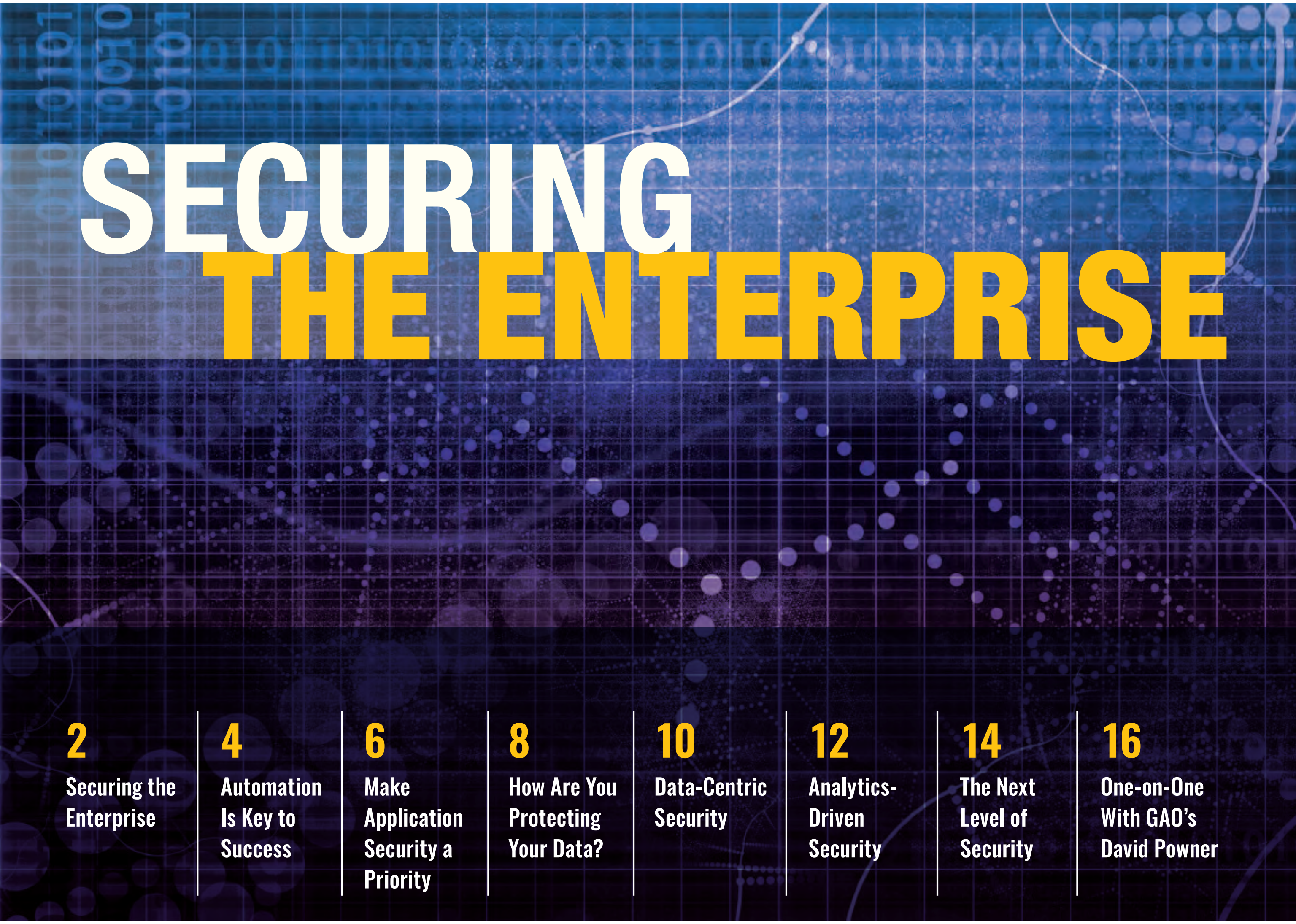
SPONSORED CONTENT

GCN

INNOVATION IN GOVERNMENT



SECURING THE ENTERPRISE

The increasing complexity of the federal IT enterprise makes it more important than ever to raise the bar on cybersecurity.

MEETING THE DEMANDS OF THE NEW ENTERPRISE

Securing the government IT enterprise is not getting any easier.

IN RECENT YEARS, agencies have been investing in technologies such as cloud, mobility, and big data that have the potential to transform how they manage their IT operations and deliver services both to their employees and to the public.

But transformation has had an unintended consequence: added complexity. That complexity makes it difficult to secure the enterprise. With so many moving pieces and dynamic workloads, it can be difficult to identify and mitigate potential security and performance problems before the damage is done.

In a recent federal buying study conducted by the 1105 Public Sector Media Group, 84 percent of respondents agreed that technology initiatives have increased in scope and complexity.

Ron Ross, Fellow of the National Institute of Standards and Technology (NIST) and one of the federal government's thought leaders on cybersecurity, argues that the increasing complexity of the federal enterprise amounts to a greater "attack surface" for hackers to exploit.

"When you look at the complexity of the things that we're building today, we've gone past the time when we can actually understand what we have and how to secure it," said Ross, speaking last year at a conference hosted by the Open Group.

Complexity, Ross has said, is "an adversary's most effective weapon in the 21st century."

The federal government recognizes this challenge. The Obama administration's budget request for 2017 includes $19 billion for cyber investments, a 35 percent increase from the final 2016 budget. The Department of Veterans Affairs, for example, is seeking to boost cyber spending by $128 million, which would be a 34 percent increase over the current year.

Despite the administration's increased focus on security, "the cyber threat continues to outpace our current efforts," Michael Daniel, the White House's top cybersecurity advisor, told reporters on a Feb. 8 conference call.

But complexity is the order of the day, as the federal government continues its push to consolidate data centers. The Federal Information Technology Acquisition Reform Act (FITARA), signed into law in December 2014, enacts the requirements of the 2010 Federal Data Center Consolidation Initiative (FDCCI).

The forthcoming Data Center Optimization Initiative, released in draft form in March, raises the bar yet again. The new policy, which will supersede FDCCI, reiterates the federal government's "cloud first" policy and directs agencies to make shared services a priority.

In the coming years, federal IT infrastructures and cyber strategies also will bear an increasing burden from digital services. During the last three years, agencies have been exploring how to better engage with their constituents through new and emerging digital media. Once they are available on a large scale, these services could begin to take a toll on the enterprise.

> "People are connecting stuff to the Internet that we never thought would be connected. You know people are working on hacking your Fitbit."
>
> —**Lt. Gen. Edward Cardon,** Head of the Army Cyber Command

In a recent survey conducted by the 1105 Public Sector Media Group, 50 percent of respondents said they were "very concerned" by the security risks associated with digital services, while 44 percent were equally concerned about the strains on the IT infrastructure.

The challenges could be even greater with the Internet of Things (IoT). With the IoT, the goal is to tap into the massive amounts of data that are already being collected in our hyper-connected world to develop new applications for managing agency operations or delivering innovative services. The sheer scale of the data and connectivity has caught the attention of federal IT leaders.

The Army, for example, is giving the IoT a lot of thought. Speaking on Jan. 29 at the Institute of World Politics in Washington, D.C., Lt. Gen. Edward Cardon, head of the Army Cyber Command, said that the Defense Department is looking for ways to leverage the military's countless IoT assets, while also thinking hard about the security.

"People are connecting stuff to the Internet that we never thought would be connected," Cardon said. "You know people are working on hacking your Fitbit."

This is a familiar dilemma for federal agencies. More often than not, the emergence or evolution of key technologies inevitably increases the complexity of the federal IT enterprise, raising new concerns about both security and performance. But there is no going back to simpler times, because the benefits of innovation are worth the extra work involved.

The task now is to leverage other new or evolving technologies to manage that complexity. Here is a look at some of the tools that are making this possible.

THE FEDERAL IT ENTERPRISE TOOLKIT

NETWORK VIRTUALIZATION

By now, just about every agency has invested in server virtualization, recognizing how it improves the manageability and scalability of the data center. Now they are realizing the value of network virtualization, which allows them to treat their physical network as a pool of transport capacity.

STORAGE VIRTUALIZATION

Like server and network virtualization, storage virtualization puts the intelligence at the virtual machine level. This simplifies the management of storage resources, while also providing storage managers with an unprecedented ability to define service levels.

ADVANCED ANALYTICS

Agencies might not realize it, but they already have a wealth of data on the security and performance of their enterprise. This is data generated by their various networks and systems. Given the right tools, IT managers can gain unprecedented visibility into inefficiencies, performance bottlenecks, and hidden vulnerabilities or cyber threats.

APPLICATION DELIVERY AND SECURITY

When it comes to enterprise performance and security, people often focus on the infrastructure. But it is also critical to optimize operations at the application layer for both availability and security. This is especially important as agencies look to mobilize the workforce.

DIGITAL RIGHTS MANAGEMENT

Video and other rich media will play a vital role in the new generation of digital services. The question becomes how to manage and protect that content across various platforms. A new generation of digital rights management software is rising to the challenge.

CLOUD AUTOMATION

As agencies begin to shift applications and services to the cloud, they will see immediate benefits in terms of the adaptability, agility and efficiency of the enterprise. But to make the transition really pay off, they need to invest in pervasive automation, as a way to both reduce the workload on IT administrators and to enforce consistent, effective processes.

SPONSORED CONTENT

AUTOMATION IS KEY TO SUCCESS

Automation is the answer to the continued push for data center consolidation and delivering cloud-based services.

ADAM CLATER
CHIEF CLOUD ARCHITECT
NORTH AMERICA
PUBLIC SECTOR, RED HAT

GOVERNMENT AGENCIES find themselves at an interesting intersection of the forces of technology and security. On one hand, agencies are being pushed to observe more stringent security guidelines to avoid breaches of public trust, core infrastructure, and national secrets.

On the other hand, there's an ongoing drive for data center consolidation and a movement toward shared, cloud-based services. These have become a cornerstone of the government's need to balance the fiduciary crunch with constituents' needs and expectations.

Even in this virtualized world, deploying resources within data centers can still take days, weeks or months. Securing workloads and infrastructure continues to be a customized process. There's little in the way of repeatable processes as projects move from development to user acceptance and on to final production environments.

Moving these workloads and processes into cloud environments often finds us no better than when we started—and possibly spending more on operations and maintenance than in our own data center. In fact, many of the "cloud" implementations of today are little more than a workload lift and shift; reminiscent of managed services providers.

When these outsourcing strategies improve processes and provide greater return on investment, they're a smart move. But let's not confuse the two. Too often cloud approaches are boiled down to lowering the total cost of ownership of individual servers or virtual machines. They don't take the leap of truly laying the foundation for innovation and holistically lowering the TCO.

At first glance, it would seem these priorities and their solutions are divergent. In fact, success with both lies in how you manage and automate your existing data center. Rest assured—the future is bright, and the cloud offers the federal government immense adaptability, agility, and efficiency.

It all depends on how federal IT administrators choose to view the cloud, and the steps they take to implement a cloud strategy. Automating deployment, security and application lifecycle management helps prepare agencies and their workloads for cloud deployment. Those same steps will also make cloud migration and moves between clouds successful.

Much of how you reap the benefits of cloud deployments will depend heavily on your ability to automate cloud resource usage. If your virtual servers require human interaction for provisioning or updating, seek tooling to automate those processes. The same goes for application deployment and scaling.

Automation is the name of the game when it comes to the cloud. As soon as a user has to log into a cloud-based server, the value is diminished. The good news is you can develop these practices within your existing data centers. All you need is new tooling to build a Continuous Integration and Continuous Deployment (CI/CD) infrastructure.

Take a staged approach to cloud adoption. Start small. Choose a small, user focused application (aka system of engagement) you can use to build a proof point around both cloud and agile development approaches.

In the beginning, stay away from applications that require wholesale change to existing data and application infrastructure. Success will breed success. You can build subsequent application migrations on the patterns and procedures you develop in the process of successfully moving these workloads.

__Adam Clater__ is the Chief Cloud Architect, North America Public Sector, Red Hat.

SPONSORED CONTENT

MAKE APPLICATION SECURITY A PRIORITY

To truly defend against evolving threats, federal IT leaders must apply security at the application layer.

RANDY WOOD
VICE PRESIDENT FEDERAL,
F5 NETWORKS

FEDERAL IT MANAGERS, CISOs and security professionals are often overwhelmed and confused with the seemingly endless volume of security threats, warnings, solutions and vendors. Firewalls, intrusion detection and prevention, APT, threat intelligence, compliance, cloud security, DLP—the list goes on and the "cyberscape" grows more confusing.

Amid all this confusion and uncertainty, there are three imperatives—the underpinnings of any sound cybersecurity implementation—federal agencies should focus on now.

1. **Zero trust means zero trust.** An analysis of recent attacks on federal IT systems reveals the vast majority have resulted from users handing over some level of trust to an attacker. The trend in application access is to trust no one, no connection, and no traffic flow; and relying on advanced encryption and identity management to establish trust. This means securing network infrastructure devices that are almost always overlooked when it comes to strong, multi-factor authentication.

The DoD Cybersecurity Discipline Implementation Plan, from October 2015 and amended in February 2016, prescribes Four Lines of Effort (LoE) to better secure DoD networks and applications. LoE 1 is Strong Authentication involving PKI/CAC-enabled authentication for all applications, accounts, servers and network devices. "The connection between weak authentication and account takeover is well-established," the plan notes. "Strong authentication helps prevent unauthorized access, including wide-scale network compromise, by impersonating privileged administrators." Implement strong authentication for not just users and applications, but also devices.

2. **You can't secure what you can't see.** Data encryption (SSL and TLS) has traditionally deterred malfeasance on websites with high-value assets. Over time, SSL adoption has extended to everyday websites to protect user information. While approximately 30 percent of popular websites currently use SSL, this trend is growing 20 percent annually. At the same time, the bad guys are using the same technology to encrypt their conversations that federal agencies are using today.

The point is federal agency IT network managers must inspect inbound and outbound traffic. This includes encrypted traffic. When using a traditional firewall or IPS device, users can expect a 70-90 percent performance tax. If there's no inspection, agencies are blind to about 50 percent of all traffic. Agencies must deploy purpose-built SSL inspection devices to eliminate security blind spots.

3. **Strong security must scale across all modes.** The security world has typically been described in rigid or structured ways. Defined perimeters are drawn across network boundaries. Today's perimeter is based simply on two things: access and applications. This is independent of time, space, and even device type and consumption mode (cloud, on-premises, or hybrid). The challenge for federal security professionals is to implement strong security that scales across all access modes, while not impeding the application experience. That's a tall order.

For applications and systems access, federal security professionals must deploy access and identity architectures based on full user, application, and network context awareness to ensure single-sign on and application access federation.

Finally, consider that 90 percent of a typical federal organization's security investment has been on threats to the network. Nearly 75 percent of attacks have been targeted at the application. It's time to make application security a priority.

Federal agencies must create and deploy consistent, tailored policies and services—on an application-by-application basis—based on risk, context and visibility at the application level.

Randy Wood *is Vice President Federal, F5 Networks.*

HOW ARE YOU PROTECTING YOUR DATA?

Data is the currency of the modern world, so you must protect it as if it were truly currency.

MONICA MCEWEN
PUBLIC SECTOR
DIRECTOR, QLIK

WHEN YOU THINK of "information" and "security" together, you automatically think of cybersecurity. The increasing need to protect sensitive data from theft is fueling the industry's exponential growth, from $75 billion today to a projected $170 billion by 2020. Cybersecurity is to this decade what plastics was to the 1960s.

There's more to protecting your data than simply keeping it out of the wrong hands. Data is the currency of today. Your data holds potential. There could be information buried within your agency's data that could change the world—the cure for the Zika virus or the missing piece that will lead to ISIS leaders' arrest. Even if it's something more ordinary, information equals value.

Data governance may be far from sexy, but it's equally as important in protecting and deriving value from your data as its more fashionable cousin cybersecurity.

With so much focus on keeping your information safe from intentional theft and ensuring its integrity, your agency's ability to make full use of that data is often stifled. According to a recent survey of Federal decision makers by Market Connections, 65 percent of organizations don't have an analytics tool in place to consolidate data. The study also found more than half (53 percent) of organizations need to consolidate information from more than one source.

So what are these organizations using in lieu of analytics? The vast majority use Excel and other desktop tools. This trend is concerning for three reasons:

- the lack of protection around the data
- the manual staff hours required to compile the data
- the subsequent inability to see the whole story within the data

The result is agencies are using incomplete and inaccurate data to make decisions. Instead of analyzing information, agencies are spending countless hours manually compiling the data. According to the Market Connections study, the more data sources an organization uses, the more manual staff hours are required.

Of even greater concern is that after spending all that effort compiling the various data sources, the data now resides in a format that is prone to errors, has no inherent security and can be easily manipulated. If ten people from the same agency come to a budget meeting, they'll likely have ten different versions of the current spend.

With data volumes growing exponentially and organizations regularly collecting billions of data records from multiple sources, the negative effects of using spreadsheets to manage the agency are magnifying.

The increased influx of data could mean a bigger burden on IT—but it doesn't have to. Imagine if your users were empowered with a governed data library that provided the freedom to explore the information they needed without the risk of data leakage or dumps into Excel? These technologies exist today.

Buried within your data are countless answers. There are likely answers to questions you haven't even yet thought to ask. To ensure the intrinsic value of that data is maintained, it's critical to compile, analyze and visualize your data with tools that protect your information through a data governance process that delivers the right information to the right people. In the end, the entire agency must be making great decisions based on timely, accurate information.

__Monica McEwen__ is the Public Sector Director, Qlik.

MALAYSIAN JUNGLES
CANDY SALES
Qlik® helps you find unexpected connections in your data.

SPONSORED CONTENT

DATA-CENTRIC SECURITY

Why agencies need agile, persistent security at the data-level.

BARRY LEFFEW
VICE PRESIDENT PUBLIC SECTOR, ADOBE SYSTEMS INCORPORATED

GONE ARE THE DAYS when agency endpoints were confined to systems connected to a LAN in a brick building– easy to secure and manage. Endpoints now include virtual users, smartphones, tablets, external consultants and partner organizations. Information is pushed and pulled to devices internally and externally, increasing the risk of exposure and likelihood of theft. Security needs to become more agile, more persistent, more predictive, and more dynamic. To get there, cyberdefenses must move to within the perimeter, the hardware, and even the device. It must move down to the data level.

Policies Drive Change

Recognizing those issues, the Office of the President recently directed the Administration to implement the Cybersecurity National Action Plan (CNAP). This plan calls for all federal agencies to take a multi-layered data protection approach to better secure the government's most sensitive data.

The Office of Management and Budget (OMB) agrees. OMB has been urging agencies to implement capabilities to "protect high value assets and sensitive information" within the next year. Those two policies point towards implementation of a multi-layered cybersecurity strategy that includes data-centric security.

What is Data-Centric Security?

Data-centric security targets and protects the data itself regardless of its location—inside or outside of the firewall and on any device. It adds another critical layer of fortification to existing security measures. Data-centric security encrypts the native file format itself. This helps ensure data remains more secure wherever it travels or is stored. The decryption server and keys often reside in a different location than the data, which further enhances protection. Only a device with the proper client technology and authentication controls can decrypt the file.

But encryption alone is not enough for data-centric security, though. It's like padlocking your wallet and throwing it into the ocean. Your wallet is safe, but you have no idea where it has gone or what happened to the contents. When choosing a data-centric security solution, select one that combines security strength with persistent, dynamic control.

Persistent, Dynamic Control

Persistent, dynamic control has four key elements:

1. Ability to remotely push dynamic policy and access changes on the fly without having to revoke and renew access
2. Continuous auditing of location and events, inside and outside the firewall
3. Digital signatures to confirm the identity of each person who signed a document, confirming it hasn't been altered in transit
4. Extension beyond LDAP authentication to support for a range of authorization sources

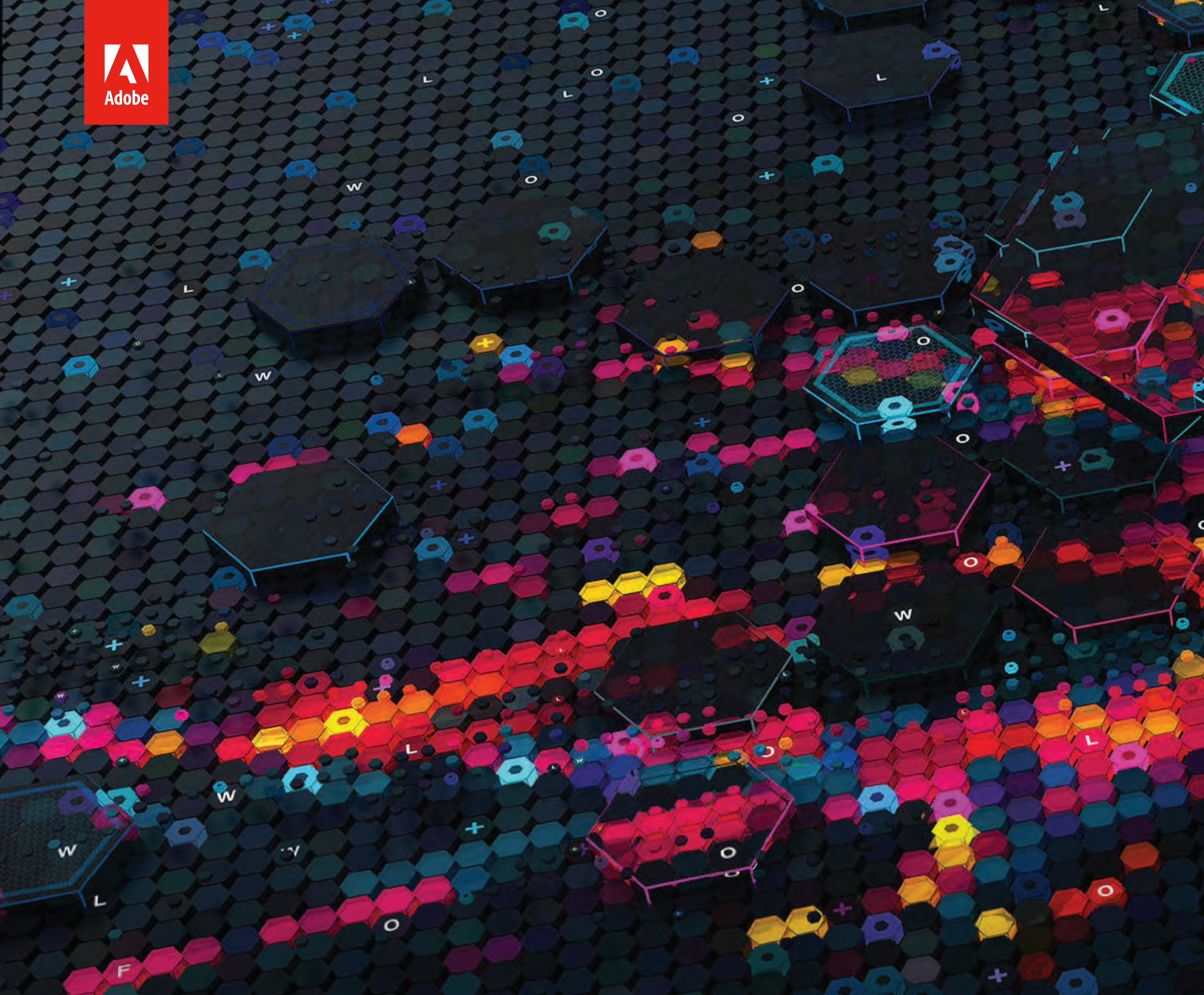
By adding persistent dynamic control to data-centric security, the agency is able to stay in contact with the data—pushing policy and access changes, receiving information about who's accessing, how it's being used and how frequently, and helping to ensure authenticity and integrity. Employing this approach, your agency will be able to better manage your data wherever it goes in the world, predict internal and external threats, and respond with agility to changing operational needs.

__Barry Leffew__ is the Vice President Public Sector, Adobe Systems Incorporated.

WHAT TO LOOK FOR IN A DATA-CENTRIC SECURITY SOLUTION

- **Flexible Deployment:** Is it available on-premises or in the cloud with FedRAMP authorization?
- **Infrastructure Flexibility:** Does it support a wide variety of infrastructures, operating systems and authentication providers?
- **Custom Workflow Support:** Does it support application development for custom workflows?
- **Client-Side Support:** Does it require a dedicated client to decrypt? Is that client available/authorized within your agency?

Adobe



Data-Centric Security

Your agency's data is on the move, now your security can move with it.

Adobe solutions deliver security capabilities at the data-level with persistent, dynamic control.

Learn more at carahsoft.com/innovation-adobe

SPONSORED CONTENT

SECURING THE GOVERNMENT

Cyber threats are on the rise, so government agencies must prepare and defend.

KEVIN DAVIS
VICE PRESIDENT
OF PUBLIC SECTOR,
SPLUNK

U.S. GOVERNMENT organizations are prime targets for advanced cyber threats. Over the past two years, attackers have targeted agencies across the federal landscape—civilian, defense and intelligence. Some attacks left a bigger mark than others; namely the high-profile breaches against the Office of Personnel Management.

The attention cybersecurity incidents are gaining is causing government CIOs and agency leaders to reexamine their security practices. Tony Scott's "cybersecurity sprint" last summer jump-started the discussions, but the strategic evaluation of how agencies approach and manage cybersecurity is ongoing.

The first piece of this is to understand the reality of the current government environment. The threat landscape is more complex than ever. Not only are there more external threats from determined and sophisticated attackers, but the challenge of insider threats is also rising.

The Office of Management and Budget just released its annual Federal Information Security Modernization Act (FISMA) report. There was a 10 percent increase in cybersecurity incidents from 2014 to 2015. So while federal leaders are undoubtedly paying more attention to security, the number of security incidents continues to climb.

The greatest obstacle agencies face is their IT systems and applications are still siloed. There is limited collaboration and communication between the teams managing these assets. Ultimately, what security teams and CIOs need most is enhanced visibility into what's happening across systems and networks. Analysts need the analytics capabilities to provide valuable, real-time intelligence where it's required.

To achieve an effective analytics-driven approach to security, agencies must understand all data is security relevant. Leveraging the power of machine data analysis, which includes records of activities and behaviors involving users, transactions, applications, servers, networks and devices, is a comprehensive approach to this challenge. Viewing information as individual, siloed data sets may not provide much value, but bringing that data together to provide an enterprise-level picture is extremely valuable for decision makers.

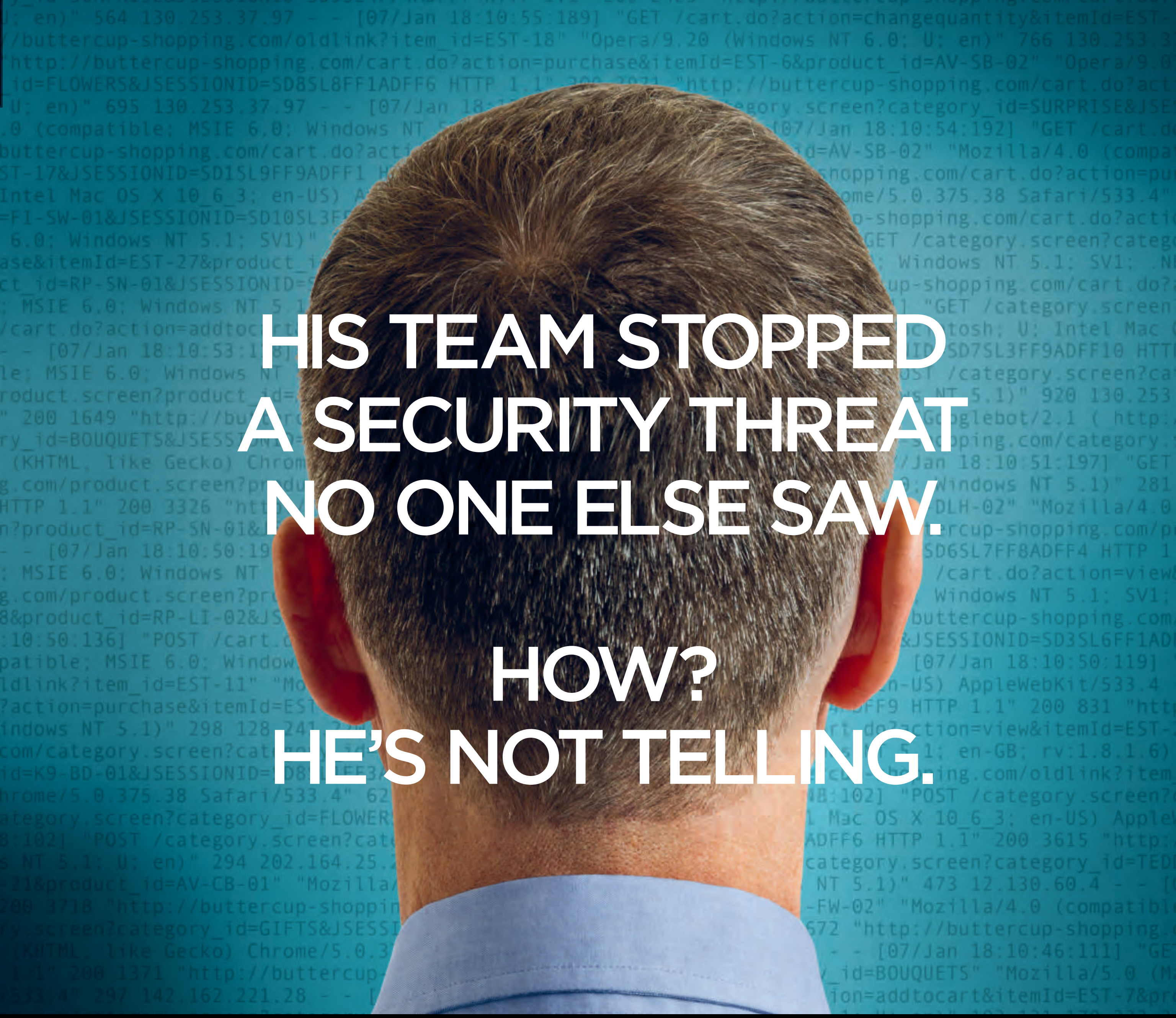
Embracing a machine-data, analytics-driven approach doesn't just help with security. It also enhances agencies' abilities to address IT operational challenges and improve citizen services delivery. If a system or process isn't performing well, it's imperative to identify the issue and take steps to ensure the problem is solved. Not only is this important from an efficiency and operational perspective, but it also affects security.

IT modernization is critical to addressing cybersecurity. Many of the vulnerabilities government agencies face today are the result of outdated, legacy technology. This is undoubtedly a big reason why the administration included a $3.1 billion IT modernization fund in the budget proposal submitted to Congress in February. That's on top of the $19 billion that was budgeted specifically to address cybersecurity.

The government's Continuous Diagnostics and Mitigation (CDM) program is a promising initiative for improving the overall government cybersecurity posture. CDM will deliver comprehensive risk and security management capabilities to agencies through a diverse set of solutions, helping agencies achieve comprehensive, single-pane of glass visibility across their environment. With that enterprise capability, CIOs and security teams can gather real-time insights to quickly and effectively respond to potential threats. This will help reduce the risks for agencies and departments.

New cyber threats emerge every day. Malicious actors will continue to seek out vulnerabilities to infiltrate agency networks and access sensitive information. As these threats evolve, government agencies, in collaboration with industry, must continuously seek to enhance and adapt their cybersecurity measures to combat adversaries.

__Kevin Davis__ is Vice President of Public Sector, Splunk.



Splunk® solutions give security teams visibility across the infrastructure so they can quickly detect and contain malicious activity before it becomes a breach. Government security experts use Splunk software and cloud services to protect their organizations, but only a few of them will talk about it.

Get Splunk's analytics-driven enterprise security through Carahsoft.
Learn more at carahsoft.com/innovation-splunk

splunk®> listen to your data®

THE NEXT LEVEL OF SECURITY

Software-Defined Networking can deliver on promises of security and functionality.

MATTHEW SCHNEIDER
SENIOR DIRECTOR
US PUBLIC SECTOR, VMWARE

FOR YEARS, enterprises and government agencies have relied on networks and security designed to support traditional client-server environments. Just as the cloud has disrupted storage and operations, software-defined networking (SDN) is now disrupting that traditional network model. The new SDN model better supports the demands of today's applications and big data.

Software-defined networking is helping agencies apply technology in places they haven't been able to before because of historic environmental limitations. Now developers are building and introducing applications as systems. That means more network traffic is "east-west," running from server to server within the data center.

The historic networking model is far different. It was designed to deliver traffic back and forth from the server to the user, not machine to machine. SDN helps system managers master their infrastructure and segment the network at a level much closer to the application. This type of segmentation greatly improves security.

Think of the network and its applications as being set up like a house. If someone leaves a window open in a house, a thief can get into that room. In a traditional environment, the thief would now be able to get into every room in the house. With segmentation, he won't be able to get into the next room because each room's door is locked.

This trend is called micro-segmentation, and it's changing the way agencies address security. In fact, it's one of the principles defined in the Federal Information Technology Acquisition Reform Act (FITARA). FITARA recommends segmenting down to the lowest level possible to protect applications and better understand what those applications do when they're running in the data center.

Obstacles to Success

The primary roadblocks to the widespread use of effective SDN are operational silos within the agencies themselves. Agencies have historically had application teams, network teams, compute teams, and security teams. When they look at software-defined networking, they ask, "Should this go to my application team? Should it go to my compute team? Should it go to my security or network team?" The answer is yes. It should go to all of them.

Successful agencies have also had leadership that ponders the question, "How can this paradigm shift empower us to enable the mission in a different way?" More often than not, though, the conversation starts with, "We've been compromised. We need to change the way we do things now."

Therefore, substantial changes have typically happened after the fact. But it takes that leadership, whether from the top or within the silos, to say, "We're going to bring these teams together who historically didn't work together day in and day out, to be a better service provider to our agency."

An Evolution in IT

SDN is the next evolution in networking. However, this is truly a cultural change more than a technology change. Agencies are seeing benefits in the way they approach the mission, and not just reordering the way they use technology to execute the mission. It's an evolution in every aspect of IT.

Agencies can learn from this convergence that leadership can have a positive impact on this evolution. They'll also learn that managers from any one silo who drag their feet or dig in their heels can greatly hamper progress.

Combining micro-segmentation with SDN leverages the full power of today's cutting-edge technology. By removing themselves from the physical cabling and limitations of the traditional network, federal agencies can realize the full potential of both the firewall for broad perimeter protection and application-level security to limit exposure to insider threats. That combination will provide agencies with the next level of security and functionality.

***Matthew Schneider,** Senior Director US Public Sector, VMware.*

vmware®

Virtualization has changed the face of the software defined data center with products like VMware NSX™.

HYTRUST
Cloud Under Control

HyTrust together with VMware NSX improve the security posture and risk profile of your data center.

Manage and secure the enterprise with VMware and HyTrust solutions available through Carahsoft.

Learn more at carahsoft.com/innovation-vmware

Executive Viewpoint

ONE-ON-ONE WITH DAVID POWNER

GAO's Director of Information Technology Management Issues describes his agency's progress on infrastructure.

DAVID POWNER
DIRECTOR OF INFORMATION TECHNOLOGY MANAGEMENT ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE (GAO)

The federal government's "Cloud First" policy is supposed to be the governing mandate on how agencies acquire and deploy information technology systems. However, a number of agencies are not yet on that path or are not very far along. David Powner, Director of Information Technology Management Issues at the Government Accountability Office (GAO), studies federal government infrastructure issues from both the agency and interagency levels. Powner recently spoke with journalist Francis Rose about what he sees government doing now with infrastructure and what he sees agencies doing moving forward.

Rose: Data center consolidation is the dominant IT infrastructure issue in government right now. Where does that effort stand? Do the Office of Management and Budget (OMB) and GAO have a handle on the number of data centers yet? Are the numbers even the most important metric to understand in data center consolidation?

Powner: We're starting to get a good handle on the numbers. The inventory changes are slowing down. We're always going to find a few things here and there, but that's starting to solidify. Obviously, the focus so far has been on those inventories, what we're closing, and the dollars we're saving. That's all well and good, and we still want to have some of that. But there's also been a real shift toward focusing on the appropriate metric. Going forward, we really want to utilize the facilities efficiently, as well as the equipment within those facilities, so we're truly optimizing these data centers.

Rose: If we're still talking about metrics for measuring data center consolidation and maximum utilization of servers, we're not going to make a broad-based transition to the cloud for a long time to come, are we?

Powner: No, we don't have as clear a picture of the extent to which federal agencies are in the cloud, or which agencies are utilizing cloud services more than others, as we do on the data centers. We know we're transitioning to the cloud somewhat, but the extent is unknown. We clearly know we're not in the cloud to the extent we should be.

There are still too many agencies that don't have credible transition plans. There are about ten agencies we see that really don't have any plans, and we have made recommendations in our latest report for those plans to be put in place. Some agencies commented they had already conducted their consolidation and savings to date. They expected few additional consolidations and savings going forward. We went back to some of those agencies and said, "You can say you're done, but you're really not, because the metrics actually show you're far from optimizing your centers."

Rose: You mentioned the intention of FITARA to remedy the issue of who's in charge of IT projects at agencies. The role of ensuring that happens falls to Congress. That could be potentially very difficult to do in the next nine to 12 months as we go through a presidential election and a transition from this administration to another.

Powner: There are several key things here. We're expecting a new scorecard on FITARA implementation to come out in May. We also expect

Congress is going to ask the GAO to do a series of reports looking at FITARA implementation issues through the transition period.

A lot of good things are happening at OMB. They're doing a lot of solid planning. When you look at the strategic sourcing initiative the Administrator of Federal Procurement Policy Anne Rung has put in place, and many of the things that Federal CIO Tony Scott has put in place, you see great plans to implement the FITARA law. It's that combination of the legislative and executive branch working together that ensures we don't lose momentum throughout the transition period.

Rose: What do you think the biggest obstacles and the biggest breakthroughs are for agencies that are working through the consolidation and optimization process for their data centers right now?

Powner: We've looked at challenges and obstacles and heard lots of things over the last several years. We've heard that agencies don't have the right metering equipment in place; they don't have the management systems to estimate savings; they don't have good solid inventories of data centers. We're starting to get beyond those challenges. I think the big thing going forward in terms of challenges with optimizing our data centers, is do agencies have real credible plans going forward? Are they focused enough on metrics?

What FITARA attempted to do was to say, "We've done a lot of work on data center consolidation, but we know there's a lot more work ahead because we're nowhere near where we need to be on meeting metrics, so let's get plans in the out years." Our work has showed that there are still too many agencies that don't have credible plans. I think you need to get those plans in place and you really need to focus on the key metrics going forward.

> **"What FITARA attempted to do was to say, 'We've done a lot of work on data center consolidation, but we know there's a lot more work ahead because we're nowhere near where we need to be on meeting metrics, so let's get plans in the out years.' Our work has showed that there are still too many agencies that don't have credible plans."**
>
> —**David Powner,** Director of Information Technology Management Issues, GAO

Rose: What are the important tools—technology tools, policy tools, or something else—that are helping agencies succeed at the consolidation and optimization?

Powner: There's no magic wand they can wave. You need to look at what your requirements are in terms of storage and the infrastructure needed to run your various applications, whether they are commodity or mission critical, and then make sound decisions on the best approach. Ask yourselves, "Are we going to maintain our own centers or are we going to go to a cloud?" That's the decision about buying versus building storage, and the security implications around both of those options. Ultimately, no matter what decision you make, you need effective governance over the execution, whether it's maintaining your own data centers or going to services.

We issued a report in early April looking at cloud contracting and service level agreements. One of the questions we examined was, "Are agencies getting the right performance out of those contracts?" We also looked at the key security measures in those contracts. There are a lot of folks that have a reluctance to go to the cloud because they want to maintain their own equipment and the security over that equipment, but you can also specify those needs adequately and still go to the cloud and accomplish what you need for your various missions.

Rose: Plans are one thing, but the actual deployment, the actual execution, is a whole different thing. I imagine there are some cases where you're seeing plans but you're not seeing much execution.

Powner: We hear several things on that. One in particular about going to the cloud is that there are still many agencies that don't want to give up control. In particular, the obstacle is trusting someone with the data, and the security around that data.

One big issue at many federal departments and agencies is whether we have the right people making the right decisions. We know that there is commodity IT that is being acquired outside of CIO shops. We know there are large mission-critical applications that don't have enough CIO involvement. We really do need to get to a point where we have qualified and strategic CIOs driving a lot of these decisions in conjunction with business partners at the various agencies and departments.

Learn more at carahsoft.com/innovation