White Paper

The Business Imperative of Secure Endpoints

Sponsored by: Apple

Tom Mainelli Michael Suby
September 2023

IDC OPINION

What keeps IT Decision Makers (ITDMs) up at night? Security. That's because smart ITDMs know that no matter how well-run a business is or how popular its product or service might be, the whole business can be in jeopardy overnight if security fails.

And, unfortunately, the world isn't getting any safer. Corporate espionage, rogue states, organized crime, and even everyday thieves have all leveled up when it comes to technology. To stay ahead of the bad actors, IT must remain vigilant and ever willing to embrace new vendors and technologies to keep their employees, customers, and data safe.

The list of security challenges IT faces is long, involving everything from endpoints (computers) to datacenters, the networks that connect everything, and the software that runs it all. In this paper, we'll focus on the importance of securing the endpoint. That's because, in the end, security across all those other domains means little if the endpoint isn't secure.

One of the key challenges with securing the endpoint is that, traditionally, a secure endpoint often means a trade-off for the end-user experience with locked-down devices that are difficult to use. And when that happens, the other primary weak point in any security scheme — the user — often finds ways to circumvent that security in the spirit of getting work done. When security becomes a friction point for users, it's no longer serving its purpose.

Technological advances have made it increasingly possible to retain a high-quality user experience while maintaining security. Advances in malware detection, data protection, authentication, and the melding of silicon and software mean that today's endpoints don't need to trade productivity for enhanced security.

METHODOLOGY

IDC conducted an online survey of ITDMs in the United States and Canada in July 2023, asking about their views on security broadly and the importance of securing computer endpoints specifically. The respondent pool represents a mix of companies with 500 employees or more from a range of different industries. These ITDMs support a mix of computer operating systems, including Microsoft Windows, Apple macOS, and Google ChromeOS. They either select, purchase, or deploy security software for their company, or they manage the people who do.

SITUATION OVERVIEW

Security remains a C-suite imperative. Forward-thinking companies recognize that good security is not a "nice to have" but rather a requirement for a healthy and thriving business that operates in a constantly evolving threat landscape, driven by coordinated and well-funded bad actors.

According to IDC's March 2023 *Future Enterprise Resiliency and Spending Survey* (FERS) of enterprise ITDMs in companies of 500 employees or more, over 50% of companies surveyed worldwide had sustained a business-disrupting ransomware attack in the past 12 months. Over one-third of that group said the attack disrupted business by one week or more. Despite arguably having more robust security protocols, larger companies are far from immune to such attacks. In fact, the highest percentage of ransomware disruptions impacted companies in the 1,000 to 2,499 employees category (71%), 2,500 to 4,999 category (72%), and 5,000 to 9,999 category (70%). In other words, regardless of size, no company is immune to such attacks.

That same survey points to endpoints as the principal entry point for ransomware attacks. Initial points of compromise include web browsing (21%), removable media (18%), email attachment (17%), supply chain (17%), URL in an email (14%), and insider access (8%).

The sustained shift toward more employees working in hybrid and remote situations has only made ransomware and other security risks more challenging for IT. IDC's December 2022 *Endpoint Security Survey* showed that over 97% of organizations have a portion of their employees working remotely. While that number is expected to shrink some in the next twelve months, it will remain very high for the foreseeable future.

As companies wrestle with the sustained challenges of a large remote workforce, more are implementing zero trust strategies. Best practice focus areas include establishing a baseline of security controls, advanced endpoint security defenses, device attestation (ensuring devices connecting to the network are legitimate), and strong user authentication.

When you factor in all of the above, it's not surprising that respondents in our survey overwhelmingly selected improving overall data security and ensuring computers are secure as their top IT priorities, as reflected in **Figure 1**.

It's worth noting that in the figure below, the third most important topic for IT was improving employee productivity through better devices. When we asked respondents to pick their top 3 overall topics, the 'better devices' option was selected most often. This drives home a key message for IT to remember: Security is important, but it can't come at the expense of employee productivity, and the best devices offer a combination of great security and end-user satisfaction that's not hampered by that security.

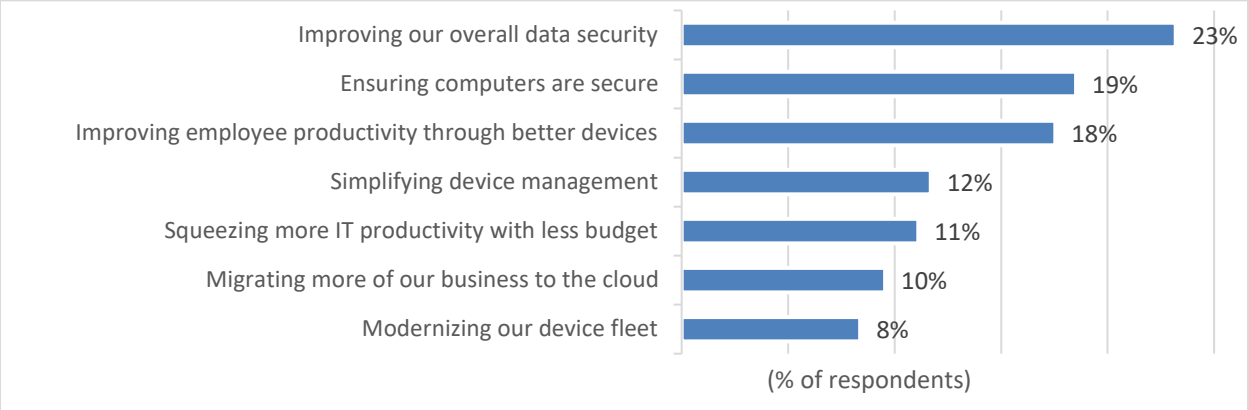
When we asked ITDMs what their top deciding factor was when choosing their next computer vendor, security came in as number 1, outscoring performance, support for existing applications, and integration with existing IT infrastructure. Perhaps most notable, the 'specifications' option was near the bottom of that list.

For a look at IT's top priorities, see **Figure 1**. For the top considerations when choosing a computer vendor, see **Figure 2**.

FIGURE 1

IT's Highest Priorities: Data and Endpoint Security

Which of the following IT topics are high priorities for your company today?



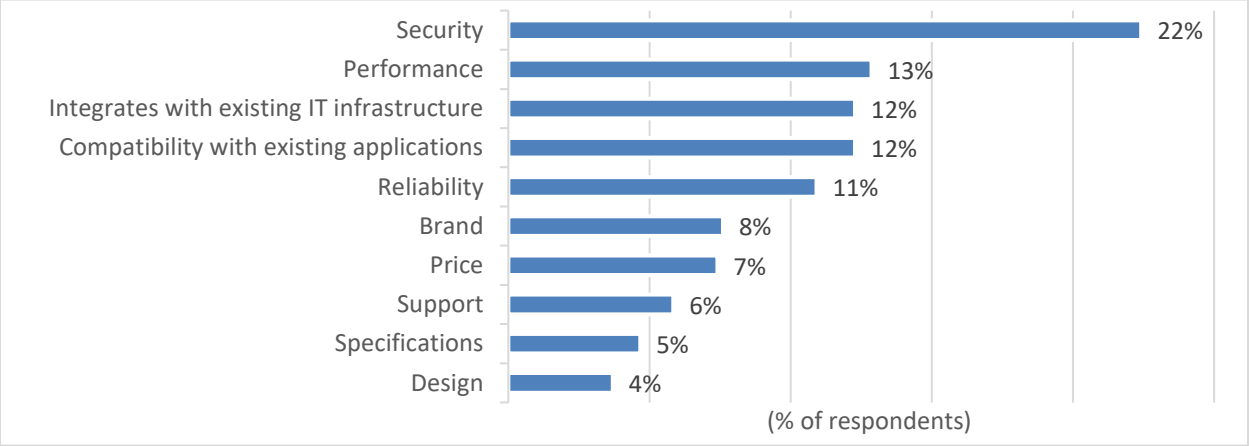
n = 513; Source: IDC's *Secure Endpoint Survey,* July 2023

Note: Data includes those ranking topmost important (#1 ranking).

FIGURE 2

Top Factors When Choosing a Computer Vendor

What are the top deciding factors when you are choosing a computer for your company?



n = 513; Source: IDC's *Secure Endpoint Survey,* July 2023

Note: Data includes those ranking topmost important (#1 ranking).

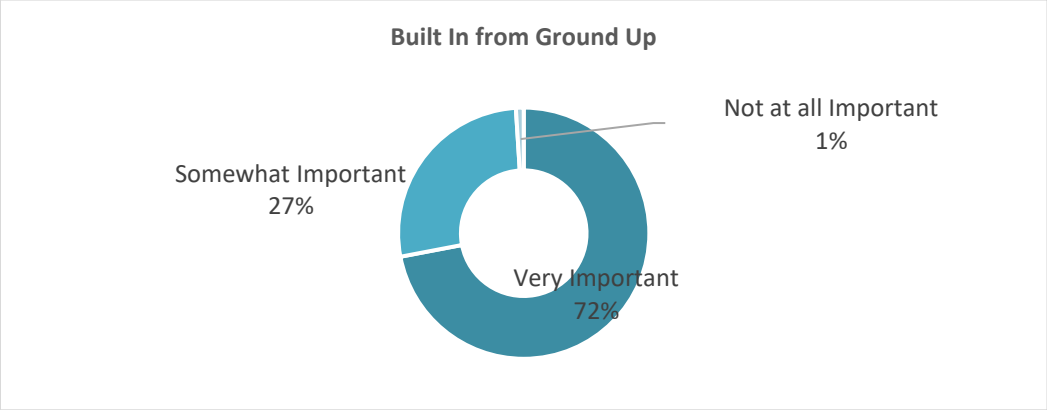
Two concepts resonating strongly with respondents were built-in security and integrated data protection. When asked, "How important would you say it is to have security built in to a computer from the ground up – including the silicon, the firmware, and the OS – to protect it from today's, and in anticipation of tomorrow's, threats?", the response was overwhelmingly positive, with 72% saying it was very important and 27% saying it was somewhat important. Just 1% said it wasn't important at all. Drilling into the data, it's worth noting that, among ITDMs at healthcare and finance organizations, the

percentage who said it was very important was even higher (84% and 75%, respectively). The concept of integrated data protection scored similarly high. We asked, "How important would you say it is to have data encryption capabilities integrated into the computer hardware?". Seventy-one percent said it was very important, 29% said it was somewhat important, and 0% said it was unimportant. For details on built-in security and integrated data encryption, see **Figure 3**.

FIGURE 3

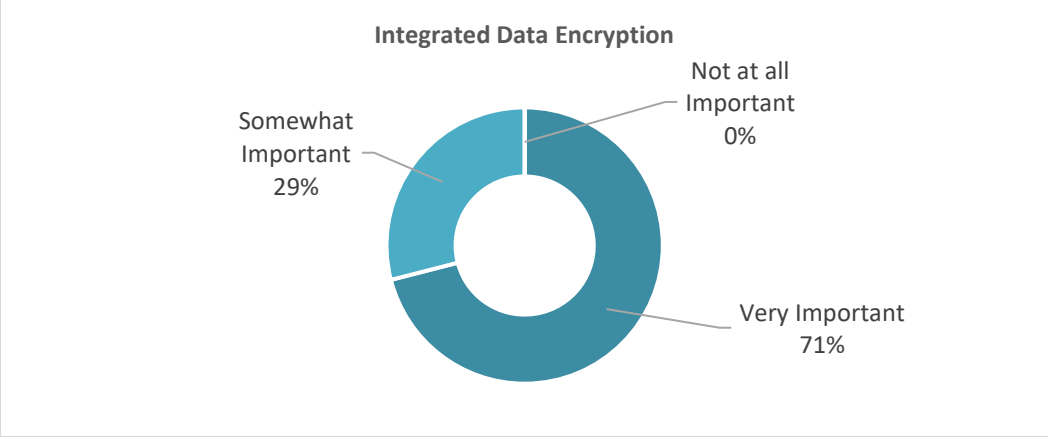
Importance of Built-In Security and Integrated Data Encryption

How important would you say it is to have security built in to a computer from the ground up — including the silicon, the firmware, and the OS — to protect it from today's, and in anticipation of tomorrow's threats?



n = 513; Source: IDC's *Secure Endpoint Survey,* July 2023

How important would you say it is to have data encryption capabilities integrated into the computer hardware?



n = 513; Source: IDC's *Secure Endpoint Survey,* July 2023

While hardware with security built in from the ground up is important and integrated data encryption is a key requirement, security experts know that the weakest link in any security chain is typically the end users themselves. That's why user authentication is so important and why technology vendors have

worked hard to evolve the state of authentication. Unfortunately, this is an area where our survey shows that many organizations are lagging.

On the positive side, our survey shows that 68% of respondents said their company requires complex passwords and 63% said they use two-factor authentication. On the less positive side, only 23% are using single sign-on technologies (SSO), and just 20% use biometric security (such as finger or face identification). It's worth noting that among our respondents, 56% said biometric authentication was a lot more secure than passwords, 35% said it was a little more secure, 9% said it was equally secure, and nobody (0%) said it was less secure.

An important new authentication technology recently introduced is passkey. A passkey is a digital credential that leverages a key pair to provide a much more secure solution than a password. Because this technology is new, just 14% of respondents said their companies use it, but smart ITDMs should be looking closely at the technology today. For details on user authentication usage, see **Figure 4**.

FIGURE 4

User Authentication Methods

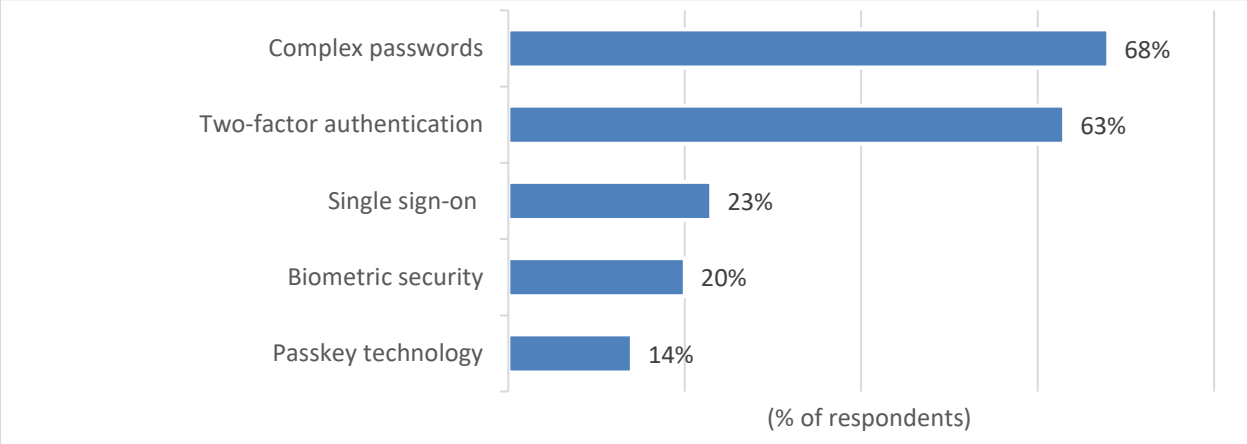
Does your company require employees to use complex passwords to log in to their computers?

Does your company deploy any computers that support biometric security measures such as finger scans?

Has your company begun examining the benefits of using passkey technology?

Does your company require two-factor authentication?

Does your company leverage any single sign-on (SSO) capabilities?



n = 513; Source: IDC's Secure Endpoint Survey, July 2023

Data indicates percent saying 'yes.'

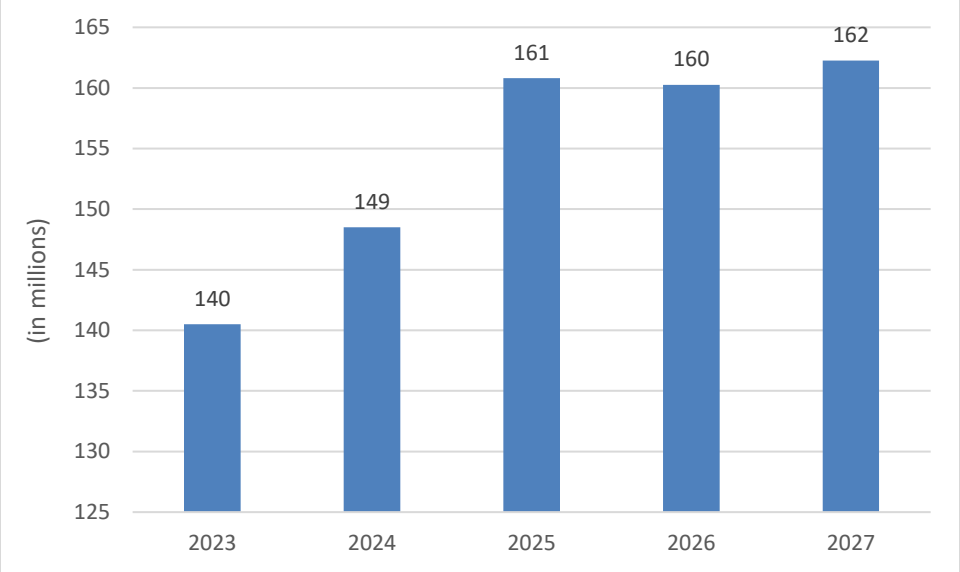
Among respondents, a shockingly high percentage have failed even to implement the baseline authentication protocols of complex passwords (32%) or two-factor authentication (37%). **A best practice worth pursuing** is ensuring that your company has implemented a consistent form of authentication across the organization. After you've established this baseline, begin to consider SSO capabilities combined with a strong master authentication protocol. Finally, as you complete your next

hardware refresh, take a closer look at computers that can support the highest levels of authentication: biometric security and passkey technology. Enabling biometrics and passkeys means a future where employees can quickly and safely log in to their computers and, from there, immediately into their apps and websites.

It's that last point – your next hardware refresh – where we'll close this section. Many companies have an aging installed base of computers that need to be replaced. Even if your organization bought a sizeable percentage of new endpoints as recently as 2020, those computers are rapidly approaching the four-year mark. In that time, hardware security has continued to evolve to meet the threats on the ground. Perhaps just as important, most of these products were shipped before the widespread shift toward remote and hybrid work, which means many lack high-quality cameras, microphones, and speakers necessary for employees to utilize now-key web conferencing and collaboration apps. After several years of slowing shipments, IDC's *Personal Computing Device Tracker* forecasts growth for the category over the next several years. For IDC's consumer/commercial computer forecast, see **Figure 5**.

FIGURE 5

Worldwide Commercial Computer Forecast



Note: Commercial units represent units purchased by non-consumer entities.

Source: IDC's *Personal Computing Device Tracker* , August 2023

Companies should continuously re-evaluate their employees' computer needs to remain competitive in the market and attract and retain top talent. Where IT once had to make serious tradeoffs between security and employee satisfaction, today, the right vendor can help drive a no-compromises solution. Finally, **another best practice to consider** is applying zero trust access principles for your next hardware deployment. This strategy assumes that whenever a device is attempting to access a company resource, it shouldn't be trusted until verified. Zero trust employs technologies and processes

to attest to the security state of the device (optimally from the silicon up through critical IT and security applications), connecting network (e.g., public Wi-Fi versus private network), and user identity.

Considering Mac in the Enterprise

More IT departments are supporting Macs today, and our survey points to a key reason why. Among our respondents, representing a mix of operating systems in their installed base, 76% said they believe Macs are more secure than other computers. And in the next 12 months, the number 1 reason for adopting more Macs was because they believe Macs are more secure (47%) – this was closely followed by ease of deployment and management (36%).

Apple is focused on providing a great user experience while elevating security by embedding security into Apple silicon up through software. An example of this is Apple's Touch ID, a built-in biometric security feature. Apple silicon features Secure Enclave, which encrypts and protects the passcode used to safeguard Touch ID data.

Apple Customer Spotlight

"Security is one of our main pillars of value at Inter. We chose Mac because of their robust security features and streamlined ecosystem, which collectively reduced our IT workloads."
- Guilherme Ximenes, Chief Technology Officer, Inter

Addressing the risk of compromised OS and boot sequences, Macs are equipped with Secure Boot and Signed System Volume. Secure Boot ensures only the cryptographically certified version of macOS is launched at start-up, and Signed System Volume protects the integrity of the OS during runtime. Out-of-date software also poses a cyber risk that Apple minimizes by automating and securing the end-to-end distribution and installation of software updates.

Great third-party software is essential for employee productivity, but that software must also be free of malware. Apple has a multi-layered approach to preventing malware. Apple's Mac App Store scans every app for malware. Since software on Macs can also be downloaded from the web, Apple requires developers to submit their apps to Apple's notary service, which also scans for malware. Apple's Gatekeeper, included in macOS, checks for notarization and prevents unsigned apps from running. Additionally, XProtect – Apple's anti-malware tool – blocks and removes any known malicious software.

Data is among an organization's most highly valued assets and must be protected accordingly. The combination of silicon-enforced FileVault encryption, Apple-supported VPN protocols, and end-to-end encryption in Apple services (e.g., iMessage and iCloud) ensures that data is protected at rest, in transit, and in use.

With social engineering among threat actors' honed skillsets, end users must be vigilant defenders: a difficult responsibility, but one that Apple assists with Safari Fraudulent Website Warning. In addition, since authentication credentials are often what threat actors steal, Apple's passkey support eases the pathway for organizations to modernize their authentication methods, again without sacrificing a positive end-user experience.

Good security is aligned with solid device management. To that end, Apple offers a range of device management capabilities, including a built-in management framework with Mobile Device Management (MDM). Apple Business Manager enables zero-touch deployment and links to MDM solutions, while Endpoint Security APIs for Mac allow developers to build solutions to monitor, analyze,

and respond to security threats. Apple also offers identity integrations with a built-in SSO framework that works with modern identity providers (IdPs).

Finally, Apple provides these security features, including both major and minor software updates, with macOS for no additional cost to enterprise or consumer customers.

CHALLENGES/OPPORTUNITIES

Despite a constantly evolving threat environment, IT is being challenged to do more with less: fewer dollars, fewer IT staff, and fewer resources. In addition to dealing with the ongoing security risks every company faces, many IT organizations have also been tasked with measurably improving employee productivity and satisfaction through the hardware, software, and services they deploy. Succeeding at both tasks — improving security and employee productivity and satisfaction — may seem insurmountable. But it also represents a key opportunity for IT: an opportunity to re-evaluate the hardware, software, and services it buys; the vendors it buys from; and the ways it deploys them to an increasingly hybrid workforce. Moreover, it is clearly time to recalculate total cost of ownership (TCO) models to better reflect how companies buy and use technology today.

CONCLUSION

Security is, and will continue to be, a top concern for IT. At a time when IT budgets are tight, and a significant hardware refresh is pending, it makes sense to re-evaluate which vendors you'll spend your dollars with going forward. Consider implementing best practices around authentication and zero-touch deployments and buy hardware that makes these shifts possible. Don't prioritize security over productivity and employee satisfaction when there are vendors who offer computers that have built-in security and data encryption that you can count on to provide both security and a positive end-user experience.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com