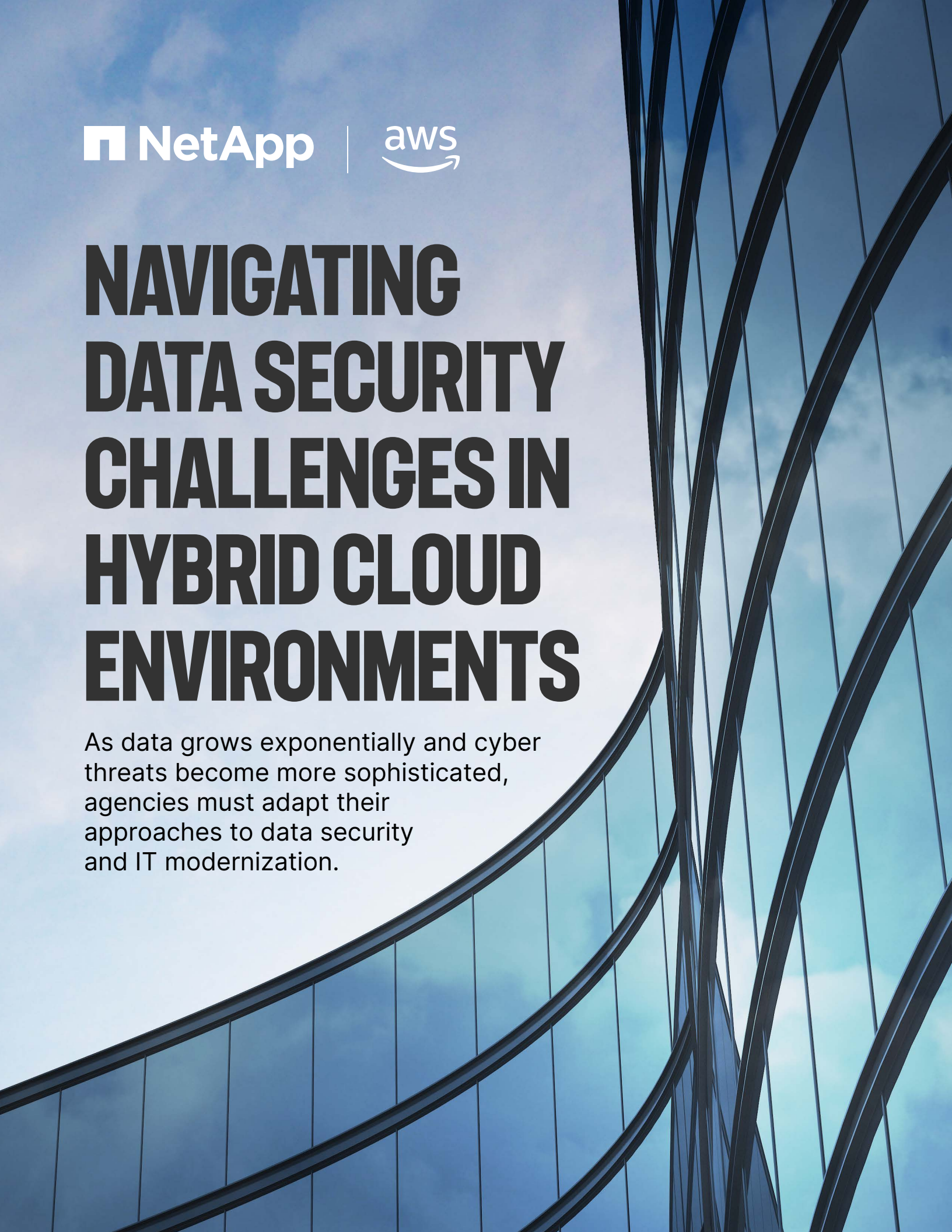

NetApp | aws

NAVIGATING DATA SECURITY CHALLENGES IN HYBRID CLOUD ENVIRONMENTS

As data grows exponentially and cyber threats become more sophisticated, agencies must adapt their approaches to data security and IT modernization.

Government agencies are navigating a rapidly evolving cybersecurity landscape in their shift to hybrid cloud environments. Rising cyber threats and an exponential increase in data volume have made managing and securing information more critical — and more complex — than ever before. Seamless, any-time-access to data is vital for operational efficiency, but agencies must balance accessibility with robust security measures.

So, how can agencies modernize their infrastructure while ensuring data security? In a recent GovExec TV episode hosted by Executive Producer George Jackson, Jim Cosby, chief technology officer for public sector and partners at NetApp, joined Mark Cantor, chief information security officer at the Government Accountability Office (GOA), and Sanjay Koyani, director of IT operations and services at the Department of Labor (DOL), to discuss the challenges agencies are facing on their digital transformation journeys and offered insights into how their organizations are charting a path forward.

Here are our top takeaways from their discussion.

Data classification and proactive security measures are critical for data protection

The shift to cloud computing has transformed how government agencies store and manage their data. However, before securing data, agencies must first understand what they possess. According to Cantor, agencies should be especially mindful that while cloud services may alleviate infrastructure burdens, they also require agencies to rethink how they secure and manage sensitive data.

"We're still protecting infrastructure, we're just shifting where that infrastructure responsibility is," Cantor said. "Now we're just having to relearn and retool our understanding of the entire control environment so that we still have those same level of protections no matter where they are in the environment."

Data classification is a vital step in this process, allowing agencies to assess the sensitivity of their data and determine the appropriate security measures. Whether the data is personally identifiable information (PII), subject to HIPAA or CCPA regulations, or other sensitive materials, understanding the data landscape is crucial for effective protection.

Tools like NetApp's classification services enable agencies to identify and baseline sensitive data, helping them make informed decisions about data placement and determine whether they should encrypt, delete or restrict data based on its sensitivity.

"We can look at all of your data on-prem and in the cloud deploy some software, let it run two weeks and

come back and help you understand the performance requirements and the security requirements," said Cosby. "Once you identify and classify what you have, then you can build out your profiles for managing the data and for protecting it."

This proactive approach supports regulatory compliance while identifying and addressing security gaps before they become threats, ensuring robust protection across cloud and on-premise environments.

Zero trust is essential for securing data across cloud and on-premises

A fundamental shift in how government agencies secure their data is underway, with zero trust emerging as a core strategy. Perimeter security historically relied on firewalls to block threats. However, recent directives from the Office of Management and Budget (OMB) emphasize that federal IT systems must not inherently trust any network or device, whether inside or outside the perimeter.

"Data is the backbone for all the work that we do. It fuels our systems and aids in our better decision-making, where we do our enforcement actions and where we place our resources," Koyani said. "We are currently leveraging things like the zero trust executive order to ensure that we're further strengthening how we look at it from both the cloud and the on-premise side, with least privilege access."

For Koyani, zero trust means assuming that breaches will occur and reinforcing security with least-privilege access, encryption and constant monitoring.

Furthermore, zero trust compels agencies to implement security at the application layer rather than solely at the network level. Under zero trust, agencies integrate security into every layer of infrastructure by using multi-factor authentication, application-specific firewalls and continuous monitoring.

In addition, as artificial intelligence and machine learning (AI/ML) grow in popularity, they'll also play a significant role in protecting federal data. According to Cosby, NetApp's anti-ransomware technology, for example, uses behavioral analysis to detect abnormal access patterns and can create instant backups to mitigate potential damage from an attack, creating a proactive security stance that helps federal agencies defend against increasingly sophisticated cyber threats.

Foster a culture of continuous improvement and collaboration

Collaboration is the foundation for tackling today's growing cybersecurity threats and data management

challenges. When IT, cybersecurity and data management teams work together, agencies can align security measures with innovation, breaking down silos that often cause delays and miscommunication.

As Cosby emphasized, "The sooner you get the security team, the data management team, the IT folks all talking together and have a game plan, that's going to work much better. Otherwise, you get finger-pointing and potential problems."

Early collaboration ensures agencies integrate cybersecurity considerations into every step of IT modernization. When stakeholders at every level understand the importance of these initiatives, agencies are more likely to secure the support needed to build resilient, adaptable infrastructures. This proactive, unified approach strengthens security while also setting the stage for continuous improvement.

Strong leadership is essential to maintaining this momentum. Koyani highlighted how sustained executive engagement helps initiatives receive the necessary funding and resources. For example, at the Department of Labor, early leadership buy-in helped secure $15.2 million for technology modernization efforts supporting zero trust.

Training is another critical element in fostering a culture of improvement. Continuous education equips teams to handle new technologies, understand emerging risks and stay aligned with security protocols. This investment in knowledge ensures that staff remain agile and prepared to adapt to new challenges.

"Too often, internal secrets of the country are divulged and they shouldn't be. But once users understand how quickly and easily that can happen, they want to help," Cosby said. "Continual education, continual process, not only for the users of the application, but even the internal folks, helps them understand why we are implementing this new security software, what it's doing, what it's helping prevent and what it's protecting. And once you get people on board, they have an interest and a sincere desire to help."

Learn more about NetApp's AWS portfolio.

Learn more about how NetApp is empowering agencies to modernize their cybersecurity approach.