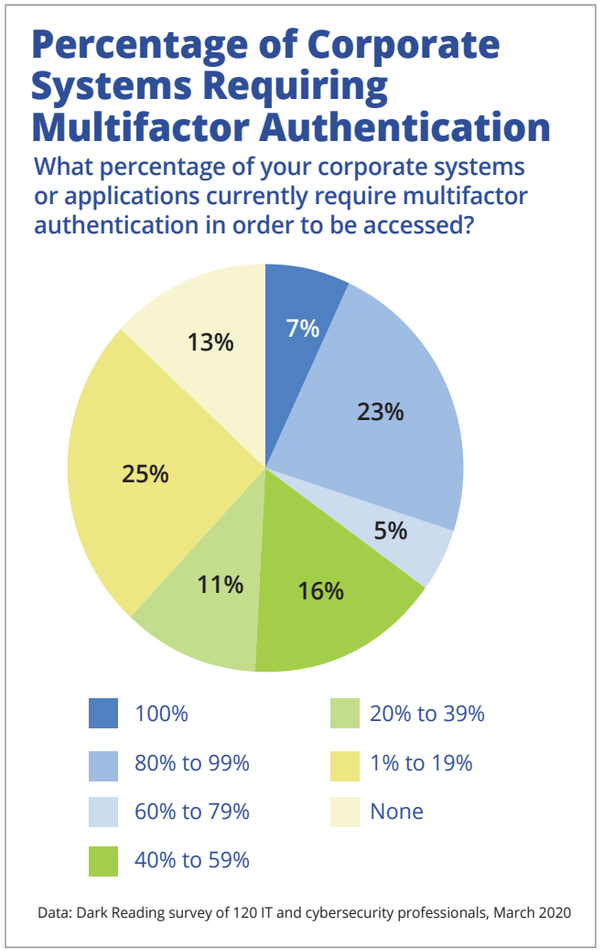
Figure 8



whitelisting to ensure only authorized apps can run on endpoint devices. In addition, 26% of the organizations use behavior analytics tools, including user and entity behavior analytics (UEBA) products, to mitigate client-side risks.

Many companies have also implemented strong authentication and identity management mechanisms to strengthen endpoint defenses. For instance, 58% of organizations currently require multifactor authentication (MFA) for end users. Thirty-percent require MFA for 80% or more of their applications (**Figure 9**).

Figure 9



Stephenson of Thinkpath Engineering Services says his company requires MFA in areas where controlled information is involved. "Dual authentication has been adopted [via] Yubico Key devices for users when accessing assigned workstations," he says. The company has also configured its Windows group policy settings to be dynamic so that access control permissions and restrictions vary depending on the sensitivity of the data or of the resources a user might want to access. Such measures are needed to comply with requirements established by the National Institute of Standards and Technology and the Defense Federal Acquisition Regulation, he says.

Dark Reading's survey shows that 40% of organizations have deployed endpoint detection and response (EDR) capabilities to address threats to client devices. EDR products are designed to help security administrators continuously monitor and analyze activities in the endpoint environment so threats can be quickly spotted and neutralized. One of the key selling points of EDR tools is that they can help organizations spot both known and unknown threats by applying static and dynamic analytics to endpoint activity data.

Researchers consider the capability critical because adversaries — especially advanced persistent threat groups and sophisticated cybercrime groups — have gotten better at evading traditional malware detection tools and lying hidden on compromised networks for months or even years.

Josh Zelonis, an analyst at Forrester Research, expects that over the next few years many organizations will consolidate their endpoint threat mitigation capabilities around EDR or similar technologies because of their versatility. EDR tools are morphing and integrating many more capabilities, such as those for analyzing application and network telemetry, he says.

Instead of having one set of products for preventing and blocking endpoint threats and another for detecting them post-compromise, organizations will increasingly choose to deploy just one technology capable of doing both, he says. EDR tools appear to fit the bill for the purpose.

"You will never have as good threat detection as you will get by monitoring the actual target environment," Zelonis says. "With EDR, you can point the security camera at the thing that you want not to get stolen so if

somebody steals it, you have it on video."

In addition to such tools, a substantial number of organizations have deployed specific protections and measures to defend against attacks involving the use of stolen end-user credentials. Topping the list is increased end-user awareness training (**Figure 10**). Seventy-eight percent of Dark Reading's survey respondents say they have ramped up efforts to educate users on how not to be tricked into sharing their credentials with adversaries or downloading malware on their systems. Considering the level of anxiety over the issue, the only thing surprising about that number is that it isn't higher.

Forty-one percent of organizations in the Dark Reading survey have implemented network segmentation to prevent adversaries with stolen credentials from moving laterally from one network segment to another. Attackers have frequently demonstrated how they can leverage their access on a business network — for instance, to gain access to OT networks because of a lack of proper segmentation. Forty percent have deployed a privileged access management platform to restrict access to privileged accounts and to limit what an adversary with access to such an account would be able to do with it. Security researchers consider such measures critical to shutting down the ability of attackers to hop around a compromised network in search of high-value systems.

One measure of the concern over endpoint threats is the proportion of respondents in the Dark Reading survey that indicate their organization has either already implemented a zero-trust initiative internally (17%) or are working on it (38%) (**Figure 11**). In a zero-trust network, every access request to an enterprise asset is fully authenticated and vetted before it is granted or denied. All users and devices are essentially considered untrustworthy until proven otherwise, and practices such as strong authentication

Figure 10

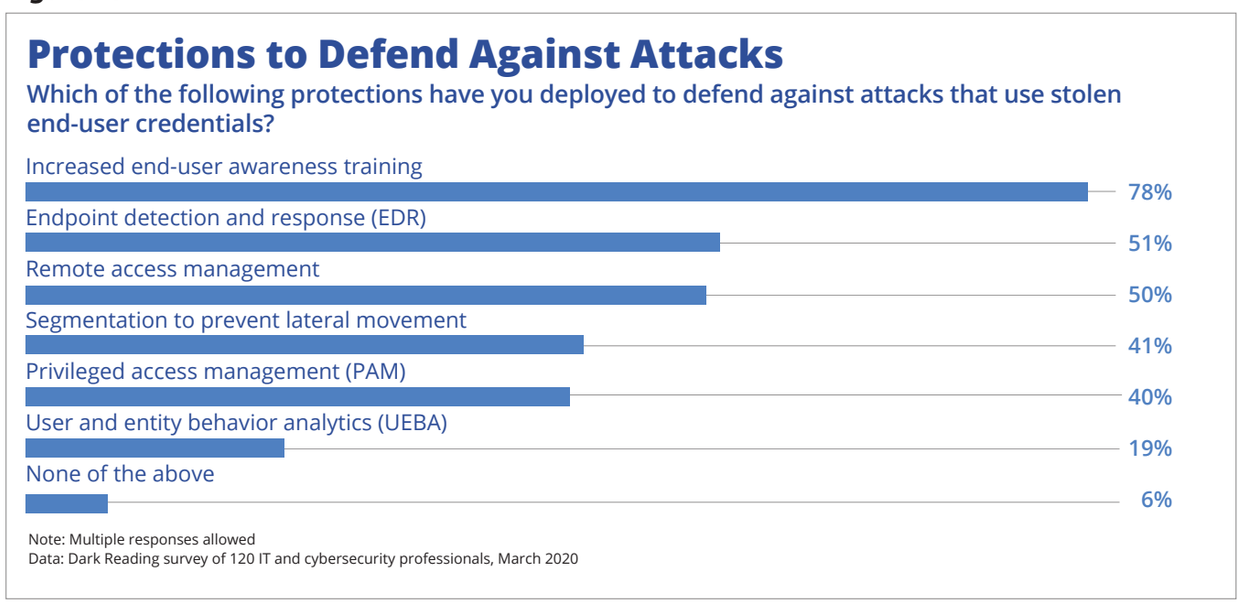
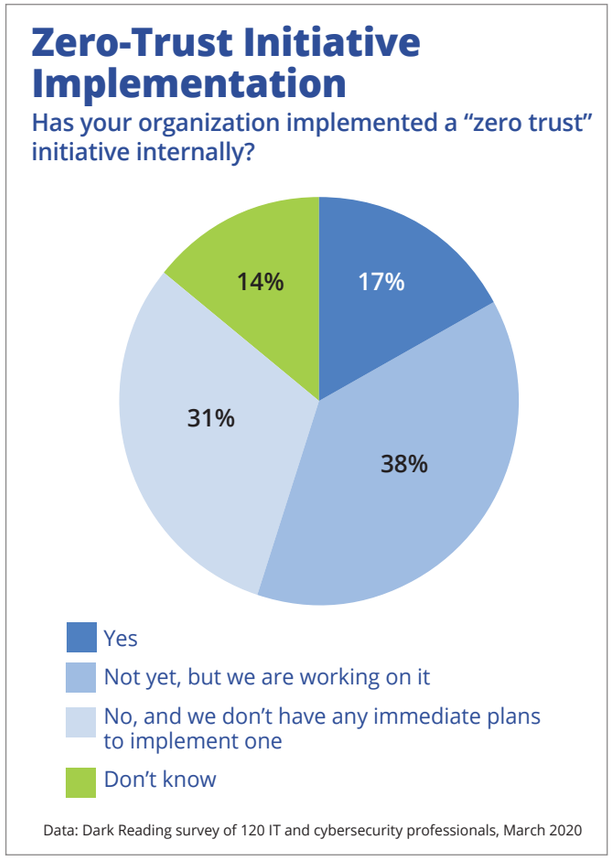


Figure 11



and network segmentation are key. In such a network, an adversary wouldn't be able to move about on a network simply by virtue of having a legitimate user's access credentials.

Interestingly, while not many organizations currently perceive mobile devices to be a major endpoint threat, they're not ignoring it entirely, either. Several security vendors recently have noted an uptick in mobile malware and threats directed at mobile devices. In February 2020, Kaspersky reported detecting 69,777 new mobile banking Trojans and more than 68,300 mobile ransomware tools last year. According to the vendor, attacks and malware aimed at mobile users increased in 2019 compared with the previous year.

Perhaps as a result of these trends, 62% of organizations in Dark Reading's survey require users to have passcodes for unlocking their mobile devices, 41% mandate the use of tools for locating missing devices, and 37% want anti-malware tools deployed on smartphones and tablets (**Figure 12**). A smaller number require other tools as well, including VPNs, secure web-browsing tools, and call and text messaging filtering apps. Also, more than four in 10 organizations have policies that permit them to use only company-issued mobile devices for work.

Gaps in Coverage

Dark Reading's 2020 survey shows that organizations across the board are taking endpoint security threats very seriously. A high percentage of them have deployed a variety of tools and processes for protecting client devices from malware and user-induced security issues. Forty-six percent estimate that their endpoint security spending will be "slightly higher" to "much higher" in the next 12 months, and another 44% expect it will remain the same (**Figure 13**).

Eight in 10 respondents point to ransomware attacks as a key reason for increasing endpoint security budgets; 73% say the increase in attacks involving end-user credentials was a factor.

"We have significantly increased our cybersecurity budget to reflect our desire to increase our level of vigilance," says Larry Mackey, a survey respondent and senior project manager at 3U Technologies. The company has boosted its endpoint budget in part over concerns that the current level of protection may not be enough, says Mackey. Another goal is to put controls in place for

Figure 12

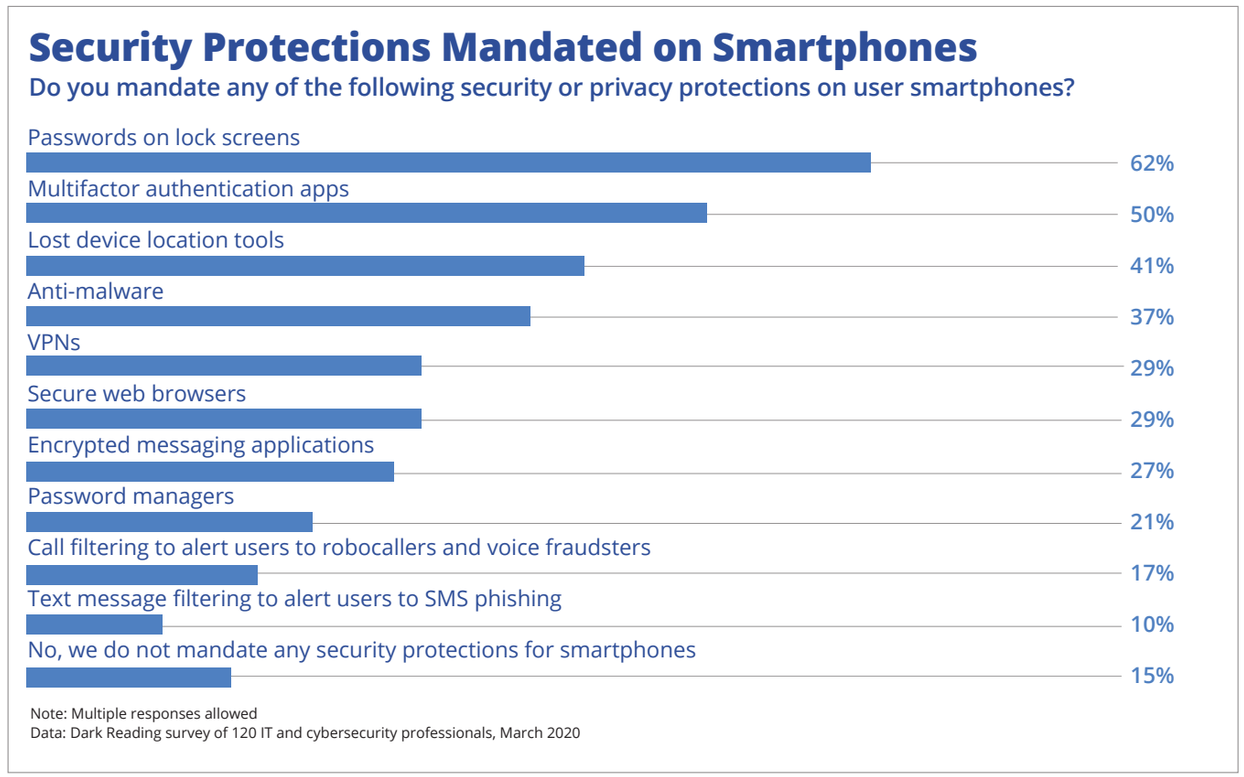
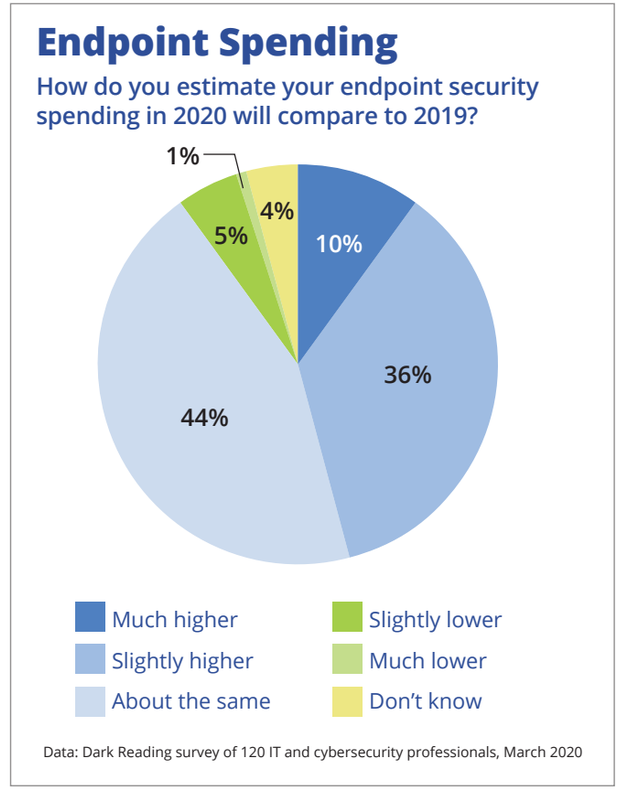


Figure 13



mitigating fallout from end-user miscues. "We are considering disaster recovery scenarios, including recovering from a loss of data from Office 365," Mackey adds.

Even so, some organizations appear considerably less prepared to deal with endpoint threats than others.

Fifty percent of the respondents surveyed have updated their organization's endpoint security policy in the past year (**Figure 14**). But the remaining 50% appear to have more static policies in place, suggesting they may not be quite as prepared to deal with new and emerging endpoint threats. Five percent have not changed it for between three and 10 years, and 16% aren't sure how long it's been.

Similarly, while 49% of organizations

Figure 14

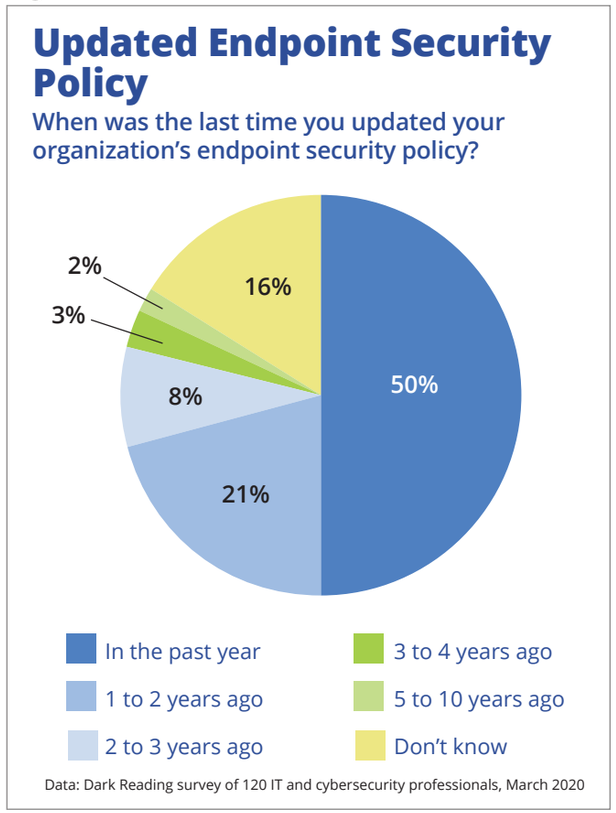
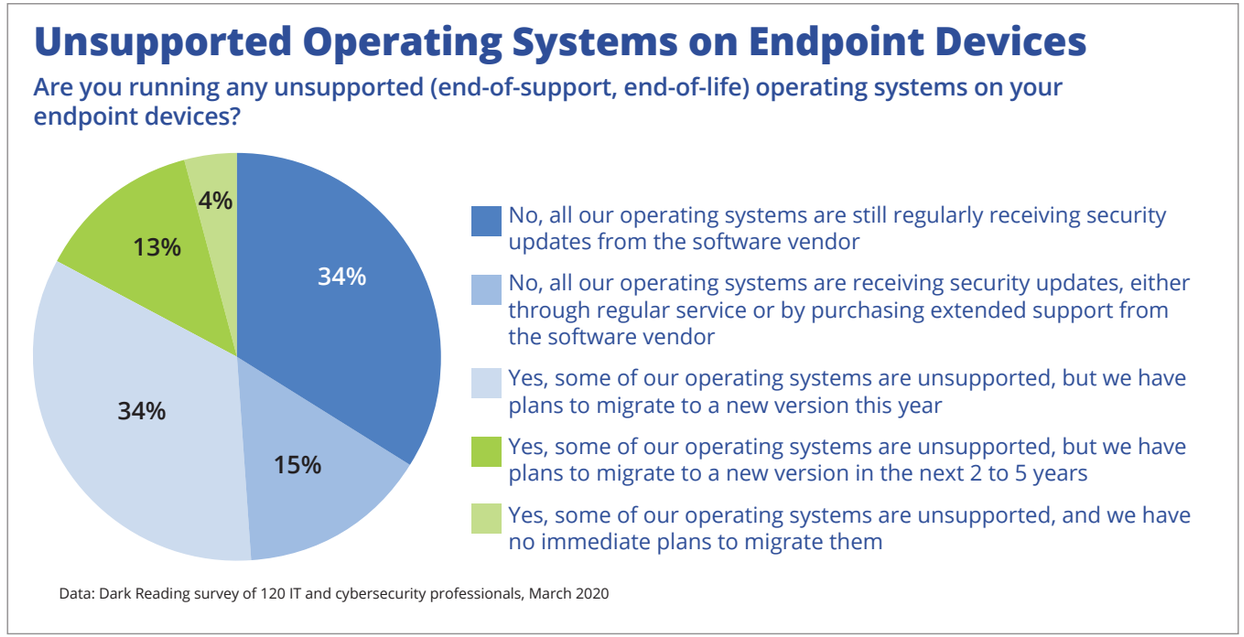


Figure 15



appear to be running properly patched and updated versions of operating systems on all their endpoint systems, 51% are not (**Figure 15**). Of that, 34% have unsupported operating system versions running on some endpoint devices but plan to migrate to a newer version this year. Thirteen percent admit to having unsupported operating systems versions in their endpoint environment but say it will take them between two and five years to move to a new version. Four percent have no plans at all to migrate from their old, unsupported software to a new version.

What the data means is that half of the organizations in our survey are not receiving security patches for any newly discovered vulnerabilities in their software. One example of why this matters is "BlueKeep," a critical, remote code execution vulnerability that was disclosed in June 2019 in multiple Windows versions, including unsupported ones such as Vista, Windows XP, and Windows Server 2003. In that particular instance, Microsoft made patches available even to users of the unsupported versions because of how critical the

bug was. But under ordinary circumstances, organizations with unsupported versions would have been left vulnerable to attack.

There are other issues as well. Seventy-seven percent and 85% of respondents, respectively, say they felt confident about their organization's approach to authentication and to manage end-user access privileges. But 50% don't even have a common identity management scheme for managing user access regardless of their location or device (**Figure 16**). And 52% don't currently have a single sign-on capability — a key enabler of zero-trust models (**Figure 17**).

Interestingly, the rush to deploy an array of technologies at the endpoint has resulted in some organizations being saddled with too many vendors. More than one-third (34%) of organizations are using endpoint security tools from between six and 24 vendors and another 36% are using tools from between three and five vendors (**Figure 18**). But a surprising 4% say they have tools from between 25 and 49 vendors, and 4% have 50 or more. According to security experts, an overly heterogeneous mix of products can cause product interoperability and integration issues as well as major vendor management issues.

Figure 16

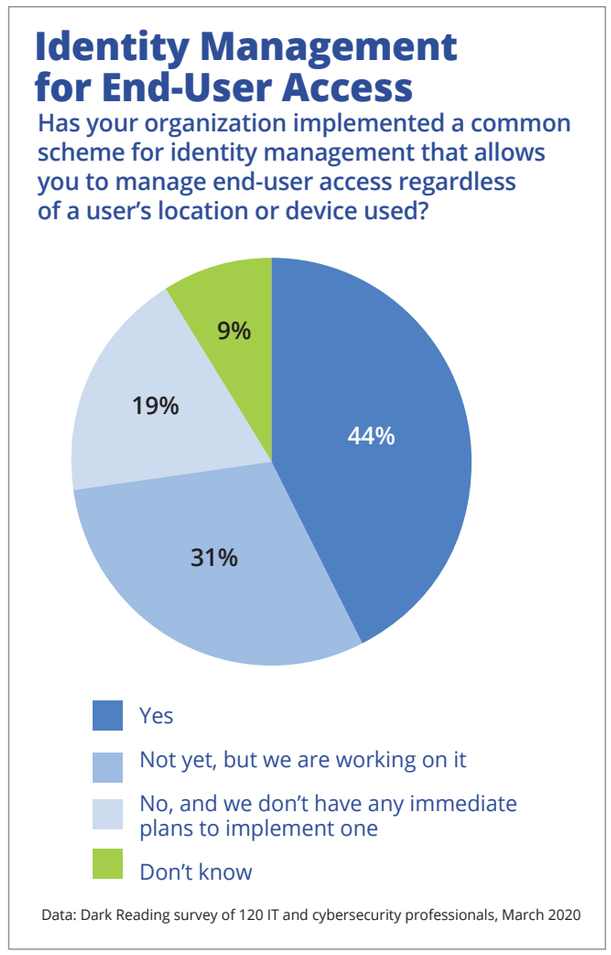
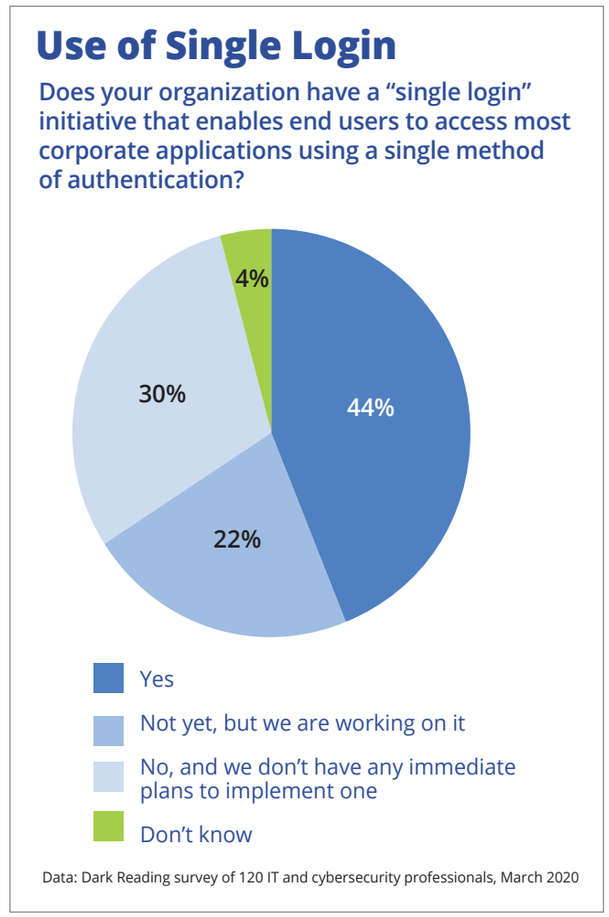
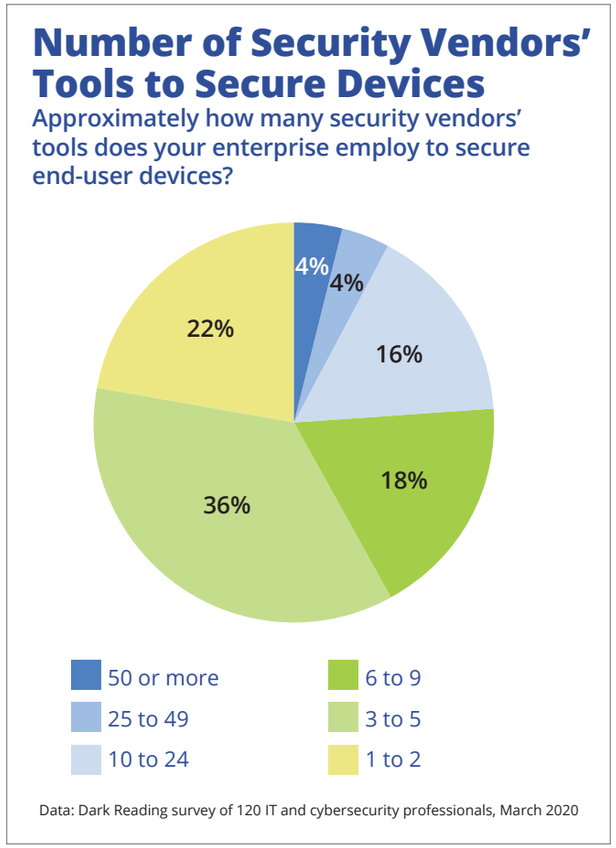


Figure 17



What other trends besides end-user-related risks and malware are driving change on the endpoint security front? Pescatore

Figure 18



from the SANS Institute says one big change is the ongoing shift away from a predominantly Windows-based client environment to one that is dominated by Android- and iOS-powered mobile devices and other thin clients. The endpoint devices accessing enterprise applications and data over the next few years are going to be different from the devices that organizations are used to protecting. As a result, expect the risk posed by traditional Windows PCs to gradually diminish, Pescatore says.

Also, as more organizations get better at defending their Windows endpoint environment and software vulnerabilities become harder to exploit, expect attackers to switch tactics, Pescatore says. Instead of using specialized tools, attackers will increasingly leverage legitimate software processes and admin tools to carry out attacks and to obfuscate them, he says. "The big guys have made advances in protecting the endpoint," Pescatore notes. "So attackers are increasingly living off the land," by using legitimate tools.

Conclusion

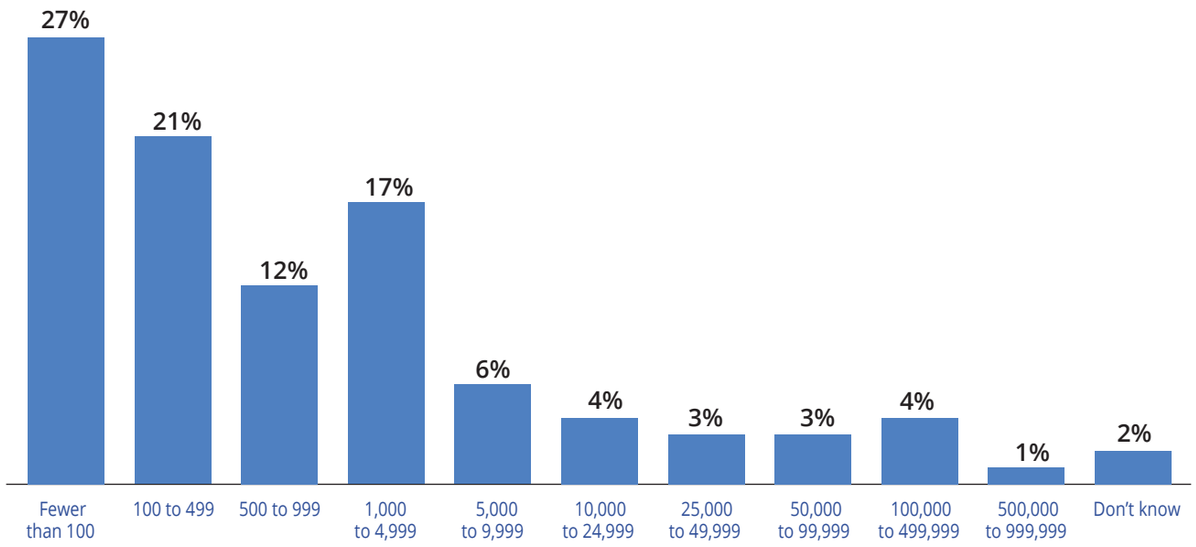
Enterprise efforts to bolster endpoint security continue to be hampered by risky user behavior. Many organizations have bolstered traditional AV defenses with new tools for preventing and detecting attacks on client devices. They have also implemented new measures such as strong authentication, network segmentation, and zero-trust approaches to limit the fallout from attacks on endpoint devices. However, end users are undermining many of these measures by indulging in risky behavior and failing to follow security policies. The situation highlights the need for a continued and greater focus on end-user security awareness and training.

APPENDIX

Figure 19

Total Number of End-User Devices Under Management

What is the total number of end-user devices that your IT organization is responsible for managing?

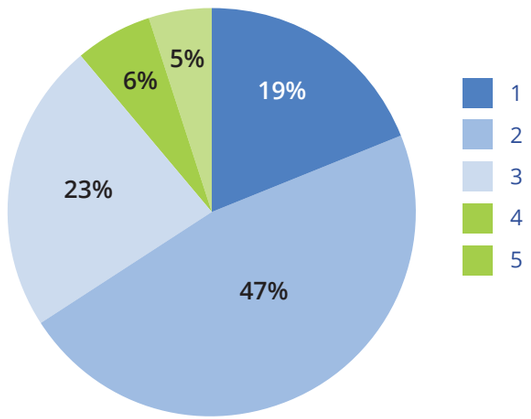


Data: Dark Reading survey of 120 IT and cybersecurity professionals, March 2020

Figure 20

Number of Devices Used by Employees

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

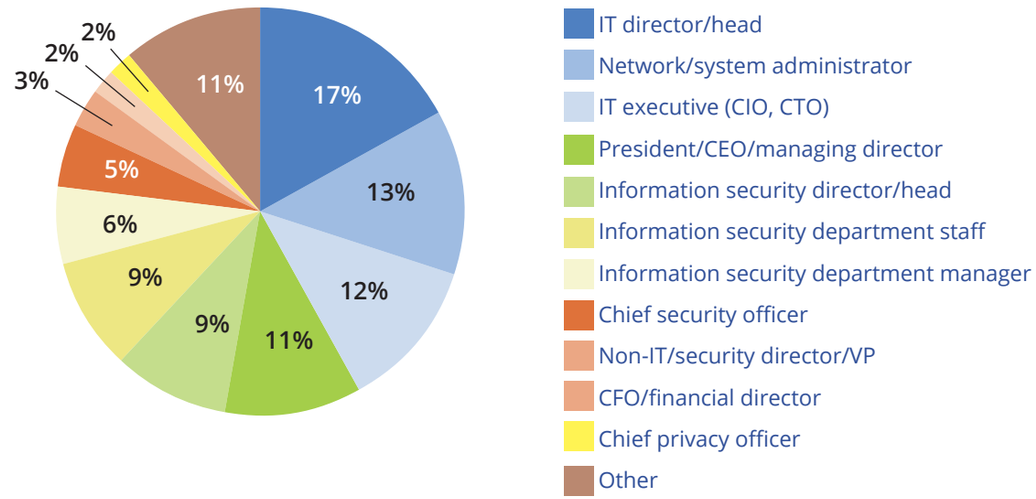


Data: Dark Reading survey of 120 IT and cybersecurity professionals, March 2020

Figure 21

Respondent Job Title

Which of the following best describes your job title?

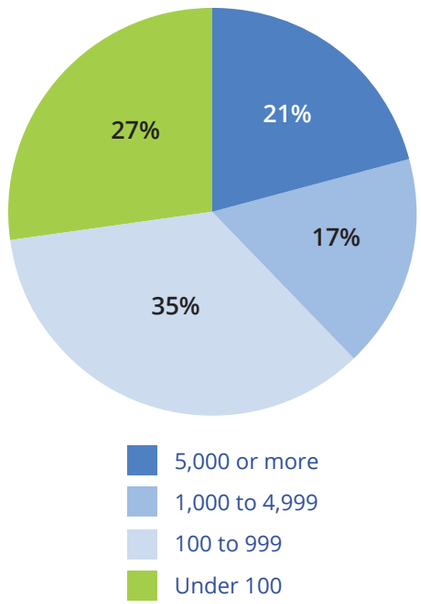


Data: Dark Reading survey of 120 IT and cybersecurity professionals, March 2020

Figure 22

Respondent Company Size

Approximately how many employees are in your organization?

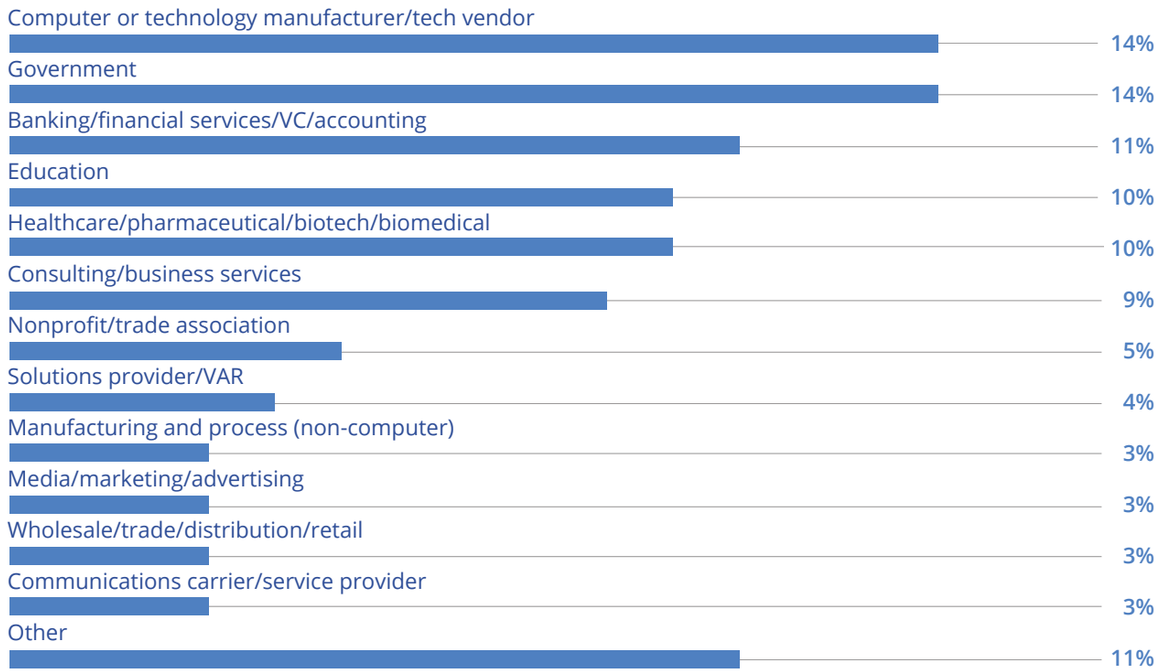


Data: Dark Reading survey of 120 IT and cybersecurity professionals, March 2020

Figure 23

Respondent Industry

What is your organization's primary industry?



Data: Dark Reading survey of 120 IT and cybersecurity professionals, March 2020