Keeping Government IT Up and Running

Ensuring anywhere, anytime availability of highly secure and compliant applications and workspaces is crucial to worker and citizen satisfaction.

Within the federal government, mobility spending is expected to reach $11 billion in 2023.

Availability is never optional for governmental units. After all, citizens turn to departments such as public safety or first responders when they most desperately need assistance. These professionals depend heavily on the information their systems provide, and if they can't get instant access to data they need in dire situations, the result could be fatal.

Of course, availability goes beyond the necessity—it also includes convenience and engagement. Consider, for instance, meeting an inspector at a local governmental unit to obtain a building permit. In most instances, these engagements are time-consuming and require the completion of far too many forms.

This doesn't have to be the case. Instead, many common transactions could be accomplished through a simple interaction with a highly mobile government employee who visits on-site and conducts all needed activity on a mobile device. The inspector can immediately pull up site plans, compare them with city ordinances, and issue the permit or make change requests within a matter of minutes.

Hewlett Packard Enterprise

vmware

CIO Strategic Marketing Services

This type of interaction assumes that the IT department has adequately empowered its mobile workforce with access to the tools needed to conduct business away from the red-tape-constricted office environment.

Avoiding government shutdowns, slowdowns

Today's governmental units often include a highly distributed workforce. They may be stationed for maximum citizen access in remote offices, such as motor vehicle registries; or they are mobile workers, such as auditors, inspectors, or first responders. To support this dispersed workforce, government agencies often have multiple departments pooling their infrastructure into a larger data center.

A data breach, regardless of size, rapidly erodes trust, which is extremely hard to rebuild. The same holds true for governmental units—perhaps even more so.

If improperly managed, this type of infrastructure can contribute to security woes as well as hamper the ability of the distributed workforce to operate effectively. Nothing is as crippling to an organization as a data leakage incident. A data breach, regardless of size, rapidly erodes trust, which is extremely hard to rebuild. The same holds true for governmental units—perhaps even more so. After all, few are entrusted with as much personal data as the government.

And, unfortunately, with so much personally identifiable data, governmental units are natural targets for today's highly sophisticated hackers. The 2015 Get Transcript breach of 724,000 tax filers, the 2015 office of personnel management breach impacting 21.5 million government employees and contractors, as well as the 2016 Shadow Brokers leak of NSA data all serve as prime examples.

Statistics also show, much like in the private sector, the investment in mobility continues to rise within government agencies. For instance, within the federal government, mobility spending is expected to reach $11 billion in 2023. There is also a widespread need for comprehensive IT infrastructure modernization. Yet, although constituents desire the level of service that only the latest technology can provide, budget constraints often stand in the way of progress.

Ensuring high availability and resiliency

Consistently empowering a distributed workforce with access to the tools they need requires a foundational infrastructure that provides anywhere, anytime availability of highly secure and compliant applications and workspaces. This is where the VMware AlwaysOn Digital Workspace solution from HPE and VMware thrives.

By combining VMware's Cloud Pod Architecture utilizing VMware's AlwaysOn Digital Workspace solution with HPE Proliant DL380 servers and HPE StoreVirtual VSA software, this solution can play a pivotal role in empowering governmental units to securely meet constituent needs.

Reducing risk of data breaches across any device or platform. AlwaysOn Workspace helps governmental units handle sensitive workloads by ensuring that data is always constrained to the data center. What is accessed by end users is essentially a pixel-based stream of the graphical interface. No data is ever sent out to the user. Users can access applications across a multitude of devices without ever fully capturing data. The issues around where the data is located or cached, or the loss of a laptop, all become meaningless, without the need to install complex encryption software. AlwaysOn accomplishes this by leveraging client virtualization to substantially reduce the attack surface–controlling access to sensitive information on end users' devices as well as desktops common in the traditional governmental environment, while keeping data safe in the data center.

With AlwaysOn most of the end-user compute experience runs within the data center. This approach protects sensitive applications and restricts data by keeping everything centralized within the data center. IT can immediately apply software updates and security patches to protect the edge from malware or cyberthreats. This is crucial in eliminating zero-day vulnerabilities. It also provides policy- and role-based access control with a complete audit trail—logging and reporting to help ensure compliance.

Unfortunately, with so much personally identifiable data, governmental units are natural targets for today's highly sophisticated hackers.

VMware Identity Manager, which fully leverages the existing Active Directory environment, provides the core authentication and entitlement functionality. This user authentication process ensures that data never leaves the data center. This capability spans on-premises, remote, and mobile use cases across any device (running Windows, iOS, Android, or OS X). With multiple levels of access controls available, customers can tailor their authentication models in a variety of forms that best suit their business requirements. The AlwaysOn Desktop solution is compatible with most of the top anti-virus protection platforms, such as Trend Micro, McAfee, Symantec, and Sophos. These platforms are capable of running their services in VMware vSphere hypervisors, thereby offloading that task from the virtual desktops, which yields higher capacity and better user experience.

Empowering mobile user base. AlwaysOn provides a very clean, clear option for delivering applications over a network to a broad set of users without the need for extensive infrastructure in the field. This provides the organization a much better option than having to support direct access or through a VPN into the data center.

When taking the traditional approach, even managed devices are essentially punching holes to the firewall by coming in remotely. Each independent device coming in is a security vector creating a path by which an exploit can enter the data center. Without the right protections in place, hackers can gain access to a mobile device and install malware to siphon data from it.

However, AlwaysOn not only delivers services to mobile users with no data attached, it allows IT to effectively drive the end-user privileges by policy down to the level where it can single out sensitive applications and disallow actions like cut and paste.

AlwaysOn also ushers in the ability to leverage rapid deployment through an improved lifecycle management process. The nature of this infrastructure is such that departments or agencies can deploy apps very quickly, shifting the entire process from a matter of months to only days. The cadence improvement results in a more iterative approach to developing powerful applications to better serve the constituent base.

Much like a cloud-based delivery system, AlwaysOn enables a highly scalable, common shared infrastructure that also can be logically segmented to present essential department-specific application sets to the appropriate users whether they are in the office or in the field.

Addressing resource availability. The VMware AlwaysOn Digital Workspace solution addresses the dire need to remove dependency on physical systems through on-demand remote access to resources, even during a disaster. In these instance, whether or not first responders have access to building schematics on file with the city could be the difference between life and death. AlwaysOn provides an architecture that has built-in, ultra-high availability—a true hallmark of the offering. The solution also has essential end-to-end redundancy. Further, AlwaysOn reduces unnecessary outages or disruption in service from failed software updates or device hardware failure.

AlwaysOn Workspace helps governmental units handle sensitive workloads by ensuring that data is always constrained to the data center.

Because workers can conduct business on true endpoints, governmental units can invest in technology that inherently has a better total cost of ownership model versus the traditional deployment of desktop computers.

HPE & VMware: Alliance for government transformation

Drawing on over 16 years of partnership, engineering, and joint investment, the alliance between HPE and VMware provides its clients with comprehensive solutions that benefit from HPE serving as the one end-to-end support provider. As industry leaders, HPE and VMware are constantly collaborating to revolutionize virtualization economics and efficiencies for the client.

For instance, HPE management tools are designed to work with VMware to enable the best managed VMware environment, with key integrations for HPE OneView, to allow the richness of management data provided through ESXi.

Together, HPE and VMware have a proven track record of addressing key business challenges for IT organizations by improving cybersecurity, supporting transformation initiatives, lowering cost, and increasing automation.

For more information, please read our white paper: HPE Reference Configuration for building a VMware AlwaysOn Digital Workspace with HPE ProLiant DL380 Gen9 servers