

SLED Organizations Are Turning to Hybrid Cloud Environments

By reducing complexities around cloud adoption and working with industry partners, agencies are finding efficient processes and security with cloud infrastructure.

Chief information officers at the state and local level, including educational institutions, are faced with increasingly comprehensive enterprise risks regarding technology, cybersecurity and compliance issues. One major challenge is the need to operate increasingly complex cloud portfolios, especially as agencies look to manage data in public, private, hybrid and multi-cloud environments.

Agencies are turning to cloud computing to get more speed and agility from their applications, and so they can deliver applications that improve customer engagement, provide new services, reduce costs and tackle new cyber threats. Guests from the education sector and the industry that supports it recently joined [a FedInsider panel](#) to discuss how they're implementing cloud solutions to reduce risk and deliver modern services.

Migrating to the Cloud

Many public agencies are in a state of infrastructure transition as they look at adopting cloud services, investing in new tools and keeping up with cybersecurity standards. Northeast Wisconsin Technical College, for example, is moving to the cloud to offer better access to both faculty and students, especially in the areas of

student finance and HR, according to its IT Director of Technology Karl Reischl.

"COVID really pushed us further along our cloud adventure because students have to get anywhere, anytime access," Reischl said. They've since moved all of Microsoft Office 365 to the cloud and adopted a cloud-first policy.

The university is also in an infrastructure transition as it moves its on-premise Oracle PeopleSoft applications to the cloud. Peoplesoft includes software for HR management systems, financial management, supply chain management and more. "With that, there is a lot of server clusters that we will no longer need," Reischl said. And since cloud-based virtual desktops were helpful during COVID, Reischl said they're planning for the environment of tomorrow where the school might not have any data centers on-site anymore.

Ultimately, these cloud-based tools are allowing staff to spend less time patching older, on-prem applications and servers, and more time in actually using software. Plus, moving to cloud keeps the university in line with federal and state data and security regulations.

Featured Experts

Karl Reischl
IT Director of Technology,
Northeast Wisconsin
Technical College



Aaron Murphy
Field Technical Evangelist,
Veeam



Choosing the Right Cloud Environment

Aaron Murphy, field technical evangelist at Veeam, said when customers are looking for cloud environments, they often want to put data securely in the cloud, either in a public cloud or one provided by a cloud service provider.

"That is important because it's a different attack plan," Murphy said, "it uses different security credentials to protect from ransom ware...it's harder to attack...but most of all, the cloud is the off-site target for that secure data copy to protect against threat actors."

Agencies turn to hybrid-cloud environments, using both private and public cloud, because some applications and data simply must remain private or on local networks. And managing different types of environments in a hybrid cloud infrastructure can be complex as they can each require their own credentials and security. Murphy said it's important for customers to truly know

their environments, and Veeam is working to reduce complexities by forming and simplifying common tasks and terminology.

"Most customers these days when they are acquiring software from us are already asking about flexibility, and they have got future plans," Murphy said. "So, if we are using one or two environments today, they know that they might be using three or four environments in the future. They want to know if they can move, is everything portable, and how to get flexible licensing." This way, customers aren't contacting vendors every time they have a change, further simplifying their management of hybrid clouds.

Securing Hybrid Cloud

Reischl said one of the advantages to using hybrid cloud at the university is that nearly all cloud applications or platforms are built with security in mind. "These systems understand the importance of cloud application security," he said.

Cloud environments also put some of the burden of security on the vendor. But it's a shared responsibility, so organizations need to make sure that they talk often about those issues. "Having those consistent vendor meetings to see how they are handling security, and to discuss any changes in the security environment is something that we do a lot," Reischl said.

And when it comes to recovering data from potential ransomware attacks in hybrid environments, Murphy said it is first important to look at each individual environment and make sure there are options for where that backup data needs to go.

"When I run recovery scenarios for clients, the recovery performance and expectations must meet their business requirements," he said. "That is what you have got to do. You need to perform recovery testing for each of the environments and then ask if you have the flexibility that you need to meet those recovery requirements."

Reduce Complexities Around Hybrid Cloud Environments

Veeam works to reduce complexities around hybrid cloud environments, in part, by conducting independent research on data protection about what IT leaders find especially challenging, and what their future plans are. Veeam then takes those findings and uses them to make their products and services better for customers.

"Inform us about what is going on," Murphy said. "The data can then be used to start conversations and get the ball rolling for change within your organization." For instance, Murphy said he knows customers want to manage their hybrid cloud in a single workload to drive out complexities.

That requires exploring vendors and solutions to ensure that certain workloads that need to remain separate due to criticality, can do so if needed.

"The workload in one cloud or another may be so significant that you require a certain sort of capability to protect it frequently enough without impacting users, and to be able to recover it fast enough because it's so critical," Murphy said.

In other words, organizations must first categorize individual workload importance, and then decide whether a cloud solution allows all of their workloads to function together, while still delivering performance or individual applications. And only after that can organizations start reducing their cloud complexity.

"Often if you get the right product, the benefit comes by just bringing together the monitoring and management with reporting and policy enforcement," Murphy said. "And maybe all those things then make it worthwhile to use a single product to eliminate your cloud complexity."

Hosky Communications, Inc.

3811 Massachusetts Avenue, NW
Washington, DC 20016
Contact: [John Hosky](#)

☎ (202) 237-0300
✉ info@FedInsider.com
🌐 FedInsider.com
📘 Facebook.com/FedInsiderNews
📎 Linkedin.com/company/FedInsider
📱 [@FedInsider](#)

Veeam Software

8800 Lyra Drive
Columbus, Ohio 43240
Contact: [Veeam Contacts](#)

☎ +1 (614) 339-8200
✉ Veeam_Team@Veeam.com
🌐 Veeam.com
📘 [@VeeamSoftware](#)
📎 Linkedin.com/company/Veeam-Software
📱 [@Veeam](#)

© 2022 Hosky Communications, Inc. All rights reserved. FedInsider and the FedInsider logo, are trademarks or registered trademarks of Hosky Communications or its subsidiaries or affiliated companies in the United States and other countries. All other marks are the property of their respective owners.