FORRESTER®

Mastering Endpoint Security In A Hybrid World

A FORRESTER CONSULTING THOUGHT LEADERSHIP PAPER COMMISSIONED BY HP, SEPTEMBER 2023

Table Of Contents

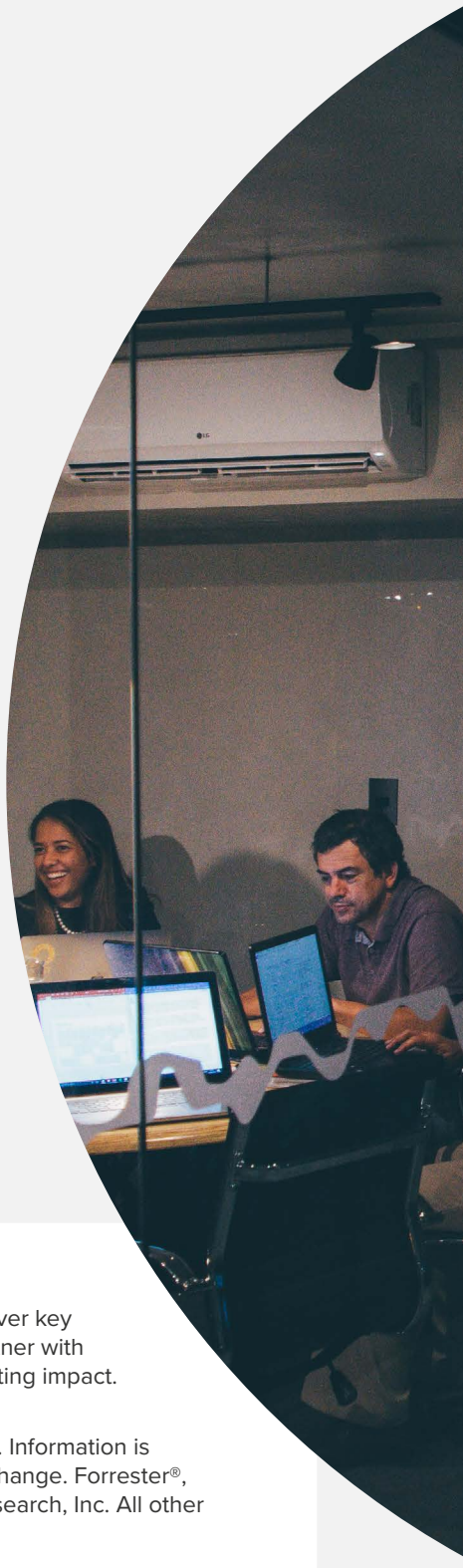
Project Team:

Sanny Mok,
Senior Market Impact Consultant

Tarun Avasthy,
Senior Consultant

Contributing Research:

Forrester's Security & Risk research group



ABOUT FORRESTER CONSULTING

Forrester provides independent and objective research-based consulting to help leaders deliver key outcomes. Fueled by our customer-obsessed research, Forrester's seasoned consultants partner with leaders to execute their specific priorities using a unique engagement model that ensures lasting impact. For more information, visit forrester.com/consulting.

Executive Summary

The evolving digital landscape has thrust endpoint lifecycle management into the spotlight with three overarching business challenges emerging: asset management, user experience assurance, and risk management. As leaders champion remote work, the need for adept device strategies becomes evident. In particular, the upkeep of accurate asset databases has become a paramount concern, especially with the mention of asset management as a mandatory control in the new Network and Information Security (NIS2) Directive in the European Union.

Yet as we navigate this digital shift, the concept of always-on PC fleet management offers a beacon of hope. This approach not only aids in managing lost devices, but also improves asset management. It guarantees robust data protection, elevates productivity, and ensures stringent compliance. Furthermore, it has a role in sustainable device lifecycles. Leveraging such real-time strategies empowers enterprises with a secure lifecycle — a framework emphasizing continuous monitoring and stringent endpoint defense.

In March 2023, HP commissioned Forrester Consulting to evaluate the current and future approach to managing endpoints in distributed locations. Maintaining management of laptops and other isolated devices efficiently is challenging in hybrid work with scenarios like missing laptops or offboarding employees. Forrester conducted an online survey with 312 IT and security decision-makers at companies with 500 or more employees to explore the impact of poor asset management and data security processes and how it affects employee experience (EX), operational efficiency, and risk management.

Key Findings

The digital workspace is evolving. With the rise of remote and hybrid models, there's an urgent call for enhanced endpoint strategies to balance productivity and security in decentralized environments.

The approach to firmware management is lackadaisical. An alarming trend sees many organizations overlooking crucial firmware updates, opening doors to security risks and inefficiencies. There's a stark need for proactive action.

Multifaceted benefits of the find, lock, and erase solutions. The find, lock, and erase solution is not merely a security tool — it's a holistic solution that promises enhanced data protection, operational efficiency, and regulatory compliance. Organizations that adopt this tool can anticipate a fortified defense against cyberthreats, augmented employee productivity, and a streamlined approach to compliance requirements, including NIS 2.

Always-on endpoint management is the linchpin of comprehensive IT resilience. Harnessing an always-on approach to endpoint management empowers organizations to promptly counteract threats, elevate asset oversight, champion sustainable device practices, bolster IT agility, and augment compliance measures.

The Transition Towards Remote And Hybrid Work Models

In today's dynamic digital landscape, businesses are navigating a profound transformation, shifting towards remote and hybrid work models. As organizations settle into this new paradigm, IT professionals are faced with the critical challenge of managing and securing endpoints, specifically laptops, effectively (see Figure 1):

- **Hybrid work dominates.** A significant shift towards nontraditional office environments was evident.[1] Forrester Research's 2021 data shows that 46% of infrastructure decision-makers said that more than half their workforce worked remotely most of the time.[2] It took the COVID-19 pandemic to change that. Now, every firm has a rare opportunity and urgent need to get hybrid working right. In our survey, 72% of respondents said their organization operates under a hybrid work model, implying that a considerable proportion of the workforce is remote at any given time. Because of this, IT professionals have been presented with the challenge of securing endpoints located outside the traditional office environment, thereby heightening the risk and complexity of asset management and data security processes.
- **On-premises work models are still persisting.** While the trend leans towards remote work, 21% of respondents noted their organization remains entirely on-premises. Interestingly, respondents anticipated this number to rise to 27% within the next year. Therefore, IT leaders find themselves balancing the demands of both conventional and emerging work environments, adding intricacies to the task of endpoint management.
- **There has been a modest uptick in fully remote work.** While presently only 7% of respondents noted their organizations have a fully remote work model, this is projected

58%

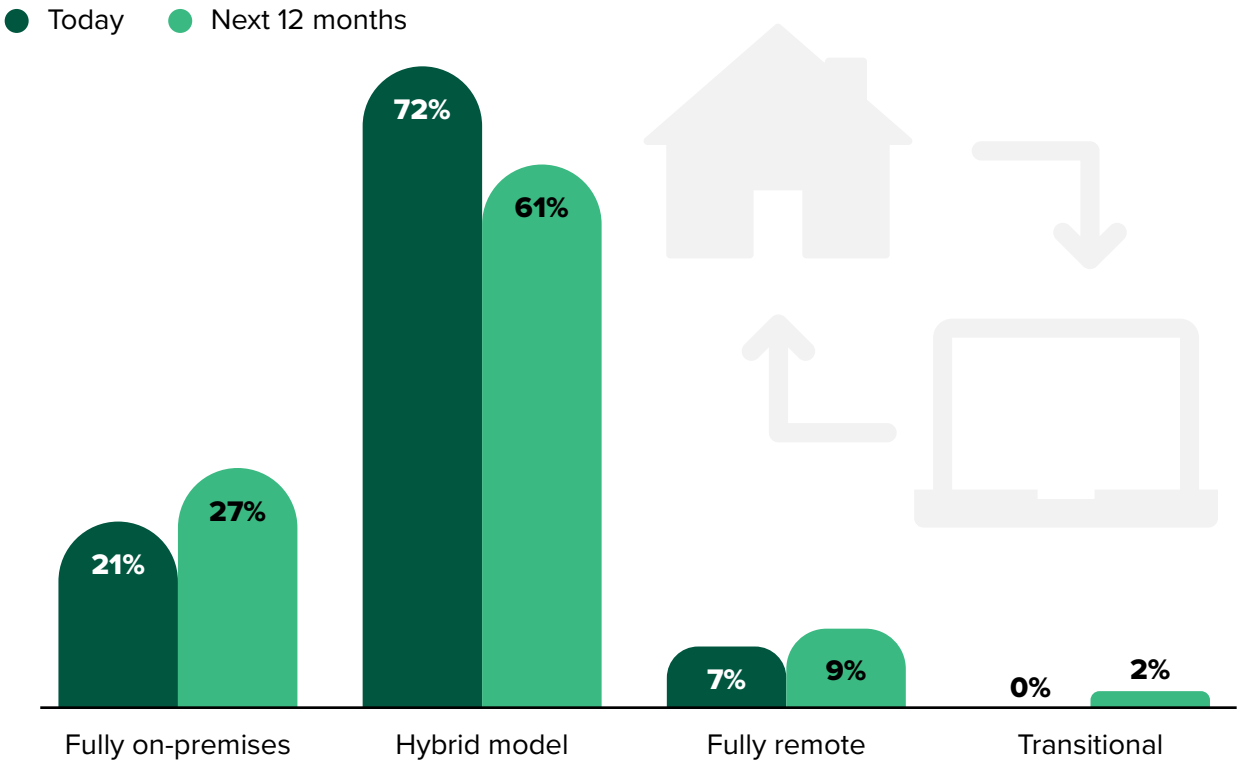
of respondents cited investing in endpoint security to maintain their firm's reputation and protect data and proprietary information against unknown threats.

to increase slightly to 9% in the upcoming year. Respondents projected that this will slightly increase to 9% in the upcoming year. Though a modest rise, it indicates a growing acceptance of a model once deemed unconventional, emphasizing the need for solid endpoint management strategies in the work landscape.

> **79%**
>
> of respondents at NA firms said they use a hybrid model, with 58% planning to continue this for the next year. In APAC, 74% said they use a hybrid model while 45% plan to continue to do so.

FIGURE 1

"Which of the following best describes your organization's implementation of anywhere work both today and in 12 months?"



Base: 312 IT and security decision-makers at companies with 500 or more employees across multiple industries
Source: A commissioned study conducted by Forrester Consulting on behalf of HP, September 2023

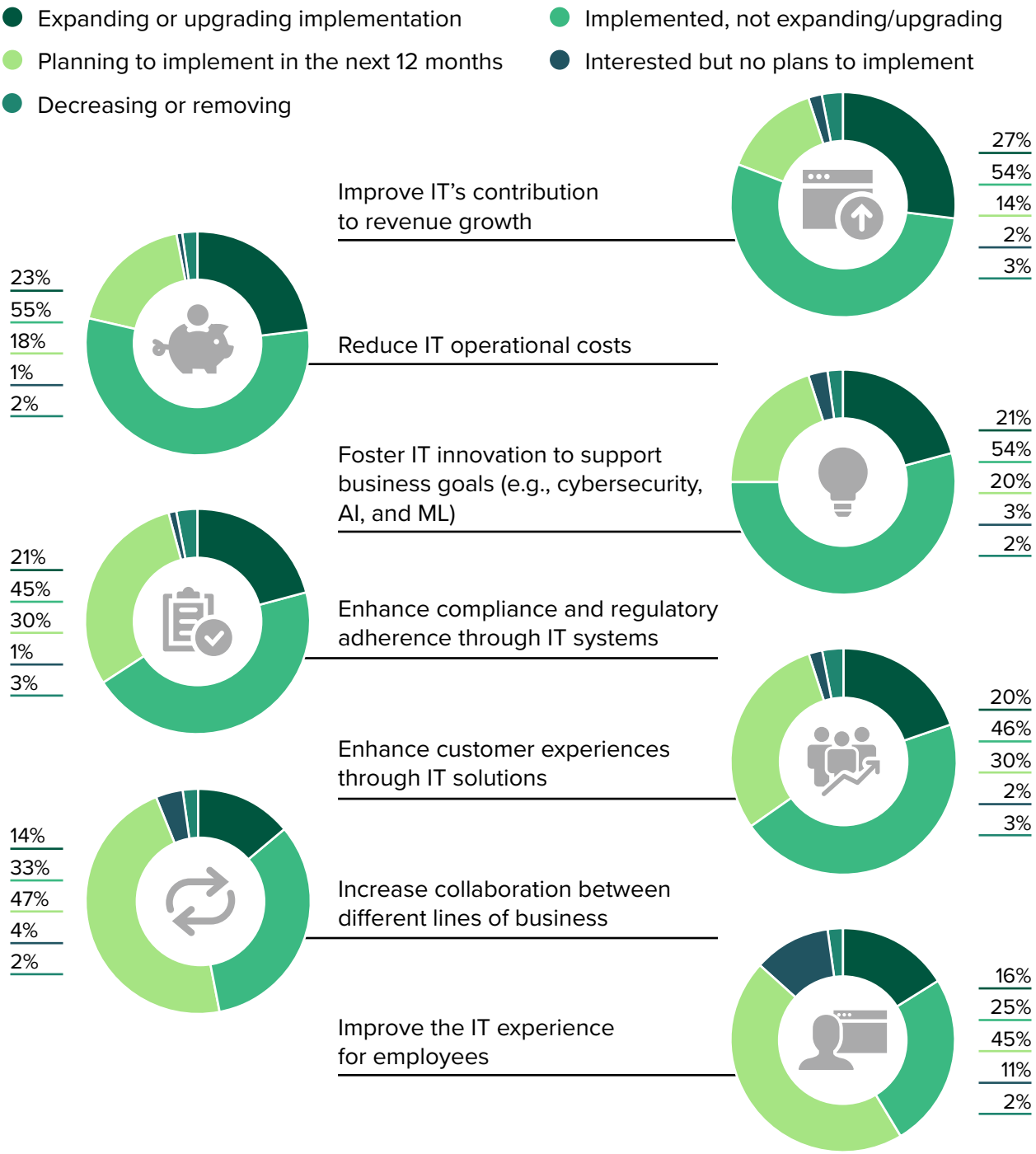
IT Priorities Focus On Growth, Innovation, And Collaboration

As the way work evolves, so do the priorities for IT leaders. These pivotal strategic initiatives set the tone for organizations' focus and investment in the coming year, with revenue growth, operational cost reduction, innovation, and collaboration taking the front seat (see Figure 2):

- **Cross-functional collaboration is increasing.** Notably, within the next 12 months, 47% of respondents said their organization plans on intensifying collaboration between various business units. This surge in interest underscores the escalating demand for cohesive and secure IT frameworks that can boost effective collaboration, even among teams dispersed across various locations. Here, the contribution of IT is not limited to merely bolstering productivity and security; it becomes pivotal for fostering cross-functional synergy.
- **Attention to the digital experience is increasing.** The IT experience for employees is witnessing a transformative phase. Only 25% of respondents said their organization implemented measures in this realm without future plans for expansion. However, a notable 45% were gearing up to introduce strategies to refine the IT experience for employees in the forthcoming year. This sizable percentage underscores the vast untapped potential in this area. The 16% that noted they are in the process of expanding or upgrading their current implementations indicate an ongoing interest in elevating the digital workspace.
- **The dual mandate of revenue growth and cost reduction.** This remains at the forefront of business objectives. A notable 54% of respondents said their business has taken proactive measures by rolling out IT initiatives designed to augment their revenue generating capacities. An additional 27% noted they are on the brink of either extending or revamping their existing IT deployments, which testifies to IT's dual role — both as an auxiliary service and a linchpin for business expansion. In tandem, cost curtailment continued to be an IT priority for respondents' organizations, with 23% intensifying their cost-reduction pursuits and a whopping 55% already deploying cost-saving strategies.

FIGURE 2

"Which of the following initiatives are likely to be your organization's top IT priorities over the next 12 months?"



Base: 312 IT and security decision-makers at companies with 500 or more employees across multiple industries
Note: Percentages may not total 100 because of rounding.
Source: A commissioned study conducted by Forrester Consulting on behalf of HP, September 2023

- **Innovation remains imperative.** While IT innovation — encompassing realms like cybersecurity, artificial intelligence, and machine learning (ML) — is already a focal point for numerous enterprises (54% of respondents noted their firm has rolled out related initiatives), about 21% were looking to either enhance or update their existing systems. The proliferation of hybrid and remote work models necessitates cutting-edge IT innovation, which is instrumental in devising secure, agile, and effective digital workspaces for a widespread workforce.

In APAC, 38% of firms prioritize improving digital experiences compared to 31% in EMEA and 21% in NA.

Device Lifecycle Management Is A Reactive Process

Managing the lifecycle of devices in an organization is more than just a routine task — it's a core aspect of maintaining operational resilience. The adoption of a comprehensive endpoint management strategy that ensures consistent updates and maintenance across firmware, operating systems (OS), and apps is not just an option but a necessity, especially as the world embraces hybrid and remote work models. Such a strategy is pivotal to achieving IT and security operational efficiency (see Figure 3):

- **Firmware updates are woefully inadequate.** The current approach to firmware updates is both reactive and potentially perilous. Patch management is critical to endpoint hygiene, but it's only useful if the enterprise has full visibility and control over the endpoint that endpoint security platforms can provide.[3] Unfortunately, the lack of coordination means that many companies struggle to patch effectively. Astonishingly, about 42% of respondents noted their organization only performs firmware updates on an annual basis, and a significant 15% stretched this to biannual updates. Such infrequent updates can precipitate a slew of complications, from compatibility issues that disrupt regular operations to security vulnerabilities. What's even more alarming is that 12% of respondents said their organization only resorts to firmware updates when it perceives an imminent threat to security or system stability. Such a laid-back attitude is not just risky; it's a clear invitation for potential cyberattacks.
- **The end-of-device life always necessitates data erasure.** The end-of-life phase for devices presents its own set of challenges. About 35% of respondents noted their organization follows an in-house process of erasing data and then dispatching the device for recycling. While this method seems security-conscious, it is riddled with manual procedures that are labor-intensive and inefficient. Ensuring thorough data erasure and handling potential data breaches during disposal are daunting tasks. These manual, labor-intensive processes that are cumbersome and

inefficient become even more challenging when dealing with devices from remote or hybrid employees.

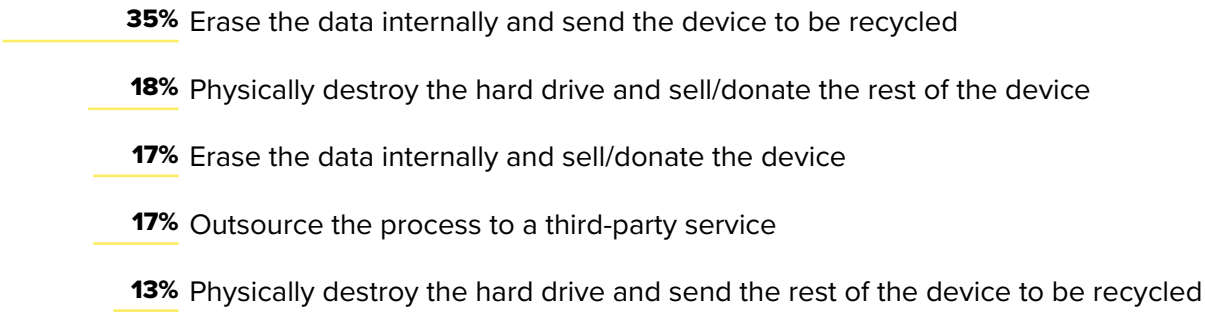
In APAC, 48% of respondents at SMBs erase data in-house before recycling devices, compared to 28% in EMEA and 35% in NA.

- **End-of-life processes are outsourced.** To bypass internal challenges, around 17% of respondents said their organization outsources its end-of-device-life processes to external specialists. This decision may stem from resource constraints or the allure of external expertise. However, such a shift mandates that these third-party services align with organizational data security protocols and meet global environmental standards. They also incur additional costs. The inclination to outsource could be driven by organizations recognizing the inefficiencies and complexities of their internal, manual processes and the desire for more streamlined solutions.

FIGURE 3

"Which of the following best describes the frequency that your organization perform firmware (BIOS) updates?"

"How does your organization typically manage end-of-device life?"



Base: 312 IT and security decision-makers at companies with 500 or more employees across multiple industries
Note: Percentages may not total 100 because of rounding.
Source: A commissioned study conducted by Forrester Consulting on behalf of HP, September 2023

Untangling Remote Endpoint Management Remains Challenging

The shift towards remote and hybrid work models has only amplified the intricacies of managing endpoints. From striving to maintain comprehensive asset databases and grappling with sustainable device lifecycle management, to bolstering endpoint security and ensuring compliance, organizations are navigating a maze of challenges (see Figure 4):

44%

of respondents at large eneterprises said they had the limited ability to effectively locate lost or stolen devices due to lack of efficient tools or systems.

- **The maze of tracking assets.** A notable 62% of respondents said their organization grapples with maintaining an accurate and continuously updated asset database, a challenge that has been universally acknowledged as a pervasive and pressing concern. This issue doesn't merely hamper efficient decision-making; it also poses obstacles to optimal resource allocation and security policy conformance, especially as workforces sprawl across varied geographical locales.
- **Device lifecycle management and sustainability.** An estimated 55% of respondents pointed out the daunting challenge of overseeing the device lifecycle with sustainability in mind. The entire gamut, from procuring devices to their eventual disposal or recycling, has become a challenging endeavor in the backdrop of minimizing environmental impact.
- **Securing the vulnerable endpoint.** A significant 50% of respondents find their organization's endpoint security solutions are inadequate. They cited a lack of robust protection or comprehensive functionality to secure devices, underscoring the importance of robust IT security solutions in an increasingly digital and distributed work environment.

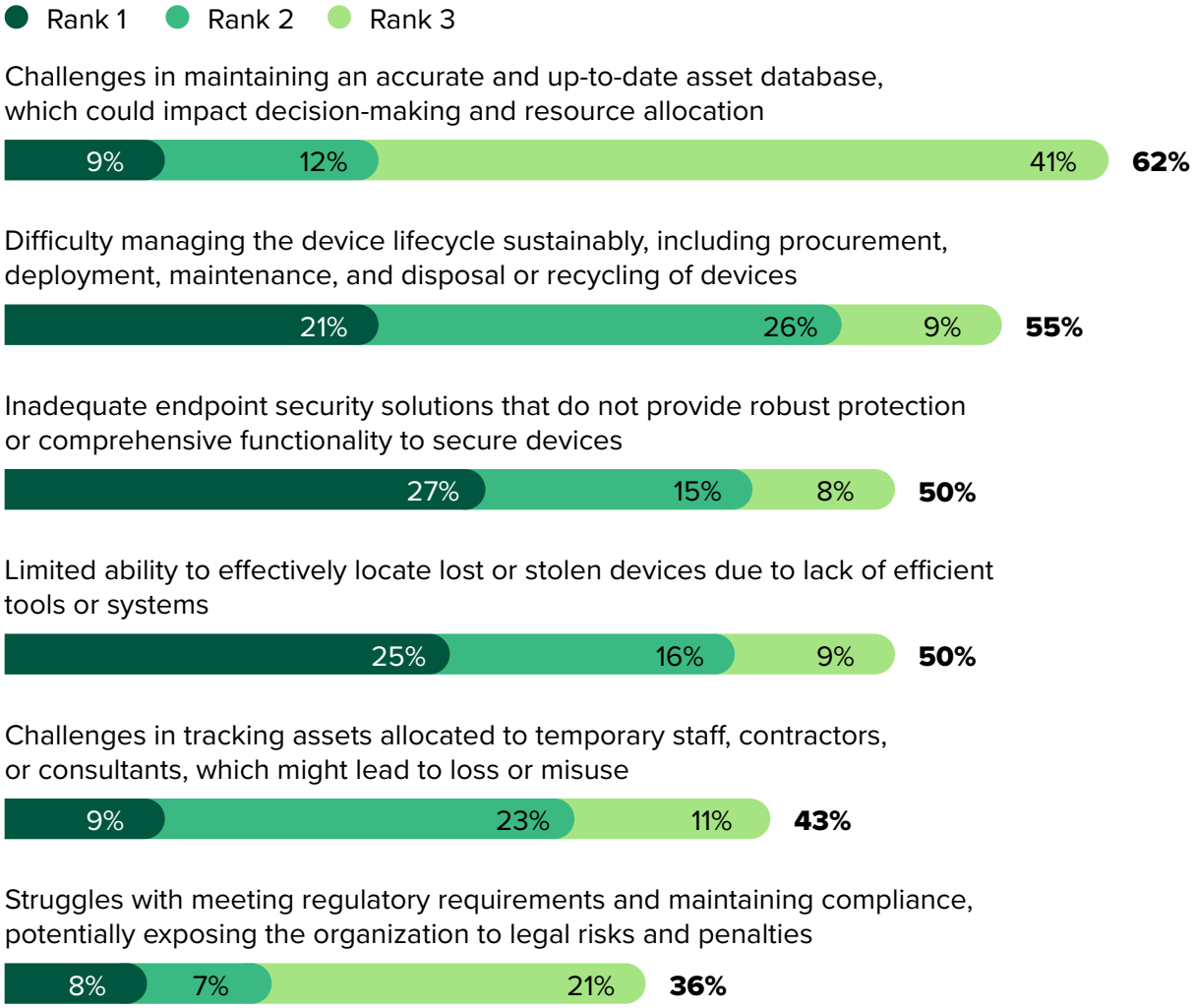
67%

believe ensuring secure communication with remote endpoints is a primary concern.

Additionally, intertwined with these challenges is the need to comply with regulatory requirements. Organizations are not only navigating external mandates but are also striving to meet internal audit standards, emphasizing the dual pressure of internal evaluations and external compliance in their bid to ensure robust endpoint management.

FIGURE 4

"What specific obstacles does your organization encounter as it addresses the challenges of remote endpoints?"



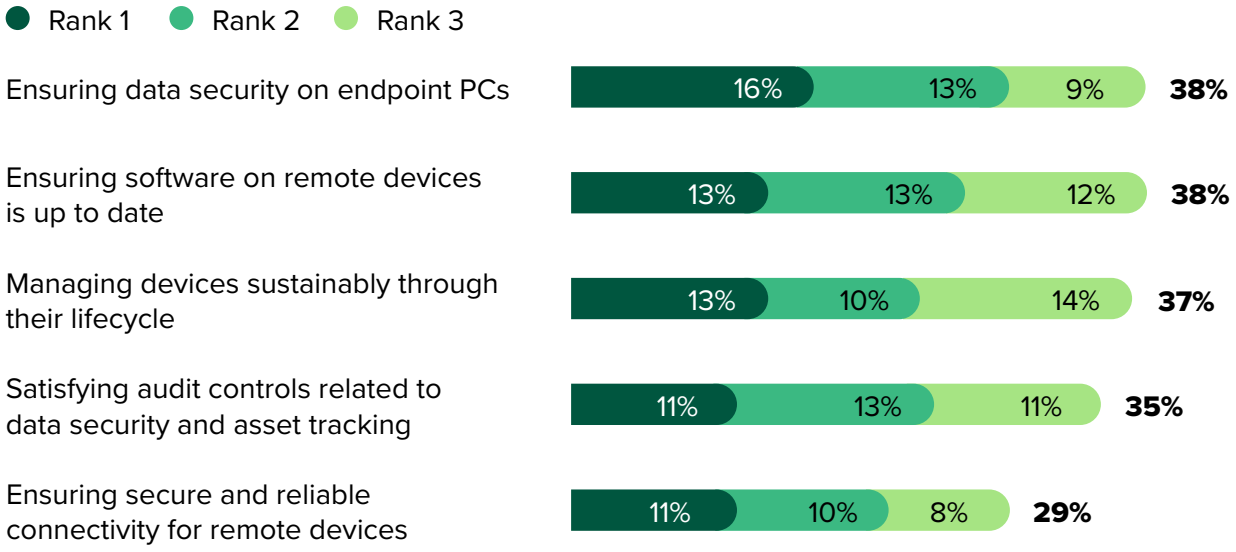
Base: 312 IT and security decision-makers at companies with 500 or more employees across multiple industries
Note: Total percentages may not equal separate values due to rounding.
Source: A commissioned study conducted by Forrester Consulting on behalf of HP, September 2023

Firms Grapple With Sustainable Device Lifecycle And Data Security Concerns

The management of remote endpoints presents an array of challenges that IT professionals are striving to navigate. Three of the most pressing issues include sustainable device lifecycle management, ensuring software updates on remote devices, and securing endpoint data (see Figure 5).

FIGURE 5

"Which of the following tasks present challenges as your organization manages remote endpoints?"



Base: 312 IT and security decision-makers at companies with 500 or more employees across multiple industries
Note: Showing top 5 responses
Source: A commissioned study conducted by Forrester Consulting on behalf of HP, September 2023

Endpoint data security is a prominent concern for 55% of respondents. In fact, 16% of respondents ranked this as their top challenge. This brings into focus the heightened risk to data security posed by remote work scenarios, where devices may connect through unsecured networks, thereby increasing vulnerability to cyberthreats. Neglecting proper data management on laptops could expose sensitive information to potential breaches or unauthorized access when those devices are no longer in use, creating potential compliance and legal problems.

The challenges identified are closely aligned in importance. For instance, the emphasis on sustainable device lifecycle management underscores the pressing need for IT professionals to strategize in accordance with evolving technological landscapes while staying committed to sustainability. Furthermore, 56% of respondents highlighted the imperative of keeping software on remote devices current. This not only underscores the logistical hurdles of dispersed work settings, where hands-on device access for updates can be limiting, but also points to the oft-neglected firmware updates that tend to languish at the end of priority lists, exacerbating the challenge. And lastly, maximizing the accuracy of the asset database was a concern for 54% of respondents. Ensuring a precise and updated asset inventory is vital, more so in hybrid work structures where device distribution is geographically dispersed.

Full Disk Encryption Is A Shield, Not A Fortress In Data Protection

Full disk encryption is seen more as a part of a broader, multilayered security strategy rather than a standalone solution. This sentiment reflects the intricacy of data protection in our increasingly digital, remote-first era (see Figure 6):

- **Full disk encryption is a vital shield for data protection.** More than half of the respondents (54%) believed that full disk encryption provides substantial protection for endpoints. However, they emphasized that additional security measures are necessary. This signals that, while encryption is a powerful tool in the security arsenal, it shouldn't be the only defense mechanism employed. Furthermore, a significant 28% of respondents viewed full disk encryption as offering limited protection and asserted that significant additional measures are necessary. This highlights the need for more comprehensive data protection strategies that go beyond just encryption. While lightweight security capabilities (e.g., setting encryption and passwords) have always been key endpoint management features, many vendors today are adding more sophisticated endpoint security technologies to their portfolios.[4]

> Respondents at SMBs in EMEA cited that full disk encryption provides sufficient protection with no additional measures necessary (30%) while only 12% of NA respondents believed the same.

- **Malware infections won't go away.** With the advent of remote work, 36% of respondents reported a moderate to significant increase in concern over malware infections. This underlines the escalating threat landscape where remote endpoints become easy targets for malicious activities.
- **Inadequate network security at remote locations.** Similarly, 36% of respondents noted a significant or moderate increase in concern over inadequate network security at remote locations. This reflects the reality of remote work, where network environments are often less secure than

corporate infrastructures, thereby increasing vulnerability to data breaches and by implementing more efficient endpoint software tracking and management (48%).

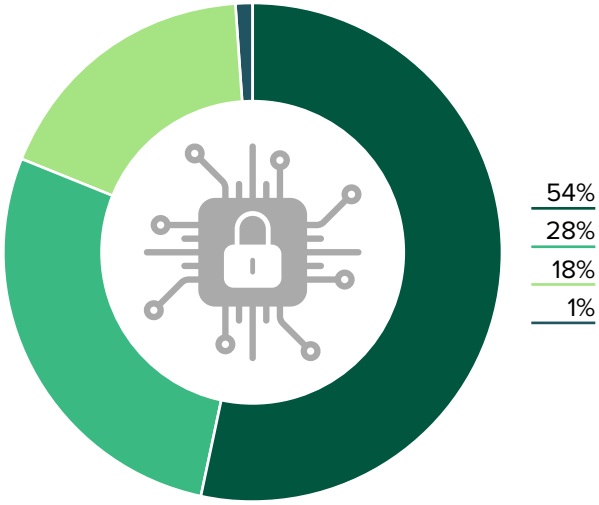
55%

of respondents cited device backup and restore capabilities helped their organization better manage company laptops.

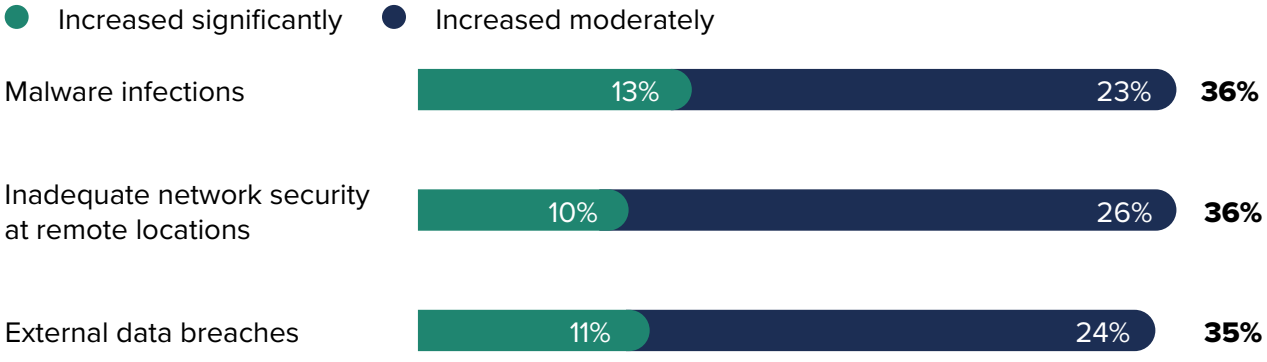
FIGURE 6

"To what extent do you feel that full disk encryption provides sufficient data protection for endpoints?"*

- It provides substantial protection, but additional measures are necessary.
- It provides limited protection, and significant additional measures are necessary.
- It provides sufficient protection; no additional measures necessary.
- It does not provide adequate protection at all.



"How has anywhere work impacted your organization's concern over the following risks in endpoint device management?"**



Base: 312 IT and security decision-makers at companies with 500 or more employees across multiple industries
*Note: Total percentages may not equal separate values due to rounding.
**Note: Showing top 3 responses
Source: A commissioned study conducted by Forrester Consulting on behalf of HP, September 2023

Investment In Endpoint Security And Efficiency Is The New Imperative For IT Leaders

With the rise of the anywhere workforce, endpoint security and management are becoming critical to an organization's operational efficiency and resilience. It is clear from the data that there is a consensus among IT leaders regarding the need to invest in advanced solutions for endpoint security and enhanced remote endpoint management (see Figure 7):

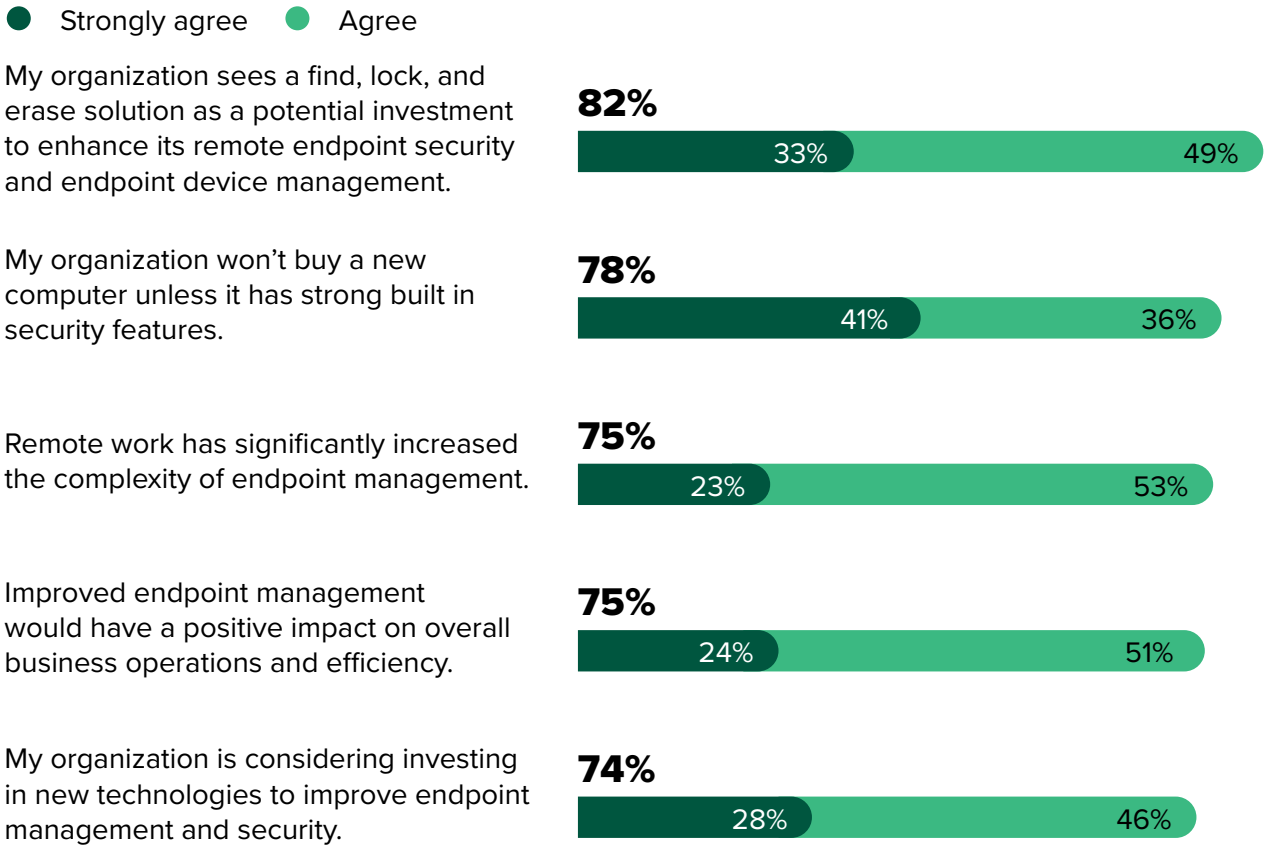
- **Always-on fleet management solutions are the ace card.** In today's world, where remote work has become more prevalent than ever, the importance of securing endpoints — devices that connect to enterprise networks — cannot be overstated. Endpoint devices, such as laptops and mobile phones, are more vulnerable to breaches because they operate outside the organization's protected environment. The majority (82%) of respondents agreed that a find, lock, and erase solution is seen as a potential investment to enhance remote endpoint security and management. This represents a substantial recognition of the importance of such a solution in tackling the complex challenges posed by the anywhere-work model.
- **Endpoint security and management has a dual role in business efficiency.** The data revealed that a striking 75% of respondents either "Strongly agree" (24%) or "Agree" (51%) that efficient endpoint management enhances overall business operations. Additionally, 74% believed that leveraging cutting-edge technologies could amplify endpoint oversight and protection. In simpler terms, businesses realize that efficient and secure computer systems form the foundation upon which they can build stronger, tailored security measures.
- **Security from the get-go.** A significant 77% of respondents prioritized built-in robust security features when evaluating new computer acquisitions. This data emphasizes that many organizations see foundational security as non-negotiable in their procurement decisions, showcasing its vital role in creating a secure environment for hybrid and remote work. Other significant areas for improvement include automation

of device recovery process (47%), and BIOS updates deployment and device location tracking (both at 46%), reflecting the multifaceted needs of effective laptop management.

> An impressive 63% of survey participants prioritized hardware-enforced, lock-and-erase solutions for remote endpoint protection, making it the clear frontrunner. In comparison, regular software updates and patching trail at 49%, while endpoint backup solutions are used by 47% — significantly behind the dominant choice.

FIGURE 7

"To what extent do you agree with the following statements?"



Base: 312 IT and security decision-makers at companies with 500 or more employees across multiple industries
Note: Total percentages may not equal separate values due to rounding.
Source: A commissioned study conducted by Forrester Consulting on behalf of HP, September 2023

Always-On Fleet Management Is The Catalyst For Enhanced Protection And Productivity

The essence of data-driven operations in today's digital world underscores the critical importance of robust data protection mechanisms. Embracing an always-on fleet management solution or find, lock, and erase solution can yield numerous benefits for organizations, particularly those embracing anywhere and hybrid work models. These benefits are anticipated to contribute significantly to data protection, productivity, regulatory compliance, and much more, as revealed in the survey results (see Figure 8):

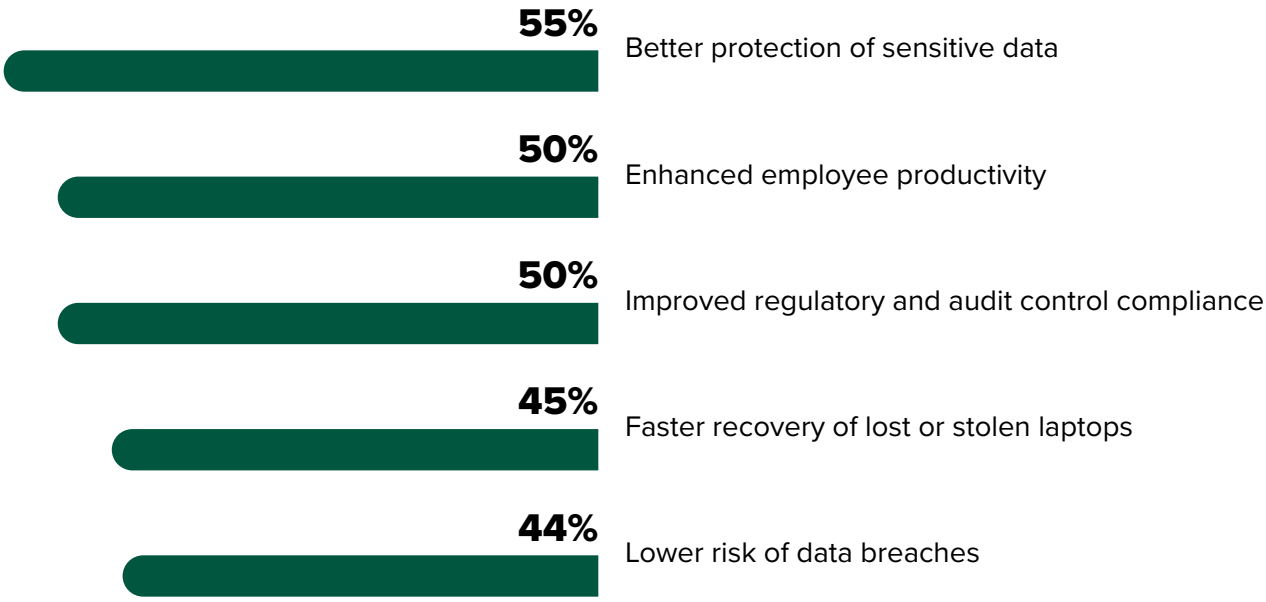
- **Bolstering data protection.** The fact that 55% of respondents identified better protection of sensitive data as the primary benefit of the find, lock, and erase solution speaks volumes. It not only emphasizes the importance organizations place on safeguarding their proprietary and confidential data but also their recognition of the potential vulnerabilities that are present in their current systems.
- **Boosting employee productivity.** Organizations are constantly seeking optimal methods to fortify their security while ensuring an unbroken chain of productivity. The integration of a find, lock, and erase solution appears to be the answer to many modern challenges, especially when 50% of respondents anticipated a significant uplift in employee productivity as a direct result. This revelation accentuates that adept endpoint management transcends mere security fortifications, driving operational efficiency by streamlining device functionality and slashing disruptive downtime.

> Respondents at SMBs in Germany cited implementing a find, lock, and erase solution for lost or stolen devices (80%) and implementing better audit controls related to data security and asset tracking (50%) more than any other country.

- **Supporting regulatory compliance.** Enhanced regulatory and audit oversight emerges as another anticipated merit, endorsed by 50% of respondents. This narrative underlines the pivotal role the solution is poised to play in guiding organizations seamlessly through the maze of compliance commitments, thereby mitigating potential legal and fiscal repercussions.

FIGURE 8

"What benefits has your organization achieved/would it expect to achieve as a result of using a find, lock, and erase solution?"



Base: 312 IT and security decision-makers at companies with 500 or more employees across multiple industries
Note: Showing top 5 responses
Source: A commissioned study conducted by Forrester Consulting on behalf of HP, September 2023

Key Recommendations

Organizations are transitioning to remote and hybrid work models, necessitating enhanced endpoint management for productivity and security in decentralized settings. However, many lag in updating firmware, risking security breaches and operational hiccups. Asset database maintenance, especially under regulatory pressures, is also proving challenging. The always-on endpoint management strategy emerges as pivotal, especially in areas with stringent data privacy norms. As cyberthreats intensify, IT leaders view such innovations as essential investments for ensuring data safety and operational robustness in the digital age. Our study revealed several important recommendations:

Adapting to anywhere work requires planned changes.

Businesses were forced into remote work in 2020 and are still struggling with endpoint management and security functions as hybrid work takes hold. Instead of making ad hoc adjustments to meet this new model, develop plans for IT and security to effectively control and protect your organization's assets wherever they are and work with your chosen vendors to ensure they can fulfill your organization's needs to meet these plans. Proper planning prevents poor performance.

Modern asset management should include lifecycle management.

When your organization's endpoints and users are no longer in fixed locations, asset management platforms need to account for the issuance, ongoing maintenance, and recovery of those endpoints. Integration in this area allows for better management of the endpoints, ensuring they're properly patched at all levels, from hardware to applications and, when it's time for the recycling bin, your organization has a complete audit trail of all management functions from start to finish so that endpoint meets compliance needs.

Utilize always-on endpoint management platforms for better overall employee satisfaction.

Managing the hardware, OS, applications, and data of the modern endpoint requires tools that allow IT and security operations access wherever the endpoint happens to be, whenever the user needs assistance. Shipping devices back to the office for maintenance lowers user productivity and digital experience, while clunky tools that are disconnected from each other make it challenging for IT and security analysts to perform the needed tasks. Choose vendors whose platforms allow for a more streamlined management approach so operations can meet the needs of the users anywhere, at any time.

Incorporate location awareness into your firm's endpoint security approach.

Securing your organization's applications and data properly requires knowing where assets are when they're accessing your firm's resources. If a user normally works in their home in Los Angeles, California and their account is suddenly logging in from Orlando, Florida, will your organization's endpoint security platform be aware that this is abnormal? Does your organization have the tools in place to investigate if this is a threat or just a user on vacation? If needed, could your team find and control their laptop to prevent corporate data from being exposed? With anywhere work, your firm's security tools need to not only identify the user and the device they're working from, but also where they're working and determine if this is an approved access method.

Appendix A: Methodology

In this study, Forrester conducted an online survey of 312 IT and security decision-makers at companies with 500 or more employees across multiple industries in NA, EMEA, and APAC to evaluate maintaining the management of laptops and other isolated devices efficiently. This study aims to explore the impact of poor asset management and data security processes, and its impact on employee experience (EX), operational efficiency, and risk management. Questions provided to the participants asked the current state of their endpoint management, the challenges that come with it, and the opportunities for the future. The study began in March 2023 and was completed in September 2023.

Appendix B: Demographics

COUNTRY	
United States	**33%**
United Kingdom	**14%**
Australia	**14%**
France	**10%**
New Zealand	**10%**
Germany	**10%**
Japan	**9%**

REGION	
EMEA	**34%**
NA	**33%**
APAC	**33%**

DEPARTMENT	
IT/IT operations	**50%**
IT security/security operations	**50%**

LEVEL OF RESPONSIBILITY	
Final decision-makers for endpoint management at their organization	**38%**
Part of a team of decision makers for endpoint management at their organization	**32%**
Influence decisions related to endpoint management at their organization	**30%**

NUMBER OF EMPLOYEES	
500 to 999 employees	**25%**
1,000 to 4,999 employees	**29%**
5,000 to 19,999 employees	**26%**
20,000 or more employees	**20%**

Appendix B: Demographics, cont.

INDUSTRY	
Manufacturing and materials	**15%**
Technology	**15%**
Retail	**10%**
CPG	**6%**
Consumer services	**6%**
Healthcare	**6%**
Financial services	**6%**
Business/professional services	**5%**
Energy/utilities	**5%**
Construction	**4%**
Transportation and logistics	**3%**
Others	**19%**

POSITION	
Director (45%)	**45%**
Manager (44%)	**44%**
Full-time practitioners (12%)	**12%**

Note: Percentages may not total 100 due to rounding.

Appendix C: Endnotes

[1] Source: "The State Of Endpoint Security, 2022," Forrester Research, Inc., July 21, 2022.

[2] Source: Forrester Analytics Business Technographics® Infrastructure Survey, 2021.

[3] Source: "The Future Of Endpoint Management," Forrester Research, Inc., June 6, 2022.

[4] Ibid.


FORRESTER®