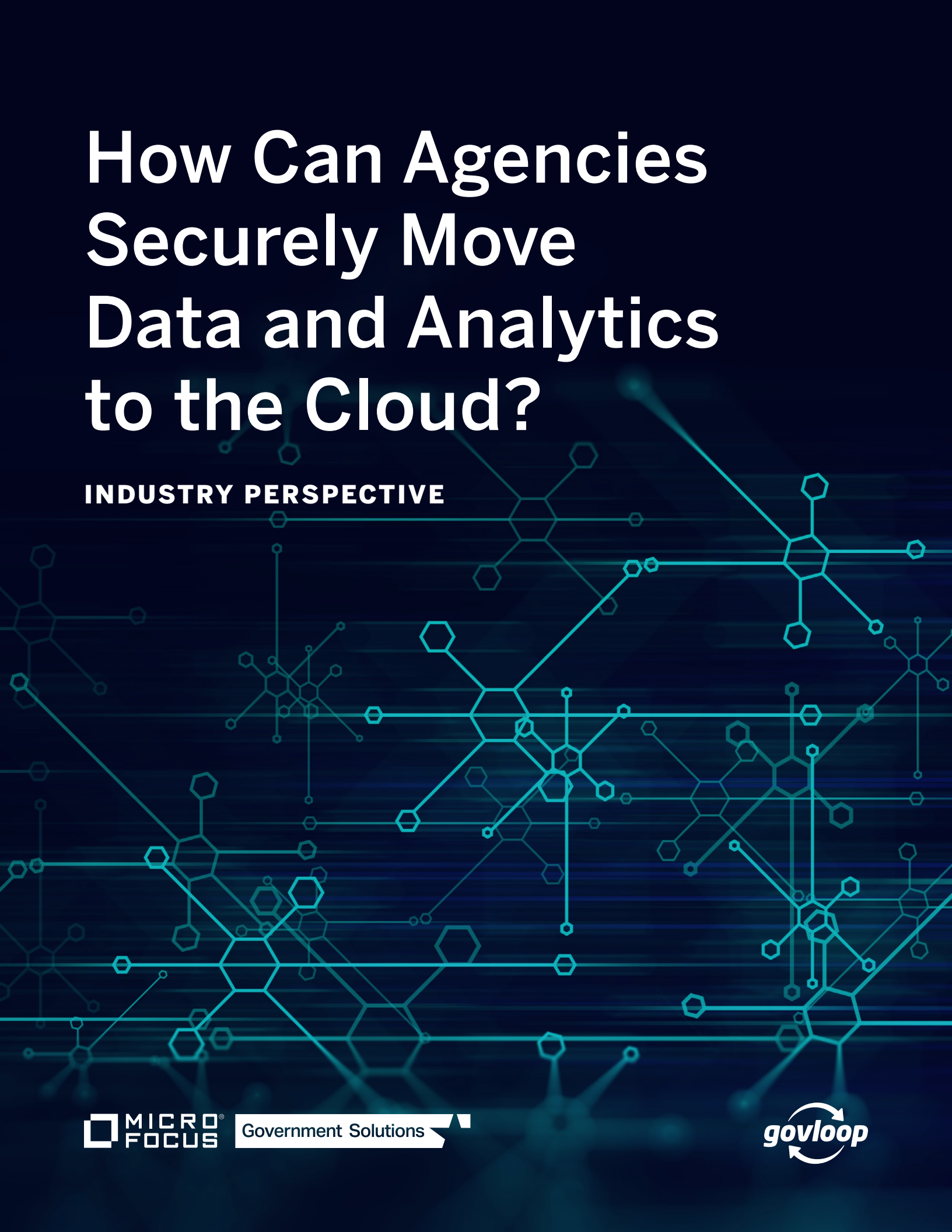
# How Can Agencies Securely Move Data and Analytics to the Cloud?

**INDUSTRY PERSPECTIVE**



MICRO FOCUS Government Solutions

govloop

# Introduction

Cloud, mobility, Bring Your Own Devices (BYOD) and other hot technologies amount to massive increases in data creation. As a result, organizations must work to keep up with the large increases in demand for the data. They are now tasked with providing big-data analytics for customers and internal use. In addition to analytics, they now must protect data throughout its entire lifecycle – at rest, in transit and in use – across on-premise, cloud and mobile environments.

Cybercriminals are astutely aware of the potential vulnerabilities at different stages of its lifecycle. Attacks on critical information and system assets are on the rise and are more sophisticated due to the increase in nation-state attacks. Take, for example, the data stolen in the massive Office of Personnel Management (OPM) breach in 2015.

The OPM data was not protected by practices like data masking, redaction and encryption, which should be the norm, rather than the exception, Rep. Elijah Cummings, D-Md., said during a hearing held by the House Committee on Oversight and Government Reform after the breach.

Agency IT and security operations teams must rethink how they protect data in a digital world where data is everywhere, particularly when data is in the cloud. Federal agencies should take a chapter from financial institutions' playbooks and adopt a data-centric approach that includes data encryption, tokenization and key management that protects data across all applications and platforms.

To help agencies better understand how to securely move data and analytics to cloud infrastructures, GovLoop partnered with Micro Focus Government Solutions, a company dedicated to helping agencies protect mission-critical data throughout its lifecycle. In this report, we'll explore challenges governments face, solutions that help agencies go beyond merely encrypting data at rest and best practices for taking advantage of these solutions. We'll also gain insight from Susannah Reed and Ernie Tarbox, Federal Account Executives at Micro Focus Government Solutions.

# The Challenge: Securing Data on the Move

In today's era of digital transformation, data is everywhere – stored on internal systems, in the cloud and on mobile devices; moving through and beyond the boundaries of an organization's networks; and being accessed and used by a digital workforce and citizens who want to make more informed decisions in real time.

Cloud providers stepped up efforts to give organizations tools to protect agency and business data as more applications and workloads migrate to public cloud infrastructures.

To the surprise of many, moving data to the cloud does not necessarily make it secure. Agency IT and security operations teams must still use cloud providers' tools and processes, as well as their own existing infrastructure, to protect data. Moreover, access to big-data analytics systems and through mobile devices increases the attack surface adversaries can exploit to steal or compromise data.

Agency managers moving data to the cloud must first recognize that data is no longer going to move between applications and data repositories in static, well-defined paths, said Reed.

"Once you're moving these systems into the cloud, the data's going to be traveling constantly, and it's going to be replicated in multiple systems," Reed said. The systems could include backup analytic systems, third-party contractors' systems or systems from other providers, which makes data inventory and data management much more complex than in traditional, on-premise IT environments.

On the other hand, traditional security controls for data protection do not work as well in the cloud environment. Plus, many of the cloud-focused solutions are complex or difficult to deploy.

To simplify data protection, IT and security managers might try encrypting the entire data store, or the entire virtual machine, or application container. "However, this just provides a false sense of security, because anytime a user or an application needs to access any part of that data in the repository or virtual machine, all the sensitive data is once again exposed and put at risk," Reed said.

The best approach is to ensure that security is an integral part of an application's entire lifecycle. Federal agencies should start looking at the commercial sector, specifically the financial industry, and how it handles encryption beyond just protecting data at rest, Reed noted.

# The Solution: Encryption Wherever Your Data Goes

Agencies need security tools that can encrypt and protect data wherever it resides and, through the process, render the data useless to an attacker.

With the dawn of big data – large and varied data sets too complex for traditional data processing applications to handle – agencies are deploying data analytics to uncover information, including hidden patterns, unknown correlations, market trends and customer preferences that can help them make informed business- and mission-related decisions. Agencies involved in agriculture, health, finance, law enforcement, research and weather forecasting are some of the organizations involved in analyzing and sharing information culled from a variety of disparate databases, devices, sensors and systems.

As agencies adopt analytics programs – whether in the cloud or on-premise – they must grapple with increasing amounts of data that will be ingested and stored in multiple locations.

"The question is, how are you going to protect that data as it moves into and through data warehouses and data repositories, or cloud-based analytics or analytics applications that might be used with the data?" Reed asked. Any system, like Apache Hadoop, for instance, that aggregates so much data is bound to be a target.

The easiest way to protect large amounts of data that are constantly moving and changing is to make the data worthless to an attacker or unauthorized users. If an unauthorized person gains access to a data lake or applications in the cloud, IT and cybersecurity teams don't want them to see the real data.

As a result, agencies need security tools that will de-identify that data using format-preserving encryption and stateless key management validated by the National Institute of Standards and Technology.

Data de-identification is the removal of personal identification information or sensitive data through data masking, encryption or redaction. Some regulations and privacy laws can get very specific in how an organization goes about de-identifying that data. Some may specifically call for Advanced Encryption Standard (AES) encryption. Given the sensitive citizen data that many federal agencies house, Micro Focus Government Solutions recommends de-identifying the data through a method that's Federal Information Processing Standard (FIPS)-certified and NIST-validated.

"Ultimately, it's all about rendering that data useless to an attacker, but it's not going to complicate the workflows or compromise the application's ability to utilize that data," said Reed.

> **"Ultimately, it's all about rendering that data useless to an attacker, but it's not going to complicate the workflows or compromise the application's ability to utilize that data."**
>
> — Susannah Reed, Federal Account Executive, Micro Focus Government Solutions

## How Can Micro Focus Government Solutions Help?

Micro Focus is a leading expert in data encryption, pseudonymization, tokenization and masking solutions for enterprise data privacy and regulatory compliance.

Micro Focus provides a solution set that lets organizations de-identify data using NIST-validated, format-preserving encryption (FPE) and stateless key management. Format-preserving encryption is a new approach to encrypting structured data. With NIST security standards, FPE integrates datatype-agnostic encryption into legacy business application frameworks without altering the data format.

The company's Voltage SecureData Enterprise solution provides flexible, data-centric protection that enables secure cross-cloud analytics on data throughout an extended enterprise, data centers and between cloud systems. Voltage FPE and Secure Stateless Tokenization embed protection into the data itself, protecting it anywhere it goes.

In addition, Micro Focus' solutions are technology-agnostic, working with many leading big-data platforms and databases such as Cloudera, Hadoop, Teradata and Vertica.

Micro Focus' portfolio of products helps organizations move to the cloud. The company's Vertica big data warehouse environment has built-in business intelligence tools that come integrated with Voltage SecureData.

Federal agencies are increasingly under pressure to protect citizen data. Micro Focus is uniquely positioned to help agencies address their data protection requirements.

# Case Study

A global financial service provider to telecommunication carriers and retail markets had a business problem: How could the company keep two competing telecom carriers safe in the cloud so their customer data could not be taken or queried by their competitor?

The company wanted to move applications off the mainframe and into the cloud to offer applications via a software-as-a-service cloud model, said Tarbox.

The company had a lot of sensitive data on the mainframe. Developers took portions of the mainframe and rewrote a new architecture to run specifically in Amazon Web Services and Microsoft Azure clouds. Two clouds were used because the two competing telecommunication carriers wanted their customer data to be separated in the cloud.

The financial company deployed Micro Focus SecureData to encrypt and tokenize sensitive data. In the Microsoft Azure environment, an application gateway was built to collect data from millions of subscribers' smartphones. A SecureData Simple Application Programming Interface (SimpleAPI) protects all the data elements. A security bus that also uses SimpleAPI is built within the AWS cloud, which then stores the encrypted data in a staging database.

By encrypting the data with unique keys for each individual customer, the telecom providers can manage their data so there is no way that an employee from the competitor could query all the data and use the information to market to them. The decryption keys are not in any of the clouds, but instead are on-premise at the telecom provider's facility within the SecureData Key management server and console.

Ideally, the repository where the data resides should not have the ability to decrypt the data, Tarbox said.

"When I put data in a single repository, and I put the key on that repository, that gives malware a single server to attack, and not only the ability to access all of the data, but also decrypt the data," Tarbox said.

The bottom line is the global finance company has a unified architecture for streamlined compliance and risk control, it has minimized sensitive data exposure in AWS and Azure clouds, enabled differentiated services with data security and cut applications while maintaining an agile strategy with the cloud infrastructures.

# Conclusion

When it comes to implementing standard encryption practices, federal agencies appear to be lagging behind other industries.

"Most agencies' security policies call for the bare minimum of either data at rest or data in motion encryption," Reed said. "That is the bare minimum that leadership is pushing down to its program areas or to their system integrators to actually deploy."

A large federal agency recently invested $18 million on mainframe encryption, which is great if it thinks its main security threat is someone breaking into its data center and using a forklift to steal the mainframe, Reed noted.

But security threats today involve unauthorized people gaining access to data via compromised credentials or security vulnerabilities at the application layer that allow hackers to steal high-value data from data warehouses and repositories.

Agency managers should rethink their encryption strategies and move beyond a piecemeal approach to data protection. They need an advanced data protection system with an adaptive architecture that combines analytics, automation and built-in security to help agencies and organizations meet demanding data protection and compliance requirements for enterprise hybrid IT environments.

## About GovLoop

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 270,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

## About Micro Focus Government Solutions

Micro Focus Government Solutions is a purpose-built, mission focused company that serves US public sector clients. A company anchored by success in the IT industry, Micro Focus Government Solutions is uniquely positioned to help your organization bridge the gap between legacy systems and modern innovation. Backed by one of the largest pure-play software companies in the world, Micro Focus, we help solve critical IT challenges with software solutions in Hybrid IT, DevOps, Security & Risk, and Predictive Analytics.

www.microfocusgov.com

1152 15th St. NW Suite 800
Washington, DC 20005
P: (202) 407-7421 | F: (202) 407-7501
www.govloop.com
@GovLoop