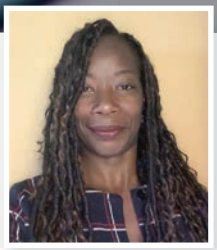
Cybersecurity and risk management in the hybrid cloud



State and local governments increasingly rely on hybrid cloud environments to simplify operations and modernize services. In this Q&A, **Maria Thompson**, former chief risk officer for the state of North Carolina and cybersecurity leader for state and local government at Amazon Web Services (AWS), discusses how to protect hybrid cloud environments from phishing, ransomware, and other increasingly sophisticated attacks.

How is cybersecurity in the hybrid cloud different from on-premises security needs?

When organizations embark on their hybrid cloud journey, they generally don't think about the impact on their security teams. A consideration should be ensuring both on-prem and cloud environments maintain the required level of security and compliance. Unlike traditional on-prem resources, cloud services offer enhanced capabilities. They provide customers a more secure foundation with the ability to modernize, scale, and innovate quickly. The application of security controls within a cloud environment can be vastly different from an on-premises environment — especially with infrastructure-, platform-, and software-as-a-service models. Technologies and methodologies may vary depending on who's responsible for what, what level of visibility an organization has, its maturity, and the levels of control.

What steps help reduce risk in hybrid cloud environments?

Organizations should start by assessing their security controls and identifying gaps between their on-prem and off-prem or cloud environments. A holistic framework for visibility that entails managing, and continuously monitoring both environments is also important. I recommend adopting native cloud security tools, which enhance the level of visibility that's not typically available in the same on-prem tools. Lastly, training — and in some cases certification specifically related to cloud cybersecurity — is critical for IT and security professionals' growth and maturity in the cloud.

If the worst does happen, what needs to be in place to recover?

To recover as quickly as possible and with the least amount of damage, it's important to develop a strong backup or disaster recovery plan that may include a cloud-based, immutable backup solution that is tested on a regular basis. Cyber insurance is also valuable — not as a measure to transfer risk, but as a means to obtain additional support for things like legal concerns, victim notifications, and forensics.

According to Marsh Insurance, cyber insurance premiums for U.S. clients rose 112 percent from August 2020 to August 2021. Price increases are expected to continue in 2022.

How can organizations get the lowest premium for cybersecurity insurance?

Insurance companies often provide a laundry list of requirements to get the lowest rate. I recommend addressing the top areas at a minimum. Multifactor authentication — not just for privileged users, but for everyone — could reduce premiums. Other key measures include patch management; a solid framework for encrypting data wherever it's stored, an endpoint detection and response solution that provides a clear understanding of what's connecting to the network and its security posture, and an email filtering solution that reduces the noise coming into the environment and allows security teams to focus on true threats. Patch management and immutable backups are also a high priority. Besides reducing premiums, all of these things also minimize the risks and impact to an organization if something goes south. But this all begins with a strong security foundation, which industry-leading cloud services can provide.

SPONSORED BY:

aws

Amazon Web Services (AWS) Worldwide Public Sector helps government, education, and nonprofit customers deploy cloud services to reduce costs, drive efficiencies, and increase innovation across the globe. With AWS, you only pay for what you use, with no up-front physical infrastructure expenses or long-term commitments. Public Sector organizations of all sizes use AWS to build applications, host websites, harness big data, store information, conduct research, improve online access for citizens, and more. AWS has dedicated teams focused on helping our customers pave the way for innovation and, ultimately, make the world a better place through technology. **www.aws.amazon.com/stateandlocal**

© 2021 e.Republic. All rights reserved.