ManageEngine

Endpoint Central

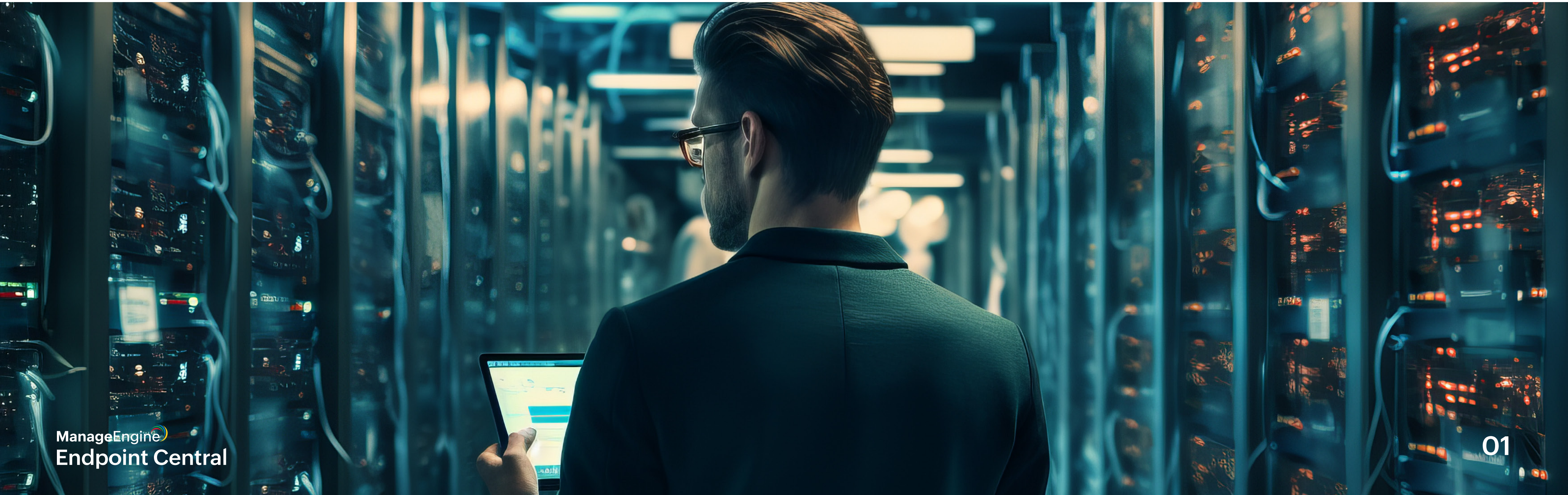
Endpoint Protection in the Digital Age: A Crowdsourced Playbook on Fortifying Your Enterprise

Introduction

In a business world increasingly driven by digital connectivity, protecting IT endpoints has never been more important. This increase in the number of endpoints has been complemented by the high complexity and frequency of cyber threats. Endpoints continue to serve as one of the most important entry points for cybercriminals into company networks. From insidious malware to stealthy phishing attacks, the dangers are diverse. Therefore, the importance of robust endpoint protection cannot be overemphasized. It serves as the first and last line of defense, protecting devices, data, apps, networks, and its users from the ever-evolving threat landscape.

We wanted to understand the pulse of enterprise IT from an endpoint security standpoint. Are endpoint solutions able to ward off new and complex threats? How much budget do orgs normally allocate for endpoint protection? We decided to find out.

In order to answer these questions, we conducted a survey asking 200 members who were significantly or heavily involved in the IT decision-making process in the DACH region about the effectiveness of their endpoint protection solutions. Here's the summary of the findings:



Finding #1: There's a big gap to fill in current Endpoint Protection strategies

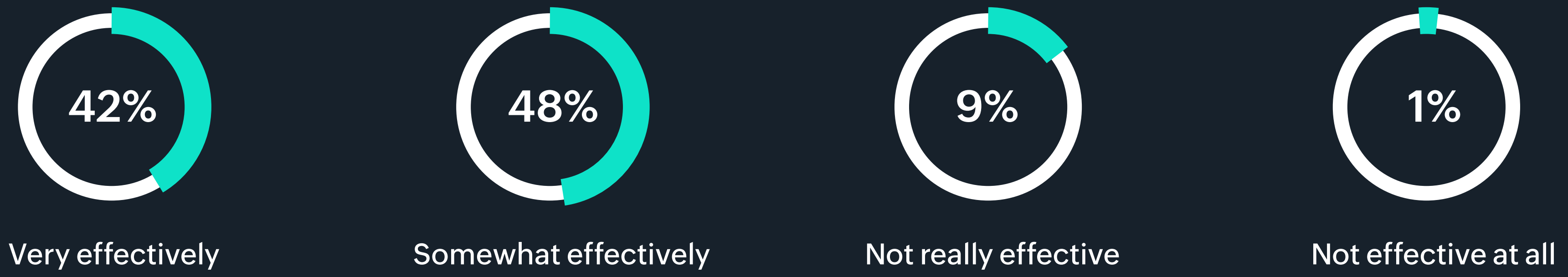
In dynamic modern enterprises, technology is the lifeblood of operations--and protecting the integrity and security of this digital footprint has never been more crucial. Be it a large corporation or a small startup, every organization relies on a variety of endpoints such as desktop PCs, laptops, or smartphones. These endpoints are also vulnerable entry points to a range of cyber threats.

But how well are companies protected against new and complex cyber attacks? 42 percent of the companies surveyed stated that their endpoint protection solution was very effective against complex attack methods.

This means that these companies already achieve a more than acceptable level of protection.

However, not all industries are equally protected against threats. Retail (21 percent), healthcare (27 percent) and public administrations (25 percent) lag behind in defending against complex threats. Another 48 percent consider their solution to be at least somewhat effective. In contrast, 10 percent of companies consider their solutions to be only slightly or not at all effective against complex threats. Retail companies (29 percent) and public administrations (25 percent) are particularly affected.

How effectively does your organization's current endpoint protection solution detect and respond to advanced threats such as zero-day exploits or fileless attacks?



Assessing endpoint protection for the advanced threats (Base: 200 companies)

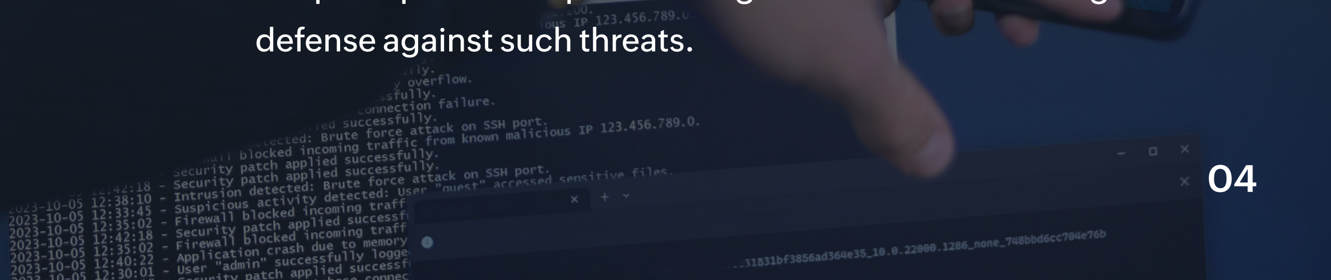
Finding #2: Struggles of balancing Endpoint protection and productivity (still) exist

Most often, companies cite the balance between security and performance as the biggest challenge when it comes to endpoint protection. Half of the companies surveyed believe that balancing security and performance is a major challenge. For example, restrictive security measures can impact employee productivity by slowing down or disrupting work processes. In the worst case, this can even lead to employees looking for ways to circumvent security measures in order to be able to work more productively. Finding the right balance between these two is crucial. On one hand, companies can maintain a strong security posture and at the same time ensure that their employees can work efficiently and without unnecessary interruptions.

41 percent of the respondents found it difficult to manage a diverse endpoint landscape. Companies often have a wide range of devices, including desktops, laptops, smartphones, or even IoT devices. Each of them may run on different operating systems with its own security requirements.

This is also reflected in the problem of securing the mobile workforce. 37 percent of companies see difficulties here. Therefore, different endpoint security solutions may be required to protect these devices. A good approach to manage a diverse endpoint landscape could be the usage of a comprehensive solution that takes into account the unique characteristics of each device.

In addition, 37 percent of companies see addressing zero-day vulnerabilities as a major challenge. Zero day exploits are a significant challenge for endpoint protection because they exploit vulnerabilities that are unknown. Traditional endpoint protection relies on known signatures of malware attacks. Zero day exploits do not match any existing signatures, making them harder or impossible to detect. A modern endpoint protection solution is better equipped to detect and mitigate zero day exploits. This can be achieved with behavioral analysis or the usage of AI and Machine Learning. A modern endpoint protection provides organizations with a stronger defense against such threats.

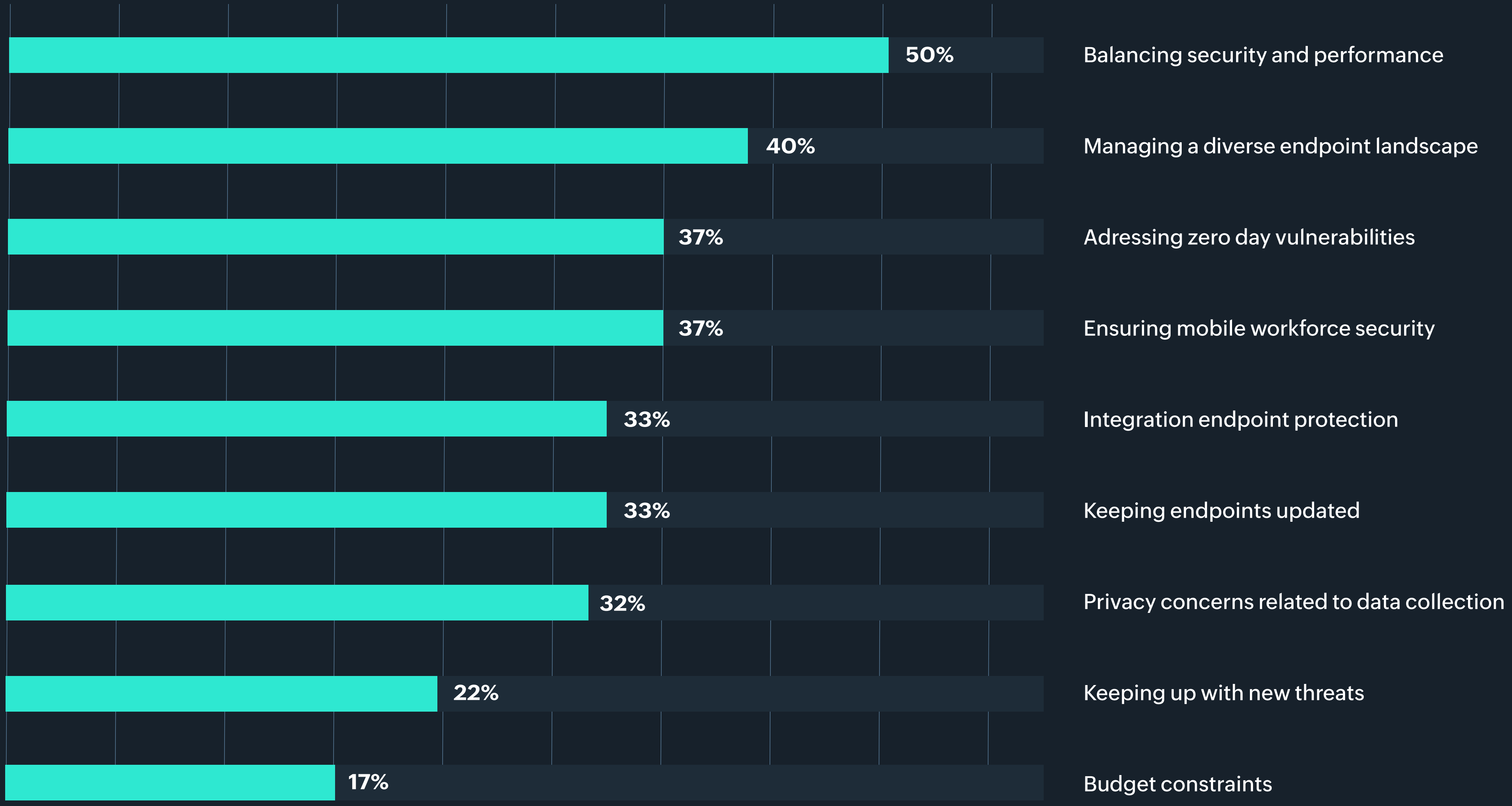


```
                                   ous IP 123.456.789.0.
                              lly.
                            y overflow.
                           ssfully.
                         connection failure.
                      ied successfully.
                  tected: Brute force attack on SSH port.
             wall blocked incoming traffic from known malicious IP 123.456.789.0.
            Security patch applied successfully.
            Security patch applied successfully.
   12:42:18 - Intrusion detected: Brute force attack on SSH port.
2023-10-05 12:38:10 - Suspicious activity detected: User "guest" accessed sensitive files.
2023-10-05 12:33:45 - Firewall blocked incoming traff
2023-10-05 12:35:02 - Security patch applied successf
2023-10-05 12:42:18 - Firewall blocked incoming traff
2023-10-05 12:35:02 - Application crash due to memory
2023-10-05 12:40:22 - User "admin" successfully logge
2023-10-05 12:30:01 - Security patch applied successf
```

Key challenges for endpoint protection solutions Base: 200 companies | multiple answers possible

What are the biggest challenges your company faces with endpoint protection solutions? (Multiple choice)

Endpoint protection in the digital age: Modern endpoint protection for a secure enterprise



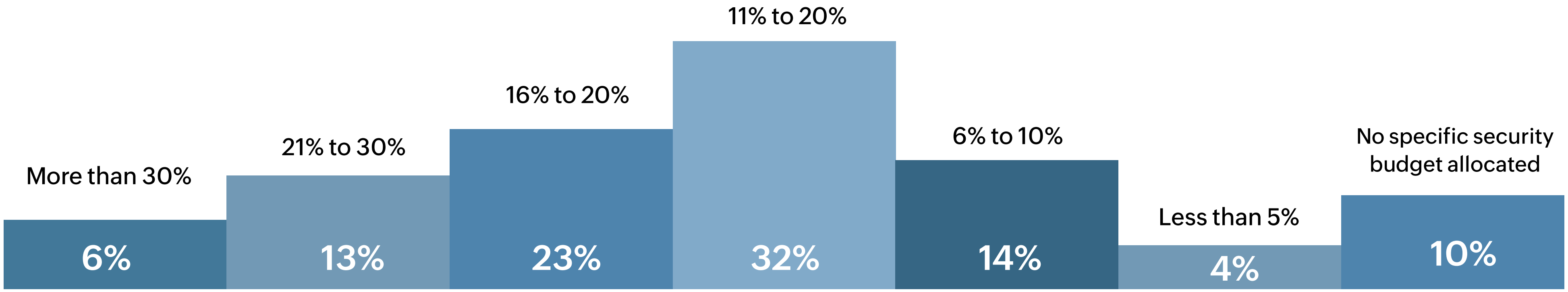
Finding #3: Adequate budget needs to be allocated towards endpoint protection

In order to make endpoint protection effective in the company, appropriate budgets must also be released for it. Not only should a general IT budget be set, but a separate budget for cybersecurity or endpoint protection. A dedicated budget ensures that companies have the resources they need to protect their endpoints from cyber threats effectively.

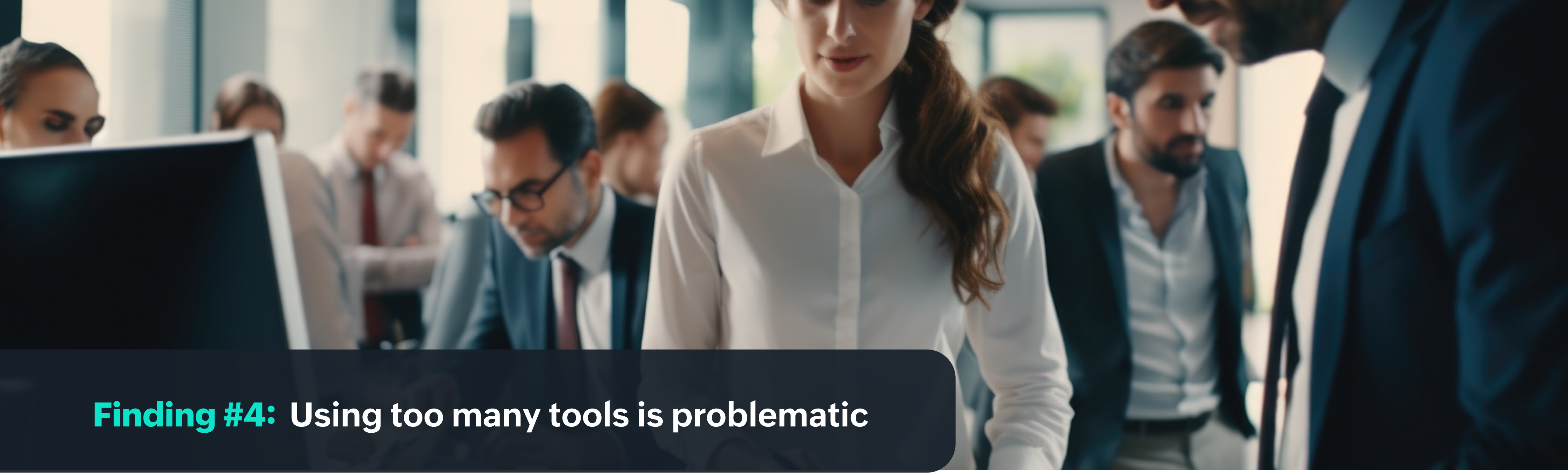
The reality is that almost a third of companies allocate a budget of between 11 and 15 percent to cybersecurity. Another 23 percent allocate between 16 and 20 percent of their IT budget to IT security.

It is worrying that 10 percent of companies do not plan any budget for IT security as part of their IT strategy. Public administrations, in particular, lack a comprehensive IT security budget. A quarter of the public administrations surveyed said they had no specific budget for cyber and endpoint security. This is fatal given the ever-increasing dangers posed by cybercrime. Without the necessary funds to improve your own IT security, you open the gates to your company network to cybercriminals. The consequences can be devastating and range from unexpected costs to loss of critical data leading to serious reputational damage.

Have you set aside or planned a specific IT budget for cyber and endpoint security in your organization? If yes, what is that percentage?



Budget allocation for cyber and endpoint security (Base: 200 companies)



Finding #4: Using too many tools is problematic

Multiple tools, multiple problems

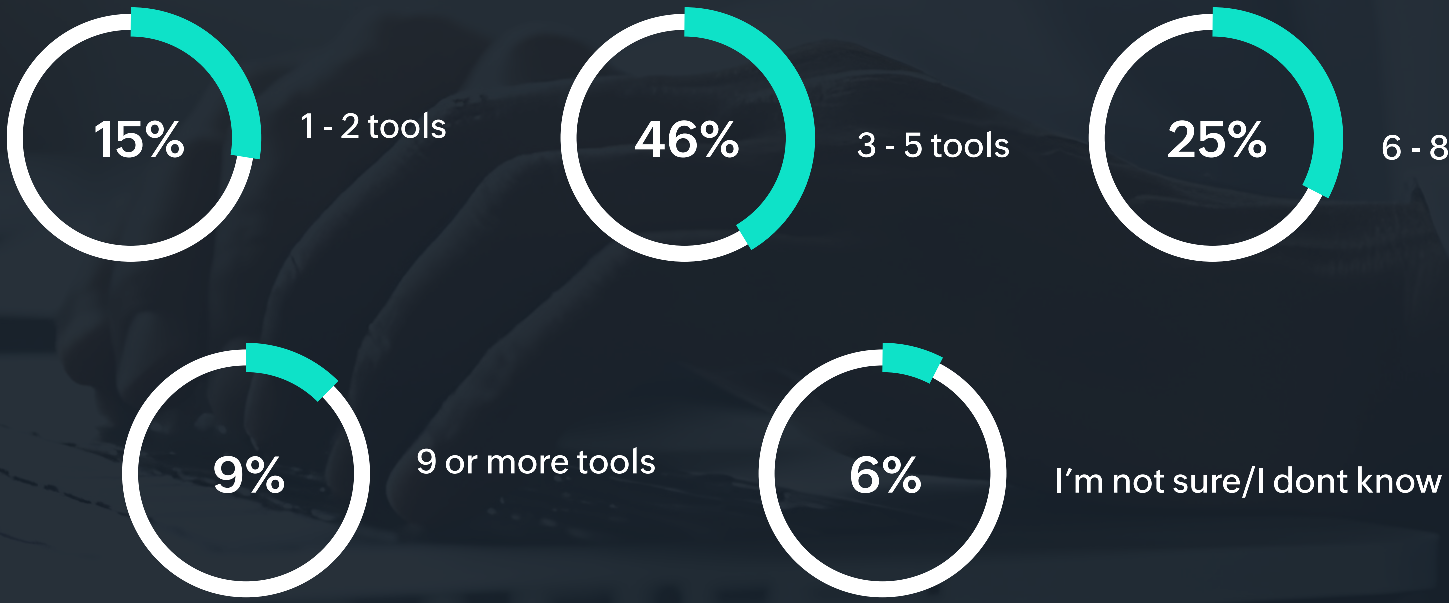
There are numerous solutions available to companies to secure and manage endpoints. Many of these solutions fulfill different functions and often cannot be used as a single instrument. A classic mobile device management solution is intended to manage mobile devices, but does not provide essential protection against cyber threats and does not include desktop devices. An endpoint detection and response solution or a next generation antivirus, on the other hand, is an effective means of combating cyber attacks, but lacks management options.

Typically, organizations use multiple endpoint management and security tools. 46 percent of companies use 3 to 5 tools, and another 25 percent even use 6 to 8 tools. 9 or more tools are used by 9 percent of companies. Almost 15 percent of companies get by with just a maximum of two tools. The main problem with using many different tools is the increased complexity of administration and therefore more time required. In addition, costs can also be saved, as licensing, deploying and maintaining multiple endpoint tools can be expensive.

Endpoint management and security tool inventory

(Base: 200 companies)

How many tools does your IT team use to manage and secure your endpoints?



15% 1 - 2 tools

46% 3 - 5 tools

25% 6 - 8 tools

9% 9 or more tools

6% I’m not sure/I dont know

Finding #5: The majority uses endpoint protection platforms

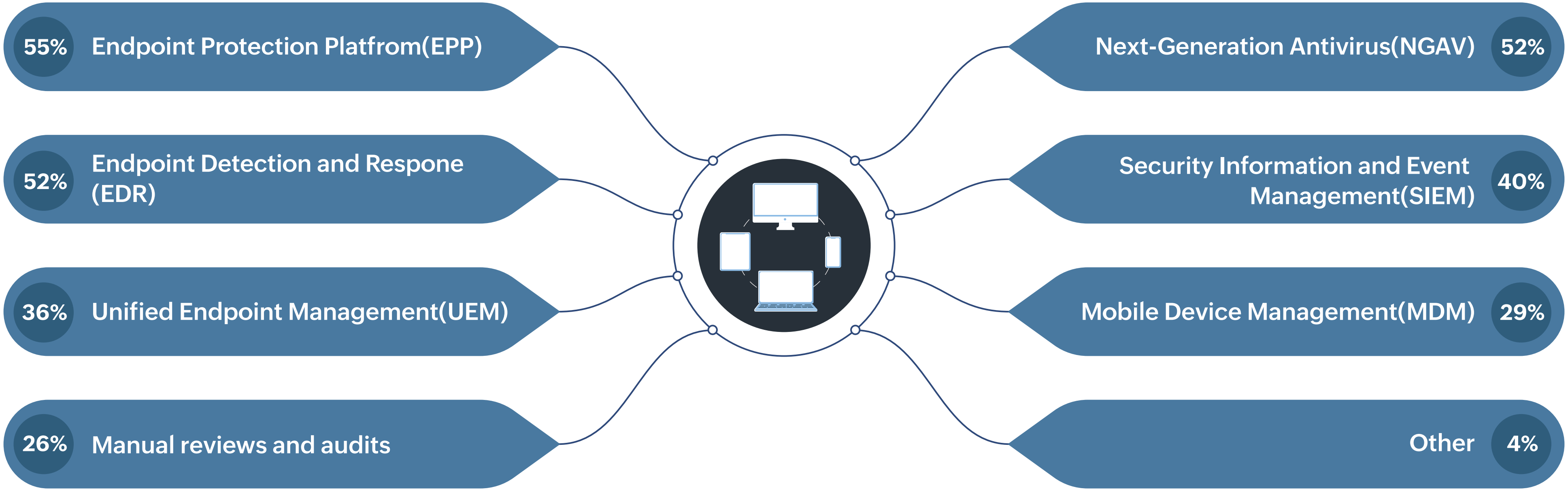
The majority of companies surveyed (55 percent) use an Endpoint Protection Platform to secure and manage endpoints. An Endpoint protection Platform is a security solution designed to safeguard different types of endpoint devices. It combines various security tools to respond to cyberattacks into a single platform and provides a centralized and holistic approach to endpoint security.

Another 52 percent also use Endpoint Detection and Response (EDR) software and a Next-gen Antivirus. Endpoint Detection and Response is designed to detect, investigate, and respond to threats and security incidents on individual endpoints. It also provides a granular visibility into endpoint activities and can quickly respond to potential threats.

A Next-Generation Antivirus is a more modern approach to antivirus solutions which incorporates technologies that provide enhanced protection against a wider range of cyber threats. But it is not suitable for providing detailed visibility into endpoint activities and should not be used as the only endpoint protection solution.

Organizations that deploy multiple solutions should carefully consider whether the increased administrative burden and cost of different solutions is really necessary to ensure effective endpoint protection. Especially when it comes to missing budgets, solutions should be consolidated. Consolidating endpoint protection tools can improve security posture, reduce complexity, and enable organizations to allocate IT resources more efficiently.

What type of solutions does your IT team use to manage and secure endpoints?



55% Endpoint Protection Platfrom(EPP)

52% Endpoint Detection and Respone (EDR)

36% Unified Endpoint Management(UEM)

26% Manual reviews and audits

Next-Generation Antivirus(NGAV) 52%

Security Information and Event Management(SIEM) 40%

Mobile Device Management(MDM) 29%

Other 4%

Deployed endpoint management and security solutions

(Base: 200 companies | multiple answers possible)

Finding #6: Endpoint protection must be mature

When companies decide to purchase a new endpoint protection solution, they pay attention to the very specific features that the solution must have. This can range from advanced features to general ease of use to 24/7 monitoring and remediation.

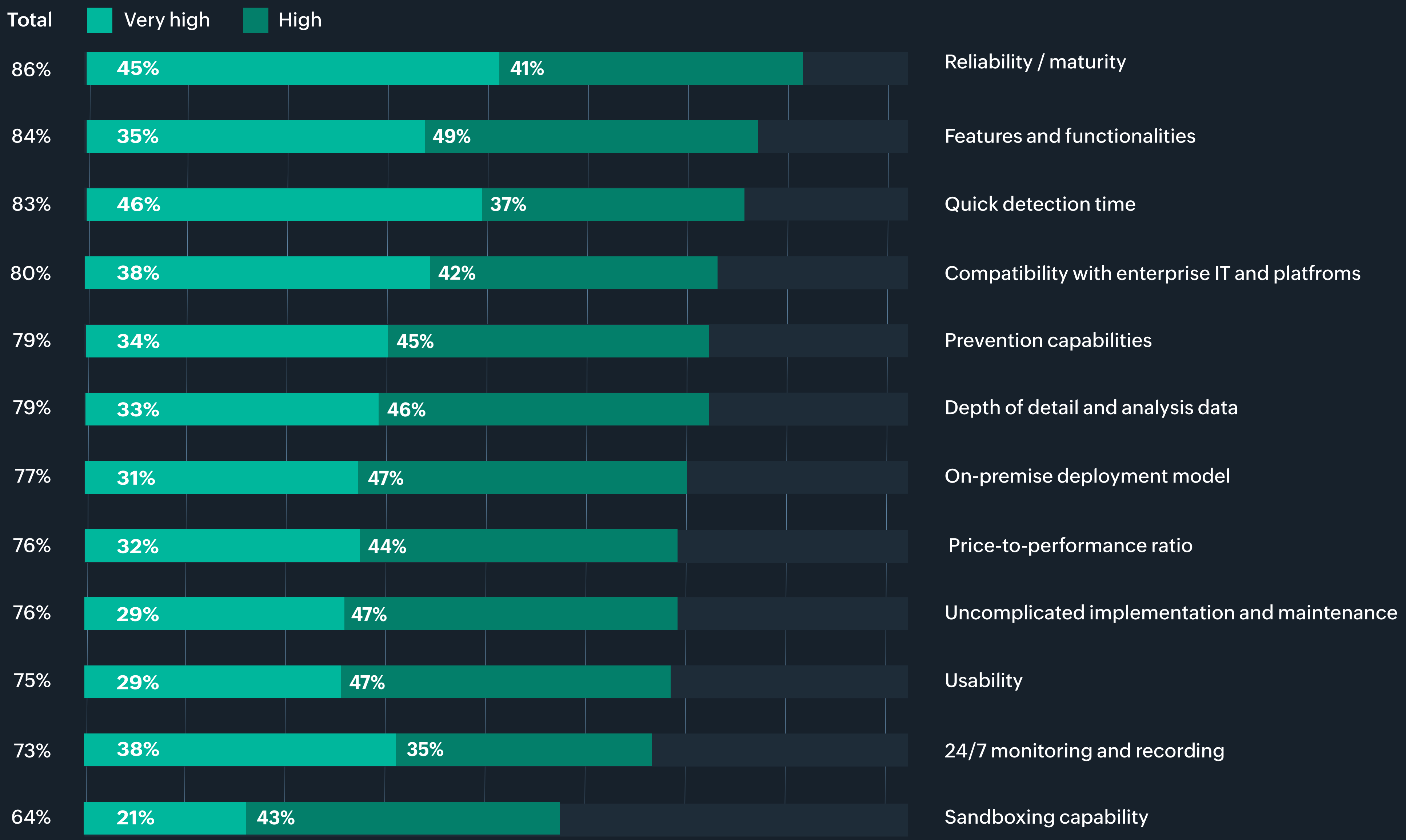
The most important feature that a solution for securing and managing endpoints must contain is a high level of reliability or maturity of the solution. For 86 percent of companies, this has a high or very high influence on the purchasing decision. This is not surprising, as a sophisticated endpoint protection solution offers a higher level of security against a constantly evolving threat landscape. For example, mature solutions like ManageEngine Endpoint Central which is already established since more than 18 years, are better at resolving zero-day vulnerabilities and have fewer false positives. This is due to years of fine-tuning, supported by a strong foundation in IT management feature-set before rolling out advanced protection capabilities over the years.

This is followed by features and functionalities of the solutions that play a crucial role for 84 percent of companies. Solutions with a wide range of functionalities provide multi-layered protection against a wide range of threats, ensuring endpoints are protected not only from known threats, but also new and sophisticated attack techniques.

For 83 percent of companies, the response time of the solution to cyber attacks is of great or very great importance. A quick response time in the event of a security incident limits the impact and, for example, significantly reduces potential damage. The longer a threat remains undetected, the more time it has to spread and cause damage.

Influential Factors in Endpoint Security (Base: 200 companies | multiple answers possible)

How much do the following factors influence your decision when selecting an endpoint security solution?



Conclusion

Today's businesses are increasingly relying on connected devices and remote workforces, and endpoint vulnerabilities are a prime target for cybercriminals. The use of an effective endpoint protection solution serves as crucial protection, not only against known malware, but also against previously unknown cyberattacks like Zero-day exploits.

A modern endpoint protection solution not only reduces the attack surfaces and minimises response times to emerging security incidents, but also creates a balance between security and productivity. An endpoint protection solution must not slow down or disrupt workflows, but enhance them. In order to integrate modern endpoint protection into the company, dedicated budgets are also required for endpoint protection. Only with the budgets in place will companies be resilient to the constantly evolving threat landscape and also against future cyber threats that are still unknown today.

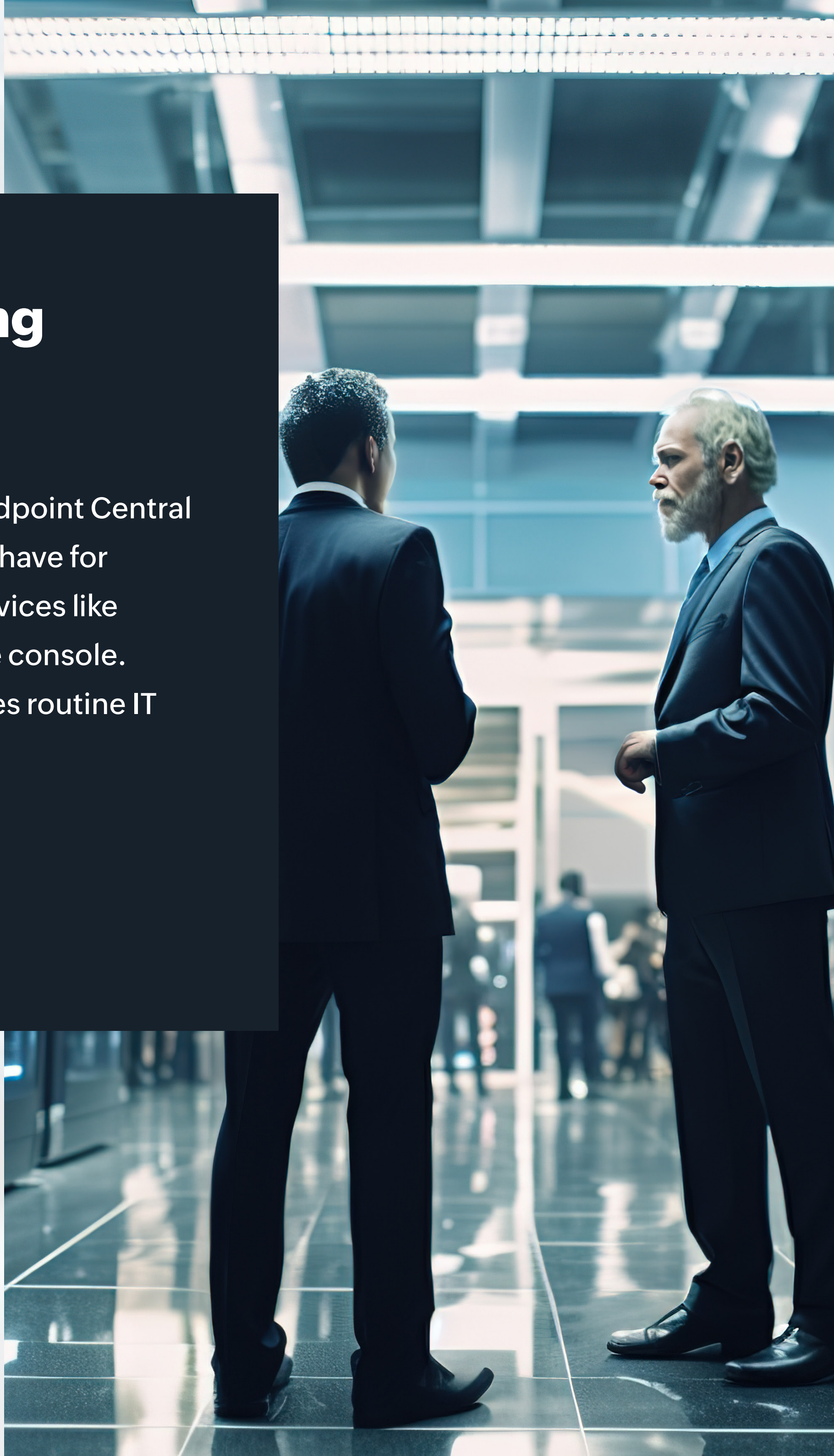
About the study

The above study was designed and carried out by a third-party vendor on behalf of ManageEngine. Two hundred people who were significantly or heavily involved in the decision-making process were asked about the effectiveness of their endpoint protection solutions, their challenges with these solutions, and important properties of the solutions.

ManageEngine Endpoint Central | **Simplifying and securing IT since 2005**

Having been a key player in the market for more than 18 years, ManageEngine Endpoint Central offers IT management and security solutions for any possible requirement you'd have for keeping tabs on a company's endpoints. Endpoint Central centrally manages devices like servers, desktops, laptops, and mobile devices across multiple OSs from a single console. Crafted for SMBs and enterprises alike, Endpoint Central simplifies and automates routine IT tasks while securing your network against cyberattacks.

VISIT ENDPOINT CENTRAL **TRY IT FOR FREE**



Follow us on in Find us on Gartner

sales@manageengine.com | +1-925-924-9500

ManageEngine
a division of Zoho Corp.