VERITAS

2023 GLOBAL REPORT

DATA RISK MANAGEMENT

The State of the Market—Cyber to Compliance

Research conducted by: VansonBourne

INTRODUCTION

Organizations and their employees, regardless of seniority, face risk. They need to balance that risk with their roles and responsibilities every day. The ability to manage risk is a foundation of a successful and growing organization. Emerging risks and risk perceptions can have a profound impact—for some organizations, they can be too much.

These risks could relate to technological advancements, market changes, economic fluctuations, regulations and compliance, and a myriad of other factors.

For instance, organizations are increasingly exposed to cybersecurity risks with the rapid advancement of digital technology. Cyberattacks and data breaches can severely disrupt business operations, causing significant financial losses and damaging reputations.

The COVID-19 pandemic underscored the risk of global health crises and the impact of economic turmoil. Many organizations were unprepared for such an acute disruption, leading to the need to adapt and find new ways to address growing threats to business resiliency and data protection.

Assessing and addressing these risks is paramount to maintaining a competitive edge and ensuring sustainable growth.

Based on interviews with 1,600 organizations, this report delves into the following key questions:

What are the greatest risks that organizations experience today?

How have organizations adapted to address data security risks in their recent history?

Do organizations and their employees believe themselves to be at risk? How does this translate into action?

Interviewees are split across two seniority levels—executives and practitioners.

The key to understanding risk is knowing how these two groups perceive and respond to threats.

Executives

come from a range of departments including IT; IT security; and risk, fraud, compliance, and governance teams.

Their job titles include:

- CISO
- CIO
- Chief Risk Officer

Practitioners

are from the same departments, but hold lower seniority levels.

Their job titles include:

- IT Manager
- IT Technician
- DevOps Engineer

KEY FINDINGS

Data security is the standout risk among a litany of threats.

- Data security **(46%)** is the standout risk faced by organizations, including ransomware and data loss/data theft. This is followed by risks related to economic uncertainty **(38%)** and to emerging technologies like AI **(36%)**.
- **87%** report actual damage, such as financial and reputational. The risks most likely to have caused damage include data security **(40%)**, economic uncertainty **(36%)**, and competition **(35%)**.

Data security is under constant, and unprecedented, threat levels.

- **65%** of those surveyed have experienced a successful ransomware attack over the past two years in which an attacker has gained access to the system.
- **39%** of organizations reported the attack publicly.
- **48%** experienced loss of data over the past two years.
- Data loss stands at **13% to 14%** across all environments (on-premises, private cloud, public cloud, and edge) on average, over the same timeframe.

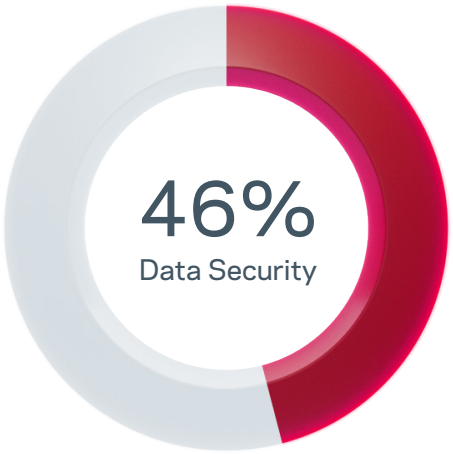
Organizations are responding to the level of data security risk.

- On average, organizations have increased data protection budgets by **28% to 30%** over the past 12 months for all environments measured (on-premises, private cloud, public cloud).
- Data protection and data security teams have increased by an average of **21 to 22** people over the same timeframe.
- **89%** believe they have adequate staffing to keep their organization secure.

Risk levels are escalating, but are often unrecognized.

- More respondents are likely to say the level of risk has increased than decreased over the last 12 months across all risk types (e.g., risks to the brand, risks from data security, etc.).
- When asked initially, just more than half **(52%)** of organizations considered their organization to be currently at risk.
- When presented with individual risk factors, **97%** indicated that their organization experiences risk. This begs the question: Do organizations underestimate the risk they currently face?
- For some, the level of risk will be too much—**15%** of organizations say the level of risk will put them out of business.

Data security is the standout risk among a litany of threats.



Managing risk is a cornerstone for every organization, no matter the size or industry. The ability to adapt to potential bumps in the road—whether minor or major—is no easy task, but it's essential for businesses to move forward.

Given this, it's important to understand the greatest risks organizations face today. When asked to identify the greatest risks, respondents were most likely to rank data security (46%) among the top three, followed by risks from economic uncertainty (38%) and emerging technologies like AI (36%) (Figure 1).

The Greatest Risks to Organizations Today

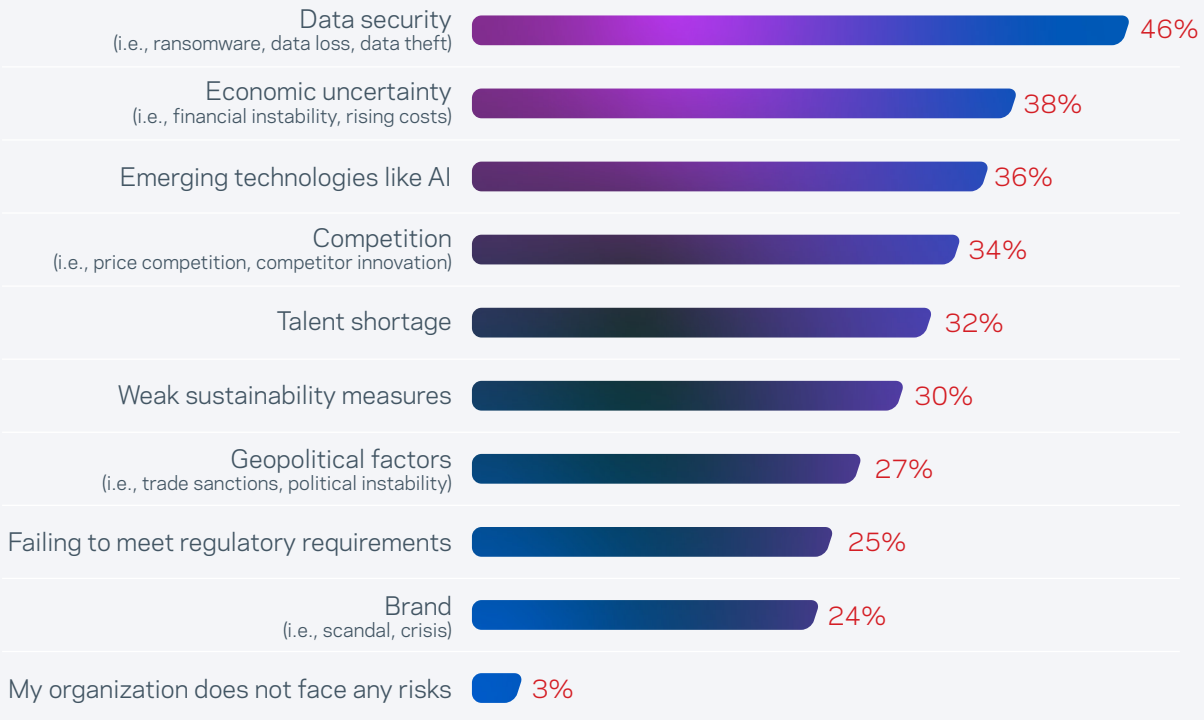


Figure 1. Which of the following are the greatest risks to your organization today? Combination of responses ranked first, second, and third. [1,600] Not all response options shown.

There are daily headlines about major data breaches across all industries. Attackers are more sophisticated and potential impacts are greater. It's not an ideal combination for any IT security leader. These breaches not only damage a company's reputation, they can also lead to significant financial loss. In the current landscape, most organizations acknowledge cybersecurity as a strategic risk, but many still struggle to handle it effectively.

In this context, it makes sense for data security to come out on top. However, it's important to note that all these risks are interconnected. For example, a major cybersecurity breach will no doubt impact an organization's brand (reduced loyalty, harm to brand image, etc.), which may also affect recruitment.

Risks truly do come from everywhere.

These risks can all cause harm to differing extents, be it financial or reputational in nature. In fact, 87% of respondents say risks have resulted in actual damage to their organization. The response differs between executives (93%) and practitioners (82%). However, executives are more likely to be involved in key conversations about operations and may have a more accurate view of the risks they face. Therefore, it's not surprising that they say more damage has been done.

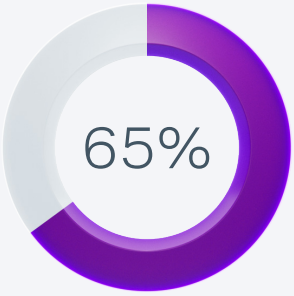
Regardless of whether executives or practitioners are more accurate, the responses show the extent to which these risks can wreak havoc. Careful management, mitigation, as well as an understanding, are crucial to minimizing the threat.

Thus, an understanding of data security challenges will be crucial to an organization's continued success. Highlighting this, respondents report data security (40%) as the threat that has caused the most damage.

87% of respondents say risks have resulted in actual damage to their organization.

40% of respondents report data security as the threat that has caused the most damage.

Data security is under constant, and unprecedented, threat levels.



Two-thirds of organizations have been hit by a successful ransomware attack in the last two years.

Almost two-thirds (65%) of organizations have been hit by a successful ransomware attack in the last two years. These are not harmless attacks that were identified and thwarted. These are incidents in which the attacker gained direct entry or access to the targeted system. It only takes one successful attack to do untold damage, ultimately highlighting the extent of threat that organizations face.

The fact that executives give a greater estimate for successful ransomware (72%) than practitioners do (57%) suggests that senior leaders may not share the state of the situation with their employees. They may be limiting transparency to avoid widespread panic.

Perhaps more concerning is that more than 26% report they've experienced an attack, but haven't reported it publicly (Figure 2). With compliance laws tightening worldwide about reporting attacks within set timeframes, organizations and decision makers walk a thin line when attackers infiltrate their defenses. In and among mitigating direct business-related consequences, compliance regulations are another element to consider when attackers come calling.

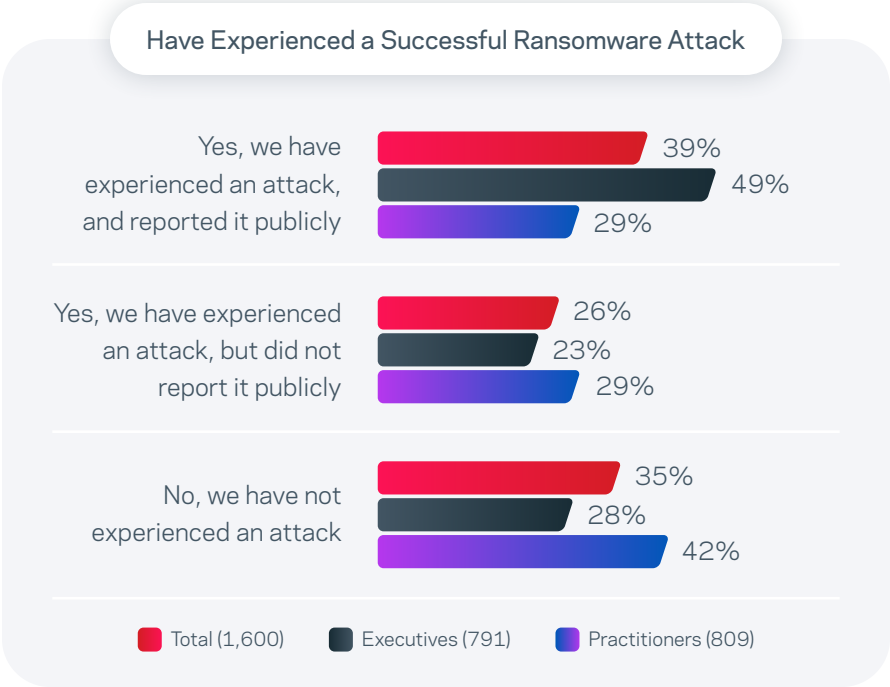


Figure 2. Has your organization experienced a successful ransomware attack in the last two years? [Base sizes in chart]. Not all response options shown. Data split by respondent type.

Ransomware attacks, of course, are not the only type of cyberattack. And they're not the only event that can lead to data loss. In fact, nearly half (48%) report their organization has experienced a loss of data over the past two years from incidents other than ransomware attacks.

Further still, these data loss events are happening across organizations' infrastructure, including cloud environments. There is a similar split over the past two years (13% to 14% on average) across the following IT environments: on-premises, private cloud, public cloud, and edge (Figure 3).

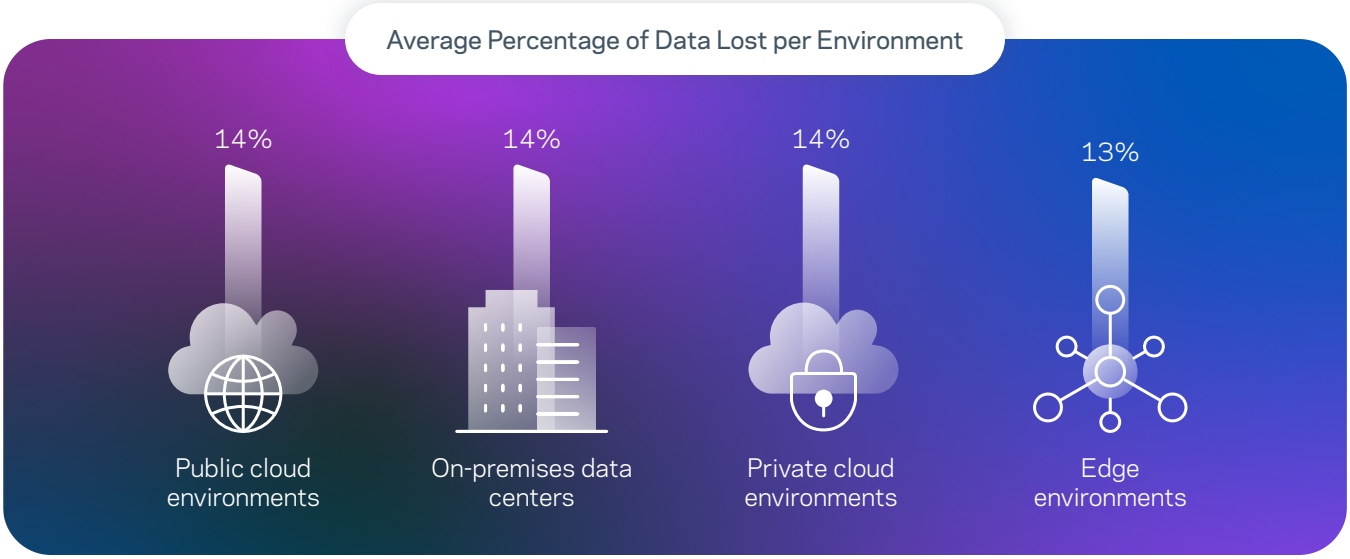
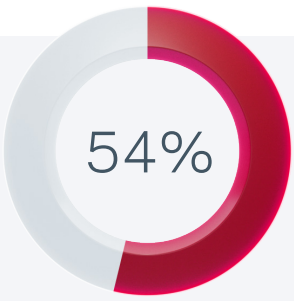


Figure 3. As a percentage, approximately how much data have you lost from the following IT environments in the past two years? [772]. Question shown only to those that have experienced a loss of data. Graphic shows the average data loss per environment.

For any digitally focused company, data is obviously distributed across multiple environments. The pandemic provided the torchlight for many organizations to accelerate their uptake in cloud services. A complex set of IT environments means that organizations must be especially aware of where their data exists.

Would-be attackers are constantly probing systems for weaknesses. For them, data is gold. Many succeed. And the more successful attackers are, the higher the risks to the organization.



54% of those surveyed are more likely to say the level of data security risk has increased than decreased (21%) over the past 12 months.

With security threats increasing, organizations must avoid falling afoul of compliance regulations.

Data security and data compliance are undeniably intertwined. Although many organizations have suffered successful ransomware attacks in recent history, it's reassuring that the vast majority (81%) say their data has remained fully compliant with all national and/or regional regulations in the past 12 months.

Clearly, most organizations are doing something right—perhaps ensuring they're abiding by legislation has been a focus over the past few years. And this explains why only 25% rank not meeting regulatory requirements in their top three risks—only slightly higher than risks to the brand (such as scandals or crises), at 24%.

With increased focus on risks from data security, leaders must ensure that they don't lose sight of regulatory requirements and remain compliant. Staying compliant ensures organizations not only avoid relevant fines, but ensure the brand stays robust.

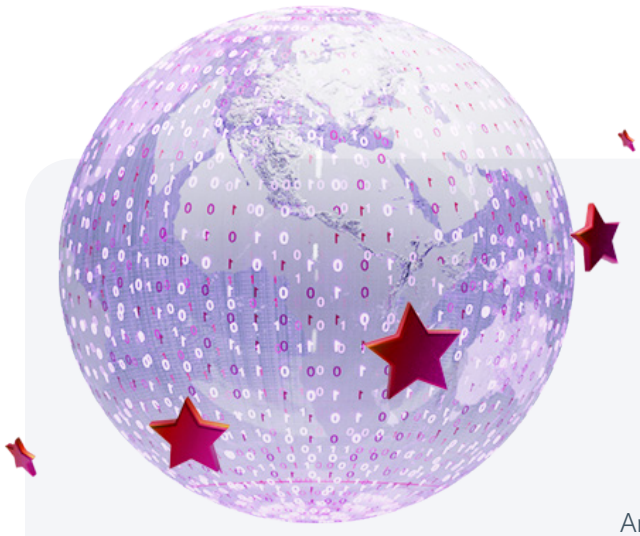
$336,219

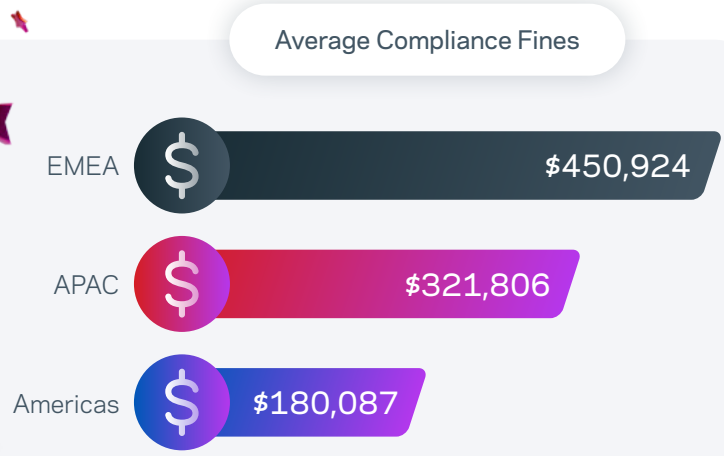
Average fine levied on those that have breached compliance regulations.

However, when organizations do face compliance fines, they can be steep. An average of $336,219 (USD) is levied on those that have breached compliance regulations. Average compliance fines are higher for organizations in EMEA ($450,924) than in the Americas ($180,087). The good news is that only 26% report they received compliance fines over the past 12 months.

Given geopolitical tensions, recent high-profile data breaches, and the advanced technologies available to possible attackers, it feels like risk level for data security has never been higher.

What are organizations doing to address increasing risks?





Organizations are responding to higher levels of data security risk.

Data Protection Budgets and Strategies

To their credit, many organizations have reacted proactively to the increased data security risk. They've funded efforts to bolster data protection, with an average increase in budgets across all IT environments, in all regions (Figure 4).

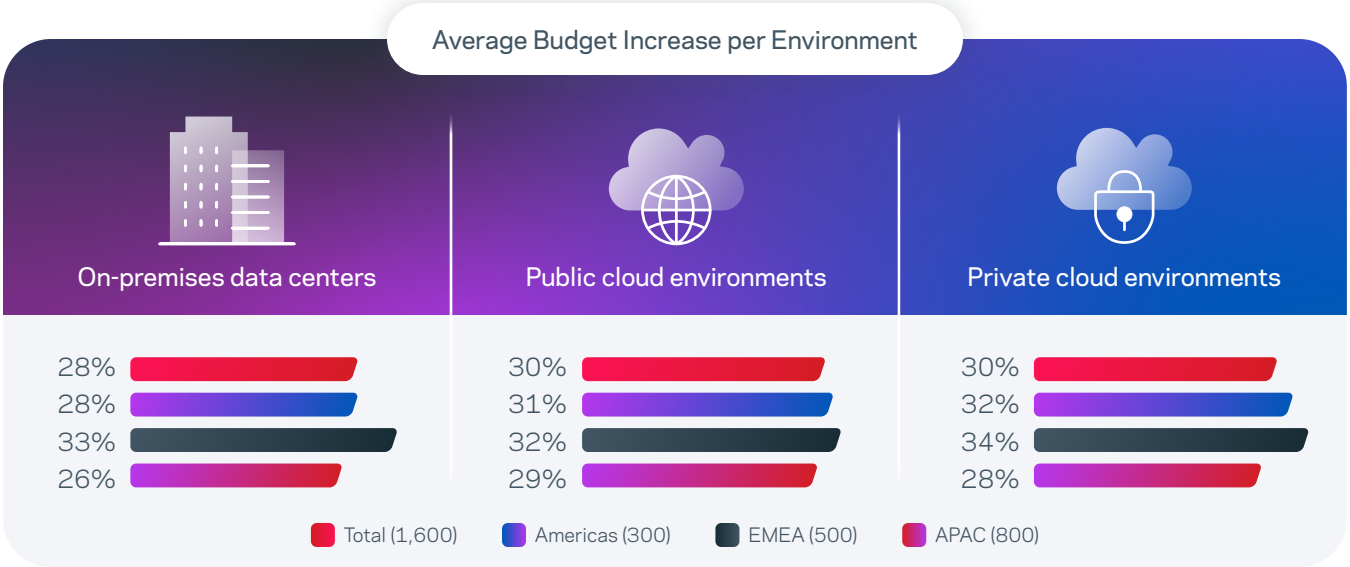
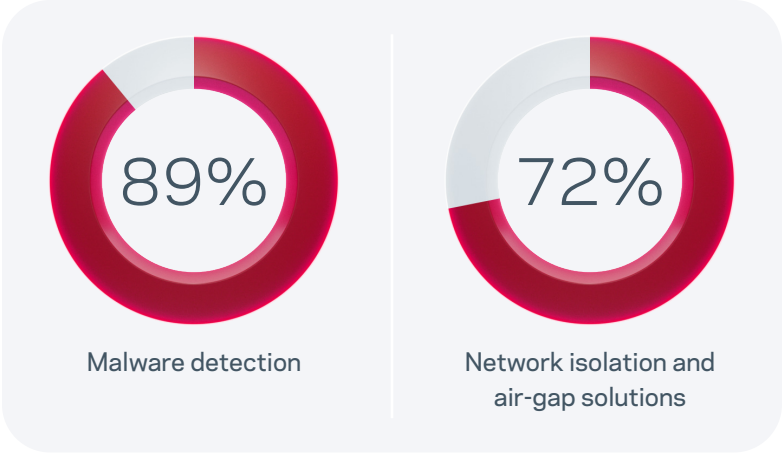


Figure 4. Approximately, how has your organization's budget for data protection changed in the last 12 months over the following environments? [1,600] Shows only the average percentage increase per environment.

The increase in spending may go toward implementing various data protection strategies. Most organizations have implemented several strategies, from malware detection (89%) to network isolation and air-gap solutions (72%).



It makes sense that more complex solutions such as immutable storage are less likely to have been implemented. However, the fact that nearly three quarters of all those surveyed have implemented each data protection strategy shows the seriousness with which they're taking the data security threats (Figure 5).

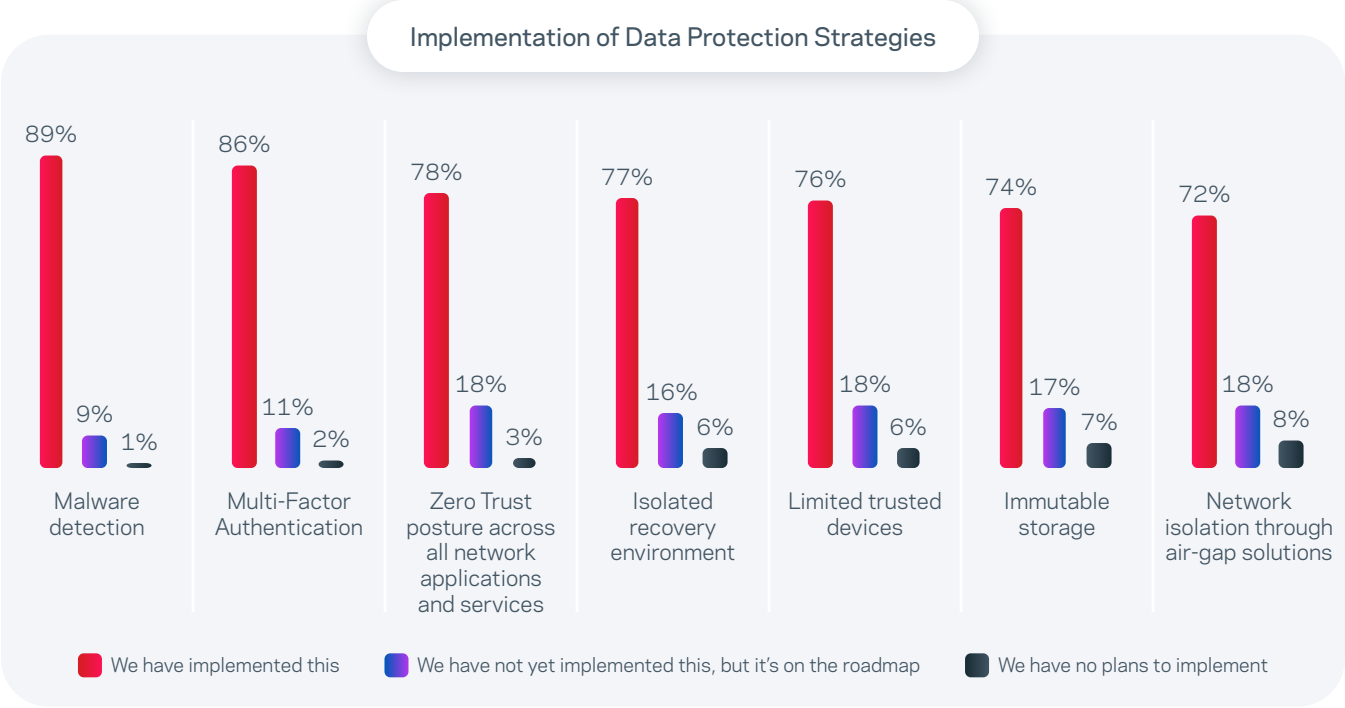


Figure 5. Which of the following timelines best reflects when/if your organization implemented/will implement the following data protection strategies? [1,600]. Not all response options shown.

Staffing is on the rise.

Data protection isn't the only area of budget increases over the past 12 months. Organizations have also increased their data protection and data security teams by an average of 21 and 22 people, respectively.

With the backdrop of economic turbulence and a challenging business environment, it may seem off kilter that organizations have been hiring in these roles, especially given near-weekly headlines of mass job cuts. On the other hand, it speaks to a level of proactive defense. Adequate staffing is part of the equation for organizations to best protect themselves.

However, there are differences of opinion between executives and practitioners when it comes to hiring numbers. Practitioners clearly disagree with the number of people who have been hired within these teams. Being on the front line, and perhaps feeling overworked, may explain why they don't feel they have the same levels of staff increases as executives report (Figure 6).

Given the extra workforce in place, it may not be surprising that 89% of those surveyed believe their organization has enough staff to keep them secure. In fact, 49% report they believe they have more than enough staff in place. Extra resources clearly help to make employees feel that their organization is taking the security threat seriously.

Ultimately, the only way for this to be judged a success is a reduction in the number of successful attacks. For that, only time will tell.

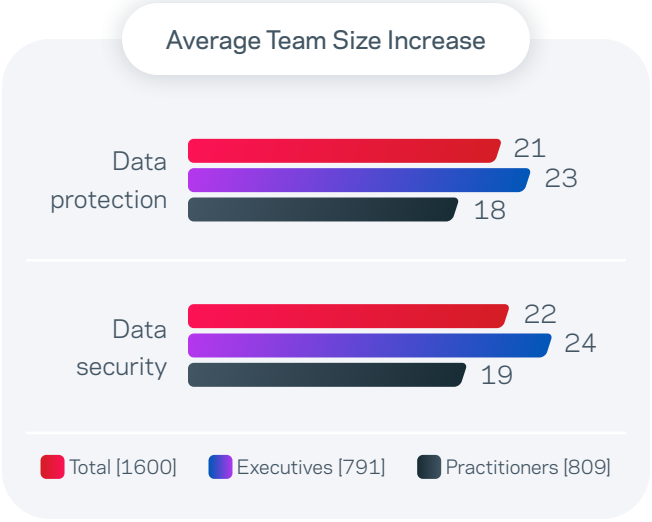


Figure 6. Approximately, how have the following teams in your organization changed in the past 12 months? [Base sizes in chart]. Chart shows only the average percentage increase per environment, split by respondent type.

Figure 7. Beyond data protection, how have your roles/responsibilities changed, if at all, in the last 12 months? [Base sizes in chart]. Showing only those executives and practitioners who say their or their teams' roles/responsibilities are more focused.

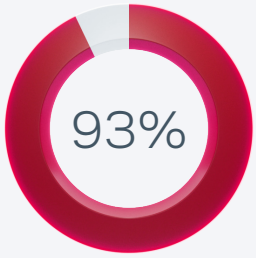
Harnessing the Benefits of AI

Beyond hiring new staff, organizations and relevant employees are looking at other ways to boost their defenses. Key among these is the implementation of AI and/or machine learning (68%). AI—no doubt the current buzzword—has the potential to improve efficiencies and help security teams. It's important to note that emerging technologies such as AI also bring new threats, a fact already highlighted by many. However, one of AI's anticipated benefits is reducing data security risk.

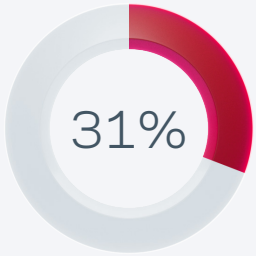
The changes imposed by the data security threats are rapidly evolving the roles and responsibilities of both teams and individuals. Executives and practitioners agree that their team and individual responsibilities have become more focused on compliance, security regulations, and managing workloads in the last 12 months (Figure 7). The increased risk in data security may be fundamentally changing how people work.

Data security—an area of huge concern—likely gives those involved in risk management nightmares when they think of the harm that can be done. Certainly, as we've seen, organizations are responding to the threat by increasing budgets and implementing several security measures to reduce the risk.

But there is still more to be done.



of respondents have a data recovery plan in place.



of respondents say it's only a partial plan.

Recovery plans and rehearsals are crucial.

One key area where progress needs to be made is planning for how to quickly recover after a data loss event or cyberattack. This is highlighted by the fact that although 93% of respondents have a data recovery plan in place, while 31% say it's only a partial plan.

Clearly, although organizations have made great progress in addressing data security risk, they still need to go further to establish well laid-out, defined, and complete recovery plans. In the event of a breach, organizations need to be able to act swiftly. A well-defined action plan can go a long way to minimize damage. Having an incomplete plan risks wasting crucial time in such an event.

Aligned with this weakness in planning, organizations currently perform automatic rehearsal and manual recovery exercises on their data and critical applications only every five to six weeks on average (Figure 8).

Recovery and rehearsal exercises must be done on a more regular basis to ensure quick recovery from data security threats, no matter how data or process has changed. The greater the preparation, the faster an organization and its employees will be able to react during a security incident.

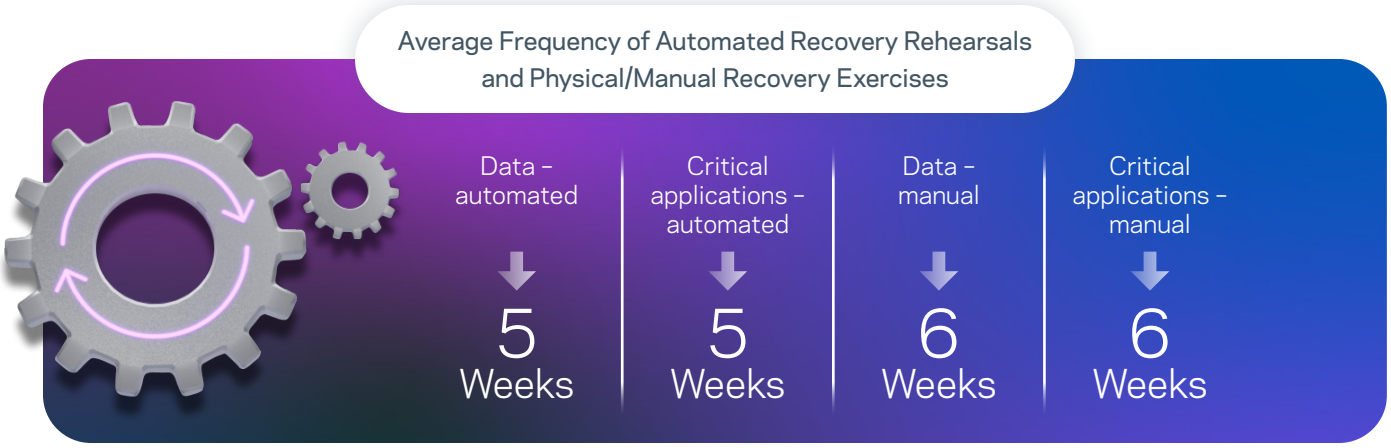


Figure 8. How often does your organization conduct automated recovery rehearsals and physical/manual recovery exercises for data and critical applications? [1,491]. Question shown only to those who have a complete or partial recovery plan. Chart shows the average length of time in weeks.

Risk levels are escalating, but often unrecognized.

Risks from data security aren't the only ones that are rising. All risk categories are seeing increases, with more respondents likely to say risks have increased (42% to 54%) across the nine risk types listed than decreased (21% to 26%) over the past 12 months (Figure 9).

There's a huge focus on data security—especially given the profile of our respondents—but are they as aware of the threat levels for other types of risk? It would appear not.

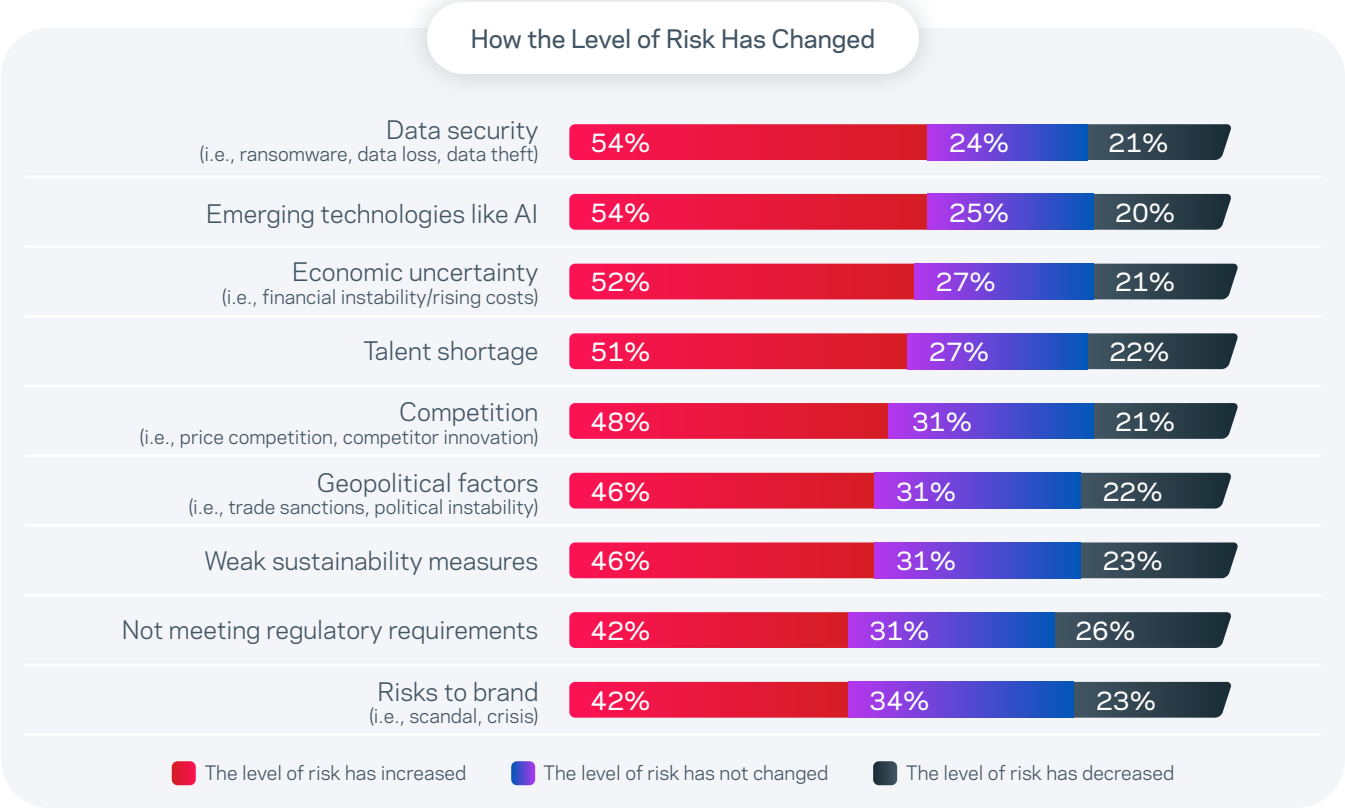


Figure 9. How has the level of risk to your organization over the following categories changed over the past 12 months? [1,551] Question shown only to those who report they experience risks today. Not all response options shown.

While it is only natural for the technical respondents to be more alert to data and technology-based risks, it's a concern to see that some essential areas are somewhat underrated. For example, if there was a brand-related scandal, a severe talent shortage, or a particularly successful competitor stole a large part of your customer base, would there even be enough value left in the data to worry about protecting it?

When asked how "at risk" their organization is in general, only a slight majority (52%) classified their business as such. More surprising is that of those who classified their organization "not at risk," 42% reported they had experienced a successful ransomware attack.

Industry also factored into a respondent's clarification of "at risk." Organizations in media, leisure and entertainment, biopharma, manufacturing and production, and healthcare are more likely to report that they are "at risk" (Figure 10).

Yet when presented with individual risk categories, 97% of those surveyed stated they currently experience risks. In fact, 45% of those who believed their organization to not be at risk also reported their organization faces individual risks, such as data security, competition, and others.

This disconnect shows that most respondents seem to underestimate the level of risk that they face. That is, until they are asked about specifics. For some, this is a level of detail they might not have to consider, let alone plan for, daily.

It's a fine line between success and failure when it comes to managing risk. It's imperative that leaders understand that risks can come from anywhere. In a world where organizations are faced with different threats every day, it's not just those that are willing to take business risks that will succeed. It's those who most effectively minimize threat risk that will be the best positioned to survive and thrive.

For some organizations, the level of risk will be too much. 15% say they don't believe their organization will survive another 12 months.

This was highest in...

- **Region:** EMEA (20%)
- **Organization Size:** 3,000 or more employees (17%)
- **Department:** Financial operations (32%), Risk/Fraud/Compliance/ Governance (26%), DevOps (18%)

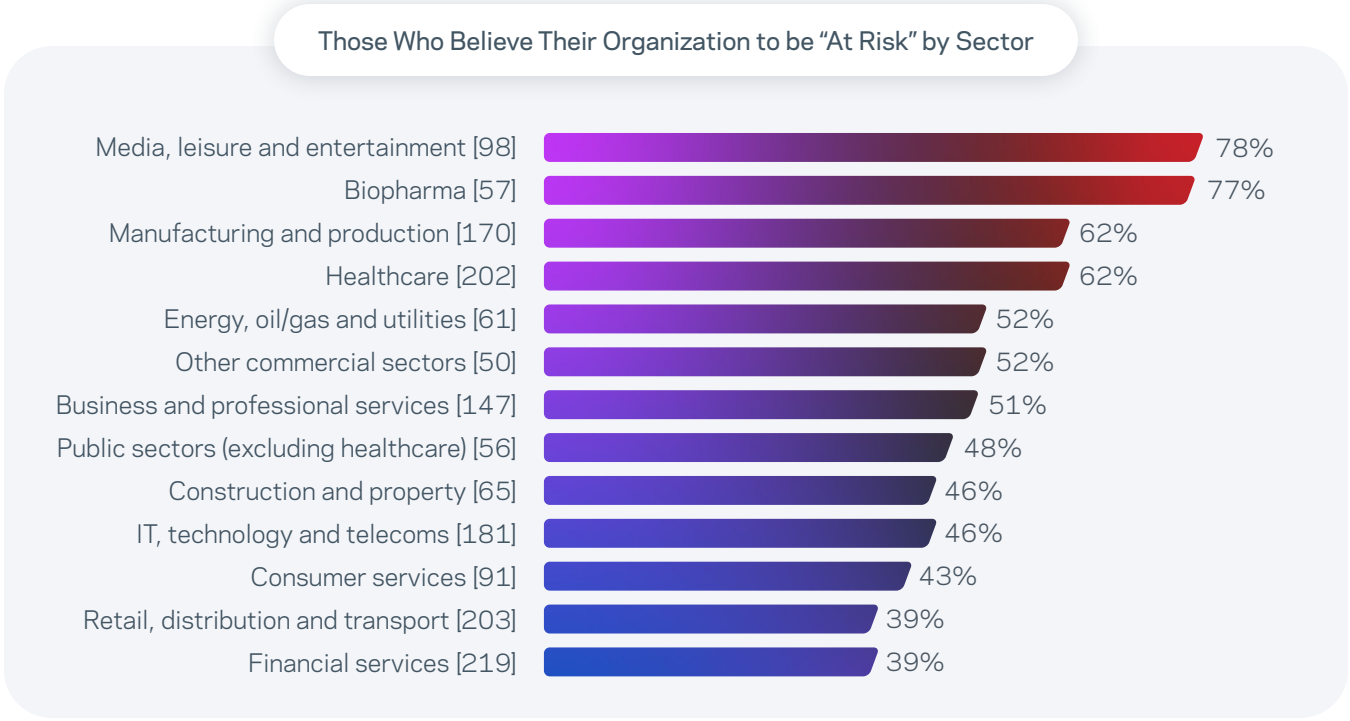


Figure 10. In your opinion, how much 'at risk' is your organization currently? [Base sizes in chart]. Chart shows a combination of those who select "Significantly at risk—I don't expect my organization to survive another 12 months" and "Somewhat at risk", split by industry.

RISK INDEX

Each organization deals with and classifies risk differently. Vanson Bourne analyzed responses from participants and calculated risk scores based upon specific survey questions. These included questions as to whether the organization had experienced a successful ransomware attack or data loss over the past two years, among others.

The calculations show an overall risk score for the whole research sample, then split it by each individual market (Figure 11) and industry sector (Figure 12). The scores provide an indication for how "risky" each market, or sector, is relative to the others.

Figure 11. Total risk score [1,600]. Split by market.

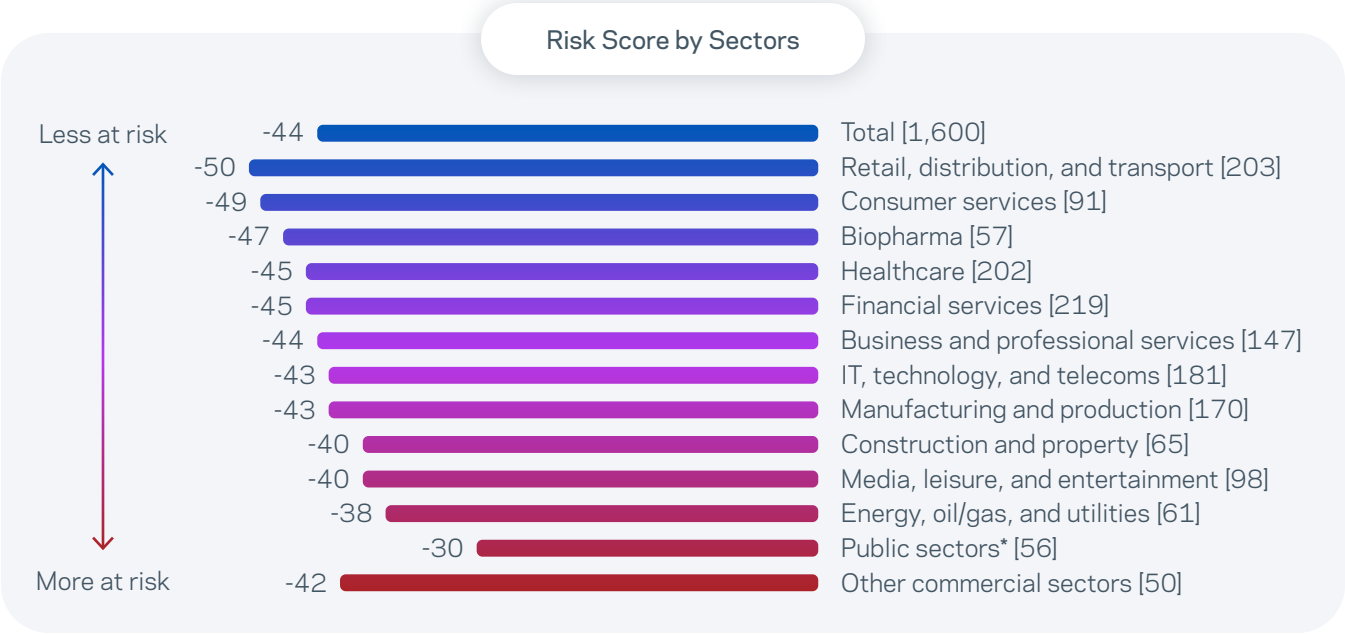


Figure 12. Total risk score [1,600]. Split by industry.

*government/state provided, excluding healthcare

CONCLUSION

Organizations, it could be argued, are defined by how successful they mitigate and manage risk. Risks vary and constantly change, with new ones emerging on a frequent basis. Navigating uncertainty can significantly impact the outcomes of any business.

Chief among the litany of threats is data security, whereby an organization faces dangers from areas such as ransomware attacks, data loss, or data theft. It's encouraging to see that many organizations keep close watch over this threat. The risk level is increasing, but organizations are responding by increasing data protection budgets and improving staffing levels. And the response doesn't stop there. Those surveyed are all looking at ways to see how they can best protect themselves.

However, it does come at a cost.

In the focus to manage risk levels from data security, organizations may be forgetting that risk can come from anywhere—from emerging technologies, from the competition, from a scandal or crisis with the brand, among others. When presented with the different risk categories, both executives and practitioners admit that their organizations are perhaps more at risk than they initially thought.

Risk, when considered on an overall level, is an intangible term. It is only when broken into sub-categories that it can be truly managed. Organizations must look to do this to survive and thrive.

Research Scope and Methodology

Veritas Technologies commissioned independent market research specialist Vanson Bourne to undertake the quantitative research upon which this report is based. A total of 1,600 business executives and practitioners were interviewed during August and September 2023, with representation from the following regions and individual markets (number of interviews in brackets):

- Americas (300): US (200), Brazil (100)
- EMEA (500): UK (100), France (100), DACH (100), Nordics (100), UAE (100)
- APAC (800): China (200), South Korea (100), Singapore (100), India (200), Japan (100), Australia (100)

All respondents are from organizations with more than 1,000 employees and represent a range of private and public sector organizations. All respondents had to at least influence purchasing for technology within their organizations.

Vanson Bourne conducted a rigorous multi-level screening process to ensure that only suitable candidates were given the opportunity to participate.

Unless otherwise indicated, the results discussed are based on the total sample.

About Vanson Bourne

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets. For more information, visit www.vansonbourne.com.

VansonBourne

About Veritas

Over 80,000 customers—including 91% of the Fortune 100—rely on Veritas to help ensure the protection, recoverability, and compliance of their data. Veritas has a reputation for reliability at scale, which delivers the resilience its customers need against the disruptions threatened by cyberattacks, like ransomware. No other vendor can match Veritas's ability to execute, with support for 800+ data sources, 100+ operating systems, and 1,400+ storage targets through a single, unified approach. Powered by Cloud Scale Technology, Veritas is delivering today on its strategy for Autonomous Data Management that reduces operational overhead while delivering greater value. Learn more at veritas.com. Follow us on X at @veritastechllc.

VERITAS

2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
veritas.com

For global contact information visit:
veritas.com/company/contact

V2000 10/23