IT and Security Teams Increasingly United in Battle Against Sophisticated Cyberthreats, Research Finds

January 25, 2024 at 8:30 AM EST

New report from Commvault and Futurum shows organizations rallying around AI to counter AI-driven threats in 2024

TINTON FALLS, N.J., Jan. 25, 2024 /PRNewswire/ -- Commvault, a leading provider of cyber resilience and data protection solutions for hybrid cloud organizations, today released a new report that found the traditional silos between ITOps and security teams are beginning to break down, as organizations realize the importance of increased collaboration to combat the onslaught of more sophisticated cyber attacks.

Commissioned in partnership with The Futurum Group, the report, "Overcoming Data Protection Fragmentation for Cyber-Resiliency," surveyed over 200 C-Suite and senior-level IT executives (more than half of which were CIOs, CSOs, and CISOs) in the Americas, EMEA, and Asia-Pacific regarding their cyber resilience positions.

According to the report, nearly all (99%) respondents indicated that the relationship between ITOps and security has grown more connected over the past 12 months. For those who described the relationship between ITOps and security as "connected," 64% stated they now have shared goals for maintaining the company's security and 70% stated they have joint processes and procedures in place for daily operations. However, there is still work to do. For example, only 48% stated they have established joint processes and procedures in place to mitigate or recover from an incident.

"Synergies between ITOps, security teams and the C-suite has never been more crucial as cyber criminals are deploying more sophisticated attacks powered by AI," said Javier Dominguez, Chief Information Security Officer, Commvault. "But, with 19 cyber attacks every second, breaches are inevitable. It's critical that ITOps and security teams jointly think about recovery as part of an end-to-end security practice tied to the NIST framework."

Using AI to Advance Security

AI is expected to be a major theme in 2024 with more than two-thirds (68%) of respondents indicating the technology will boost their security efforts by identifying and responding to threats more quickly and accurately. Respondents identified several ways AI could improve their organization's security posture, including:

- Augmenting and automating employee training and security awareness (67%)
- Increasing efficiency by automating day-to-day operational processes associated with data protection (66%)
- Augmenting user authentication and access control (57%)
- Augmenting compliance monitoring and reporting (52%)

Data Fragmentation Creates Cyber Resilience Challenges

Organizations continue to grapple with fragmented data protection solutions, which not only creates management complexities but cyber resilience challenges. More than 90% of respondents say fragmentation of data protection tools has a direct, negative impact on their organization's cyber resiliency and 54% indicated that fragmentation hinders their organization's cyber resiliency efforts.

"Utilizing a host of fragmented data protection products can drive up costs, create management nightmares, give bad actors more avenues to exploit, and slow down recovery," said Krista Macomber, Research Director, The Futurum Group. "This research serves as a good reminder that organizations should consider a modern platform that can reduce fragmentation, protect a vast array of workloads across any location, predict threats faster, and speed up response and recovery times."

To review the full survey results, click here.

Methodology
Commvault sought to learn how data sprawl and fragmentation of data protection tools are threatening organizations' overall cyber-resiliency. To facilitate this research, Commvault commissioned The Futurum Group to conduct an independent effort in finding answers to these important issues.

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.

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 cyberattacks—keeping data safe and businesses resilient and moving forward. TodayCommvault 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.

View original content to download multimedia:https://www.prnewswire.com/news-releases/it-and-security-teams-increasingly-united-in-battle-against-sophisticated-cyberthreats-research-finds-302043914.html

SOURCE COMMVAULT

Media Contact: Kevin Komiega, Commvault, 978-834-6898, kkomiega@commvault.com. Investor Relations Contact: Michael J. Melnyk, CFA Commvault, 646-522-6160, mmelnyk@commvault.com