Futurum

Cloud, Complexity, AI: The Triple Threat Demanding New Cyber Resilience Strategies

NETAPP – FUTURUM GROUP CYBER RESILIENCE STUDY 2024

AUTHORS

Krista Case
Research Director | The Futurum Group

Camberley Bates
Chief Technology Advisor | The Futurum Group

NOVEMBER 2024

IN PARTNERSHIP WITH

NetApp®

Content

Overview and Methodology

In the Fall of 2024, NetApp partnered with Futurum to survey more than 1,300 cybersecurity decision-makers. Respondents held C-Level, VP, and Director-level titles within IT and Security across a variety of industries, globally. This in-depth report highlights findings from the survey and 15 one-on-one interviews with select decision-makers who participated in the research.

Key Takeaways

- More than half (54%) of enterprises have experienced an attack in the last 12-18 months.
  - One in five were unable to recover data.
  - More than 60% of the time, identification of data was their top issue to recovery.
  - Of the organizations that could not recover, only 20% indicated having data classification – whereas more than half (52%) of organizations that could recover their data indicated having data classification.
- Security risks will abound in cloud environments. Security risks related to usage of cloud environments ranked as the top threat across the world, being noted by 38%-40% of survey respondents.
- New tools won't necessarily fix the problems. The respondents, 70% indicated that their organization is using more than 40 tools for cybersecurity and 84% indicated that this vast number of tools is a problem when it comes to cyber-resiliency.
- More than 90% of the organizations we surveyed plan to increase cybersecurity spend over the next 12-18 months.

Executive Summary

The rise of cyber-attacks has become a board-level concern. No organization is immune. More than half (54%) of the enterprises surveyed reported having experienced an attack in the last 12-18 months. What is perhaps even more concerning is that cyber-attacks are only becoming more impactful, as malicious actors use tools such as AI to increase their efficacy. According to a study by IBM and Ponemon Institute, the average cost of a data breach increased from $4.35 million in 2022 to $5 million in 2023.

Quotes from IT and Security Leaders

"The biggest problem we have is the growth in sophisticated threats and attacks. And by this, I mean we're starting to see a shift in the world from old style cybersecurity threats, which would be exploiting existing vulnerabilities, social attacks, things like that. We're starting to see this very worrying trend shifting to AI, where AI models, very extensive machine learning paradigms, are being used to leverage not just software weaknesses, social engineering weaknesses or straight out spam based threats, but we're starting to see [AI widening] the gap to the point where I've actually had our CISO, who's very versed in cybersecurity, reach out to me on a couple of cases so far in just the last couple of weeks to show me some of the attempts that that he's seeing at a broader level."

- IT Director, Technology Sector, 5,000+ employees

"If our clinical information system is withheld from us, the potential to impact patient health and patient life is very real in a very short amount of time. So, we can't permit those attacks to happen."

- Chief Data Officer, Healthcare Organization, 5,000+ employees

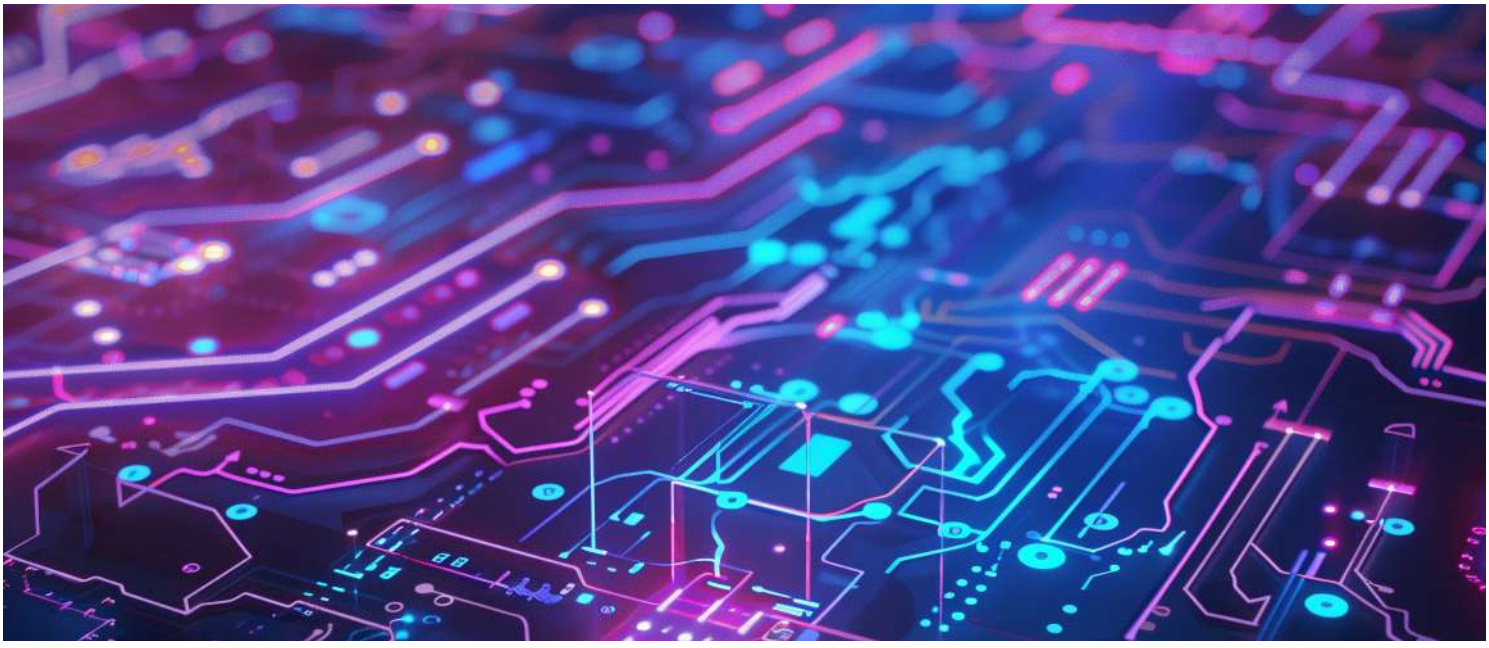
The need to maximize cyber-resiliency is clearly impacting technology requirements. In fact, more than 90% of the organizations we surveyed plan to increase cybersecurity spend over the next 12-18 months. This is especially true for information storage, protection, and management – as it is the data that the malicious actors are after, at the end of the day. Data classification is the lynchpin when it comes to both optimizing defenses against cyber-attacks and getting critical business services back online following an attack. In fact, in our study, one in five (21%) of the respondents that indicated having been attacked also indicated being unable to recover their data. More than 60% of the time, identification of compromised data, as a result risking reinfection, was their top issue that is slowing, or that they believe would slow, their recovery. Of the organizations that could not recover, only 20% indicated having data classification, whereas more than half (52%) of organizations that could recover their data indicated having data classification.

By cataloging data according to its sensitivity, value, and risk, it is possible to prioritize the highest protection measures toward the most valuable data, to avoid overly permissive access policies to prevent unauthorized access to data, and to better identify the scope of an incident and prioritize subsequent response.

This thread carries through when we look at the top threats impacting organizations, including security risks related to the usage of cloud environments – which ranked as the top threat across the world, being noted by 38%-40% of survey respondents. The ability to identify and prioritize critical data was cited as the top challenge experienced by respondents' organizations, followed by data sprawl.

The issue of data sprawl across hybrid multicloud environments is compounded by the fact that approximately 70% of respondents indicated that their organization is using more than 40 tools for cybersecurity and 84% indicated that this vast number of tools is a problem when it comes to cyber-resiliency. This is particularly an issue when the need to improve threat and breach detection, and to accelerate resulting response and resolution/recovery, is critical in order to mitigate business service downtime and data loss (RPO and RTO) following an attack.

More intelligent, AI-enabled data services can help when it comes to keeping pace with continually changing and more sophisticated attack vectors. In fact, AI-based detection technologies topped the list of tools in use for cyber-resiliency today (40%) and the top investment area in the future (30%), particularly for the primary production environment, in order to detect attacks, with confidence, as quickly as possible.

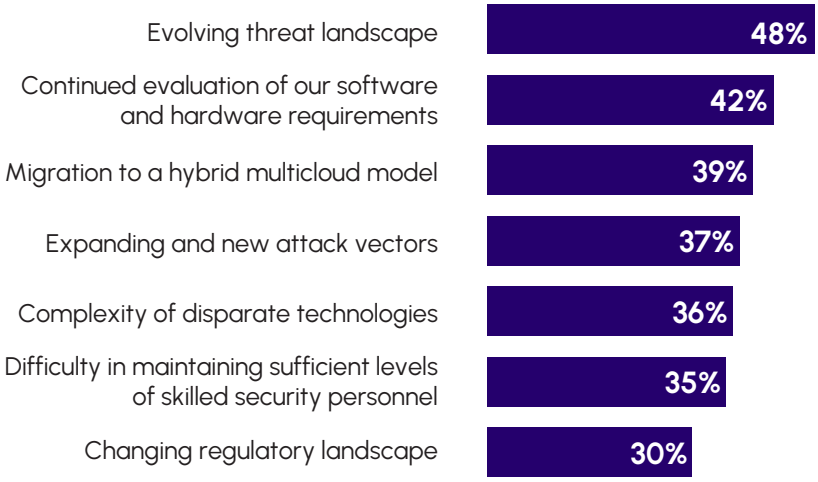


Key Customer Challenges: Cyber-Resiliency

Practitioners are finding it difficult to keep pace with evolving threat vectors such as the rise of AI-fueled identity-based attacks, as well as the expansions to the attack surface that are resulting from the shift to hybrid multicloud. This introduces opportunities for misconfigurations, creates data silos, and makes it challenging to manage user access. These compounding variables make it difficult to keep pace with, and as a result identify in a timely manner, attacks. Additionally, it becomes very challenging to obtain visibility into what is stored where, the data's privacy requirements and importance to the business, and what was impacted in the event that a breach occurs. These trends are having a material influence on technology requirements.

What approaches are your organization using to keep up with the constant changes to the threat landscape?

Base: n1,326 Senior decision makers who are knowledgeable of organization's global cyber-resilience practices and governance.



What approaches are your organization using to keep up with the constant changes to the threat landscape?

Base: n1,326 Senior decision makers who are knowledgeable of organization's global cyber-resilience practices and governance.

Quotes from IT Security Leaders

"The main concern is that cyber criminals are one step ahead. So how can we make sure that we will be not in catch-up mode, but stay one step ahead of them, so that our customers and their clients don't have to experience a cyber breach and huge losses. That is our main concern, because it involves not only the financial loss, but also the reputational risk to our customers, which is detrimental for their business, and, in turn, to us."

- VP, Global Technology, Financial Services Organization, 5,000+ employees

"Regulations like HIPAA, GDPR, mandate the protection of patient data, and failure to comply with this can lead to legal actions and reputational damages. So this is quite a concern for us as an industry."

- CTO, Healthcare Organization, 5,000+ employees

"The most important thing is business continuity. Everybody talks about data loss, which is very, very important also. But, in our case, we build parts for cars, so if we can't ship and we can't build or do manufacturing, we're losing money every single minute. So for us, that's the highest priority."

- IT Director, Manufacturing Organization, 5,000+ employees

"The top concern for me is the complexity. Each platform, each cloud environment, our on premises environment - even on premises, we have multiple data centers that we maintain. They're not maintained by one group. The toolsets used across those different instances are diverse. They have some good capabilities. Others don't. Some are growing. Some are not accelerating with that. So there's various levels of capability there. There's no uniformity, though, and that's the problem."

- IT Director, Technology Services, 5,000+ employees

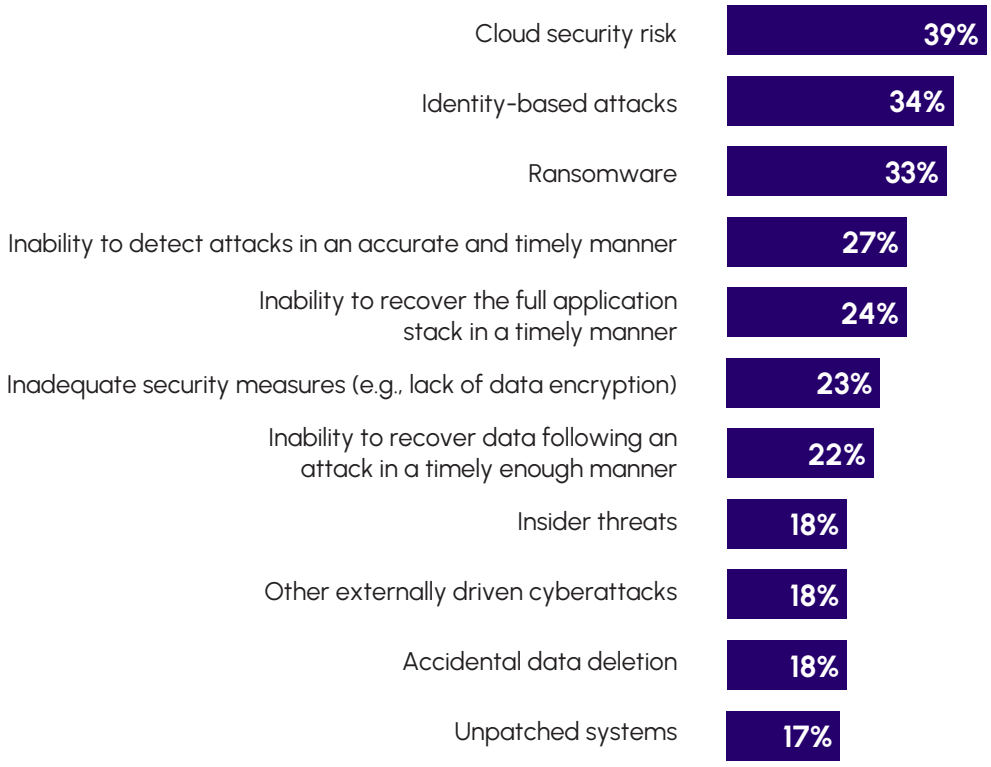
When asked what has the most material impact on their organization's cyber-resiliency, respondents most often indicated the evolving threat landscape (48%, nearly half). This alludes to the pace at which cybercriminals are evolving their approaches, which is in turn leading to new attack vectors – also selected more than one-third of the time.

Given that approximately 90% of respondents indicated that their organization is using a hybrid cloud environment, it is not a surprise that migration to a hybrid-multi cloud model was selected third-most often as having the most material impact on the cyber-resiliency of respondents' organizations.

It is natural that evolving threat vectors and the sprawling attack surface are driving a re-evaluation of technology requirements – as noted by more than 40% of respondents. Along this vein, 46% of respondents indicated that they are investing in new technologies such as AI-powered threat detection to keep pace with the constant changes to the threat landscape – the most frequently selected option.

What do you perceive to be the top threats to your organization's information assets?

Base: n1,326 Senior decision makers who are knowledgeable of organization's global cyber-resilience practices and governance.



Quotes from IT and Security Leaders

"The ability to access information, to breach our security protocols, is significantly increased by virtue of the on-prem environment and people being able to [directly] access our server infrastructure. So, we're moving it to the cloud. And I get that we talk about the cloud as though there's not actually machines somewhere else that are supporting it. But there's not a nine-story office building full of bare metal servers that are all our data that somebody can walk into and know this is all of our data for the last 25 years."

"By moving our primary storage environment away from our premises to multinational companies who specialize in this arena, and whose livelihoods are built on safeguarding our information, permits an increase in the level of trust. We understand that at the end of the day, there's still potential for natural disasters to wipe things out, so you still have to have redundancies built in. But it minimizes the local threat, I think, and it also federates the risk through others. We are a public healthcare institution, so a malware attack costs us [millions]. I would much rather federate that risk across a service provider, rather than us as a service delivery organization."

- Chief Data Officer, Healthcare Organization, 5,000+ employees

"The combination of the old systems, which have been unsupported in part, as well as the increasing distributed [cloud] systems, [is] opening up more loopholes."

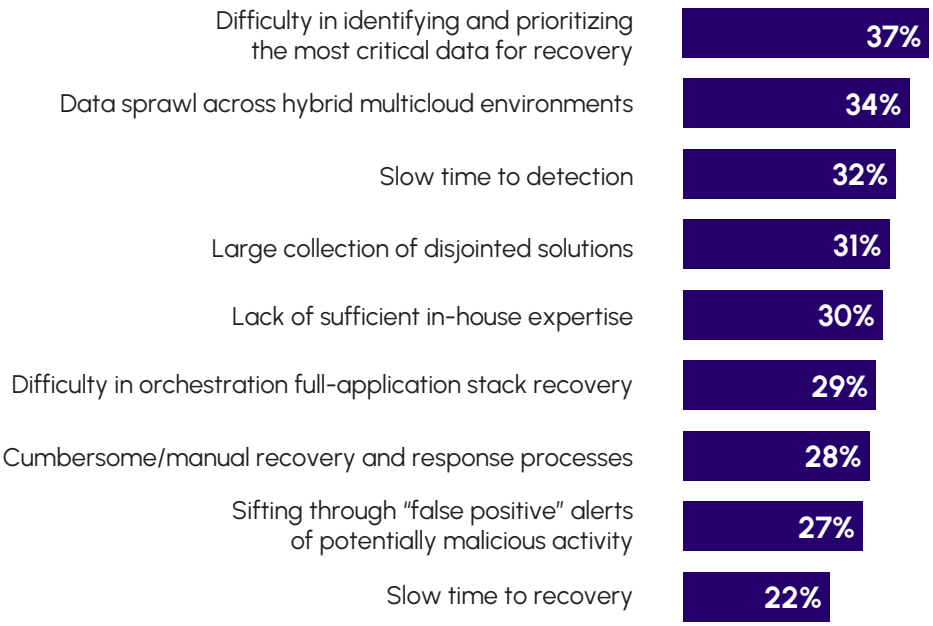
- CIO, Financial Services Organization, 5,000+ employees

It is notable that cloud security risks such as misconfigurations and identity-based attacks were most commonly perceived as top threats to organizations' information assets, even above ransomware, in the survey. As organizations increasingly adopt cloud-based solutions, misconfigurations and vulnerabilities in cloud environments have become a major source of security breaches. This is especially true as complex and sprawling hybrid multicloud environments grow ubiquitous.

At the same time, some interviewees did note the potential benefits of federating risk to a number of public cloud data centers, and public cloud service providers charged with being experts in cloud security. This reflects the fact that, while there are some potential advantages to cybersecurity and cyber resiliency for moving to the cloud, there are unique requirements and risks that need to be factored in.

Currently, what are your organization's top challenges relating to cyber resiliency?

Base: n1,326 Senior decision makers who are knowledgeable of organization's global cyber-resilience practices and governance.



Quotes from IT and Security Leaders

"The difficulty is knowing what data's been lost or compromised."

- Security Director, Consumer Goods Organization, 5,000+ employees

"While primary storage is safe. It's not the only copy of the data. Ultimately you have several copies to the extent that you can have from the source system to the actual end system. You can have 70 odd copies of the data."

- CIO, Financial Services Organization, 5,000+ employees

When it comes to their cyber-resiliency, respondents are most commonly struggling with difficulty in identifying and prioritizing the most critical data to recover – as noted by close to 40% of respondents. This ties into the visibility challenges related to data sprawl across hybrid multicloud environments indicated across a number of questions in this study, and which was noted in this question by more than one-third of respondents.

Slow time to detection was noted by just under one-third of respondents. As indicated in qualitative interviews and by well over one-quarter of survey respondents in this question, organizations are struggling with false positives, making it difficult to keep pace with quickly evolving attack vectors and the ever-expanding and siloed potential attack surface.

Hybrid multicloud cloud environments are compounding issues pertaining to the large collection of disjointed solutions (31%) and cumbersome/manual recovery and response processes (28%). This is particularly true given the complexities of cloud-native applications, resulting in difficulty in full-application stack recovery (29%).

What Approaches are Organizations Using Today?

The cybersecurity toolchain is vast and diverse. In fact, nearly three-quarters of respondents indicated that their organization is using more than 40 cybersecurity tools. The Futurum Group notes that this is driven by a longstanding preference for best-of-breed tools that address point requirements.

72% of respondents indicated that their organization is using more than 40 cybersecurity tools.

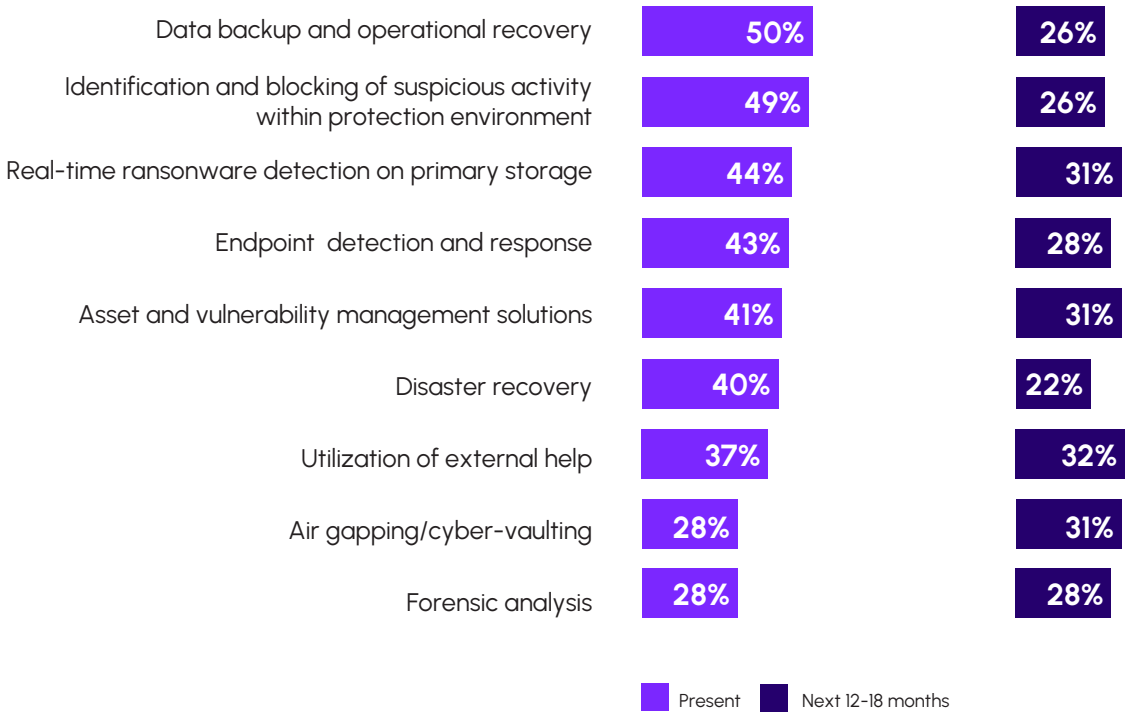
The issue is that this is creating protection gaps and operational complexities. In fact, 70% of respondents indicated that the number of security tools their organization uses inhibits their cyber-resiliency. The Futurum Group notes that adopting a more centralized approach may ease the need for so many tools and so much complexity. Given the fact that attackers are targeting critical data, embedding capabilities for cyber-resilience at the primary storage layer can prove particularly beneficial. In fact, an overwhelming 93% of respondents indicated their intent to use more capabilities that are built-in/native to their organization's information infrastructure over the next 12-18 months.

70% of respondents indicated that the number of security tools their organization uses inhibits their cyber-resiliency.

93% intend to use more capabilities that are built-in/native to their organization's information infrastructure over the next 12-18 months.

One of the important priorities that comes out consistently in The Futurum Group's conversation is the ability to mitigate any potential downtime or data loss resulting from a breach. Data classification and AI stand to play a strategic role here, as does orchestrating full-application stack recovery. The culmination of these capabilities can help organizations detect attacks as quickly as possible, recover faster, and guide and prioritize both protection and recovery operations based on the sensitivity and business value of data.

Which of the following approaches does your organization currently use or plan to implement for cyber-resiliency for your information assets?



Quotes from IT and Security Leaders

"We're using multiple...availability zones. We're always having redundant environments. We have redundant servers available to us at any time. What the CrowdStrike incident taught us is not to have...all eggs in one basket, and maybe have a set of servers that do not have CrowdStrike on it, or do not have it enabled in case of a situation like that."

- IT Director, Technology Services, 5,000+ employees

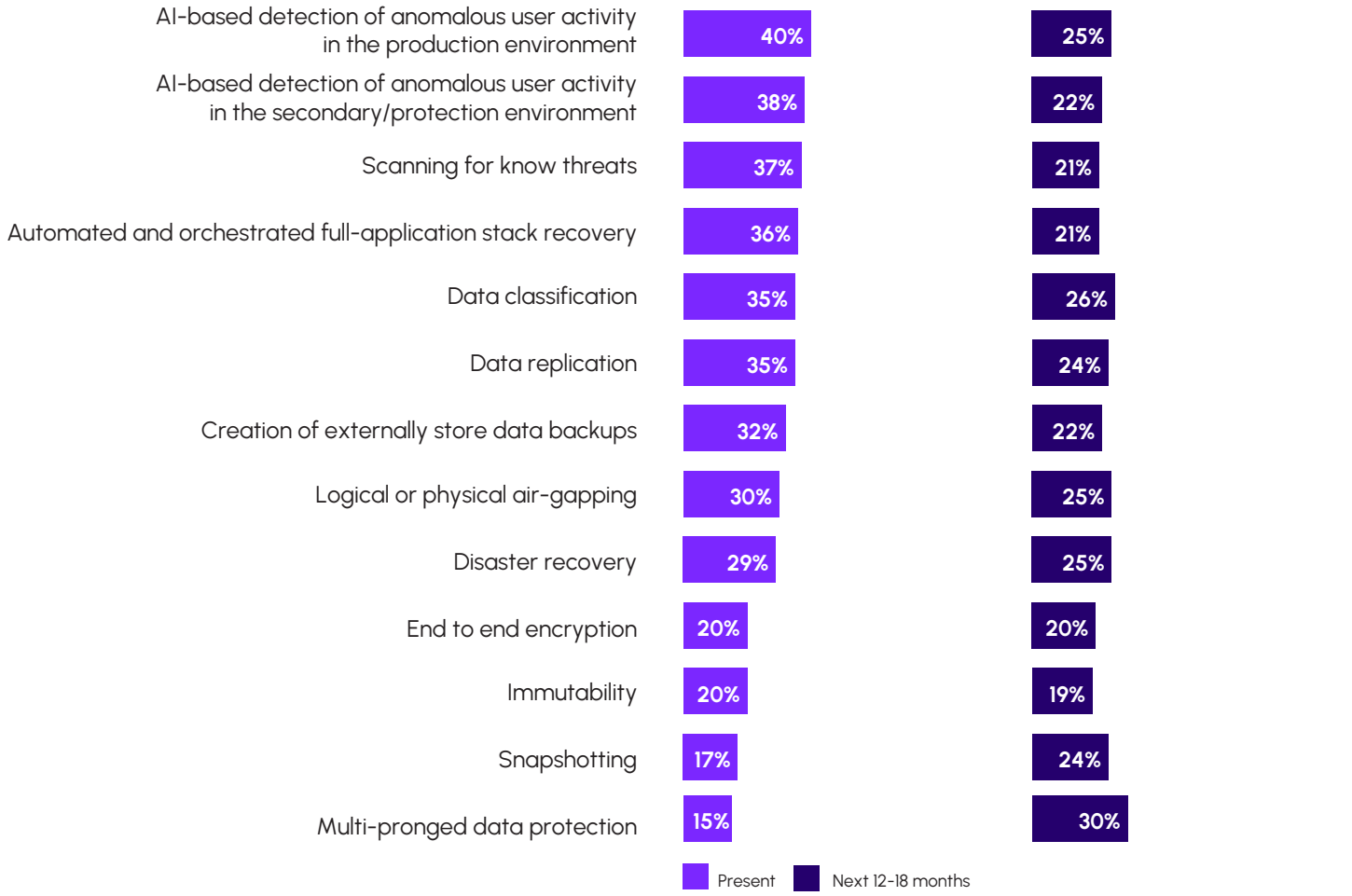
"As an organization, we have a comprehensive data encryption system...both at rest and in transit. So, our HR systems, financial data, they are not very vulnerable to breach, because they remain unreadable to unauthorized users."

"We have data classification categories. We have highly sensitive data, like protected health information, personally identifiable information, financial data, and maybe research and clinical trial data...For such data, we use very strong encryption, both at rest and in transit, and also we employ MFA for access. We also have the role-based access control and continuous monitoring and logging of access and activity."

- CTO, Healthcare Organization, 5,000+ employees

Digging into the approaches that customers are currently using, and that they plan to use moving forward, real-time detection of attacks on primary storage emerged prominently, with 44% of respondents using it today, and 31% planning to use it moving forward. This is critical when it comes to detecting attacks as quickly as possible. In terms of facilitating a comprehensive approach to detection, it complements identification and blocking of suspicious activity within the protection environment, which was also in the top three in use today, being used by approximately 50% of respondents.

Which of the following techniques does your organization currently use or plan to implement for cyber-resiliency for your information assets?



Quotes from IT and Security Leaders

"Our classification of data right now is done on a manual process, so we are relying on an individual to appropriately categorize into one of our four or five categories, and then make decisions based on that. I believe in the future, we will move to AI-supported categorization that then increases our understanding of what data is where, and supports additional safeguards around our most sensitive or regulatory information."

- Chief Data Officer, Healthcare Organization, 5,000+ employees

"You can detect more, but you can have more false positives. So nothing is 100% accurate even in the anomaly detection world……The only way around this is you keep on deploying more and more sophisticated models. It's not an easy thing, it's a very hard thing to do."

- CIO, Financial Services Organization, 5,000+ employees

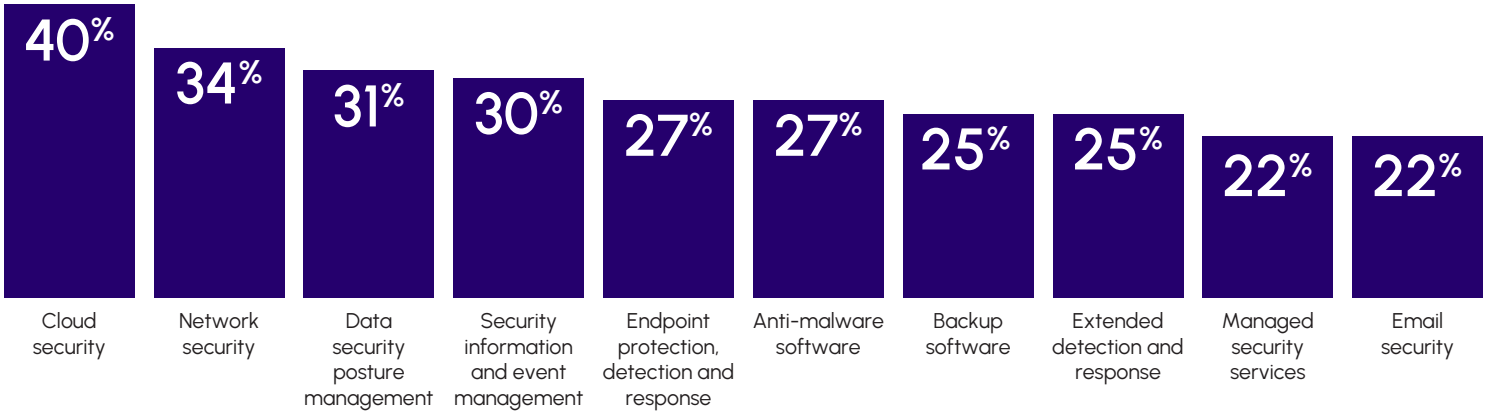
Common themes emerged when respondents were surveyed about the specific techniques used for cyber-resiliency for their organization's information assets. Specifically, these include the use of AI-based detection of anomalous user activity in the production environment – including, but also extending beyond, the storage layer. According to responses, this is the most popular technique in use today, being noted 40% of the time, and one-quarter of respondents intend to add it moving forward.

Data classification is the third-most often used technique today, being noted by 37% of respondents – reflecting the criticality of gaining visibility into, and understanding of, data's sensitivity and importance, for cyber-resilience. Automated and orchestrated full-application stack recovery is the technique most commonly slated by respondents for addition moving forward – underscoring that this is a difficult process, especially across hybrid multicloud environments, and especially when there is pressure to act fast following a cyber incident.

Ecosystem Considerations

What ecosystem integrations are most important to accompany storage-native cybersecurity in the next 12-18 months?

Base: n1,326 Senior decision makers who are knowledgeable of organization's global cyber-resilience practices and governance.



Quotes from IT and Security Leaders

"We're looking more like for cyber platforms that are more encompassing, that include SIEM, DLP, zero trust technologies all in one platform, and we're starting to see the big vendors having those capabilities, and we're the point of evaluating those particular technologies to see where we would go to end up, probably with maybe two platforms instead of 10."

- IT Director, Manufacturing Organization, 5,000+ employees

Simply put, ecosystem integrations are key to providing cyber-resiliency solutions that comprehensively address evolving requirements. Given the value of data, ecosystem strength is particularly critical in a production storage vendor.

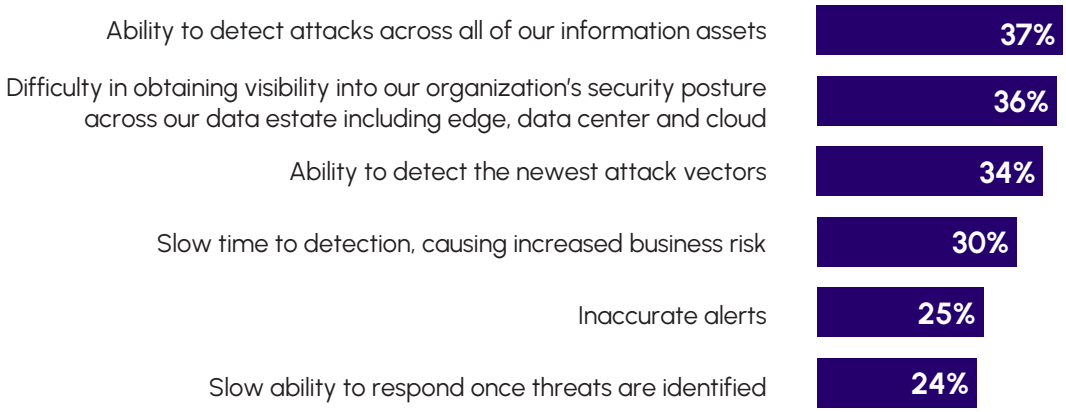
It is not a surprise that respondents prioritized cloud security integrations to accompany storage-native cybersecurity in the next 12-18 months, according to survey feedback. Given the complexities of hybrid multi-cloud implementations, avoiding misconfigurations and obtaining a pulse on the security posture, for example, become critical. These complex environments, coupled with end-user device sprawl and the shift away from a traditional perimeter, make network security integrations key. Integrating DSPM into production storage can provide a centralized view of the security posture across the entire data estate, centralizing visibility, avoiding blind spots, simplifying management, and facilitating proactive protection of data. At the same time, closer integration with SIEM tools improves threat detection and incident response.

State of Attacks

Cyber-attacks are pervasive, and identifying the impact of an attack is even more troublesome. This is due to issues pertaining to identifying the data that was impacted across hybrid multi-cloud environments, and coordinating recovery operations to prioritize the most mission-critical and sensitive data as well as the most business-critical IT services. Our survey feedback is especially notable given that practitioners are often reluctant to admit that an attack has occurred, and even less likely to admit difficulties in recovery; reporting is often done through "rose-colored glasses." Respondents clearly indicate that they are looking to detect attacks sooner, and to optimize their ability to respond in a rapid and surgical manner that is aligned with the organization's most critical assets.

What are your organization's key challenges when it comes to detecting cyber threats and attacks?

Base: n1,326 Senior decision makers who are knowledgeable of organization's global cyber-resilience practices and governance.



Quotes from IT and Security Leaders

"We have a lot of third-party risks, you know. We work with a lot of suppliers. They're offshore and other challenges come through. With respect to that, you try to restrict them as much as possible, but the whole sprawl is just exhaustive."

- CIO, Financial Services Organization, 5,000+ employees

"I have seen a lot of engineers talking about alert fatigue, which is a primary concern we have. But I think as the practice gets into more maturity, and as we gain a lot of context and fine tune the settings and adjust the security system to strike a balance between the sensitivity and accuracy, we do get a lot of stability and reduce the noise."

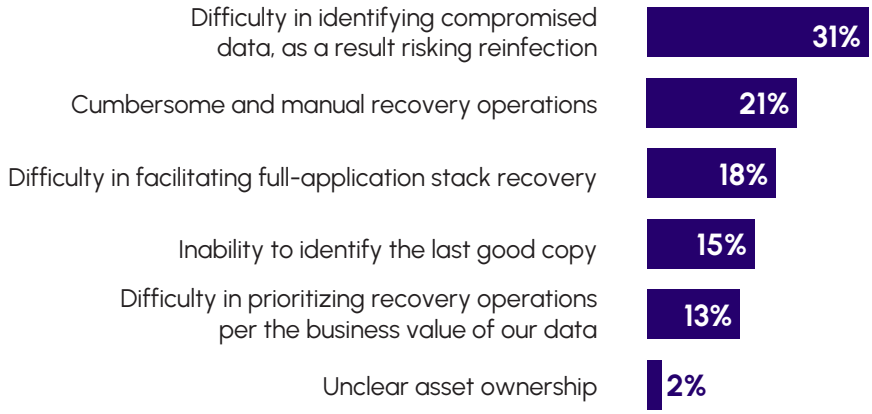
"False positives are definitely wasting a lot of resources, time and effort for product and engineering teams."

- CIO, Financial Services Organization, 5,000+ employees

Despite their likely reluctance to admit it, more than half of respondents indicated having experienced a successful attack. Equally as notable, one in five outright acknowledged that they were unable to recover all of their data following a successful breach. Along this same thread, more than 40% were able to identify what data was compromised across their environment, but it was difficult – and more than 50% were unable to prioritize their recovery operations based on the importance of their data – at least not easily. Only one in five indicated that they did not have to pay a ransom because they were able to recover their data. Additionally, The Futurum Group notes that another scenario for not paying a ransom is that the data compromised is understood as being low value and thus not worth paying the ransom. This is where an effective data classification and prioritization strategy can come into play, helping organizations to make decisions about whether or not to pay a ransom

What has slowed, or do you believe would slow, your cyber recovery?

Base: n1,326 Senior decision makers who are knowledgeable of organization's global cyber-resilience practices and governance.



Quotes from IT and Security Leaders

"One of the biggest ways [we can tell what data was stolen] is having the correct database structure and having the capability to find out when it was last accessed by WHO, but what, by what IP address, and all that goes in accumulation to be able to determine what information was exposed."

- CIO, Financial Services Organization, 5,000+ employees

When asked about the key challenges their organizations face in achieving effective cyber recovery, respondents indicated struggles in accurately identifying compromised data, pointing to the need for robust data classification and monitoring processes to detect and isolate compromised data. They also pointed to the need to automate time-consuming and error-prone manual recovery processes. In particular, recovering entire applications and their dependencies can be complex, especially in modern, cloud-native environments. Respondents pointed to the need to ensure that they can recover applications quickly and effectively.

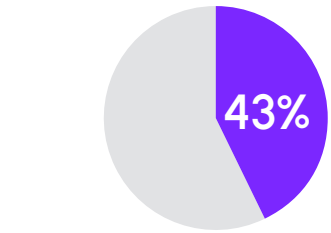
AI Introduces New Cybersecurity Challenges

Practically all (92%) of respondents indicated that they are increasing projects related to AI or generative AI over the next 12-18 months. While not necessarily surprising, this is still staggering, and it is introducing some new challenges from a cybersecurity perspective.

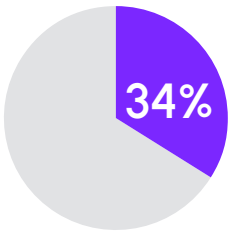
One in four indicated having limited/partial visibility into access and permissions for sensitive/compliance data, as usage of AI increases

What are the top challenges that your organization's AI/generative AI initiatives create from a cybersecurity perspective?

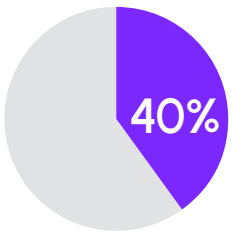
Base: n1,326 Senior decision makers who are knowledgeable of organization's global cyber-resilience practices and governance.



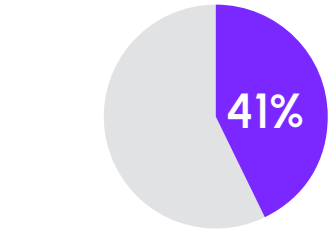
Ability to ensure the availability of, and secure access to, AI models themselves



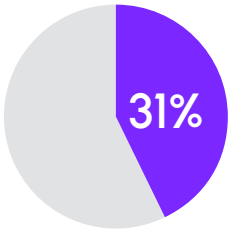
Data that was previously never exposed is now more exposed



Ability to ensure the availability of, and secure access to, training data sets



Ability to meet regulatory and compliance requirements for secure access to private and sensitive data used or training and inference



Data proliferation

Respondent feedback indicates that the key challenges pertaining to cybersecurity include securing AI models and training data, and meeting compliance requirements that are emerging, and that will continue to emerge. Additionally, a vast majority indicated only having limited or partial visibility into access and permissions for sensitive/compliance data. Having a strong foundation of data classification becomes critical to address these challenges.

Budget and Procurement

A very substantial **86%** of respondents expect their organization's spend on cyber-resiliency to change over the next 12-18 months. IT remains highly influential when it comes to information infrastructure budgets, but the influence of security is on the rise. More than half of respondents indicated that this additional budget will come from IT, and one-third indicated that it will come from Security.

The story is similar when we look at the roles influencing information asset security and protection requirements. Three-quarters of respondents indicated IT Management, and more than half indicated the CIO and the CISO. By far, respondents indicated that decisions for new cyber-resiliency technologies for information assets are driven by IT Ops with input from CISO.

Quotes from IT and Security Leaders

"If I looked back, five years ago, we didn't have an explicit budget for cyber, and today, we could easily spend 50 to 100 million without anybody actually blinking."

"We're not necessarily interested in who can bid the cheapest on an RFP to support cyber. We want to make sure that we are partnering intentionally with the correct vendors who will provide us the best security. And that is a marked deviation in process, because we would have, in the past, had significantly fewer dollars, it would have taken significantly more time to free up those dollars, and would have been very focused on price point as a key scoring for an RFP, as opposed to alignment with ongoing data strategies."

- Chief Data Officer, Healthcare Organization, 5,000+ employees

"The real pain point of using AI, you cannot just put it out there and then sit back and relax. You have to really stay on top of it, making sure that you know what you are using the AI for, and that it is doing what it is supposed to do. And you keep monitoring and changing the rules as needed, especially in the area of cybersecurity."

- CIO, Education Institution, 5,000+ employees

Conclusion and Recommendations

Cloud, Complexity, AI: The Triple Threat Demanding New Cyber Resilience Strategies

Complexities of hybrid multi-cloud environments – specifically, the siloed data environments that they result in – create inherent security risks in the form of visibility gaps, operational complexities and tool proliferation. AI creates further issues. Finally, there is a need for better overall understanding and governance-protection of data assets based on data value. Going forward there are a number of recommendations on how to stay ahead of these challenges and improve cyber resiliency.

- Adopt a strategy for automated data discovery and classification, which provides centralized visibility into scattered data sets, and helps to align the strongest protection policies with the most valuable and sensitive data, as well as to guide recovery operations in kind.

- Embrace common security practices. This is especially critical when it comes to simplifying operations and avoiding protection and visibility gaps across hybrid multicloud environments, and vast and complex security toolchains. Consolidating functionalities into fewer tools – especially via a simpler, more unified primary storage layer – can help to streamline operations and avoid protection gaps. The ability to drive integration between the primary storage layer and security tools such as SIEM platforms can also help, from the standpoint of detecting vulnerabilities and attacks, as well as accelerating response and remediation.

- Address complexities, and as a result challenges, when it comes to recovering entire application stacks across hybrid multicloud environments. The ability to protect all components of the application, to accurately map data to applications, and to orchestrate recovery for the application and needed components with data recovery should be looked for. Recovery is not just about restoring data and restarting the application; it is a complicated process spanning both the application and data, and the orchestration to handle what is necessary for the application to resume operation is valuable.

- Investigate ways to use AI to better thwart attackers that are also armed with AI – especially in areas such as threat detection, automating incident response, and identifying the best recovery point. While it is still early days in this space, practitioners are experiencing success with AI capabilities that are built into their products.

- Evaluate tools that allow for attack detection as quickly as possible, given that this is paramount to optimizing recovery point and time objectives. With this in mind, the ability to identify and block attacks in the production environment will continue to grow in focus and importance.

- Analyze existing technology implementations and potential future purchases from the standpoint of their ability to encompass the evolving threat landscape and allow for adaptation. New technology acquisitions and deployments need to integrate with and support the go-forward strategy for cyber resilience, including their ability to address evolving threat vectors, and to mitigate downtime and data loss in the event that a breach should occur.

Important Information About this Report

CONTRIBUTORS

Krista Case
Research Director | The Futurum Group

Camberley Bates
Chief Technology Advisor | The Futurum Group

PUBLISHER

Daniel Newman
CEO | The Futurum Group

INQUIRIES

Contact us if you would like to discuss this report and The Futurum Group will respond promptly.

CITATIONS

This paper can be cited by accredited press and analysts, but must be cited in-context, displaying author's name, author's title, and "The Futurum Group." Non-press and non-analysts must receive prior written permission by The Futurum Group for any citations

LICENSING

DISCLOSURES

The Futurum Group provides research, analysis, advising, and consulting to many high-tech companies, including those mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

NetApp®

ABOUT NETAPP

NetApp is the intelligent data infrastructure company combining unified data storage, integrated data services, and CloudOps solutions to turn a world of disruption into opportunity for every customer. NetApp creates silo-free infrastructure, then harnesses observability and AI, to enable the best data management. As the only enterprise-grade storage service natively embedded in the world's biggest clouds, our data storage delivers seamless flexibility and our data services create a data advantage through superior cyber-resilience, governance, and applications agility. Our CloudOps solutions provide continuous optimization of performance and efficiency through observability and AI. No matter the data type, workload, or environment, transform your data infrastructure to realize your business possibilities with NetApp. Learn more at www.netapp.com or follow us on X, LinkedIn, Facebook, and Instagram

Futurum

ABOUT THE FUTURUM GROUP

The Futurum Group is an independent research, analysis, and advisory firm, focused on digital innovation and market-disrupting technologies and trends. Every day our analysts, researchers, and advisors help business leaders from around the world anticipate tectonic shifts in their industries and leverage disruptive innovation to either gain or maintain a competitive advantage in their markets.

Futurum

CONTACT INFORMATION

The Futurum Group LLC | futurumgroup.com | (833) 722-5337 |