

Zero Trust and Ransomware Protection:

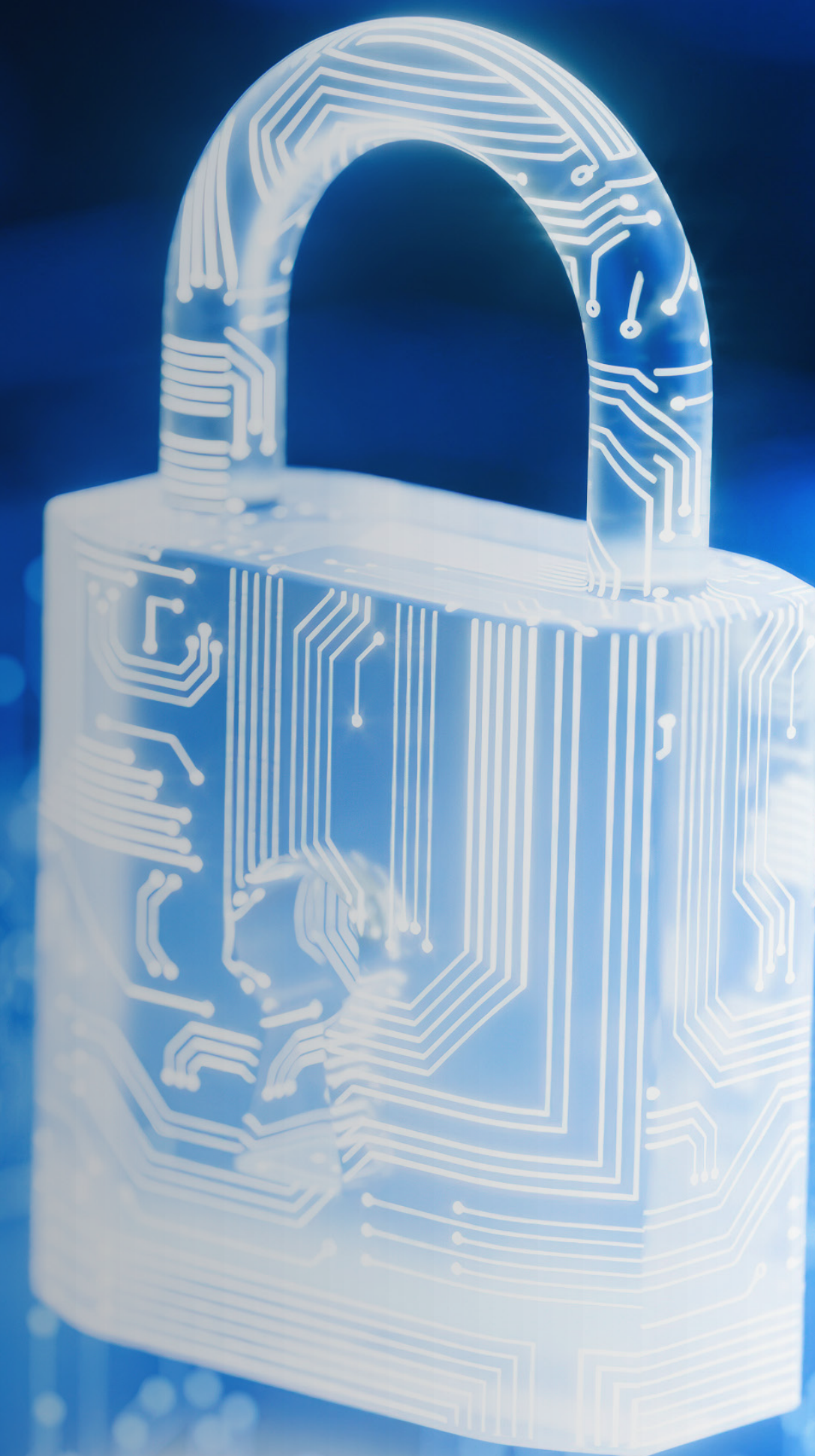
How Organizations Are Rearchitecting Their Backup
Storage Environments in the Ransomware Era

Simon Robinson | Principal Analyst
Keir Walker | Senior Market Research Analyst

ENTERPRISE STRATEGY GROUP

APRIL 2025

This Enterprise Strategy Group eBook was commissioned by Object First
and is distributed under license from Informa TechTarget, Inc.



Research Objectives

This eBook explores how organizations are evaluating their backup and broader data protection environments in the context of the evolving ransomware threat. As ransomware attacks become increasingly sophisticated and increasingly target backup environments, organizations are responding by adopting Zero Trust approaches and modern backup techniques to both reduce the impact of a breach and enable the organization to recover more quickly in case of a breach.

This research was commissioned by Object First and executed by Informa TechTarget’s Enterprise Strategy Group in a blinded fashion, such that respondents were not aware of the research’s sponsor.

The data discussed in this eBook is from a web-based survey conducted in late 2024 of 200 IT managers and executives at organizations in North America and Western Europe with 1,000-9,999 employees who are directly responsible for their organization’s purchase of IT solutions. For more information, please see the “Research Methodology and Respondent Demographics” section of this eBook.

HIGHLIGHTED FINDINGS

Most organizations have experienced at least one ransomware attack in the last two years.

The impacts are substantial; it takes half of affected organizations up to five business days to recover, and most do not recover all of their data.

Target-based backup storage appliances are overwhelmingly viewed as more aligned with Zero Trust. They are also viewed as offering better security overall, as well as stronger backup/restore performance.

Organizations are rearchitecting their backup environments to align with modern Zero Trust security principles to better protect against future ransomware attacks. Immutable storage, segmentation, and multiple copies are also viewed as important tactics.

Hardening, monitoring, and analytics are important for protection, but breach must be assumed according to Zero Trust. Multiple immutable backup copies are critical for recovery in case of a ransomware breach.



CONTENTS





The Business Impact of the Ransomware Epidemic and Why Backup Matters


Ransomware: A Case of ‘When,’ Not ‘If’

The ransomware epidemic shows no sign of slowing, with two-thirds of organizations experiencing a ransomware attack in the last two years.

Of these, 69% have experienced multiple attacks, accounting for 45% of total respondents.

This brings the need for every organization to have a robust preparedness strategy with a major focus on backup data resilience in the form of true immutability.

81% of respondents agreed that backup storage immutability is the last line of defense and the most important component of any ransomware protection strategy. Even when an IT environment and backup storage are compromised, truly immutable backup remains immutable, providing the best and last data copy to recover from.

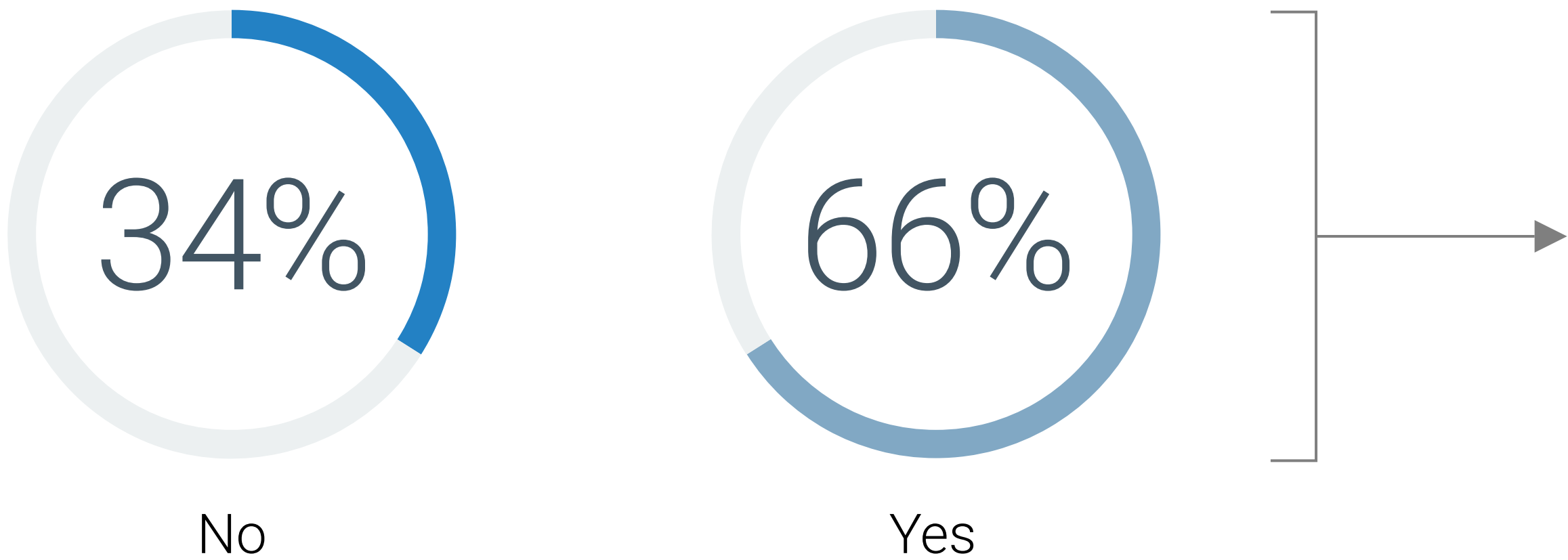
81% 

of respondents agree that **the best way to protect against ransomware is to have immutable backup storage.**

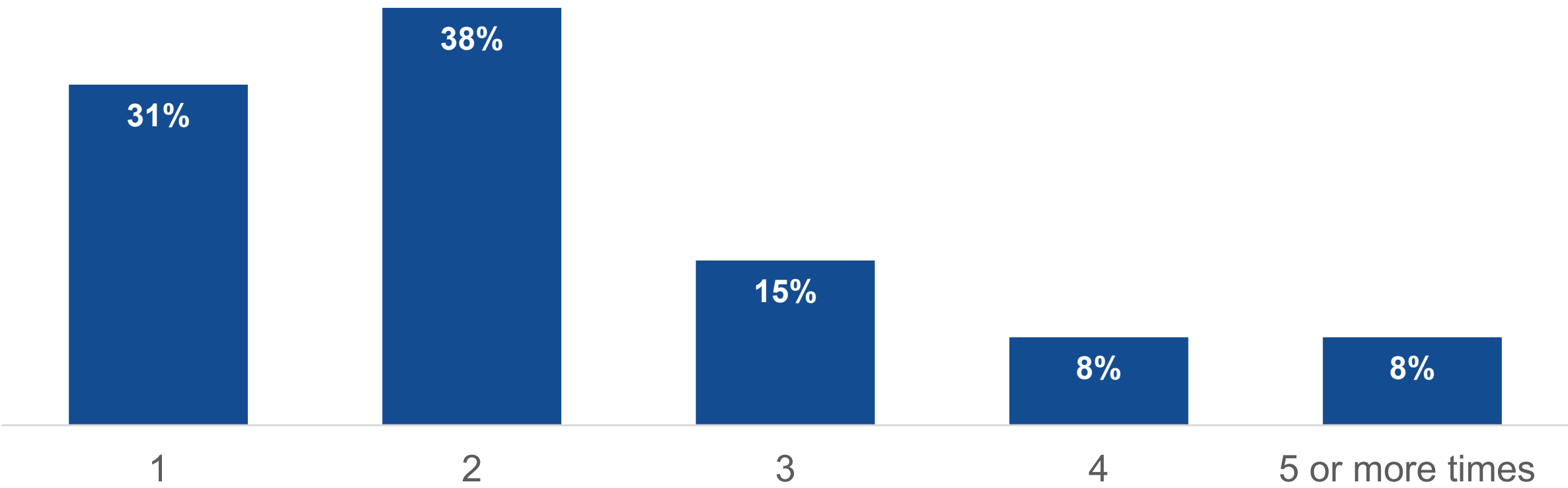
TWO-THIRDS 

of organizations have experienced a **ransomware attack** in the last 2 years, and **45%** have experienced **multiple attacks.**

Organizations that have experienced ransomware attacks in the past 2 years.



Number of ransomware attacks experienced in the past 2 years.



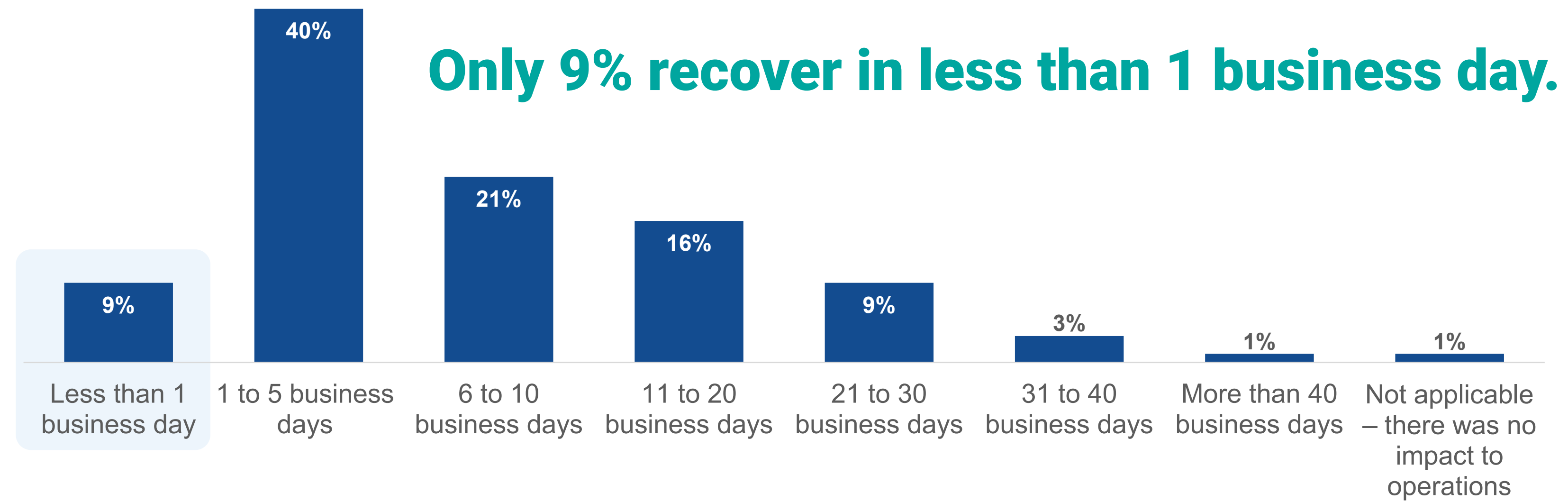
Understanding the Cost Of Ransomware Recovery –Time to Recovery and Volume of Data Recovered

Research showed organizations are struggling with ransomware recovery in two ways:

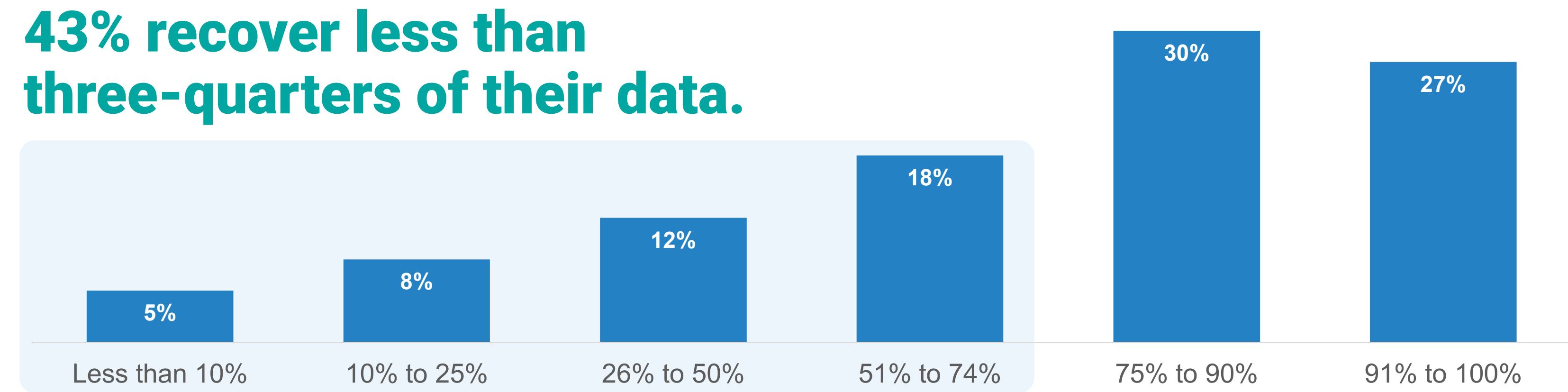
- 1. **Time to recovery.** Less than one in ten organizations are able to operationally recover from an attack within one day, and for many it's much longer.
- 2. **Volume of data recovered.** Many struggle to recover all of their data: 43% recover less than three-quarters of their data.

The impact of taking critical systems offline for an extended period, or being unable to recover all data, can be disastrous. These impacts extend beyond the direct consequences to aspects such as reputational damage with customers and partners.

Ransomware Recovery Time.



Ransomware Data Volumes Recovered.



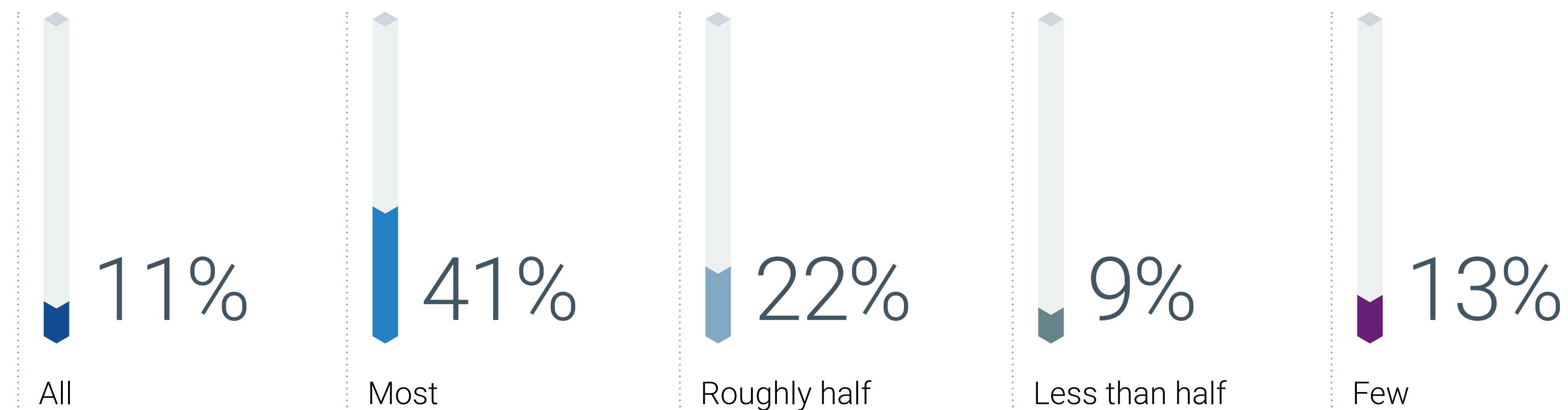
Attackers Have the Backup Environment in Their Sights...

Threat actors are targeting backup data because a clean, uninfected backup copy is often the only way to avoid a ransomware payment

Almost every organization (96%) that has experienced a ransomware attack in the past two years said that their backup data has been targeted at least once.

Over half said most or all attacks have targeted backup data. More than one in ten organizations (11%) reported that every attack has targeted backups.

Frequency of Ransomware Attacks Targeting Backup Data.



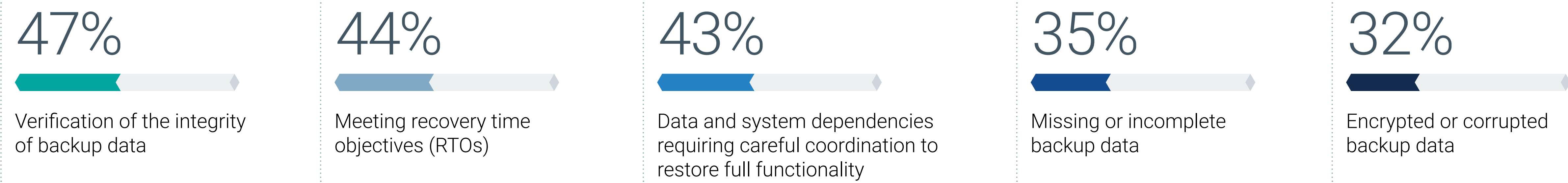


Compromised Backup Data Creates Multiple Challenges...

This growing ransomware threat is creating multiple challenges for IT orgs, including verifying the integrity of backup data, meeting recovery time objectives (RTOs), coordinating multiple data and system dependencies, managing missing or incomplete backup data, and dealing with encrypted or corrupted backup data.

This highlights the criticality of protecting the enterprise backup environment, providing organizations with the ability to effectively recover from, or even negate, the impact of a ransomware attack.

Top Ransomware Backup-related Recovery Challenges.

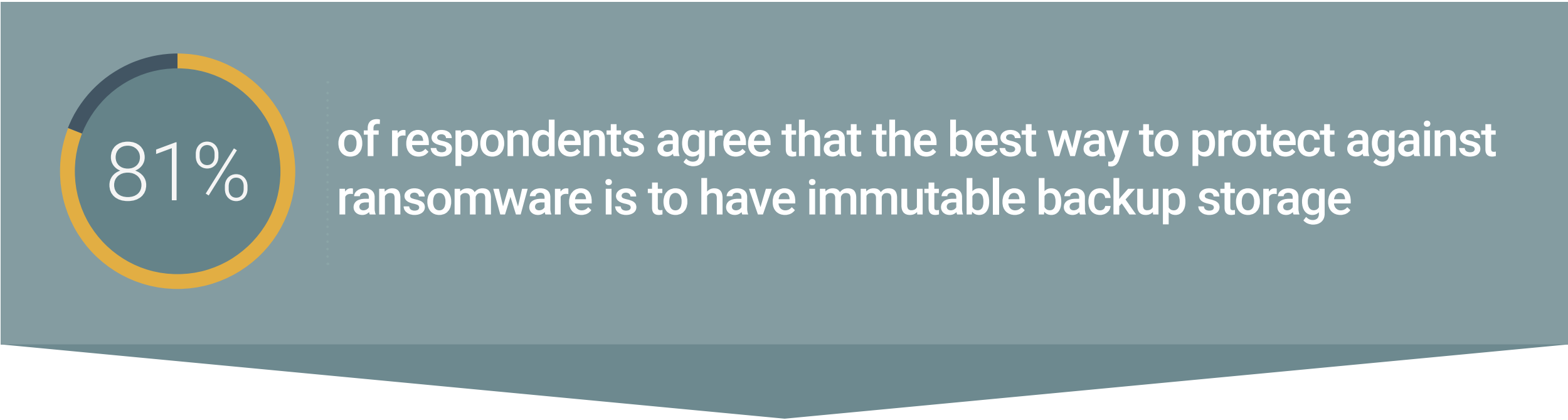


Hardening, Monitoring, and Analytics Are Important, but Multiple Immutable Backup Copies Is the Ultimate Answer

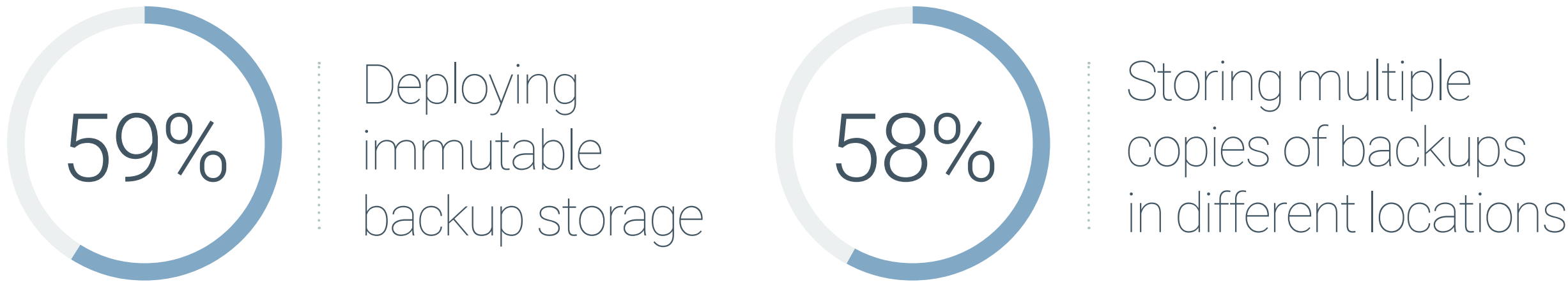
Organizations still rely on more traditional approaches, such as security analytics tools, anti-malware, and security monitoring solutions, in their ransomware protection strategy. But protection alone is inadequate, and a breach must be assumed to adequately prepare for recovery.

Only 59% of organizations are deploying immutable storage, and only 58% are adhering to the 3-2-1 rule for maintaining multiple backup copies to ensure recovery.

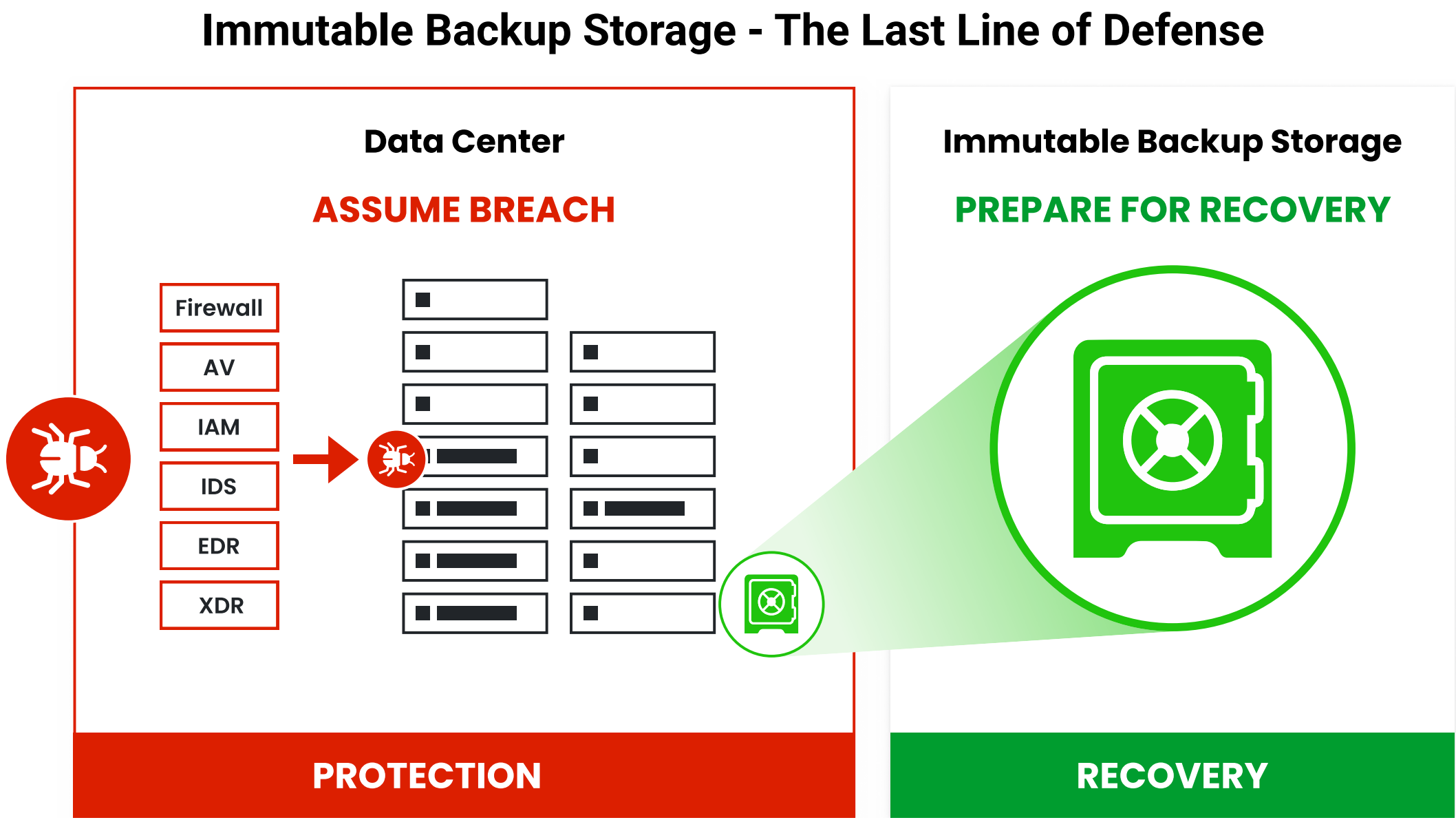
There is more enterprises can do to defend against ransomware, specifically having multiple immutable backup copies to recover their data in the case of a disaster.



Overview of Key Ransomware Defense Measures.



Protection is important but Immutable Backup Copies are the ultimate answer.



“Of major concern is that 61% of respondents believe IT security hardening is sufficient protection against ransomware.”

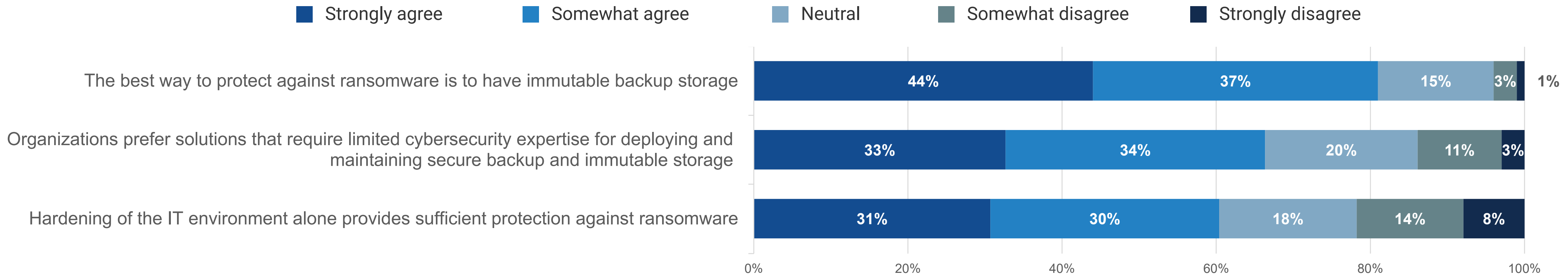
Immutable Backup Storage Is Essential—Hardening Alone Is Not Sufficient

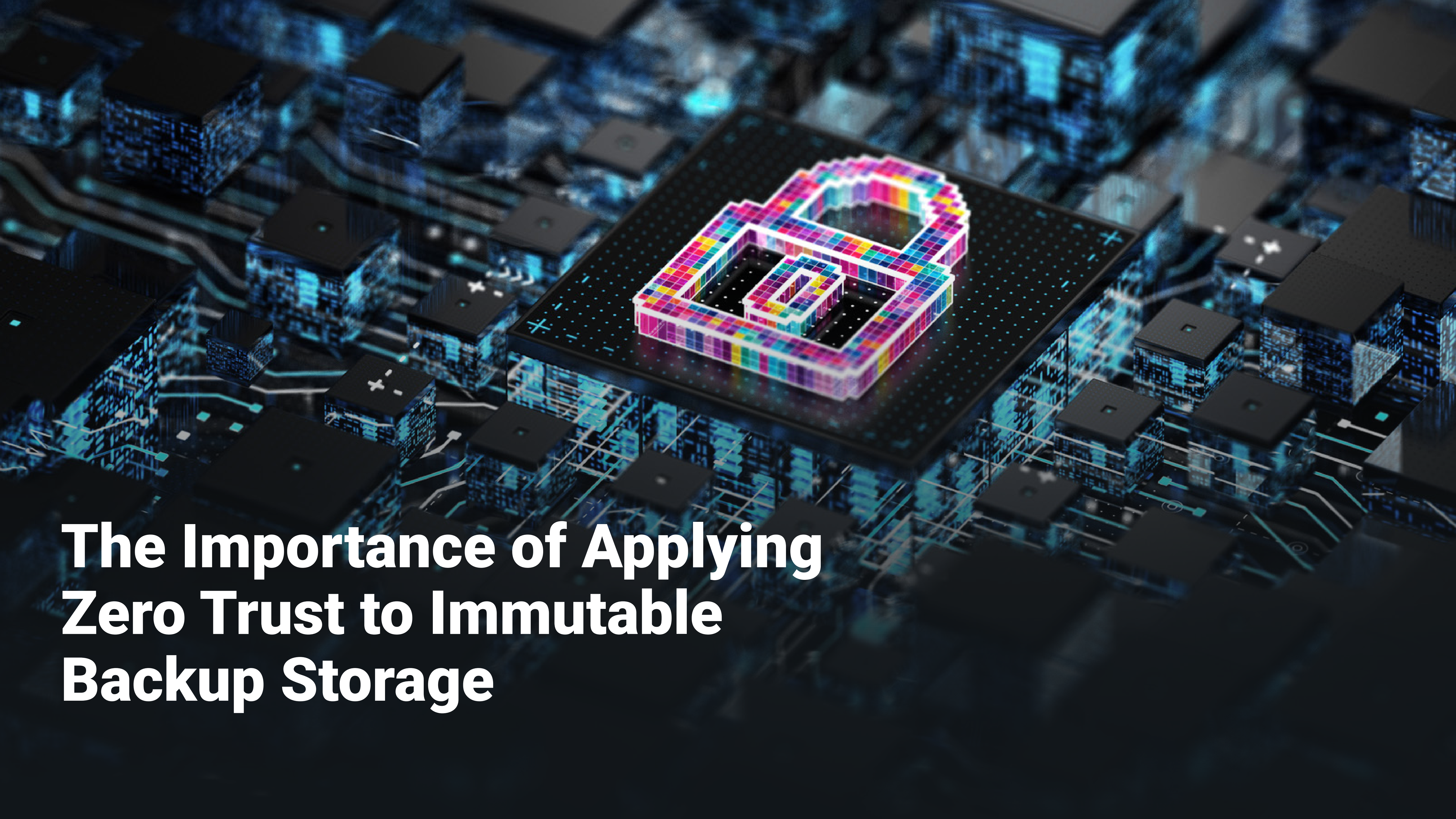
Over four in five respondents agreed that deploying immutable backup storage is the best way to protect the organization against ransomware since it ensures that clean backup data copies cannot be encrypted by malicious code.

However, immutability should not introduce excessive management challenges. Given broader environment complexities, organizations have a strong preference for simple solutions that require limited cybersecurity expertise to deploy and maintain.

Respondents are more divided on whether hardening the IT environment alone provides sufficient protection against ransomware. Of major concern is that 61% of respondents believe IT security hardening is sufficient protection against ransomware. This contradicts the Zero Trust principle, which states that one must “assume breach” despite IT security hardening. Immutable backup storage is the ultimate defense to provide for ransomware recovery.

K.I.S.S: Keep Immutable Storage Simple.





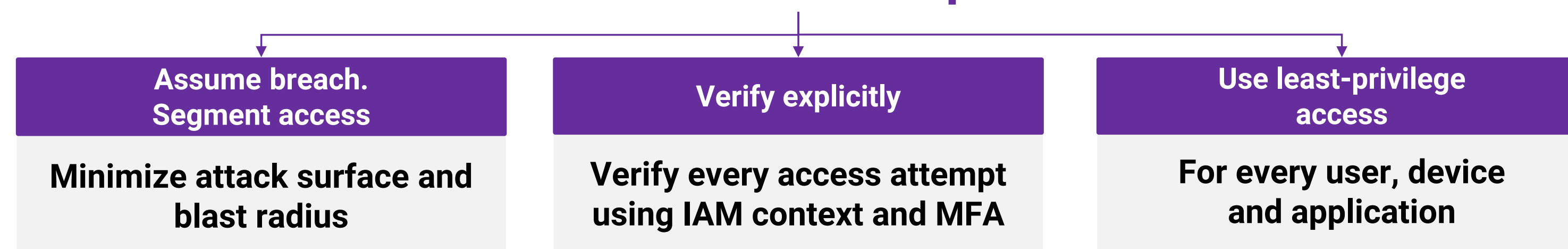
The Importance of Applying Zero Trust to Immutable Backup Storage

What Is Zero Trust?

Zero Trust is a security strategy that assumes no device or person should be automatically trusted or connected to an organization's infrastructure.

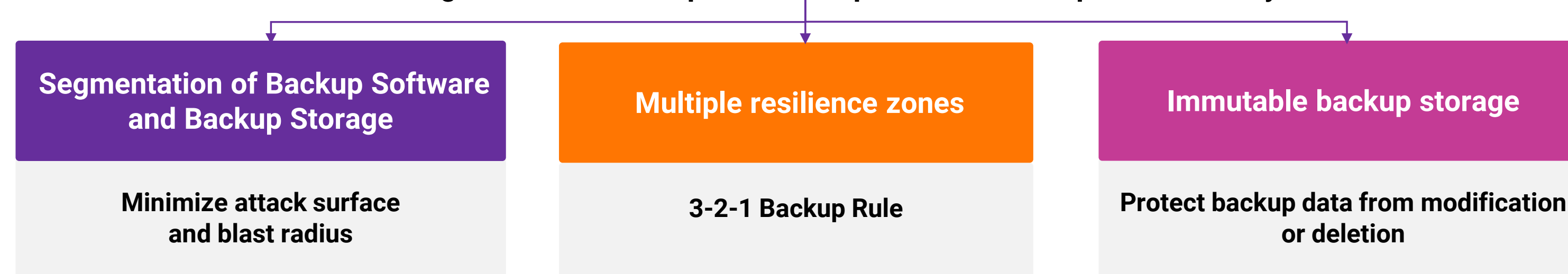
Zero Trust is especially important in the context of data resilience and is driving backup infrastructure modernization around key tenets of segmentation, resilience zones, and immutability.

Zero Trust Principles



Zero Trust Data Resilience (ZTDR) Principles

Extending Zero Trust Principles to Enterprise Data Backup and Recovery



Note: The Zero Trust Data Resilience Principles is a method jointly developed by Object First and Veeam.

“A Zero Trust model needs to be applied to **all IT resources in an environment, including their backups**. Now, that isn’t going to occur overnight; it needs to be a coordinated effort that touches upon all the Zero Trust pillars and needs to be looked at as ongoing.”

Vice President of Infrastructure Technology, *Multinational auto services organization, with over 1,000 employees globally*



Zero Trust: A Foundation for Ransomware Defense

Along with reducing cybersecurity incidents overall, ransomware defense is a top factor driving Zero Trust adoption.

Top Drivers for Zero Trust.



59%



Reducing the number of cybersecurity incidents



55%



Elevating ransomware defense



Security and Zero Trust Are Reshaping Backup Solution Considerations

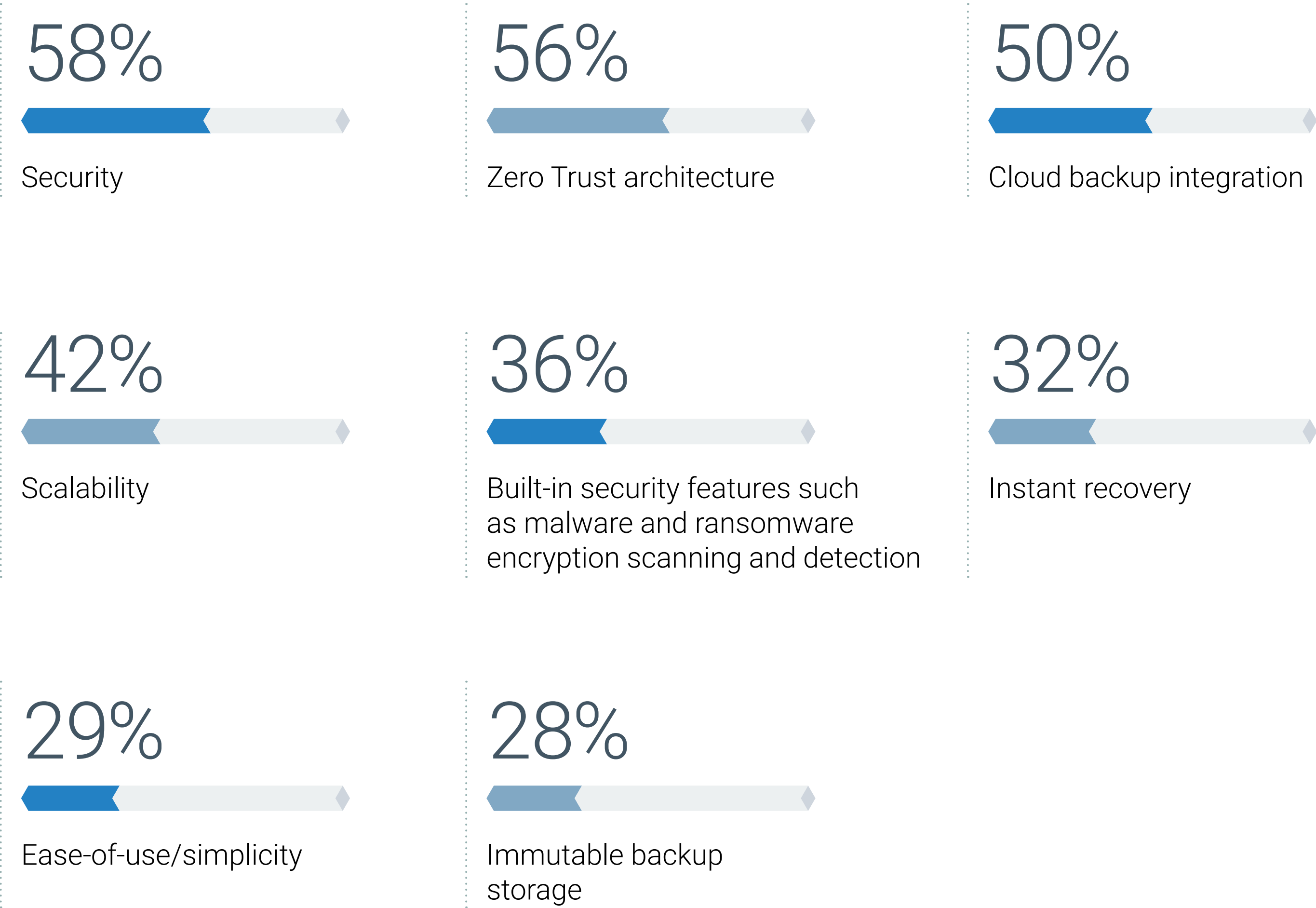
The extent of the ransomware threat is radically reshaping how IT orgs think about their backup environment. Backup and recovery is now becoming an integral component of organizations’ security strategies.

Along with broad security considerations overall, Zero Trust architectures are regarded as one of the most important capabilities that enterprises will prioritize in future backup and recovery solutions.

Critical Zero Trust capabilities such as immutable backup storage do feature in future plans, but their lower incidence reinforces that there is more organizations can do to protect themselves here.

Security and Zero Trust Are Priorities for Backup Investments.

WHAT CAPABILITIES DO YOU BELIEVE YOUR ORGANIZATION WILL PRIORITIZE WHEN MAKING FUTURE DATA BACKUP AND RECOVERY SOLUTIONS? (PERCENT OF RESPONDENTS, N=200, FIVE RESPONSES ACCEPTED)



Target Backup Appliances Align More Strongly to Zero Trust Principles Than Integrated Backup Appliances

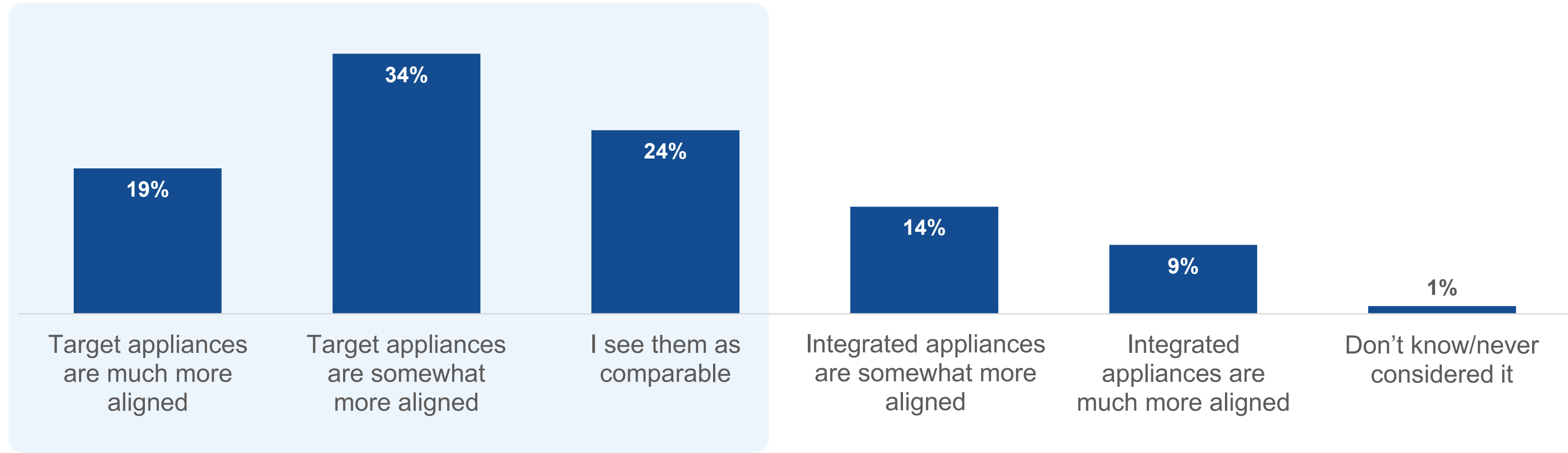
A purpose-built backup appliance (PBBA) is a standalone disk-based storage device that is configured and optimized for storing backup data.

Such a device can either be a target for data coming from a backup application (Target Backup Appliance) or have the backup software tightly integrated into the hardware (Integrated Backup Appliance).

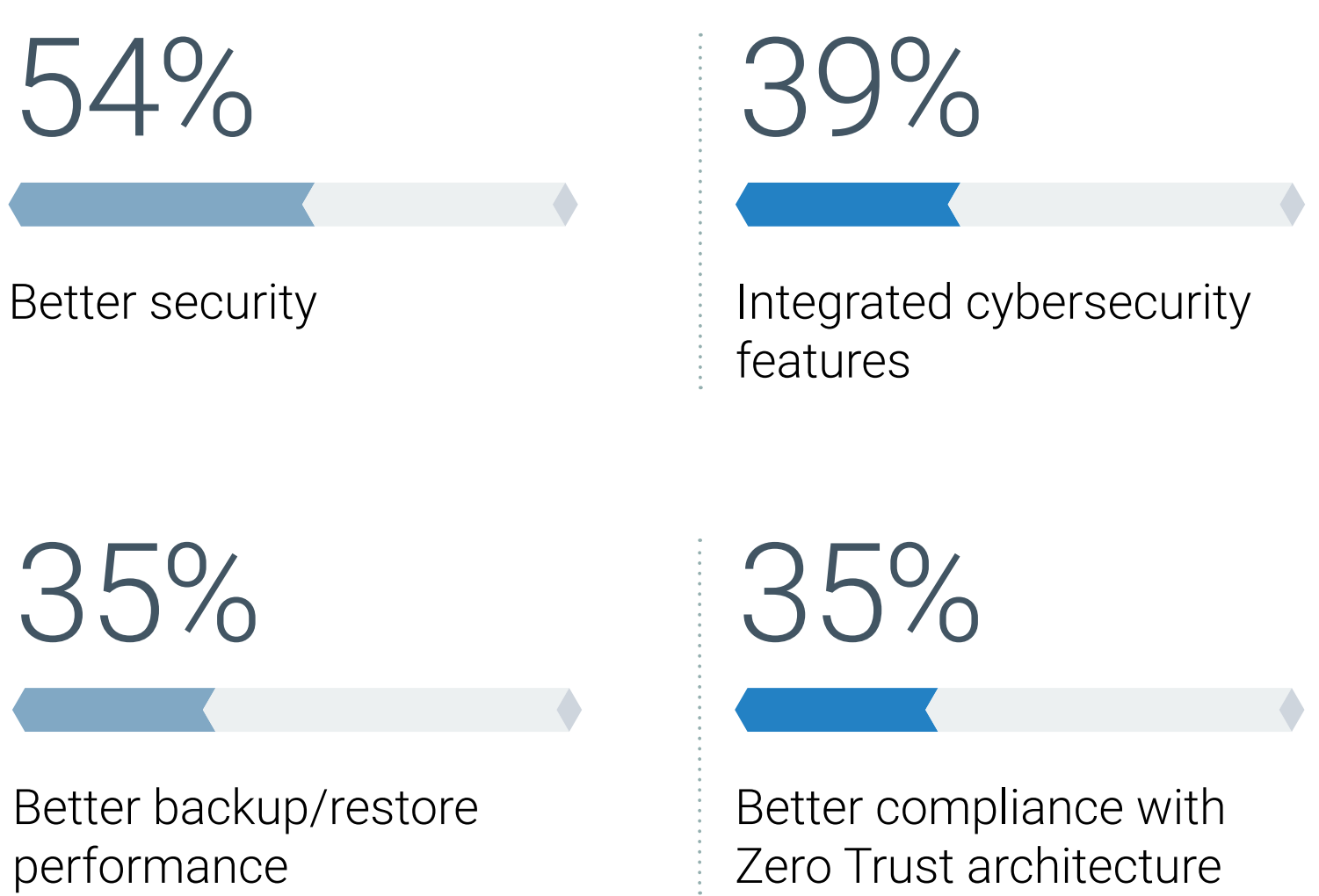
Organizations overwhelmingly view Target Backup Appliances as more closely aligned with Zero Trust principles. Many orgs adopting target appliances also cite better compliance with Zero Trust as a key adoption factor. This is because Integrated Backup Appliances do not offer the same degree of isolation between the backup storage hardware and backup software; thus, a compromise in one could affect the other.

Additionally, organizations cited better security overall, integrated security features, and better performance as key adoption factors for Target Backup Appliances.

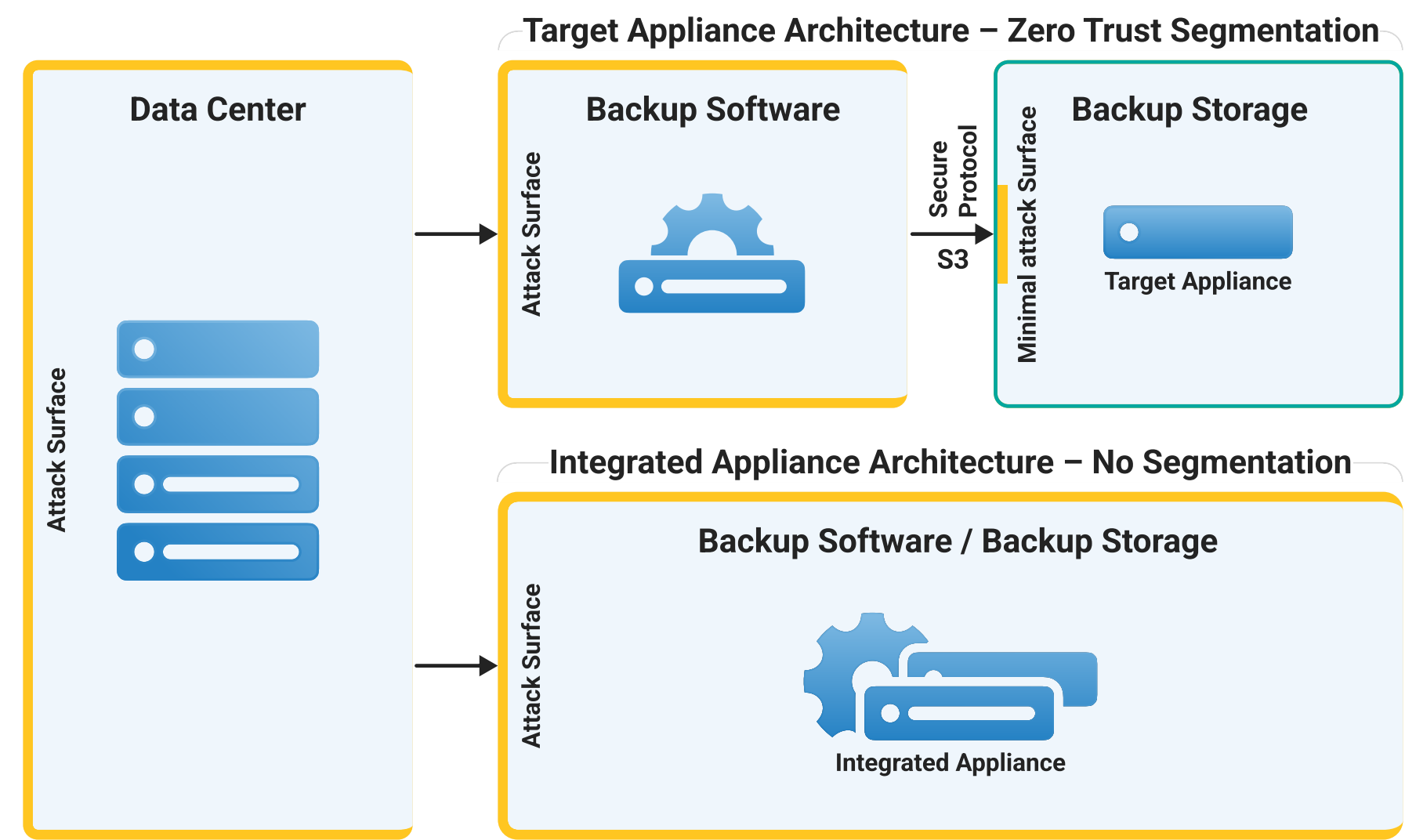
Target Backup Appliances vs. Integrated Backup Appliances for Zero Trust.



Key Factors Driving Target Backup Appliance Adoption.



Target Backup Appliance vs. Integrated Backup Appliance.



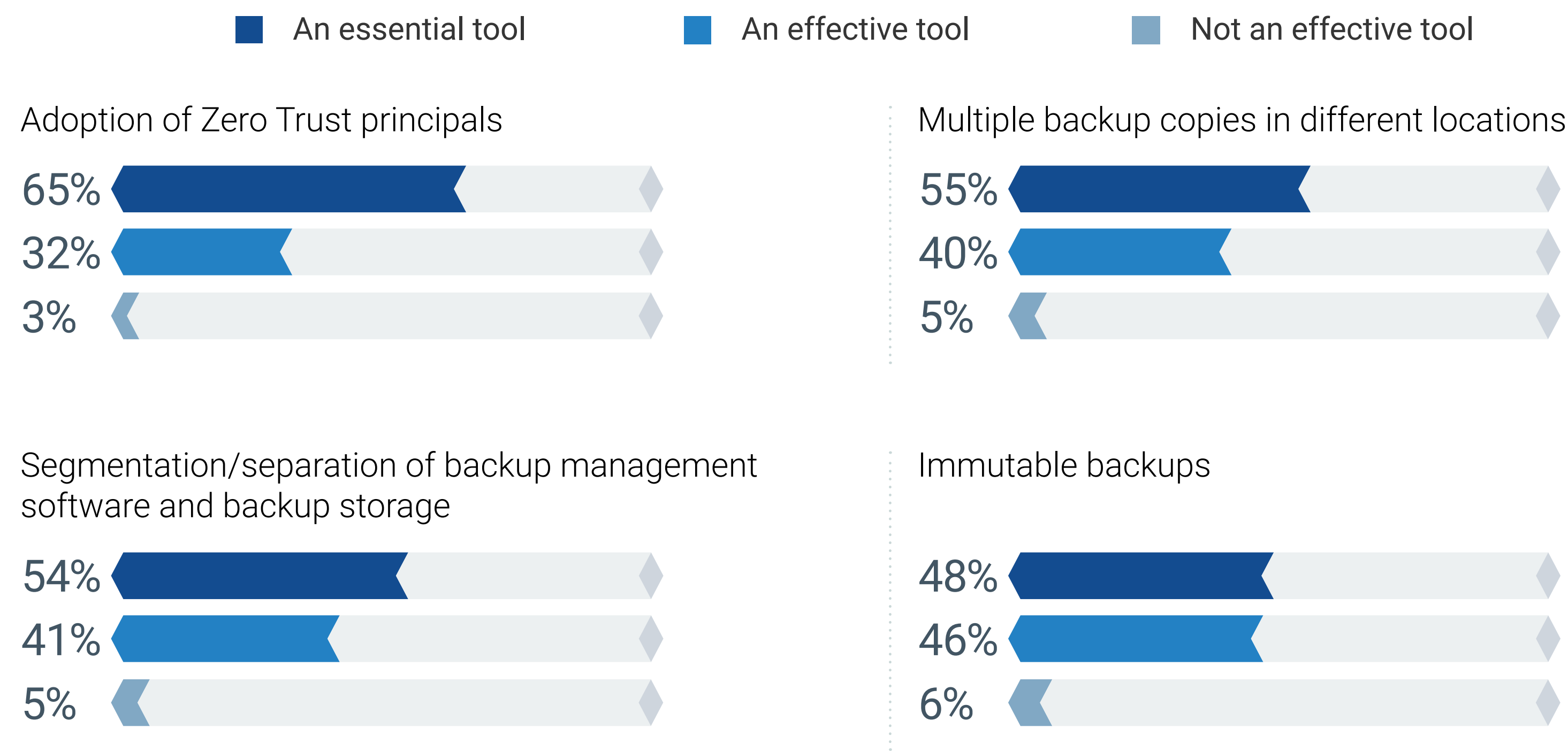
Better Together: Zero Trust, Segmentation, Immutability, and 3-2-1 Provide an In-depth Defense to the Ransomware Threat

Over 90% of IT decision-makers view the following as “essential” or “effective” tools in building a comprehensive ransomware prevention strategy:

- Zero Trust.
- Copies in multiple locations (e.g., the “3-2-1” rule).
- Segmentation of backup software and storage.
- Immutable backups.

Organizations looking to build a robust, in-depth approach to ransomware prevention should consider industry solutions that provide or support these important capabilities in a simple and easy-to-deploy form factor.

Ransomware Resilience – Key Tools and Strategies.



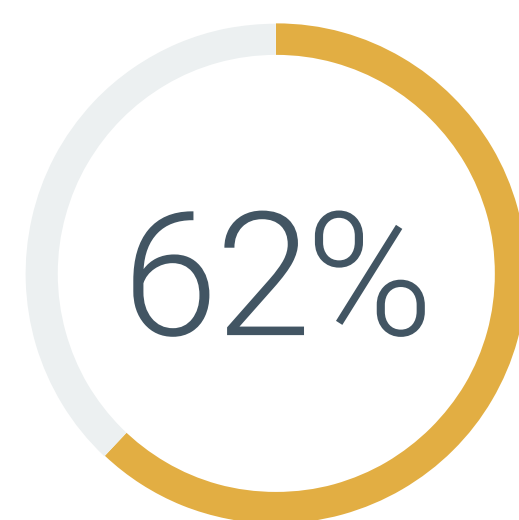
Trust, but Verify: Third-party Validation of Backup Solutions Is Key

Industry solution providers are making strong claims around their cybersecurity capabilities; however, rather than taking these at face value, almost all organizations verify these claims through a variety of means, with most favoring security testing and reporting by an independent third party.

Appetite for Verifying Vendor Claims.



Preferred Verification Method.



Security testing/report by an **independent third-party company**

Conclusion

This brand-new data from IT decision-makers revealed the extent to which security challenges, and the ransomware epidemic in particular, are reshaping organizational backup and data protection environments. As the backup infrastructure increasingly comes under direct attack from malicious actors, IT organizations simply must respond; most are concluding that they need to align and rearchitect their backup environment around the same Zero Trust principles they are commonly applying to their broader IT environment.

IT buyers are, therefore, assessing how to best modernize their backup environments to meet these challenges. The research shows that the characteristics of Target Backup Appliances are regarded by IT decision-makers as much more closely aligned to Zero Trust than Integrated Backup Appliances. Hence, target-based appliances would be a logical consideration for organizations looking to modernize their backup environment along Zero Trust lines. Zero Trust, segmentation, immutability, and 3-2-1 provide an in-depth defense to the ransomware threat.





How Object First Can Help

Ransomware-proof and immutable out-of-the-box, Ootbi by Object First delivers secure, simple, and powerful backup storage purpose-built for Veeam. The appliance can be racked, stacked, and powered in 15 minutes. Ootbi helps Veeam admins implement a Zero Trust Data Resilience architecture for unbreakable backup and recovery.

Read about how Zero Trust principles can be enhanced for backup in Object First’s Zero Trust Data Resilience paper.

[LEARN MORE](#)

Learn the three reasons why Object First offers the best storage for Veeam.

[LEARN MORE](#)



RESEARCH METHODOLOGY AND RESPONDENT DEMOGRAPHICS

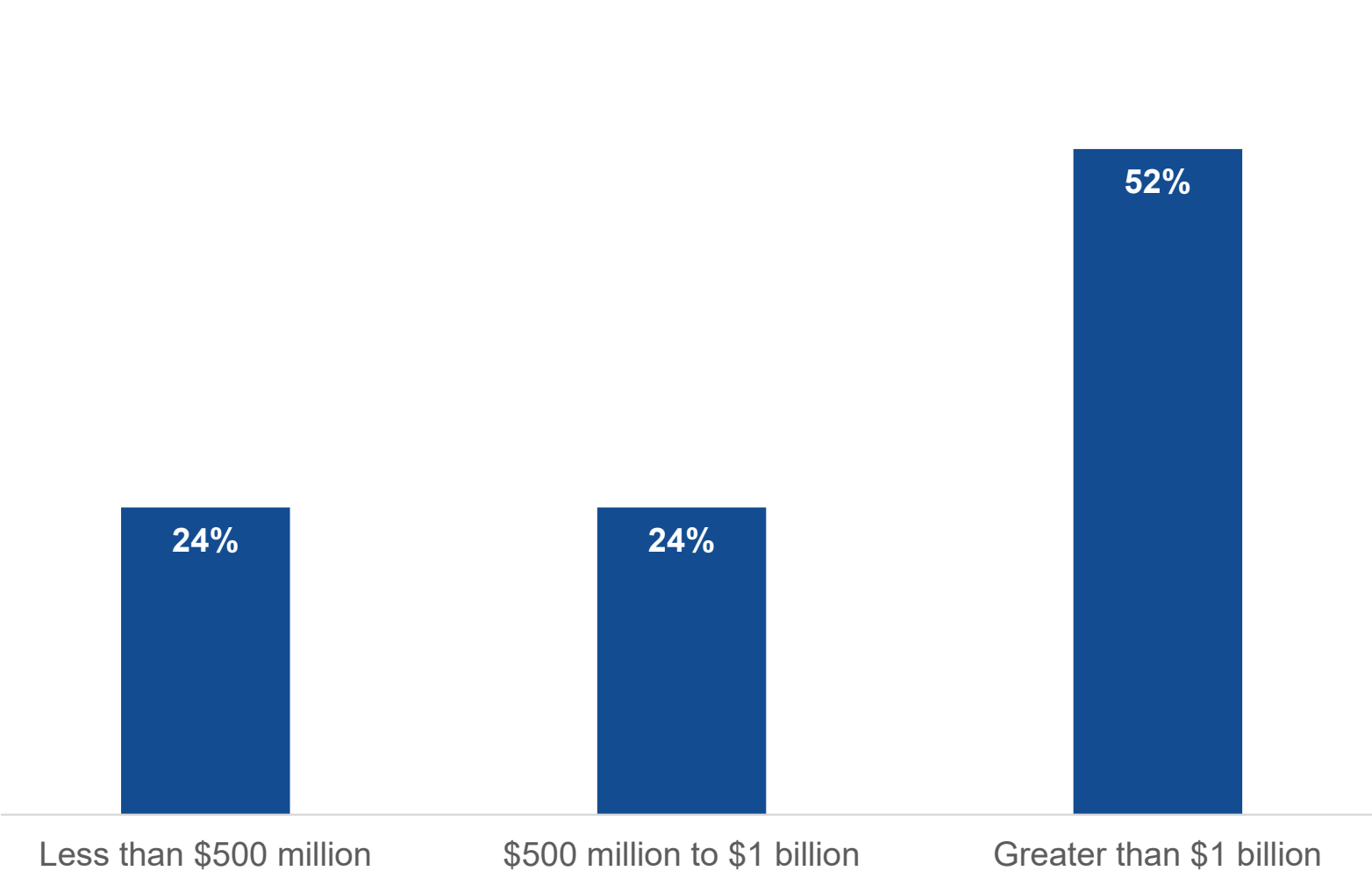
To gather data for this eBook, Enterprise Strategy Group conducted a comprehensive online survey of 200 IT decision-makers knowledgeable about their organization’s backup environment.

All organizations represented had between 1,000 and 9,999 employees, split 50-50 between North America (U.S. and Canada) and Western Europe (Germany and the U.K.). Organizations spanned multiple verticals, including financial, technology, manufacturing, and retail/wholesale, among others. The survey was fielded between September 19 and October 4, 2024.

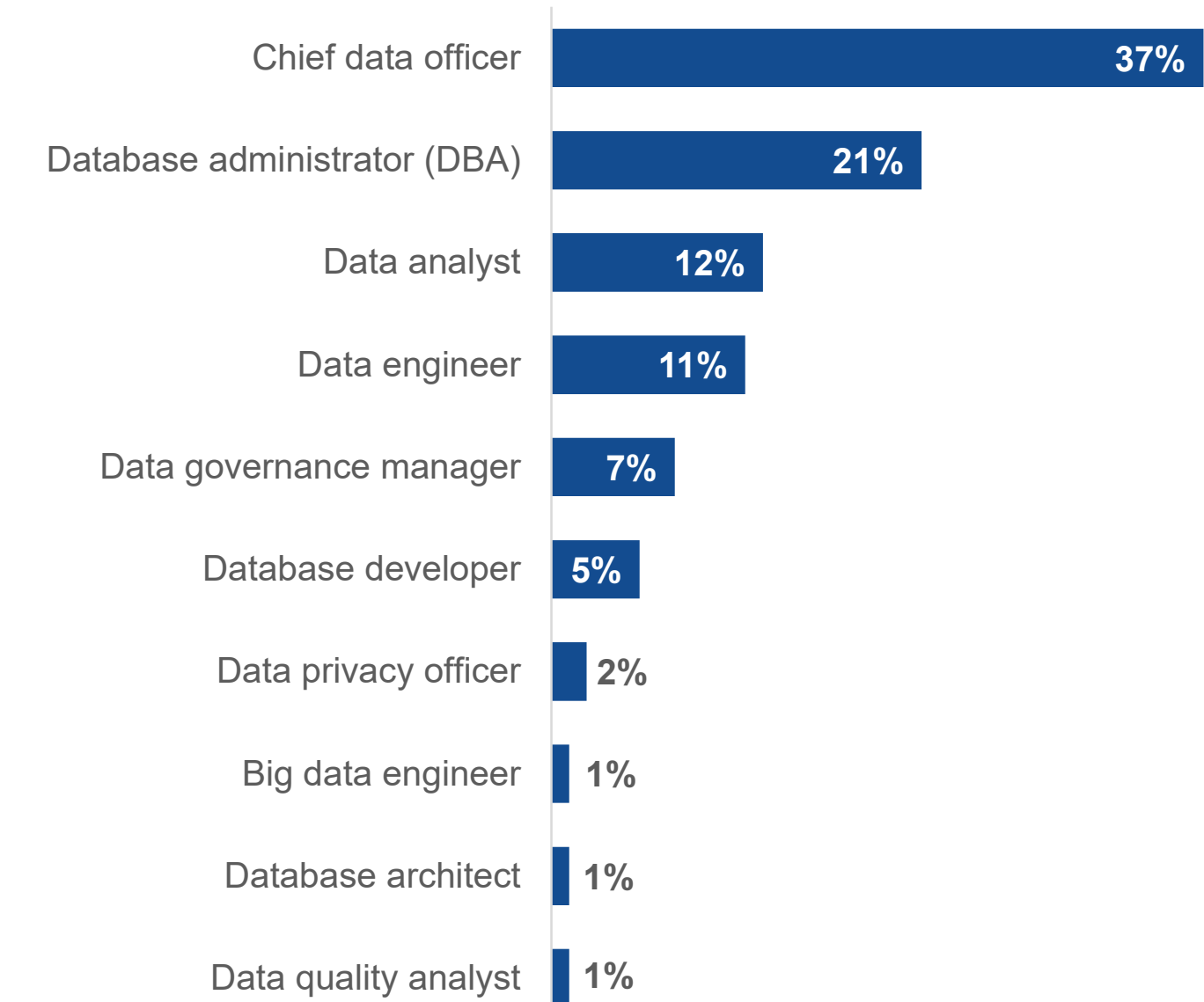
This survey has a 95% confidence level, with an estimated 6.9% margin of error.

Note: Totals in figures and tables throughout this report may not add up to 100% due to rounding.

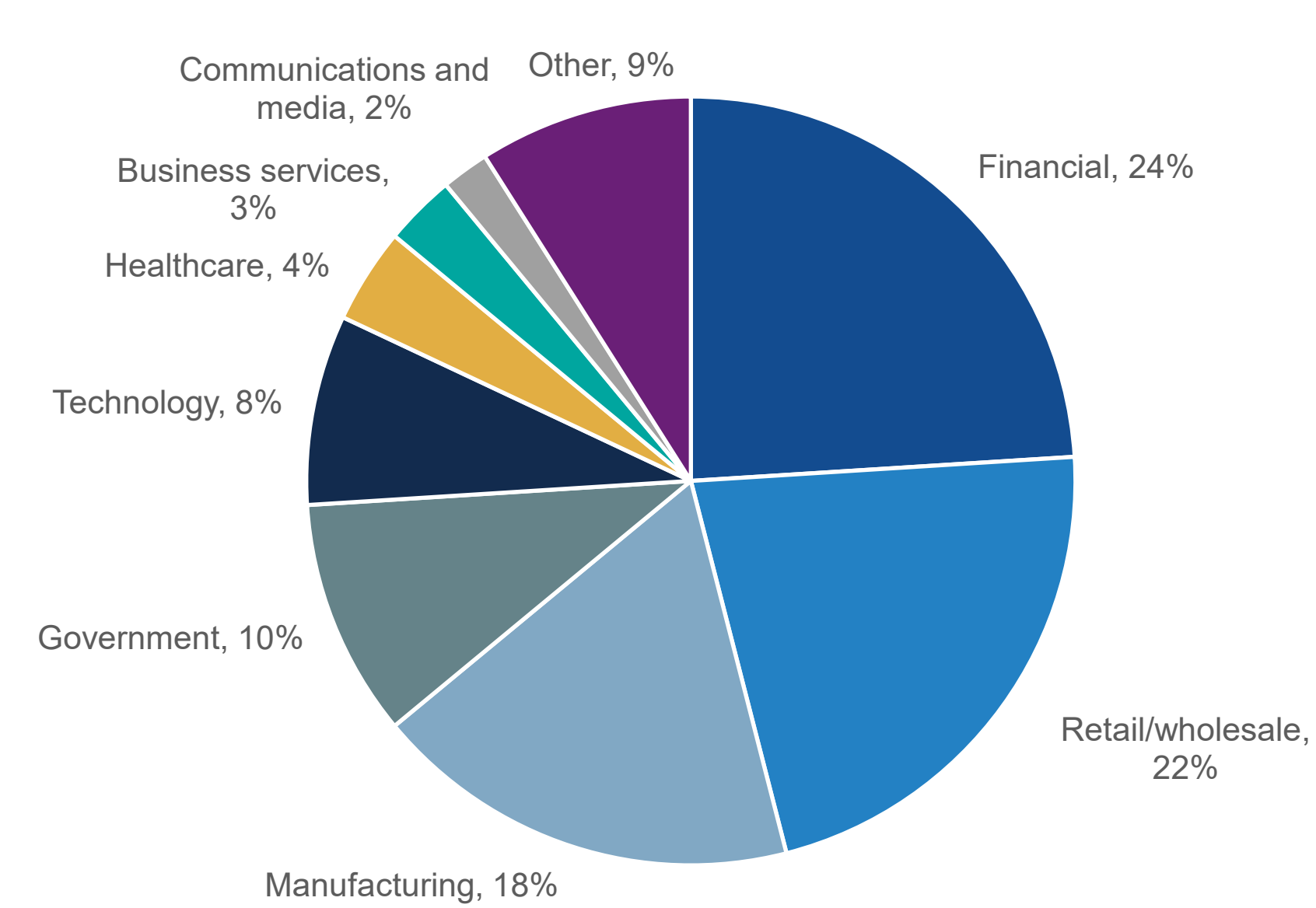
Respondents by Annual Revenue



Respondents by Role/Job Level



Respondents by Industry



All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.'s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

This publication is copyrighted by TechTarget, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at cr@esg-global.com.



Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.

© 2025 TechTarget, Inc. All Rights Reserved.