Boosting workforce productivity — and network security — virtually

BY FEDSCOOP STAFF

A new generation of virtualization tools can improve workforce productivity while providing IT managers more granular security controls inside their data centers — and on federal workers' devices.

Workforce productivity is on the minds of most agency leaders. Their challenge is how to empower federal workers to deliver better results for taxpayers in an era when funding remains a constant question.

Enterprise leaders routinely turn to technology innovations for the answer. Technology can spur productivity by connecting a dispersed workforce, fueling collaboration and automating workflows; it can also help workers use real-time information to make smarter decisions.

But the growing complexity of technology continues to produce "IT friction" that can undermine productivity. When workers can't readily access the data and tools they need for work, because of equipment configurations or bulky applications, they often turn to their own devices and solutions. That's especially true across federal agencies.

GAPS IN SUPPORT
FOR WORKERS' PERSONAL DEVICES

3/4
of workers rely on **PERSONAL TABLETS FOR WORK**

1/2
rely on **PERSONAL SMARTPHONES**

ONLY 35%
OF MANAGERS SUPPORT personal tablets in their organizations

A recent FedScoop study of federal agency IT trends, underwritten by VMware, found that among federal workers polled, 74 percent rely on personal tablets — and 49 percent rely on personal smartphones — to do some of their work, even though only 35 percent of IT managers in the survey say they support those devices for their organizations.

That gap puts IT leaders in a bind over how to reduce IT friction for workers while still keeping their networks and data secure.

HOW VIRTUALIZATION CAN BOOST PRODUCTIVITY AND SECURITY

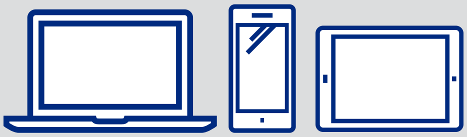
While virtualization is only one part of the solution, a new generation of data center and endpoint virtualization tools can go a long way in providing workers the user experience they've come to expect — while also providing IT managers greater safeguards on data at rest and in motion.

In addition, virtualization tools offer IT departments other benefits, including ways to improve network performance and reduce the frequency of equipment refreshes and upgrades and trim hardware maintenance costs. Virtualized work environments can also enable organizations to use mobile technology more effectively, reducing the need for desktops and the overhead costs associated with supporting them, while increasing operational resiliency.

And because virtual copies of the infrastructure and applications remain available on endpoint devices, even during network interruptions, agency workers can be more productive by being able to work when, where and how they want to.

Half of federal workers polled in the FedScoop study, in fact, say that virtualized work environments, if available to them, could yield a four-hour-per-week gain in productivity. That equates to 200 hours per year in added productivity per worker — an opportunity agency leaders ought not dismiss. Workers aren't alone: Nearly 6 in 10 government IT managers polled in the study also believe that a digital workspace, serving up standardized

DIGITAL WORKSPACES CAN IMPROVE PRODUCTIVITY



NEARLY 6 IN 10
government IT managers believe a
DIGITAL WORKSPACE
that serves up a standardized environment
WOULD MAKE USERS MORE PRODUCTIVE.

IT environments regardless of device or location, would make users more productive.

Much of that productivity gain would come from reducing the IT friction federal workers say they encounter daily on their endpoint devices. Among workers polled:

- 82 percent say work-issued devices don't support the apps they need for work
- 64 percent can't get access to all the apps they need
- 58 percent say multiple password requirements hinder access to the apps and data they need
- 56 percent say applications aren't optimized for mobile devices.

Those figures, and the fact that over 66 percent of federal IT users surveyed say they don't trust the security of their mobile devices, all point to the technical and economic advantages of using a combination of virtualization tools. Included in that mix are tools like VMware's Network Virtualization and Security Platform (NSX) and End User Computing (EUC) technologies, which can provide scalable and secure, end-user connectivity to agency data centers.

PUTTING VIRTUALIZATION TO WORK

If IT managers generally see the value of virtualization, both at the endpoint and in their data centers, what's holding them back?

Agencies face a historic challenge of silos stemming from legacy systems and the evolution of separate teams to support end-user devices, desktops, data centers, scalable network architecture and security, among other technologies. This separation makes it difficult for agencies to modernize and increase productivity among their employees, says Matt Schneider, senior director for VMware's public sector network security business.

Agencies also struggle to manage a multitude of users — employees and contractors working on- premise and remotely using a wide range of devices — and controlling what data and applications they can access from within agency data centers. Add to that the complexity of making applications work on all those devices and integrating security measures within siloed and interdependent networks.

Virtualization tools designed to work across networks and provide standardized experiences for end users can overcome many of those challenges. Agency leaders can start by initiating dialogs among all of their IT specialty teams to discuss how best to address productivity and security issues. Any solution must be a team effort for it to be long-lasting and impactful, says Schneider.

GAINING MORE GRANULAR SECURITY

Traditional security models typically operate centrally within siloed networks and often lack granular and lateral control of resources and data protection. Applying virtualization within disparate networks, without a broader management view, risks further isolating traffic, which could lead to easier propagation of malware or other malicious events through the data center.

More modern solutions, such as VMware's NSX, provide an efficient way to manage desktop-to-application traffic. Each virtual desktop is treated as its own security perimeter with a hypervisor-based firewall between each virtual machine and the infrastructure.

The approach gives IT departments a non-disruptive and agentless method to introduce security into existing virtual desktop infrastructures. It's also easier to manage, with policy controls and automation capabilities that use common language rule sets. Users are defined by user group or what they're doing, for instance, versus the old method of tracking users via IP address. But it also gives IT administrators greater control over which resources users can access from agency data centers.

Inside the data center, agencies previously didn't have controls to stop one server from talking to another, says Schneider. Agencies also struggled to control one virtual machine from talking with others, meaning they had limited control over lateral movement. With solutions like NSX and EUC, however, the east-west movement inside the data center is tightly controlled, and capable of restricting traffic inside their networks that rarely hits a firewall.

> **"NSX allows you to move the security guard from the entrance gate to the perimeter and next to every door in the building on a scaled basis,"** says Schneider. "This is a departure from traditional IT security, which executes security measures between IP addresses, and introduces a new way to manage data security regardless of where the data travels and what device the data resides in."
>
> **— Matt Schneider, Senior Director for VMware's Public Sector Network Security Business**

"NSX allows you to move the security guard from the entrance gate to the perimeter and next to every door in the building on a scaled basis," says Schneider. "This is a departure from traditional IT security, which executes security measures between IP [Internet Protocol] addresses, and introduces a new way to manage data security regardless of where the data travels and what device the data resides in."

Combining network virtualization and security platforms like NSX with virtualized end user computing technology, like VMware's Workspace One, creates a more holistic security posture, while also giving users a more functional, and standardized work environment.

Workspace One, for instance, knows the identity of the user at the edge of the data center. When paired with NSX, this allows agencies to extend policies to determine whether the user should have access to certain applications, whether they can get access from home, and whether the user should be able to talk to this type of server in the first place, according to Mike Wilkerson, VMware's senior director for federal end user computing and mobility. It also offers single-sign-on capabilities to enable agencies to handle multiple endpoints.

MEETING THE NEEDS OF A CHANGING WORKFORCE

Virtualization brings one more advantage: It works the way a growing portion of the workforce has learned to work. One-third of federal government employees are eligible to retire by 2020, according to a Government Accountability Office study released earlier this year. A new generation of workers are set to replace them, who have grown accustomed to working anywhere and at any time.

In order to attract future talent, agencies need to modernize the tools they give their workers to use, and that means modernizing their infrastructure and applications while maintaining the strongest attention to IT security.

Virtualization provides this capability along with the ability to boost productivity, and doing so in a manner that is relatively simple and cost effective to implement and manage.

Virtualization means there's no need to tear infrastructure down and start all over. The power of virtualization, whether in the workspace, virtual desktop or virtual network is to start small and scale quickly. The ability to work within the current infrastructure, and network, and bring virtual machine technology online as an overlay is invaluable.

Federal agencies can thus pay as they go, and increase their virtual network footprints as their IT teams gain more familiarity and expertise with this new, modern technology. With solutions like NSX and EUC, agencies can make these transitions to boost productivity, while always remaining completely secure and within compliance of all federal regulations and best practices.

> **Virtualization means there's no need to tear infrastructure down** and start all over. The power of virtualization, whether in the workspace, virtual desktop or virtual network is to start small and scale quickly. The ability to work within the current infrastructure, and network, and bring virtual machine technology online as an overlay is invaluable.

For more on improving government workforce productivity and security, see FedScoop's Public Sector Innovation Priorities series.

This article was produced by fedscoop for, and sponsored by, vmware