ORACLE
Cloud

carahsoft.

GOVFORWARD
carahsoft.
Produced by: GovExec
FedRAMP Headliner Summit

The Role of Data and Risk Management in the New Threat Landscape

1 Sharing is key to secure data

2 Data sharing supercharges defenses

3 Agencies and industry increase teamwork

4 Automation makes a difference, good and bad

1 The Role of Data and Risk Management in the New Threat Landscape
carahsoft. | splunk> | ORACLE

The Role of Data and Risk Management in the New Threat Landscape

Thank you for downloading this Oracle resource. Carahsoft is the Public Sector Reseller for our vendor partners and working with resellers, systems integrators and consultants, our sales and marketing teams provide industry leading IT products, services and training through hundreds of contracts.

To learn how to take the next step toward acquiring Oracle's solutions, please check out the following resources and information:

For additional Oracle resources:
carah.io/oracleresources

For upcoming Oracle events:
carah.io/oracleevents

For additional Oracle solutions:
carah.io/oraclesolutions

For additional MultiCloud solutions:
carah.io/multi-cloud

To set up a meeting:
Oracle@carahsoft.com
855-618-3114

To purchase, check out the contract vehicles available for procurement:
carah.io/oraclecontracts

For more information, contact Carahsoft or our reseller partners:
Oracle@carahsoft.com | 855-618-3114

The Role of Data and Risk Management in the New Threat Landscape

1

Sharing is key to secure data

2

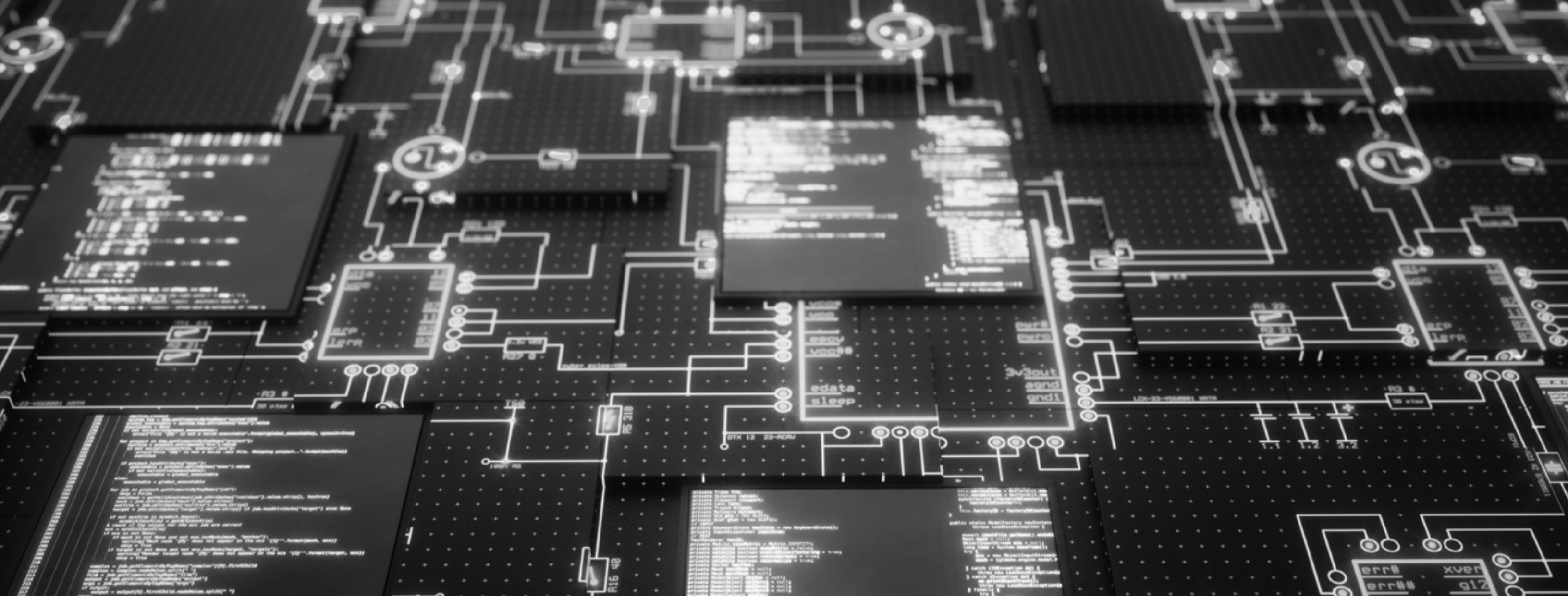
Data sharing supercharges defenses

3

Agencies and industry increase teamwork

4

Automation makes a difference, good and bad



1

Sharing is key to secure data

Federal IT and cybersecurity managers know that it's not a matter of if their networks will get hit with a cyberattack, but when. The good news is sharing data can help manage that risk.

"These threat actors are not slowing down," said Gabriel Davis, risk operations team lead at the Cybersecurity and Infrastructure Security Agency (CISA) during a panel discussion on threat data at the recent **Carahsoft FedRAMP Headliner Summit**. "At the same time, we're also seeing an expansion of our networks. The landscape isn't getting any smaller. We must be proactive about meeting threat actors in the place they're trying to exploit."

Davis was joined on the panel by Susan Valverde, senior manager of Federal Solutions Engineering at Oracle, and Juliana Vida, group vice president, chief strategy advisor, public sector, at Splunk.

Being proactive, said Davis, entails taking away known vulnerabilities that attackers like to use, implementing secure-by-design and secure-by-default operations.

The vast majority of threat actors tend to use what works and design attacks around known vulnerabilities, instead of doing the sometimes-arduous work of developing new methods of attack, according to Davis. Being able to forecast the bad things that will happen,

> "These threat actors are not slowing down.
>
> **GABRIEL DAVIS**
>
> Risk Operations Team Lead, Cybersecurity and Infrastructure Security Agency (CISA)

fighting through them, and handling the consequences is the kind of resilience agencies need in an emerging threat environment, according to Vida. “The idea is to have a full visibility or observability across the entire environment and make sure teams are sharing information and data, so the whole organization can build resilience,” she said.

“Being able to respond quickly to threats is what makes a difference,” said Valverde.

Technologies like artificial intelligence (AI) and machine learning, she said, can help detect network anomalies and prompt quicker responses to them—without human interaction.

> “
>
> Being able to respond quickly to threats is what makes a difference.
>
> **SUSAN VALVERDE**
>
> Senior Manager, Federal Solutions Engineering, Oracle

2

Data sharing supercharges defenses

Data siloing across agencies and the mindset behind them, should be a thing of the past, according to Vida. “Breaking down those silos and trusting agencies to leverage data is the key to open observability” that ensures resiliency, she said. Data barriers waste time, money, effort and energy, according to Vida.

“If organizations just did that one thing – broke down those silos and shared information over open API platforms and other technologies – they would get so much more value out of the technologies they’ve already invested in,” she said. “Just share. You’d be amazed at what you can do with all the data that’s already resident in your environment.”

That sharing of data can also apply across government, according to CISA’s Davis. If an agency had data about an attack on another agency, it might be able to blunt or prevent a similar attack.

“We have to start thinking about this as a security community approach, because we’ll all be victimized” by attackers, he said.

“We’ve been managing mission-critical data for decades,” said Valverde. “We built our cloud with security first. We have those tools to allow sharing.” Those tools allow users to fine tune who gets to see log and risk data, which is critical to ensuring security, as well. Oracle has no access to its cloud customers’ data, providing another layer of security, according to Valverde.

3

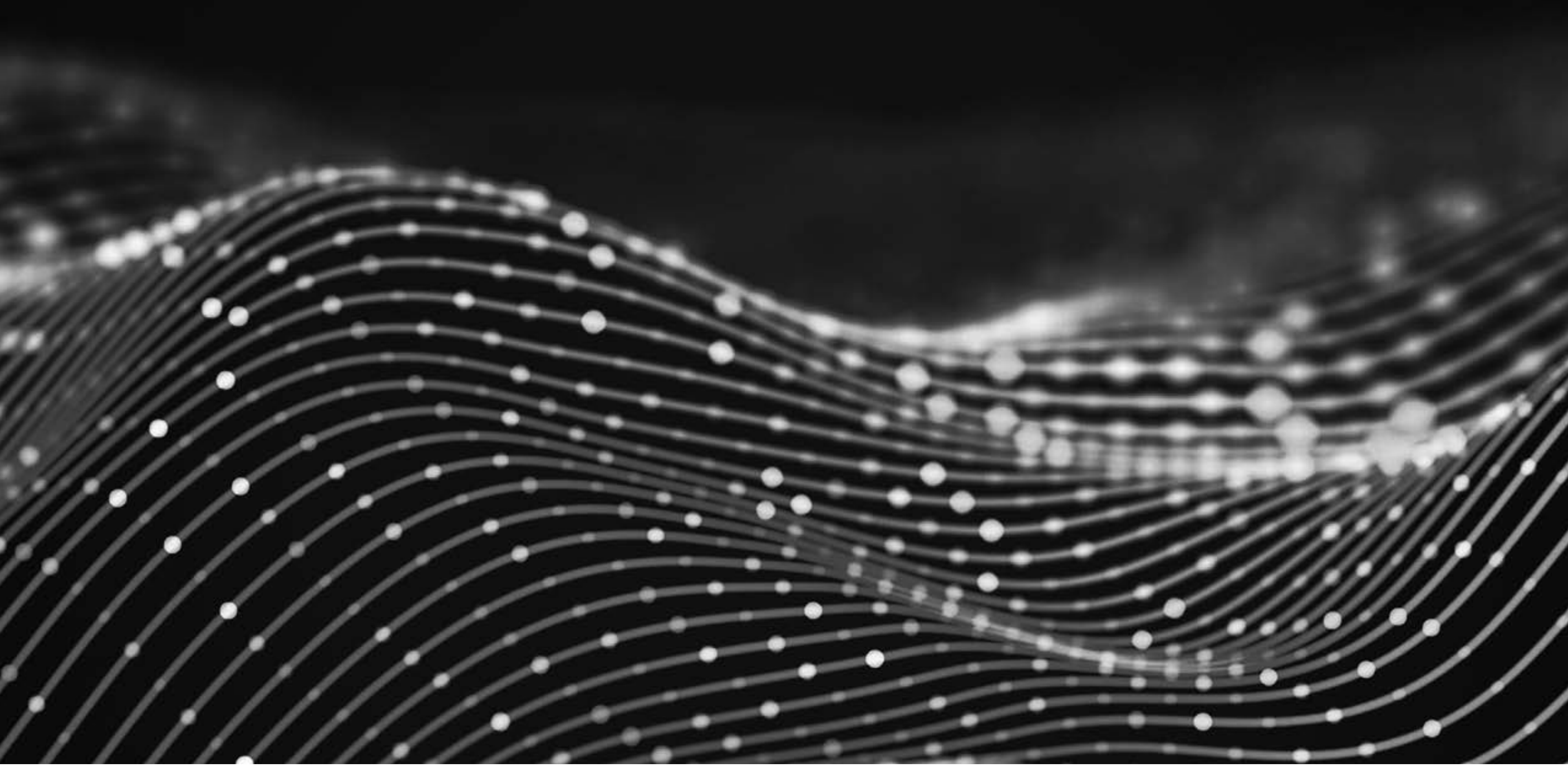
Agencies and industry increase teamwork

If all agencies stay the current course, however, nothing will change.

“We’re being open. We’re saying we can’t do this alone and need the help of professionals who are working in industry and privately. We don’t need everyone to come work for the government, but we need your cooperation,” said CISA’s Davis. One of CISA’s many cybersecurity tasks is to track and provide information on threats to industry and to federal agencies. To gather that information, said Davis, requires industry and agencies to share it for wider distribution to help stave off threats.

Vida agreed that increasing interaction and partnership between industry and the federal government is a recent welcome development.

“Partnering between industry and the federal government is fairly new,” she said, adding that ten years ago there was very little openness with data. “This opening of conversation with government coming to industry seeking our help, looking for a partner – we need more of that.”



4

Automation makes a difference, good and bad

Automation is a double-edged sword for bad actors and good actors, according to the panelists. Threat actors tapping generative AI to supercharge their efforts is a worrisome emerging threat, said Valverde.

“Being able to address the rapid growth of attacks using generative AI is going to take a lot of effort to address,” she said.

On the flip side, however, automating threat data gathering by agencies and cyber defenders can be an extreme force multiplier, according to Davis. Automation can allow CISA to use open-source data to find vulnerabilities in state and local networks and notify those organizations of the potential problem. CISA partners with state, local and tribal governments to bolster those organizations’ cybersecurity capabilities.

Automation has moved into daily life, said Vida. It’s made life easier and more efficient. Automating processes that consume people’s time and use paper slows that process to a crawl. The FedRAMP certification process, she said, could benefit from automation. What takes nine months using paper-based processes, she said, could be shortened to days if it were done electronically.

“There are a thousand different examples of how routine, administrative paper-based tasks” can benefit from automation, she said.

Automating security processes, however, can take a lot of thought. “We should not risk security for the sake of automation,” said Davis, noting that employing automation has to be “right sized” and tailored to organizations. “There are amazing tools out there but be mindful in how you apply these tools. Fit the tool to the need, not the need to a specific tool," he added.

The FedRAMP process, which certifies security for products used by federal agencies, offers a baseline for security. The certifications provided by the process, he said, offer agencies a go-to set of vetted secure tools they can trust, instead of having to do a security check for every piece of equipment and software agencies obtain for their networks.

Generative AI presents challenges for agency cybersecurity, as well as the FedRAMP process and the products it monitors.

"We need to set guidelines for the use of generative AI" in developing products, said Valverde, and those guidelines need to be very clear. Oracle, she said, has set policies and doesn't allow employees to use generative AI at will.

Generative AI, said Davis, is going to make cyber criminals' jobs easier because they will be able to make attacks more effective and efficient almost automatically. "Conversely, it can make our jobs easier, if we use it properly and where it's appropriate," he said. "There is a ton of risk associated with generative AI" as it can replicate voices, images and data. Davis said those applications, however, carry the seeds of how to detect them by using telltale data that can be tracked.

Learn more about how industry partners like **Oracle** and **Splunk** can help agencies stay ahead of cyberthreats.