TheFuturum Group

Overcoming Data Protection Fragmentation for Cyber-Resiliency

AUTHOR

Camberley Bates
VP and Practice Lead, Data Infrastructure | The Futurum Group

Steven Dickens
VP and Practice Lead, Hybrid IT | The Futurum Group

Krista Macomber
Sr. Analyst, Data Security and Protection | The Futurum Group

IN PARTNERSHIP WITH

Commvault®

NOVEMBER 2023

Executive Summary

With cybercrime continuing to be on the rise, the need for data security and recoverability has taken center stage and is not going away any time soon. This is only exacerbated by the growth of cloud deployments, use of software-as-a-service (SaaS) applications, and a global economy.

To explore these topics in greater depth, The Futurum Group, in collaboration with Commvault, surveyed 205 C-Suite, VP and Director-level IT Operations and Security professionals globally, and conducted five in-depth interviews. Specifically, we dug into how data sprawl and fragmentation of data protection tools are threatening organizations' overall cyber-resiliency, while also influencing how IT Operations and Security teams organize and collaborate, from both the strategic and the tactical, day-to-day perspectives.

More than 90% of respondents surveyed indicated a level of concern that their organization will suffer a ransomware attack – and nearly 40% indicated being extremely concerned. Practically all (97%) indicated concern about the ramifications/fallout resulting from a ransomware attack.

While the threat and rising impacts of ransomware and other cyber-attacks has been well-established in the market, the survey uncovered that a staggering 98% of respondents indicated that data recoverability influences their ability to be resilient against ransomware attacks, with three-quarters of respondents indicating that it is very or critically influential.

The research clearly indicates that data protection has become recognized by C-Level leadership as an important component of the security infrastructure. This is progress, but 88% of these "C-Level" respondents still indicated a need for their data protection to be changed; it is too complex, the level of risk is too high, and it is too expensive.

These complexities and costs stem largely from sprawl of data, as well as of the number of data protection tools in use by the average enterprise. The Futurum Group's consulting and conversations with IT Operations teams points to an average of approximately three or four data protection tools in use among most large enterprise IT organizations, with this multitude of tools typically being driven by the need to protect specific applications, infrastructure or workloads. According to 90% of respondents, this fragmentation of data protection tools impacts cyber-resiliency. And operations are on a path to only get worse, due to the ever-growing complexity of multi-hybrid cloud environments. Nearly half of respondents indicated that they are using more than 150 SaaS providers, 36% indicated that they are using more than three IaaS providers, and 75% stated that both of these figures will grow over the next 12 months.

In sum, reducing the silos and complexity of data protection is necessary for enterprises to maximize their cyber-resiliency, as their data grows increasingly fragmented across a heterogeneous mixture of on- and off-premises applications and infrastructures.

Key Takeaways

- The link between data protection and overall cyber-resiliency is well-established at the highest executive ranks.
- Fragmentation of data and of data protection tools is a key threat to cyber-resiliency, and with the growth in use of cloud-hosted SaaS apps, is only getting – and will only continue to get – worse. Change is needed, and leadership recognizes the need for change.
- Collaboration between IT Operations and Security teams is necessary in order to prevent and recover from cyber-attacks. Long-standing silos between these two teams are beginning to break down, thanks to a shared vision and shared goals for security. There is still room for improvement, however. For example, integration of systems and processes remains in progress.

Survey Overview

As noted in the Executive Summary of this report, The Futurum Group surveyed 205 C-Suite, VP and Director-level IT Operations and Security professionals. Surveys were collected in September 2023. Specifically, 84% of respondents held C-Level titles, 18% held security-related titles, and 14% held VP/IT-Director level titles. We focused on the C-Suite to get the view from the top, given the visibility and critical importance of cyber-resiliency.

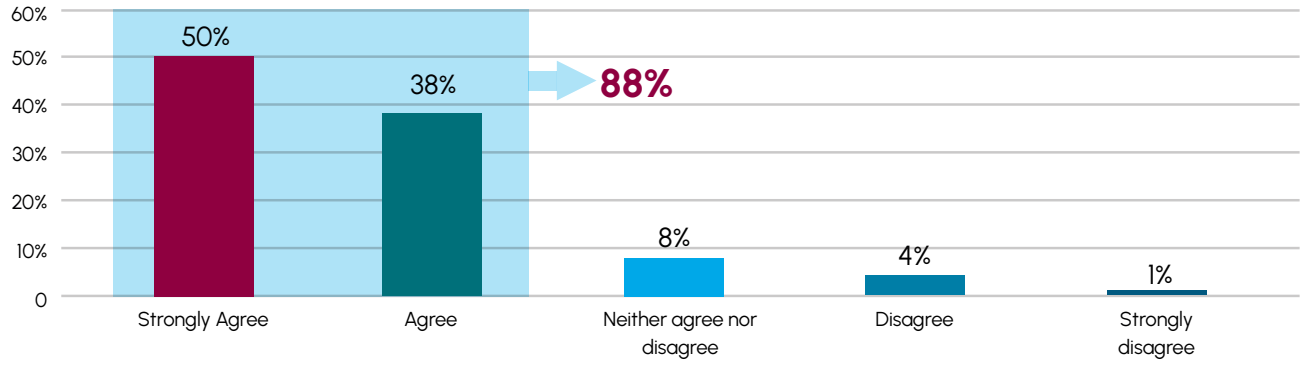
Well over half (57%) of respondents came from organizations with 1,000-5,000 employees. The major geographical regions (the Americas, EMEA, and APAC) were fairly evenly represented.

Survey Findings

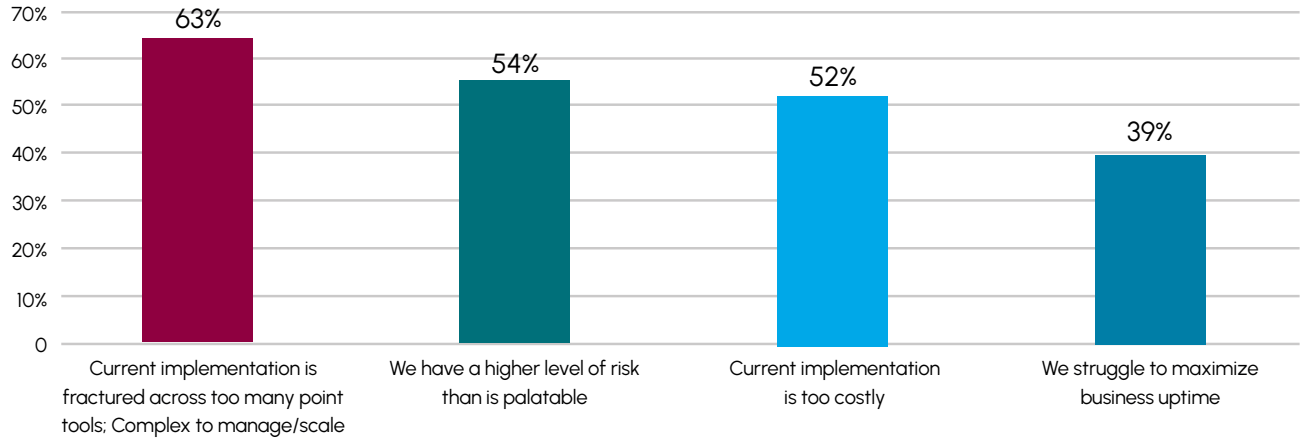
The Fragmentation of Data Protection Solutions is Impeding Cyber-Resiliency

Nearly 100% of respondents indicated that they view data backup and recovery as a part of the security infrastructure. While this is good validation, responses also indicate that this respondent base view data protection as a component of the infrastructure that needs to be changed, however – with more than 60% of respondents pointing to the fragmented and, as a result, complex nature of data protection implementations as a problem. This complexity is driving up the cost of data protection implementations that, based on The Futurum Group's conversations with IT practitioners and responses from more than half of this respondent base, has been perceived as too high since the inception of data protection. it is also resulting in the arguably more alarming result of creating an unpalatable level of risk, as noted by 54% of respondents.

There is a belief within company leadership thar the approach to data protection needs to be changed? Agree or disagree?



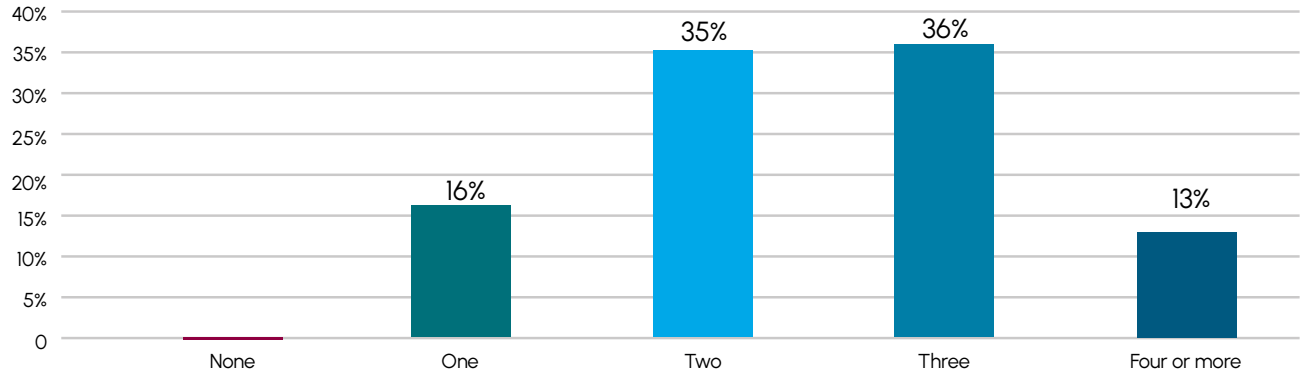
You indicated that company leadership believes that the approach to data protection needs to be changed. Which of the following are the focus for change?



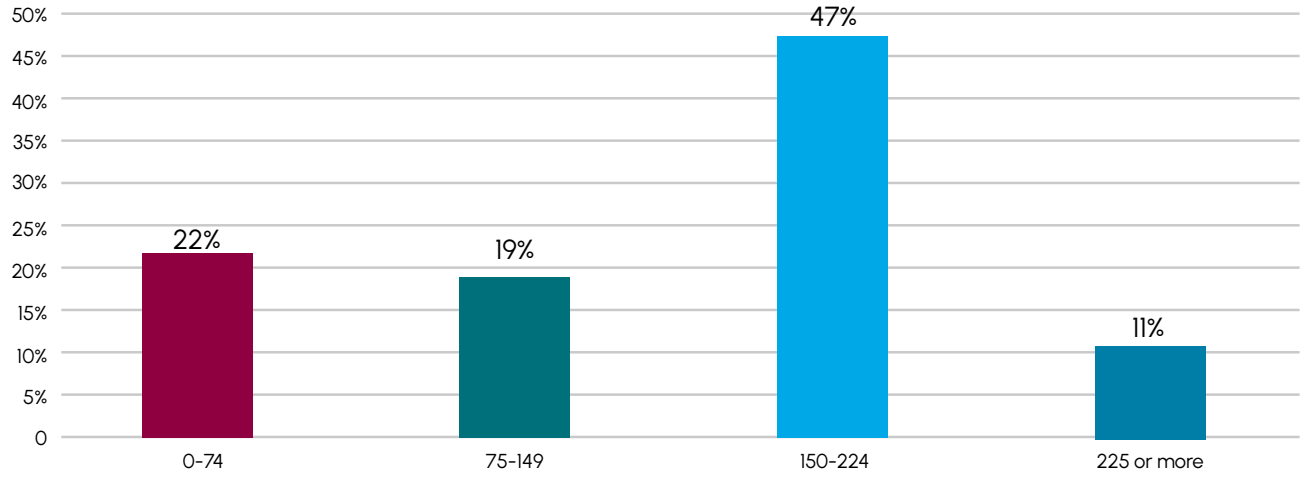
Data – and Data Protection – Fragmentation is Being Exacerbated by Booming Cloud Usage

The number of cloud providers in use is already vast, and approximately 75% expect it to further increase over the next 12 months. Enterprises continue increasing their use of cloud-based applications and infrastructure for a variety of reasons including increased scalability, agility, and ease of use and adoption. To meet this demand, cloud providers are responding with a range of new services, capabilities, and pricing models – contributing to proliferation of the number of providers that enterprises are working with. This includes the ongoing rise of cloud-hosted applications and cloud environments that are specialized for specific industries such as healthcare, finance, and education. At the same time, these cloud-hosted resources coexist with on-premises resources.

How many public cloud IaaS providers are you currently working with?

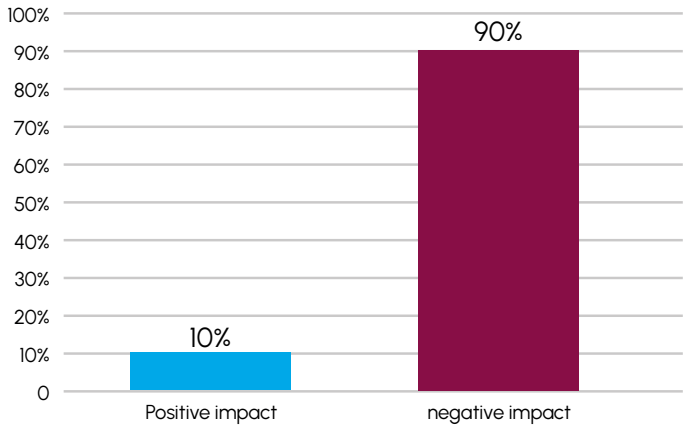


How many public cloud SaaS providers are you currently working with?

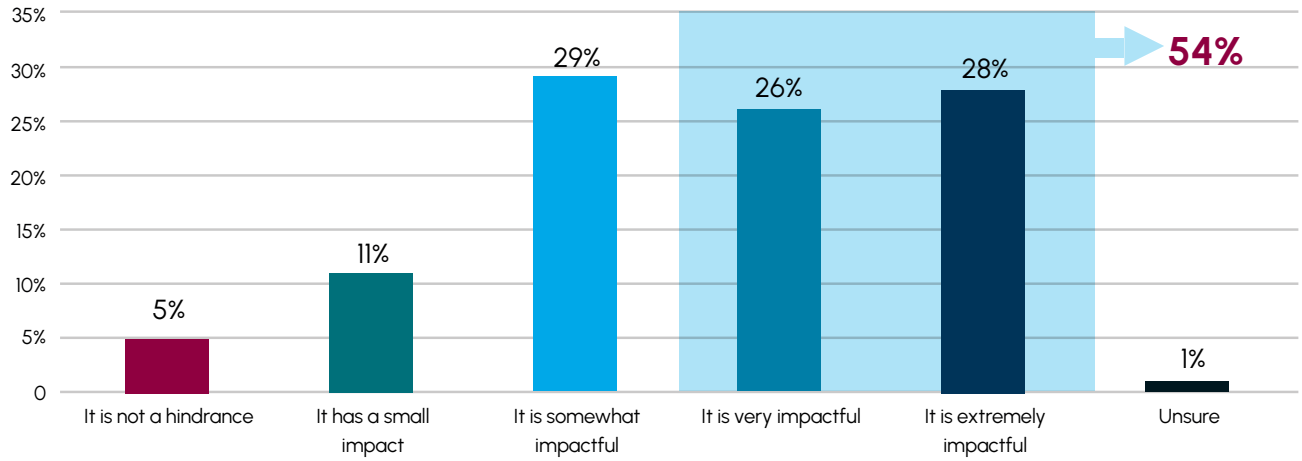


The Futurum Group sees this multi-hybrid cloud reality as contributing to a growing number of siloed data protection tools. We already see most enterprises using multiple data protection solutions – often three or four, in fact – in order to be able to protect environments, and for various, specific capabilities. Just as the advent of virtualization brought new protection requirements, and as a result new protection tools, we are seeing that new data protection tools are being adopted for the specific purpose of protecting a SaaS application, with Microsoft 365 being the prime example. We are also seeing that data protection solutions are increasingly being evaluated for their ability to protect cloud infrastructure alongside on-premises data center environments.

On a scale of 1 to 10, one in five survey respondents indicated that their data protection tovols are a 10 – that is, extremely fragmented across public and hybrid cloud deployments. This is significant because, as noted by more than 90% of respondents, this fragmentation of data protection tools is having a direct, negative impact on their organization's cyber-resiliency.



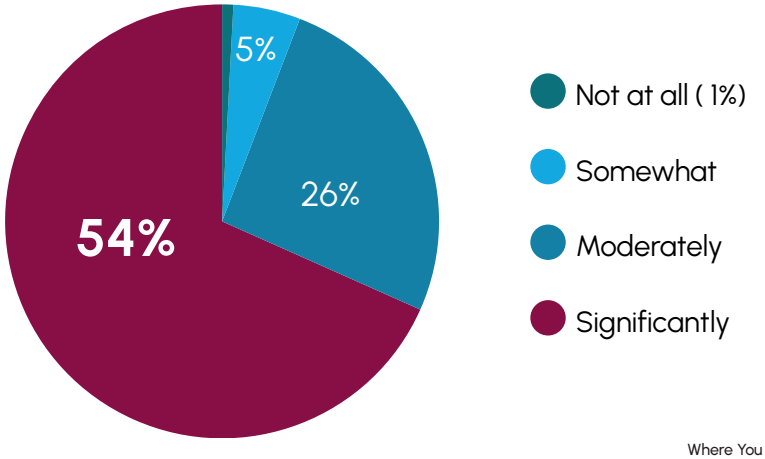
To what degree do you believe that data fragmentation hinders your organization's cyber-resiliency



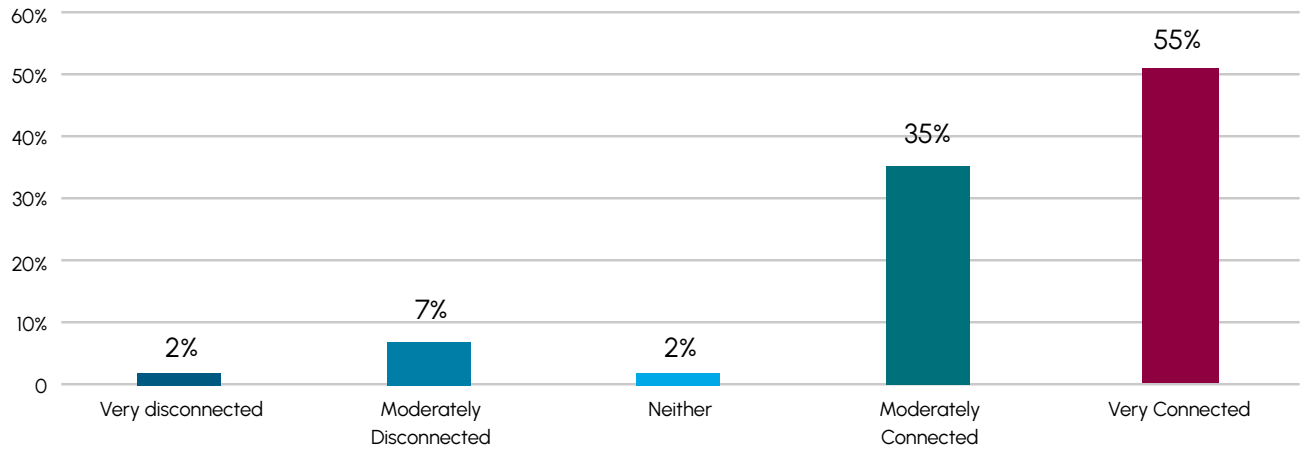
Ransomware is Driving SecOps Collaboration, but Work Remains for Base-Layer Systems Integration

In part due to the important role that data protection plays in organizations' cyber-resiliency, The Futurum Group is seeing increasing alignment between historically siloed IT Operations and security teams. Specifically, a staggering 99% of respondents indicated that the relationship between these teams has grown more connected over the past 12 months. This is because, as the threat landscape continuously evolves, and as cyberattacks become more sophisticated, a holistic approach to security is required in order to identify, mitigate, and respond quickly and effectively to vulnerabilities and breaches. There is still more work to be done, however – as evidenced by the fact that nearly half of respondents still indicated that nearly half of respondents still indicated that this relationship is moderately to not connected.

To what extent has this relationship grown more connected over the past 12 months?



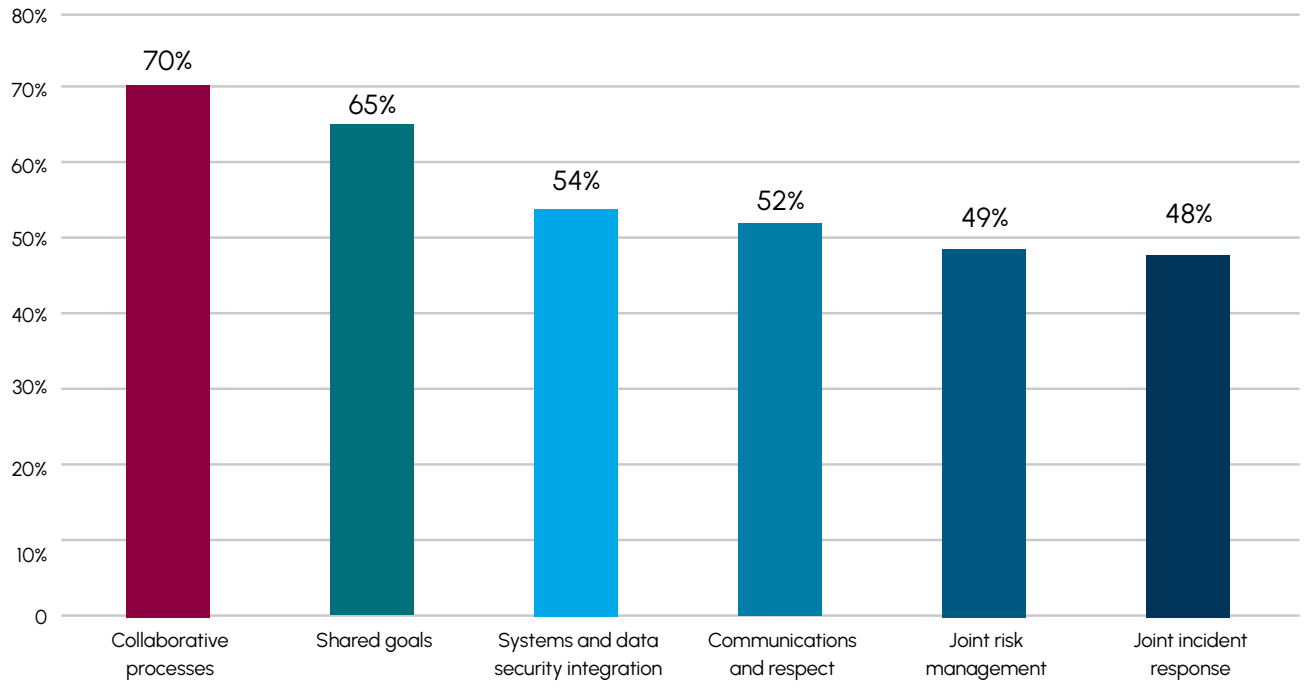
Which of the following best describes the current working relationship between your IT operations and security teams in general?



While the common goal of keeping the organization's IT infrastructure and data safe and secure is fostering greater collaboration between these teams, historically they have not spoken the same language or used the same tools. The role of IT Operations has been to maintain system and data availability, while security teams have focused on protecting systems and data from threats. It has not been uncommon for these differing perspectives to lead to differing priorities and friction, in the past.

This is beginning to change, starting with the establishment of shared goals and a common vision for security, which is beginning to nurture collaboration. This is evidenced by survey feedback, as well as qualitative conversations that The Futurum Group has had with IT Operations and security team stakeholders.

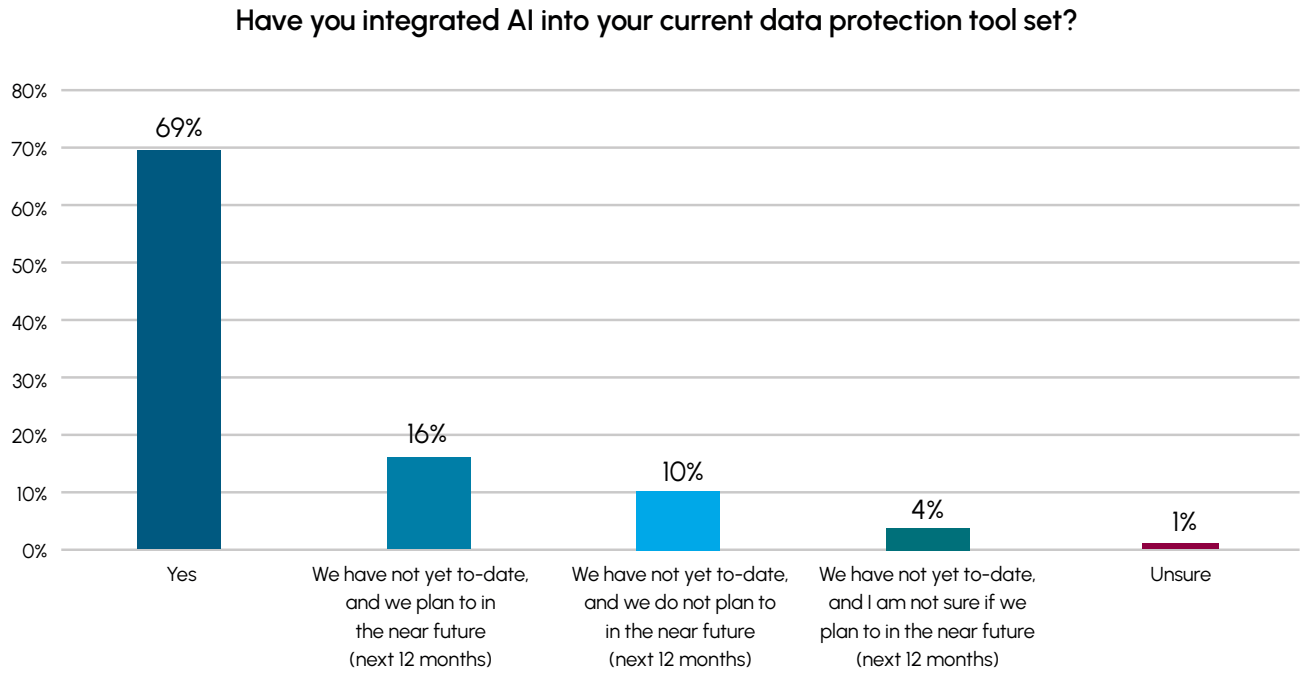
You indicated that the relationship between your company's IT operations and security teams could be described as "connected." Which of the following best describes that relationship?



The large majority of respondents indicated that, while collaborative processes and shared goals are steadily on their way to being established, only about half indicated that their organization has integrated their systems and data security. Further leaning into shared tools and processes, such as security information and event management offerings that provide a more holistic view across the IT environment in order to uncover, analyze, and respond to security threats, is a key area of opportunity to improve joint response to, and remediation of, incidents. The Futurum Group also notes opportunity for IT operations teams to provide security teams with more insight into the IT environment, so that security teams can better understand the organization's risk posture. Similarly, security teams can provide IT operations teams with more threat intelligence data, as well as guidance on how to mitigate vulnerabilities, in order to position the organization to respond more quickly to attacks and to shift to a more proactive, as opposed to reactive cyber-resiliency posture.

Utilization of AI is in the Works for Most Customers

The entire IT market is abuzz with artificial intelligence (AI), and the data protection and security spaces are no exception, with vendors across the spectrum messaging about how they are integrating AI functionality into their offerings. Against this backdrop, nearly 70% of respondents indicated that they have integrated AI into their data protection toolset. The Futurum Group notes that this is likely inflated due to the industry-wide AI-washing, but this figure is still a bullish indicator of customers' appetite to utilize AI to augment and otherwise improve their cyber-resiliency.



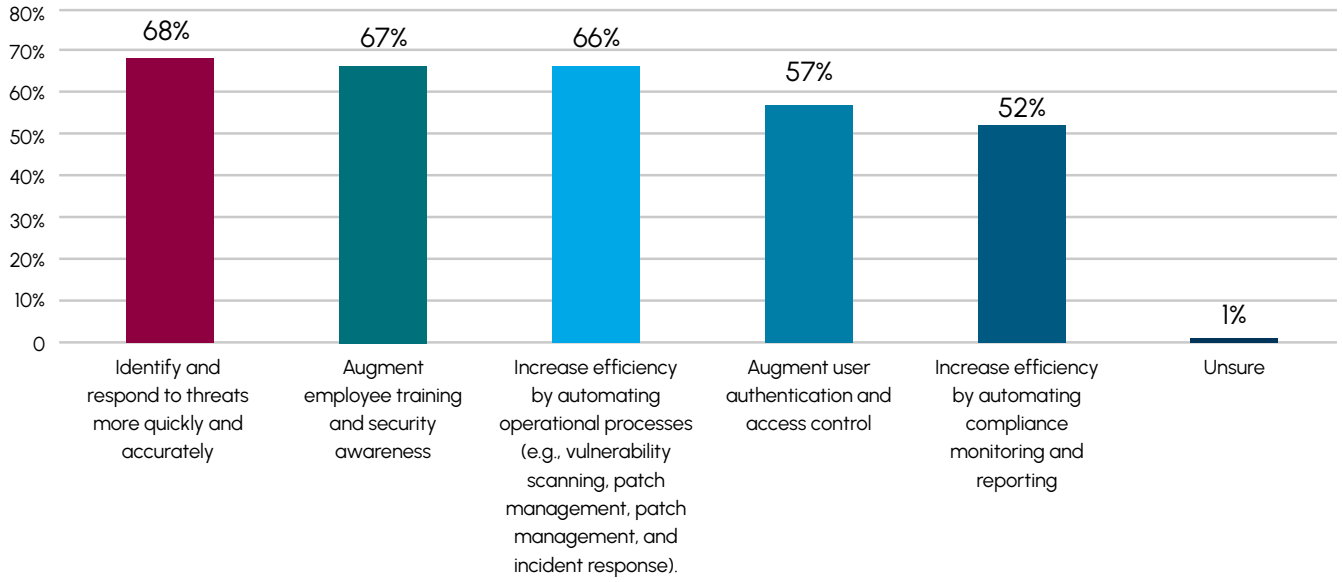
Survey feedback indicates that customers are looking to infuse their data protection and security tools with AI for a number of reasons. The most popular benefit either perceived or expected from AI is the ability to identify and respond to threats more quickly and accurately. With the ongoing need to shift protection operations from being reactive to being more proactive, it is not surprising that capabilities such as the ability to detect anomalous and potentially nefarious user activity within the environment. While the anomaly detection capabilities currently built in to data protection software have largely been based on machine learning, they stand to be augmented materially by AI – for example, through enhancing the ability to learn and track how user behavior and attack methodologies change.

Another area for AI to potentially add value is around augmenting employee training and security awareness. For example, it can be used to personalize training content per individuals' specific needs and risk profile as it pertains to their job function and risk exposure – as well as to provide feedback and identify areas where an employee might require more training. It can also be used to make training content more relevant, including to new types of attacks that emerge, and to make it more engaging and immersive. For example, it could be used to simulate phishing emails, or as a chatbot for on-demand support and training.

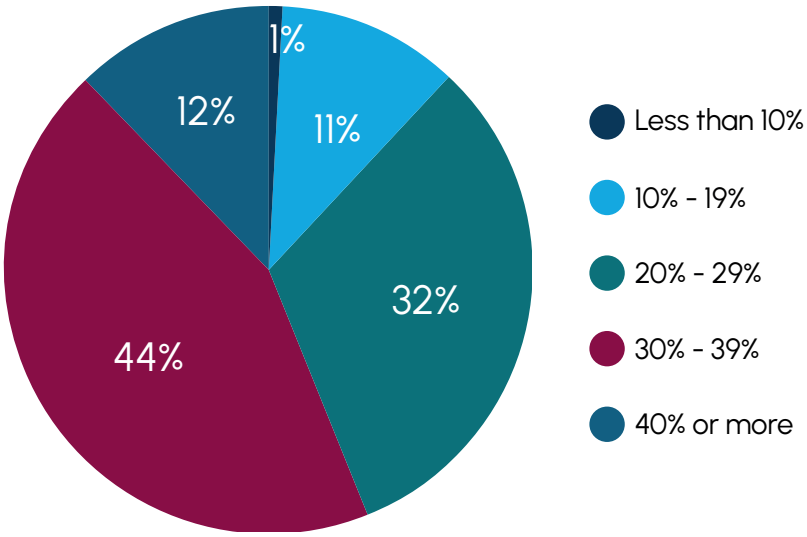
In addition to these specific applications, AI can also be used to increase efficiency by automating many of the tasks associated with employee security training, such as developing and delivering training content, tracking employee progress, and generating reports. Along a similar vein, it can be used to increase efficiency by automating day-to-day operational processes associated with data protection – a huge win because of how strapped for time IT Operations teams are today.

It is relevant to add that, for its potential value, AI also opens up issues around data access, privacy and control with employees potentially working with AI outside of IT's control. Enhanced policies and regulations will be needed.

How is AI improving, or how would you expect AI to improve, your organization's security?



What percentage improvement do you expect AI to bring to your security efforts over the next 12 months?



Conclusion

The recognition of the fact that the ability to recover from backups is a critical part of a cyber-resiliency strategy may seem obvious, but the fact that it is echoed by the senior-level individuals who participated in this survey is significant. At the same time, The Futurum Group recognizes that there may be an assumption among leadership that data protection is established as a component of the overall security strategy, and that IT operations and security teams are actively collaborating, without fully understanding if their organization has been making any of the procedural and technological changes necessary to facilitate this collaboration and improve cyber-resiliency.

The understanding that there are too many data protection tools in use and that they create complexity that threatens the organization's resiliency is a bright spot indicating that executive leadership has been listening to the infrastructure teams and see the problem. Leadership recognizes that, while their organization is taking steps forward in SecOps collaboration, it is just the first step and there is more work to be done from a technology perspective. This is important, as addressing gaps and areas for potential exposure, and marrying IT operations' knowledge of the organization's IT infrastructure with security teams' expertise in identifying and mitigating risks, are both critical to creating a resilient security posture.

Addressing the need for operational simplicity will be increasingly important, in order to free up time for resource constrained IT Operations teams to address evolving cyber-threats. AI is largely still in development, in terms of technology solutions and use cases. However, executive leadership clearly views it as an opportunity to help both IT Operations and Security teams to react more quickly to attacks, and to be more preventative in terms of enhancing end-user training.

Recommendations for IT Operations and Security Professionals

- **Adopt a comprehensive approach, evaluating each of the following in detail, for security that spans:**
  - Data loss prevention.
  - Identity management and privileged access management.
  - Security of data in motion in addition to rest, considering the number of applications and services that utilize streaming data that needs to be secured.
  - Patching and device security handled in a way that does not disrupt user productivity.
  - Supply chain resilience.
  - Promotion of security awareness with videos, roadshows, and incentivizing employees.

- **Balance the approach for security to being proactive, in addition to reactive.**
  - Reactive is how well are the gates built around the moat so to speak. It is important, and it is largely where the backup strategy and network protection play in.
  - Proactive is becoming more important, however, especially in regulated industries with personal identifiable information (PII). Capabilities such as data classification and network isolation play in, as do penetration, phishing and controls testing.

- **Establish an approach to security that is inclusive of all business units, including:**
  - Garnering feedback on what data is critical to the business to secure, in order to avoid productivity loss, to avoid protection gaps, and to focus on recovering the most critical assets first.
    - While critical, data cataloging and data loss prevention are not easy. They are already broad areas, and they are becoming more sophisticated (e.g., with adoption of email, web, SaaS applications). At the same time, access controls cannot be tightened up so much that it inhibits business users from doing their job. And the reality is that exceptions to access permissions will be needed, and it is likely that IT might forget to remove them. Tools and permissions will need to be evaluated and adjusted per business feedback. Automated versus manual auditing and scanning has become a necessity.
  - Ensuring that LOB managers are apprised of the risk and liabilities involved with adopting new technologies, such as SaaS applications, and processes.
  - Building an appreciation across the enterprise for the fact that everyone has a role to play; they cannot just sit on the sidelines waiting for IT.

- **Create the environment for participation in recovery exercises by C-Suite leadership including the CMO, CFO, Chief of HR, etc. This can help to cultivate preparedness for how the full enterprise will respond to an attack. Furthermore, this provides a form for C-Suite leaders who are sitting on other boards to share what it is learning from peers about breach response.**
  - On that note: utilize the fact that CIOs and CISos are now sitting on the board, to help build awareness among nontechnical board members of potential security risks and their repercussions.

- **If audit requirements are not already in place, it is likely that they will be coming up. With this in mind, work closely with regulators on evolving requirements and the types of tools to be adopted. Conducting mock audits can help teams understand gaps in capabilities, processes, and policies.**

- **Utilize the additional collaboration with the business to drive a security-oriented culture that sets the expectation, top-down, for productive and synergistic collaboration between security and operations teams.**
    - Clear roles and delineations with measurable goals and outcomes should also be established, for most effective collaboration. Specifically, having security and IT Operations teams spend time with each other to understand each other's challenges, as well as synergies between the two and opportunities to collaborate, is helpful.
        - Security teams should be risk advisors responsible for uncovering, assessing, and mitigating vulnerabilities, not maintaining IT tools and being systems administrators. Furthermore, the role of IT Operations should evolve from policing systems to enabling secure access to information and data to the right employee at the right time. Compliance with threat auditing requirements will help to drive the realization that security teams cannot work on these tech issues.
    - Tools should be evaluated jointly by Security and IT Operations teams, with business units providing input on how data is being used, and its criticality. On that note, there is budget for new security tools; it does need to be justified though, which can prove to be a challenge. In these conversations, there is some crossover between IT Operations and Security, and the Board of Directors has a role to play, as well.

- **In order to drive continued awareness of risk factors and how to deal with them, consider outsourcing the Security Operations Center (SOC) to a third party. This can help keep up with day-to-day issues and alarms and expedite triaging. It also can have the additional benefit of being more cost-effective versus employing internal help to run a SOC 24/7.**

- **With the AI-washing that is occurring, bear in mind that AI and ML are different, with AI allowing data security tools to be able to analyze and take action without intervention from administrators. For example, for network analysis, AI and pattern recognition can be used to correlate events across the network and identify potential data leaks/ breaches and take subsequent action. This addresses a task that is difficult for administrators to achieve, considering how rapidly data is streaming, providing little time to identify and respond to attacks. Consider factoring in pattern recognition, generative AI, and other such capabilities into RFPs for use cases such as event management, vulnerability assessment, and penetration testing.**

Important Information About this Report

CONTRIBUTORS

Camberley Bates
VP and Practice Lead, Data Infrastructure | The Futurum Group

Steven Dickens
VP and Practice Lead, Hybrid IT | The Futurum Group

Krista Macomber
Sr. Analyst, Data Security and Protection | 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.

Commvault®

ABOUT COMMVAULT

Commvault (NASDAQ: CVLT) is the gold standard in cyber resilience, helping more than 100,000 organizations to uncover, take action, and rapidly recover from cyber attacks—keeping data safe and businesses resilient and moving forward. Today, Commvault offers the only cyber resilience platform that combines the best data security and rapid recovery at enterprise scale across any workload, anywhere with advanced AI-driven automation—at the lowest TCO.here

The Futurum Group

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.

The Futurum Group

CONTACT INFORMATION

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