TRANSFORM SECURITY

Evolve Federal IT to Strengthen Cybersecurity and Compliance across Information Systems and Infrastructure

AT A GLANCE

VMware's end-to-end cybersecurity solutions streamline compliance and extend security from the data center to the endpoint device with identity-based access management, network and application micro-segmentation, and real-time enforcement of security-hardening guidelines and policies. With VMware, federal agencies can securely deploy digital-first infrastructure while maintaining vigorous cybersecurity standards across users and endpoints.

KEY BENEFITS

- Transform security architecture by distributing security functions across the data center
- Leverage micro-segmentation to extend security beyond VDI and mobile endpoints
- Enforce compliance and automate remediation against security threats
- Enforce role-based policies and granular DLP controls from a unified management platform
- Streamline compliance processes and enable visibility on and off premises

Firewalls Are No Longer the First Line of Defense

The U.S. Government Accountability Office (GAO) issued a cybersecurity report in 2017, stating that it "consistently identified shortcomings in the federal government's approach to ensuring the security of federal information systems and cyber critical infrastructure as well as its approach to protecting the privacy of personally identifiable information (PII)."[1]

In an environment where end users are no longer neatly contained behind perimeter firewalls, attackers are more sophisticated than ever before, and internal data leakage—whether intentional or not—is both a constant threat and reality, federal agencies must evolve security architecture to protect existing infrastructure and defend against rapidly emerging threats.

VMware Solutions for Federal Cybersecurity

When the only constant is change—and identity has become the primary attack vector—it's time for federal IT to re-evaluate its approach to cybersecurity and how it can adapt to keep data and applications safe. VMware can help agencies stay on top of changing security needs with a multilayered, software-defined approach to cybersecurity that maximizes visibility and control of the entire ecosystem. A ubiquitous software layer abstracts underlying infrastructure from the applications running on top of it, allowing agencies to attach and automate policy-based security controls to individual users, applications, and endpoints—creating an intrinsically stronger foundation for protecting agency data and maintaining compliance.

Secure Application Infrastructure

Cybercrime is the fastest-growing cause of data center outages. While specific methods vary, most breaches employ a common strategy that exposes the fundamental weakness of the perimeter-centric network security model—penetrating the perimeter and spreading laterally from server-to-server (east-west). To prevent this lateral movement across infrastructure, VMware offers a network virtualization solution that abstracts the underlying infrastructure from the applications running on top of it—whether that infrastructure is on-premises or in the cloud.

By embedding networks in the hypervisor layer, agencies can attach network, automation, and security services to policy-driven workloads. This layer of abstraction enables micro-segmentation, applying the principle of application-centric least privilege by letting security policy follow an individual application—effectively reducing the infrastructure's attack surface. This abstraction layer also provides a platform for IT to insert additional third-party services for more advanced security protection and provides an ideal point to encrypt data at rest at the workload level.

Secure Identity and Endpoints

As missions go mobile, the devices, applications, and OS's powering mobile workflows are proliferating fast. VMware helps solve the challenge of supporting and securing disparate devices and platforms with endpoint management solutions—including VMware AirWatch® and VMware Workspace ONE™—that apply a ubiquitous software layer across users and endpoints to verify user identity and device posture. Protect all endpoints, including physical desktops, smartphones, tablets, laptops, and IoT devices, and seamlessly deploy any app—including native, web, remote, virtual apps and Windows desktops—through a single app catalog with built-in single sign-on and endpoint compliance across any virtual, physical, or cloud-based environment. Protect and encrypt data in transit and at rest; support two-factor authentication across web, cloud, and native apps using CAC and PIV cards, derived credentials, certificate-based login, biometrics, and third-party authentication services such as Symantec and RSA SecurID; and maintain compliance across the infrastructure.

Maintain Compliance

Managing risk and maintaining compliance is always a major concern for federal agencies. Regulations and requirements are growing as cyber threats continue to evolve, making it more difficult than ever to ensure and demonstrate compliance. Agencies can leverage VMware's ubiquitous software layer to apply compliance controls and visibility across application infrastructure and endpoints, and dynamically insert validated tools and services from VMware ecosystem partners to further streamline the compliance process. The VMware Compliance Reference Architecture Framework links integrated software and hardware capabilities and specific regulatory controls with independent audit validation. Through an independently validated program, agencies can securely run highly regulated workloads while complying with federal standards such as FedRAMP, Common Criteria, CJIS, and more.

Learn More about VMware Solutions for Federal Government

To protect critical infrastructure, national security, and citizen PII, federal agencies must align cybersecurity architecture to today's threat landscape. VMware's comprehensive security architecture, rooted in the Software-Defined Data Center (SDDC), protects federal data and systems across application infrastructure and endpoints. Using the infrastructure as the first line of defense grants IT the most control and visibility across users, applications, and networks, and enables advanced capabilities such as identity-based access, role-based policy enforcement, and network micro-segmentation. With VMware, agencies can securely deploy a digital-first vision without compromising end-to-end security of digital assets, data, and citizen PII.

Realize the possibilities with VMware.

Visit www.vmware.com/solutions/industry/government/federal

[1] United States Government Accountability Office. "Cybersecurity Actions Needed to Strengthen U.S. Capabilities." GAO-17-440T. Published February 14, 2017

vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com