MeriTalk
Improving the Outcomes of Government IT

Underwritten by:
ViON
Building your enterprise solutions

Executive Q&A: ViON, Forcepoint Leaders Discuss Proactive Security in Multi-Cloud Environments

MeriTalk recently caught up with Ray McCay, vice president of solution sales, ViON Corporation, and Eric Trexler, vice president of global governments and critical infrastructure, Forcepoint, to discuss multi-cloud security risks, success factors, and how Federal IT teams can move from a reactive stance to a more proactive security posture in multi-cloud environments.

MeriTalk: Why is security not a given in the cloud, and what are some challenges and tips for securing remote data throughout the Federal government?

Eric Trexler: There are no assumptions with security in the cloud. Many Federal agencies assume they're getting more from their cloud service provider than they actually are. Many times we'll see a line of business that went into the cloud – "shadow IT" – without considering the security implications.

A MeriTalk survey on multi-cloud environments found only a quarter of the 150 Federal IT decision makers surveyed rated their agency with an "A" for multi-cloud cybersecurity posture. The main reasons for this were budget constraints, difficulty meeting Federal requirements, lack of a skilled workforce, and an increased attack surface. It's important to understand the difference between security of the cloud and the security in the cloud.

When you look at the major cloud service providers, they all have a shared accountability model that talks about what they will protect, and what a customer still needs to protect. The cloud provider will protect security of the cloud. The end user – and the business owner – need to provide security in the cloud, for their people, and for their data.

Security is a process, not a product. You can't buy a product from a cloud service provider that says, "Okay, now I'm secure." It's a process. You need to work through it with security, with IT, with business operations, and see the cloud service provider as the integrator. There's a lot more to do, and Federal IT teams need to think about it in that context.

In my experience, multi-cloud environments create more opportunity. They'll help agencies drive pricing and they can play off of the different clouds. One cloud may be better than another. One cloud service provider may have features or capabilities that are better for your agency in one area. It increases the attack surface though, and creates greater security challenges.

Ray McCay: Traditionally, some of the adopted methods have been reactive, like using firewalls to keep threat actors outside of sensitive networks. Methods around log files like log shipping, consolidation, mining, or monitoring all lead to a lengthy discovery remediation and/or recovery time. I've heard of organizations taking six to 18 months from the original point of discovery to complete remediation and recovery back into operations. This is unacceptable. During this time there are potential open windows for attack, insider threat issues, and even sensitive data exfiltration and leveraged exploits.

MeriTalk: How can agency IT teams move from a reactive stance to a more proactive security posture and reduce these attack surfaces?

Trexler: Traditional methods were very reactive. The dissolving of the perimeter has changed the way cybersecurity personnel need to work and protect their infrastructure. Agencies still need boundary firewalls. But what happens when a larger part of agency transactions never crossed the physical boundary and entered the data center, or transactions don't enter the system until it's almost complete? How do you pool all the log files together?

We don't have enough personnel for problems that continue to worsen each year. We're not going to magically invent analysts. How do we drive inspection of what's happening on the networks?

Your personnel aren't even working in your traditional office spaces anymore. We have to throw the traditional methods out and change the paradigm a bit to get more proactive in the way we do IT. That's not to say we can't learn from past processes, that we shouldn't do certain things. But we have to recognize that the world changed, and Federal employees are now everywhere, using all types of devices.

Forcepoint calls this human-centric security – focusing less on the threat, and more on the humans who are using the data and the data itself – understanding what they're doing with the data, as well as the value of the data and the risk equations. IT teams can't manage the threats anymore. It's a losing proposition; every year we spend more money trying to combat threats and fail to do so, as the threats evolve.

MeriTalk: Let's talk about continuous monitoring and behavioral analytics for a moment. Is one tactic better than the other?

Trexler: There's a good bit of overlap when you talk about continuous monitoring versus behavioral analytics. When we perform behavioral analytics, we're looking at the behaviors, the intent, the location. Are we in the National Capital Region – which is where we expect that user to be – or are we coming from Indonesia, which is out of character for this employee?

But the other piece of continuous monitoring is evaluating how we are monitoring the agency employee or contractor. When IT teams use zero trust where one of the concepts means providing the least amount of privilege required to do the job for a specific asset, they can spot where they have a much better handle on what the employee is doing and what they should be doing.

MeriTalk: Zero trust was briefly mentioned earlier. Ray, can you explain how zero trust architecture helps to secure Federal multi-cloud environments?

McCay: Zero trust allows credentialed users to access sensitive data. With zero trust, users only get access to information required for operations. In the military, they make sure personnel have the proper security clearance, and the need to know. Within the public cloud space, multifactor authentication should always have end periods, no matter how often the users complain about it. It's a fine balance between increasing security and keeping things usable for everybody.

With cloud access tracking that movement, it becomes a lot more critical because now it might not be a threat actor, it could also be an insider trust issue. This could lead to exfiltration of data to exploit, or open up holes for others to get in.

When you're looking at the different cloud models, there are some similarities and some differences within the authentication methods that exist between them – even between the identity and access management. For example, using a PIN for card systems to authenticate users in the network provides a greater level of security. Implementing multifactor authentication methods in public clouds helps maintain that zero trust.

MeriTalk: What are some of the Federal security regulations that agencies have to follow?

McCay: Cybersecurity Maturity Model Certification (CMMC) is a mandate, not a directive of one of the Federal standards. CMMC is a trajectory used to protect U.S. data and warfighter efforts. The CMMC Accreditation Body evaluates Department of Defense agencies and contractors on the strength of their cybersecurity from a scale of level one to level five. Only third-party assessed companies can provide goods and services based on their certified maturity levels. This supersedes security control initiatives, supply chains, and security performance measures.

Trexler: Another is Raise the Bar (RTB), a cross-domain specific regulatory rule. As the leading provider in cross-domain, all of Forcepoint's cross-domain products are RTB-compliant. Led by the National Cross Domain System and Security Management Office of the National Security Agency, RTB ensures there are controls in place on these products that allow either transfer of data to move from a network level to a lower level Non-classified Internet Protocol Router Network (NIPRNET) or a Secret Internet Protocol Router Network (SIPRNET). It also allows access to the SIPRNET and NIPRNET on the same system. RTB drives controls that exceed the National Institute of Standards and Technology Risk Management Framework requirements, specifically to deal with adversarial attacks against or through a Cyber Test System, or fix mistakes made in configuration and implementation or development.

MeriTalk: How can agencies create multi-cloud security governance, centralization, and orchestration with human-centric security policies to enable that zero trust environment?

Trexler: Agencies don't want to have different teams managing security across the different clouds. It gets very complicated. Agencies want to reduce complexity. The best organizations have a cloud management office of some sort, that manages the cloud environments across the agency in the commercial world – and understands what resources are available.

Agencies should establish a practice for continuous monitoring. Focus on your people, understand how they're working with the applications to better protect the business. There's a lot of IT in these equations. When you break it down to people and data, it makes the problem so much simpler.