TECHNOLOGY PERSPECTIVE

EXPANDING GOVERNMENT CLOUD ADOPTION

Intel and Red Hat solutions accelerate digital transformation

Gartner estimates that U.S. federal cloud spending will more than double by 2020. [1]

As a result, cloud computing will soon be considered the normal means of handling infrastructure requirements and application deployment in government IT.

facebook.com/redhatinc
@redhatnews
linkedin.com/company/red-hat

redhat.com

INTRODUCTION

According to a recent report by Gartner, government cloud technology adoption is accelerating. In 2009, the Obama administration established a cloud-first mandate for federal agencies, leading to rapid reprioritization of IT objectives. Gartner estimates that U.S. federal cloud spending will more than double by 2020.[1] As a result, cloud computing will soon be considered the normal means of handling infrastructure requirements and application deployment in government IT.

Through collaboration with industry leaders and the creation of proofs of concept, reference architectures, and demonstrations highlighting hybrid cloud deployments, Intel and Red Hat have co-engineered solutions that can help federal agencies quickly expand their hybrid cloud computing efforts and take advantage of the latest advances in related technologies. These solutions automate operations, delivery operational efficiency, and support agile development capabilities within a standard operating environment (SOE) that is flexible, cost-effective, and easy to configure and maintain.

TABLE OF CONTENTS

[1] *"Gartner Says by 2020 'Cloud Shift' Will Affect More Than $1 Trillion in IT Spending." Gartner Newsroom. 2016. gartner.com/newsroom/id/3384720*

HYBRID CLOUD COMPUTING

Hybrid cloud implementations consist of a mix of environments. These environments can include a private cloud in a datacenter, public cloud services such as Amazon Web Services (AWS) or Microsoft Azure, existing traditional systems and applications, supporting components and solutions from third-party vendors, and multiple data sources. Orchestrating these components effectively within a hybrid cloud environment requires the right management tools. Effective solutions offer seamless, united visibility across the entire infrastructure—including compute, storage, network, and security elements. In addition, a properly planned and deployed hybrid cloud provides significant operational efficiency across the infrastructure and creates an environment that simplifies development of new products and services. By offering greater efficiency and faster application development, hybrid cloud computing can help government agencies resolve long-standing challenges—such as reducing the cost of deploying, managing, and maintaining IT infrastructures—whether an Infrastructure-as-a-Service (IaaS) or Platform-as-a-Service (PaaS) model is selected. For example, IaaS and PaaS cloud models offer benefits that include:

- Quantifiable service-level improvements.
- Increased flexibility through the use of an on-demand model.
- Greater scalability to accommodate changing compute resource demands.
- Closer geographic proximity to end users.

GOVERNMENT CLOUD ADOPTION

To take advantage of cloud innovation, government agencies must meet strict requirements. According to Intel, there are six essential criteria for effective government cloud adoption:

- **Security**. Cloud-based services must be verified and protected from threats to ensure data confidentiality and integrity.
- **Agility**. Services should be manageable using dynamic orchestration to reduce deployment and management time.
- **Dependability**. Cloud-based services must offer reliable performance and comply with selected service levels.
- **Openness**. Open standards, including interoperability and portability, should be incorporated into cloud-based services.
- **Transparency**. Cloud-based services should be easily evaluated, monitored, and audited.
- **Awareness**. Services should be designed to take full advantage of cloud infrastructure and computing device capabilities.[2]

Collaborative projects by Red Hat and Intel have addressed these criteria to support government adoption of hybrid cloud computing. Learn more in the following sections.

[2] *Kenneally, Jim, Kieran Mulqueen, and Jimmy Wai. "Government Cloud Computing: Planning for Innovation and Value." Semantic Scholar. 2014. https://www.semanticscholar.org/paper/Government-Cloud-Computing-Planning-for-Innovation-Kenneally-Mulqueen/ad4c98d48cfae7cf71b1a5331e01a03f52aaf4ae*

INTEL CONTRIBUTES TO SECURE, RELIABLE CLOUD ADOPTION

According to Gartner, the need for increased security will surpass the need for cost savings and agility for government agencies migrating services to the public cloud.[3] A strategic planning assumption made by Gartner states that proper security should be an integral part of the cloud adoption process, both to meet regulatory mandates and to ensure data protection.

Fundamental security considerations include strong identity authentication, protections against threats to application and data integrity, reliable encryption and decryption of data, and secure communications across channels used by government staff. A number of technologies from Intel address these concerns, in addition to bolstering security at the hardware level with built-in protections that complement software security measures.

PREBOOT PROTECTION

Increasingly sophisticated datacenter attacks target basic input/output system (BIOS), hypervisor, firmware, and other software components at the prelaunch stage. Intel® Trusted Execution Technology (Intel® TXT) counters these threats by measuring the hardware and preboot software in a known good state and using these values to validate the integrity of these components before launching the system. A specialized microcontroller, based on the Trusted Platform Module standard, assists in these operations by providing secure storage for security keys and passwords, as well as performing encryption and hash operations. The unique set of measurements within the boot process are recorded to provide a system fingerprint for later comparisons.

With the creation of trusted compute pools across the servers in private, public, or hybrid cloud environments, IT administrators can apply specific policies to label sensitive data and determine its workload placement during operations.

Hybrid cloud operators can use these protections to enhance IT compliance with regulatory mandates and create a layer of protection that is active before the complete system is placed online. Figure 1 shows the sequence followed by Intel TXT to validate the integrity of the components.

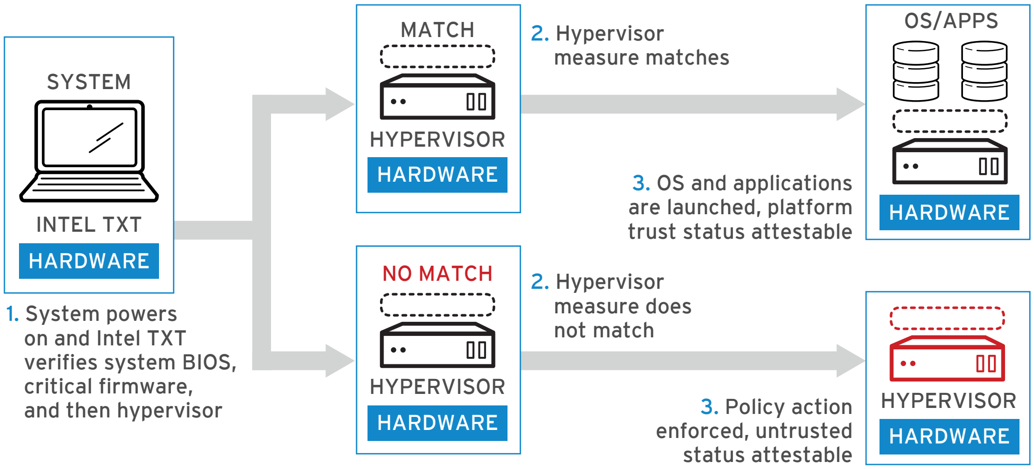
SYSTEM
INTEL TXT
HARDWARE
1. System powers on and Intel TXT verifies system BIOS, critical firmware, and then hypervisor
MATCH
HYPERVISOR
HARDWARE
2. Hypervisor measure matches
OS/APPS
HARDWARE
3. OS and applications are launched, platform trust status attestable
NO MATCH
HYPERVISOR
HARDWARE
2. Hypervisor measure does not match
HYPERVISOR
HARDWARE
3. Policy action enforced, untrusted status attestable

Figure 1. Intel® TXT startup sequence

[3] *"Get Ready for the Inflection Point in U.S. Federal Government Cloud Adoption." Gartner. 2016. https://www.gartner.com/doc/3187120/ready-inflection-point-federal-government.*

A related technology, Cloud Integrity Technology, was co-engineered by Intel and Red Hat to take advantage of the capabilities of Intel TXT and the Intel Trusted Platform Module. Implemented as an enhancement of OpenStack®, Cloud Integrity Technology protects workloads and data during runtime, guards virtual machines (VMs) and containers against intrusions or corruption, and ensures that workloads only run on trusted servers. This technology lets government agencies exercise control over encrypted hybrid cloud workloads by ensuring cloud service providers cannot access encryption keys until an integrity validation of the VMs and container contents is performed.

VIRTUAL MACHINE ISOLATION

Agency CIOs are concerned about ensuring device isolation in multitenant cloud environments to prevent direct memory attacks and protect cloud workload integrity. Continuous memory monitoring is also needed to detect and eliminate malware in production environments.

Intel® Virtualization Technology (Intel® VT) provides hardware-enhanced support that ensures isolated execution of workloads running on IA-32 (Intel Architecture, 32-bit) and IA-64 (Intel Architecture, 64-bit) platforms. This solution includes Intel® VT for Directed I/O, which extends hardware support to strengthen the isolation of I/O operations in shared environments. Direct memory access remapping through hardware creates regions of protected resources that are critical for isolation. Translations are accomplished in hardware, rather than through intermediate software emulation. As a result, government agencies gain extra protection in hybrid cloud environments to alleviate the concerns of agency CIOs and IT professionals.

CLOUD ACCESS ENDPOINT PROTECTION

With a diverse range of devices accessing cloud services, government security strategies are not complete until endpoints are protected as rigorously as datacenter components. 6th Generation Intel® Core™ vPro™ processors offer built-in, hardware-enhanced security capabilities to strengthen overall cloud security. Secure identity access is provided by Intel® Authenticate, using multifactor techniques such as PINs, device proximity, and biometrics to verify individual identities. This feature helps government agencies effectively assign and validate workforce credentials. Another important security feature, walk away lock, automatically locks an unattended computer after a specified period of time.

Hardware protections are also embedded in other areas. For example, Intel® Platform Protection with BIOS Guard uses built-in processor features to protect against BIOS threats and attacks. Similarly, Intel® Platform Protection with OS Guard offers hardware-enhanced capabilities that protect against malware attacks on the operating system. To protect data at rest—whether inside or outside of datacenters—Intel® SSD Pro Series solid-state drives offer hardware-enhanced support for full disk encryption based on the OPAL 2.0 standard established by the Trusted Computing Group.

RED HAT CONTRIBUTES TO AGILE CLOUD DEVELOPMENT AND DEPLOYMENT

Red Hat® technologies offer agile, cost-effective alternatives to traditional, proprietary IT environments that previously dominated government installations. The open source software development model uses a community-powered approach to create innovative cloud-based solutions that are then tested and secured by Red Hat. With flexible IT optimization and hybrid cloud deployments that can interoperate with traditional systems, IT organizations can run traditional applications on existing systems while deploying modern, cloud-based solutions to take advantage of technology advances.

Intel and Red Hat have partnered to provide proven interoperability across Red Hat's software portfolio and Intel architecture hardware components. As a result, government agencies can run a broad selection of standards-based solutions on industry-standard hardware. Together, Intel and Red Hat have defined and implemented trusted cloud solutions that address fundamental security issues to help agencies guard data, communicate securely, and meet auditing and compliance requirements.

For open hybrid cloud configurations, using Red Hat Enterprise Linux® is common across cloud providers. With an SOE, such as Red Hat Enterprise Linux, agencies benefit from timely upgrades, maintenance, and interoperability across infrastructure.

In addition, the following Red Hat open source technologies help strengthen government cloud deployments.

MANAGE HYBRID CLOUD WITH RED HAT CLOUDFORMS

To meet regulatory mandates, IT administrators need visibility into all areas of the infrastructure and a way to audit transactions. Orchestrating the components of a hybrid cloud using Red Hat CloudForms can provide this visibility (Figure 2).

With Red Hat CloudForms, government agencies can deliver services faster using self-service portals and perform ongoing life-cycle management of all services. Expanded visibility into hybrid cloud infrastructure components—including private and public platforms, container-based environments, and virtualized components—supports continuous discovery, monitoring, and inspection of managed resources.

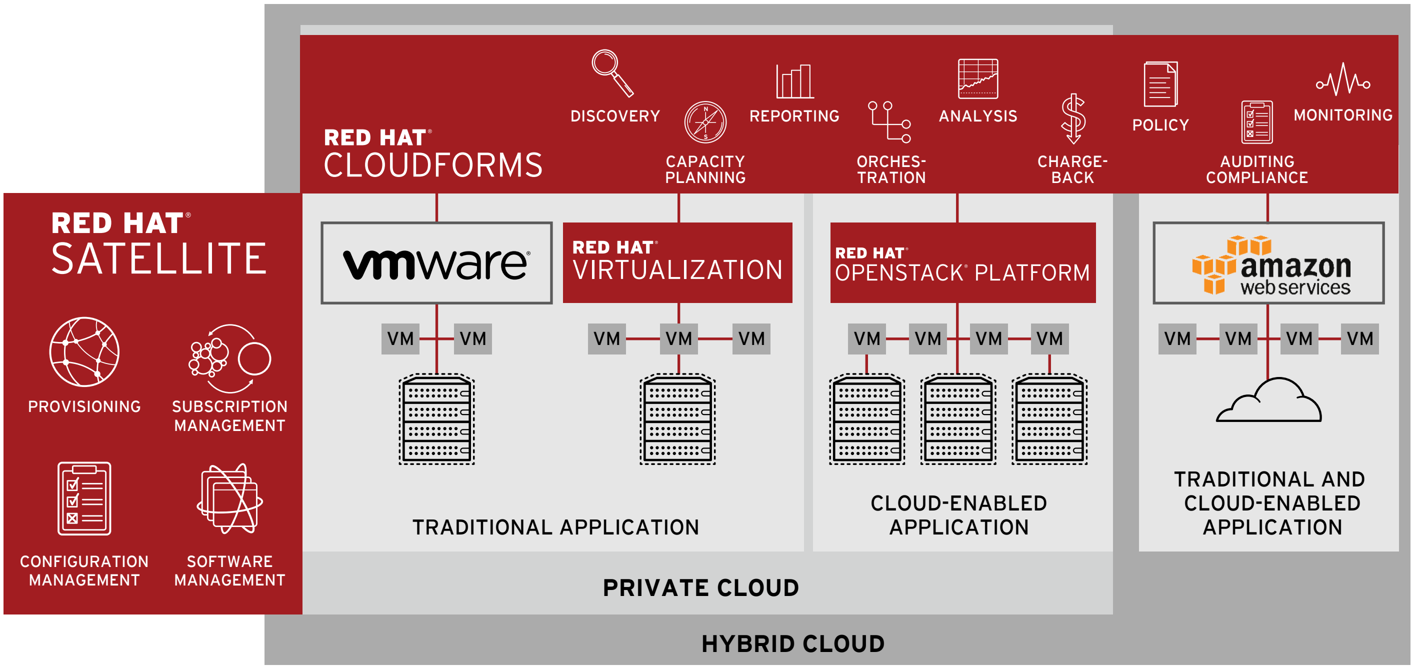

Figure 2. Red Hat CloudForms streamlines hybrid cloud management

DEPLOY A PROVEN CONTAINER PaaS WITH RED HAT OPENSHIFT CONTAINER PLATFORM

Linux containers offer a rich set of capabilities to help government agencies achieve mission goals, including increased flexibility, faster application performance, and more efficient server resource use. In addition to isolation and standardization benefits, containers offer opportunities for innovation by providing portability of massive workloads across public, private, and hybrid cloud environments. As a result, government IT professionals can lower operational costs and improve IT teams' efficiency.

Red Hat OpenShift Container Platform supports container-based deployments alongside traditional core applications. OpenShift Container Platform introduces agility through a production-ready framework that can scale and adapt to massive government IT requirements. This PaaS incorporates co-engineered components developed upstream from Docker, Google Kubernetes, Project Atomic, and OpenShift Origin for full compatibility with Red Hat Enterprise Linux and Red Hat OpenStack Platform.

AUTOMATE I.T. WITH ANSIBLE BY RED HAT

The complexity of hybrid cloud IT environments can present a considerable challenge for government agencies and affect their productivity and expenses.

Ansible by Red Hat is an easy-to-deploy automation engine for many IT tasks, including cloud provisioning, configuration management, application deployment, and service orchestration. Based on the YAML language, Ansible playbooks offer a way to define automation operations in simple terms.

In addition, Ansible uses a simplified model of the IT environment to offer visibility into the resources available throughout the infrastructure. As a result, DevOps development practices can be readily accomplished and teams can work together to automate routine tasks without a need for coding expertise.

ESTABLISH A STRONG HYBRID CLOUD FOUNDATION WITH RED HAT OPENSTACK PLATFORM

Red Hat OpenStack Platform has been co-engineered with participation from Intel to function seamlessly in an environment featuring Intel architecture hardware, Red Hat Enterprise Linux, and Kernel-based Virtual Machine (KVM). As OpenStack relies heavily upon technology built into the Linux kernel, Red Hat and Intel have certified integration between cloud, operating system, and hardware platform components.

For government agencies adopting hybrid cloud, the finely tuned and tightly integrated components of this platform can simplify deployment and reduce maintenance needs (Figure 3).

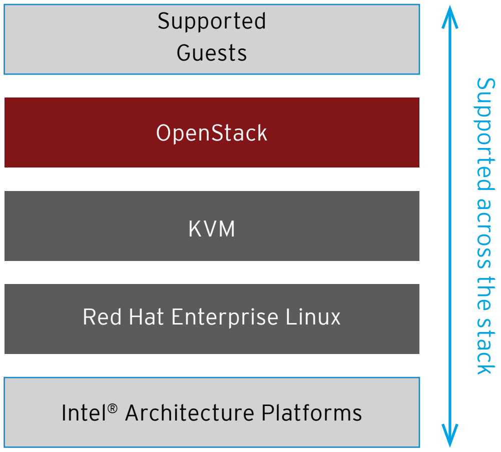

Figure 3. Integration between Intel architecture platforms and OpenStack

MAINTAIN HIGH COMMON CRITERIA RATINGS WITH RED HAT SOLUTIONS

Common Criteria (CC) ratings are used by government agencies to evaluate the security and assurance capabilities of technology products. On a scale ranging from 1 to 4+, Red Hat solutions consistently rate highly.

Red Hat Enterprise Linux 7.1 received CC Certification Evaluation Assurance Level 4+ for an unmodified commercial operating system under the Operating System Protection Profile. This certification marks the first time that an operating system with Linux container framework support has achieved this recognition.

Certification of cryptographic modules is also key for sensitive government installations. Tested for compliance with the Federal Information Processing Standard (FIPS) 140-2, Red Hat Enterprise Linux has achieved 23 of these certifications.

Coupled with built-in hardware security features from Intel, Red Hat solutions provide a protected foundation, from the lowest levels of hardware through the complete software environment.

CHANGING FEDERAL SOFTWARE POLICIES

According to Mark Bohannon, vice president of corporate affairs and public policy for Red Hat, in an article for GCN, policies around the use of open source software in federal agencies have been progressively changing from the question of whether agencies should adopt open source to how they can deploy open source solutions.[4]

The Federal Source Code Policy includes policy updates that encourage greater use and sharing of open source software code and support reuse of custom-developed code to reduce vendor lock-in, decrease the costs of duplicating code, and save money for American taxpayers.[5] This shift proves the effectiveness of the open source development model at improving programming costs and efficiency in the federal government.

"When something open source came across our desk … Ten years ago we were trying to explain it's OK to use it. Today, I think it's about how to use it," said Bohannon. "How can it help you? How are we implementing it? I think we're in a much different chapter these days."[6]

[4] *Bohannon, Mark. "An important fix for the federal open source software policy." GCN. 2016. https://gcn.com/articles/2016/04/13/open-source-policy-gots.aspx.*

[5] *"Federal Source Code Policy." https://sourcecode.cio.gov/*

[6] *Mitchell, Billy. "Open source exploding, generating benefits in new areas." Fedscoop. 2016.fedscoop.com/open-source-exploding-generating-benefits-in-new-areas.*

EXAMPLES OF GOVERNMENT CLOUD SUCCESS

Red Hat is in use in 100% of cabinet-level agencies and in all 50 states.[7] Red Hat engagements with government agencies have yielded positive results at both the state and federal level. Examples of recent collaborations include:

- **North Carolina Department of Information Technology.** A coalition of agencies created the NC Digital Commons to improve state websites by reducing costs and providing more accessible, useful content to the public and government employees. With help from Red Hat, the project team developed a content management system (CMS) running on Red Hat OpenShift Dedicated, hosted on AWS. After these updates, maintenance and staffing costs dropped by US$400,000 a year and web managers can more easily launch and update content. In addition, session traffic to the state's website rose by 58%.[8]
- **NASA Jet Propulsion Laboratory (JPL).** NASA and Red Hat collaborated to develop a private cloud using Red Hat OpenStack Platform. Designed to support NASA's mission of exploring the solar system with robotic space vehicles, the new platform incorporates OpenStack and Linux technology and the scalability to meet the requirements of hundreds of engineers and scientists. In addition, this flexible system maximizes server and storage capacity across the facility by using hybrid cloud technology to respond to peak demands by taking advantage of AWS and other public cloud resources.[9]
- **U.S. Department of Defense.** To improve the elasticity and flexibility of its IT infrastructure, the Department of Defense engaged Booz Allen Hamilton, a technology consulting firm. The firm deployed an updated infrastructure that included Red Hat Enterprise Linux, Red Hat JBoss® Middleware, and Red Hat Virtualization. As a result, the department can meet sudden bursts in user demand more effectively and saved US$5.1 million during the 2015 fiscal year.

For more information about Red Hat engagements with government agencies, visit redhat.com/government.

A COMMON STRATEGIC VISION

For government cloud adoption to succeed, agencies must ensure that cloud solutions will effectively support their data and services and help them resolve IT challenges. Similarly, industry and national regulatory organizations that oversee government operations need to ensure that privacy and data sensitivity laws are followed at all times.

[7] *redhat.com/government*

[8] *"North Carolina transforms its state websites." Red Hat. 2016. https://www.redhat.com/en/resources/north-carolina-transforms-state-websites-case-study.*

[9] *"NASA's Jet Propulsion Laboratory Powers Planetary Exploration with Red Hat OpenStack Platform." Red Hat. 2016. https://www.redhat.com/en/about/press-releases/nasa%E2%80%99s-jet-propulsion-laboratory-powers-planetary-exploration-red-hat-openstack-platform.*

By addressing security concerns, focusing on reliability and stability across complex infrastructures, and building IT environments that support rapid application development and deployment, Intel and Red Hat offer a clear path to safe and secure government cloud adoption. Together, Red Hat and Intel technologies provide visibility into complex virtualized environments and offer control over cloud components for:

- Compliance with regulatory frameworks.
- Effective auditing methods.
- Geolocation of servers across IT infrastructures.
- Support for data sovereignty requirements.
- Automated, fine-grained control of provisioning and VM distribution.

With these capabilities in place, government agencies can confidently invest in cloud deployments.

ABOUT INTEL

Intel Makes Possible the Most Amazing Experiences of the Future

You may know us for our processors. But we do so much more. Intel invents at the boundaries of technology to make amazing experiences possible for business and society, and for every person on Earth.

Harnessing the capability of the cloud, the ubiquity of the Internet of Things, the latest advances in memory and programmable solutions, and the promise of always-on 5G connectivity, Intel is disrupting industries and solving global challenges. Leading on policy, diversity, inclusion, education, and sustainability, we create value for our stockholders, customers, and society.

2200 MISSION
COLLEGE BLVD.

SANTA CLARA, CA
95054-1549, USA

PHONE: (408) 765-8080

ABOUT RED HAT

Red Hat is the world's leading provider of open source software solutions, using a community-powered approach to provide reliable and high-performing cloud, Linux, middleware, storage, and virtualization technologies. Red Hat also offers award-winning support, training, and consulting services. As a connective hub in a global network of enterprises, partners, and open source communities, Red Hat helps create relevant, innovative technologies that liberate resources for growth and prepare customers for the future of IT.

NORTH AMERICA	EUROPE, MIDDLE EAST, AND AFRICA	ASIA PACIFIC	LATIN AMERICA
1 888 REDHAT1	00800 7334 2835 europe@redhat.com	+65 6490 4200 apac@redhat.com	+54 11 4329 7300 info-latam@redhat.com

facebook.com/redhatinc
@redhatnews
linkedin.com/company/red-hat