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.