FEDInsider

Innovating with Data: Protecting Critical Assets

Expanding Federal Datasets Require Exceptional Categorization and Management

Both the number of sources generating data and the endpoints that need to access it are growing at nearly every federal agency. This has led to a data renaissance where collected information is being used in innovative ways to improve citizen services and better help agencies accomplish their missions. But there is also a danger, because the growth in data is also expanding the attack surface and the associated risk. To compensate, agencies are improving security so they can continue modernizing while keeping their critical data safe.

Two data experts from government and industry spoke at a recent FedInsider webinar about how agencies are leveraging emerging technologies to manage new services and combat threats.

The following are some of the most important aspects of those efforts.

Understanding Federal Data

The Federal Deposit Insurance Corporation may not be receiving data from millions of IoT sensors, but increasingly it deals with structured and semi-structured data from financial institutions and well-formed data on financial health.

"We do have the ability to ingest so much data that's out there," said FDIC Chief Data Officer Jacques Vilar. Data volume is increasing over time, as the agency collects massive amounts of new data to supplement the core of what it has already gathered, and to build onto existing datasets. Then, it analyzes everything over time to help make critical decisions.

For agencies that are experiencing an influx of IoT-generated data, Daniel Carroll, cybersecurity practice lead for Dell Technologies Federal, said that the magnitude of incoming data is becoming a challenge. An increasing number of devices are connected online, and there are also more sensors and cameras being attached to that hardware, Carroll said. All of that is contributing to the amount of data agencies are now responsible for managing and protecting.

"How they utilize that data, and what they utilize it for is something they're continuing to figure out," Carroll said. "There's a lot of research going on within government to figure out how to more effectively manage that data."

Agencies are also challenged to protect large amounts of data, and need an effective data analytics capability that uses artificial intelligence and machine learning to detect threats in real-time.

The Challenges of Data Silos

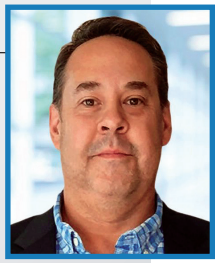
Often, data silos are created over time out of habit, Vilar said. Agencies need unfettered access to all types of data to help inform decisions that will create value for the business. This ends up driving innovation.

"To drive value with the data we have available, we have to have a clearer understanding of what data is even available," Vilar said. "If it's in a silo, whoever is working in that unit might have a very good understanding of what is in that data... but the rest of the corporation may not."

As the FDIC continues to modernize, it is looking at existing processes and its business architecture to determine what assets are available, how well those assets are understood and who

Featuring:

- **Jacques Vilar**
  Chief Data Officer,
  FDIC



- **Daniel Carroll**
  Cybersecurity Practice Lead,
  Dell Federal

can access them. Understanding these processes will help the agency build a base level for a data program. "We want to protect the data. We have to do that from day one. But to protect the data, we have to understand it," Vilar said.

Keeping Data Safe During a Pandemic

The pandemic accelerated the adoption of remote work for the government by a decade. Agencies had to suddenly set employees up to work from home while continuing to support federal pandemic relief efforts.

"That meant enabling [and expanding] a lot of systems …for remote work that they hadn't done before," Carroll said. While agencies tried to be as effective and secure as they could by expanding VPN capabilities and providing workers with secure remote desktops, it was still new territory with less control. Carroll continues to work with agencies on how to enhance capability from a cybersecurity framework perspective.

The FDIC had to shift 6,000 employees into a remote workforce over a single weekend when the pandemic hit. Vilar said the infrastructure team had people up and running quickly, and they were focused on improving remote work with upgraded VPN and laptop refreshes over time.

As remote work evolved, the FDIC focused on how staff were accessing the network differently. "The nontraditional work hours, the video calls, remote access to systems, we had to reconcile that with the concept of the cyber executive order," Vilar said, "That speaks to how we are going to protect data in this new environment."

Vilar is now focused on identity, credential and access management, and how to implement Zero Trust as required by the executive order on improving the nation's cybersecurity. "Ensuring that we understand what data is coming in from our edge and what that means to our operations and to the security posture, all of those things are top of mind as we're moving forward," Vilar said. And he's looking to industry to help them get there.

Protecting Federal Data Now & in the Future

As agencies continue to focus on securing networks and data in hybrid and remote work environments, concepts like zero trust, multifactor authentication, endpoint protection and data governance will be key, Carroll said.

"You must have the capability to understand what your data is and what the protection level should be that you want to apply against it," Carroll said. This will help agencies determine who should have access to their data, and how critical that data is. Once they understand that, the next step is to carefully classify the data, and use those classifications as the basis for an access control program.

Data classification and governance is also critical for the FDIC, Vilar said. The agency examines banks for safety and soundness, and often collects semi-structured data via reports about those banks that are written by FDIC officials. To help classify that information, the agency now has a machine learning program that studies those reports to provide feedback and classification suggestions. And that program is continuing to evolve as the FDIC moves to the cloud.

In terms of meeting executive order cyber requirements and ensuring data protection, Carroll suggests not starting from scratch. Rather, find the gaps and implement Zero Trust and multifactor authentication where needed after evaluating current planning and capabilities.

"Zero trust is a principle. It's a guiding way to approach a security model. It's not a framework. It's not architecture. It lays on all those things," Carroll said. And then, once data is properly protected, capabilities like analytics platforms and AI can ingest alert data and look for markers or changes in behavior to prevent or respond to attacks in the future. That is how agencies will be able to protect their critical data assets in the future, regardless of how large their data lakes grow.

FEDInsider

Hosky Communications Inc.
3811 Massachusetts Avenue, NW
Washington, DC 20016

- (202) 237-0300
- Info@FedInsider.com
- FedInsider.com
- Facebook.com/FedInsiderNews
- Linkedin.com/company/FedInsider
- @FedInsider

carahsoft.

Carahsoft
14993 Sunset Hills Road, Suite 100
Reston, VA 20190
Contact: Erica Raymond

- (866) Dell-2-Go
- DellTechnologies@Carahsoft.com
- Carahsoft.com/vendors/dell
- Facebook.com/Carahsoft
- Linkedin.com/company/Carahsoft
- @Carahsoft