EBOOK

HYBRID CLOUD BEST PRACTICES FOR FEDERAL AGENCIES

BROADCOM SOFTWARE

Considerations and Strategic Guidance for Hybrid Cloud Adoption

Cloud computing is an integral part of the digital transformation initiatives rolling out across industries and market sectors. Cloud adoption is a recurring topic in White House mandates and ongoing guidance around **NIST, FedRAMP, CMMC,** and other major compliance frameworks in the Federal industry.

Broadcom Software is deployed throughout a number of government agencies and we've been working closely with them to drive cloud-based operations in all areas of government. In this eBook, we'll explore what cloud adoption looks like in a Federal context, the primary drivers of cloud adoption, and how Federal agencies navigate hybrid cloud implementations and create scalable, strategic approaches to the cloud that protect their IT investments and modernize their missions.

Table of Contents

The Evolution of Cloud in the Federal Industry

With the emergence of the cloud came the promise of increased efficiency, agility, and, perhaps most importantly, security. However, software providers, government entities, and IT teams have seen varying degrees of success in implementing cloud solutions across their infrastructures.

The term "cloud" is very broad, and there's no standard, long-term roadmap for cloud adoption. However, several common themes inform how agencies use the cloud today and how they plan to expand upon it in the future.

From Cloud First to Cloud Smart

This accelerated, all-in move to the cloud sounded beneficial in theory but created unforeseen challenges as early adopters moved past fast-moving implementations into more complex ones. Some mission-critical workloads were not suitable for the cloud, e.g., bare-metal workloads or those with data rates that exceeded cloud provider capacity.

The "Cloud-Smart" policy emerged several years later to replace Cloud First with a more feasible approach to cloud. Rather than mandating full-scale adoption for every agency, Cloud Smart encourages a **practical application of cloud technologies.**

Cloud Smart provided agencies with a common-sense approach to infrastructure selection, enabling them to make informed decisions and develop hybrid cloud environments that fit the needs of their missions.

BROADCOM SOFTWARE

70%

Seventy percent of state and local government executives stated that the cloud is their preferred environment for hosting citizen and mission data.

Source: Maximus: "FedRAMP Survey Results Report."

Cloud in the Zero Trust Framework

The shift to Cloud Smart gave agencies more control over how they implement cloud-based solutions. Security has remained a top concern as the cloud presents a unique set of data security risks.

In 2022, the White House released a **memorandum on the Federal zero trust architecture** (ZTA) strategy. It denotes a **shift from boundary-based data security toward a more comprehensive framework that mitigates risk on-premises, on-cloud, and at every touchpoint in between.** This perimeter-less approach is also designed to enable remote work in the public sector, an effort that goes hand-in-hand with cloud adoption and infrastructure modernization.

Zero trust reflects a **"never trust, always verify"** security strategy. Rather than a single software implementation or tool, it's a holistic framework behind which Federal Agencies must align their processes, technologies, and mindsets. And no matter what their path to zero trust looks like, the cloud will continue to play a central role in their transition and ongoing success.

Defining the Best Path Forward for Federal Agencies

Cloud transformation is well underway in the Federal industry. Early cloud adopters have achieved notable success and learned hard lessons. The Cloud Smart policy empowers agencies to develop solutions that will meet their security, financial, and growth needs now and in the future.

However, it's critical to note that cloud transformation is a marathon, not a sprint. It's increasingly evident that many agencies will require hybrid implementations forever due to the nature of their missions. The key to success is implementing a security approach that addresses the hybrid cloud from core to edge device.

Federal agencies must carefully examine their current cloud strategy and the vendors they use to implement it. Rather than simply replacing data center infrastructure with cloud infrastructure services, agencies should **take an intentional approach to adoption that acknowledges the long-term reality of hybrid cloud environments.** Then, create a decision framework that guides your cloud and on-premises infrastructure selection.

BROADCOM SOFTWARE

"Never trust, always verify"

Best Practices for Hybrid Cloud Operations

There are many considerations for how, when, and why you should move specific tools or data systems to the cloud and an array of barriers to overcome as you build your ideal hybrid cloud ecosystem.

No matter your agency's specific IT needs or current cloud strategy, several best practices can help you create a viable hybrid cloud adoption plan.

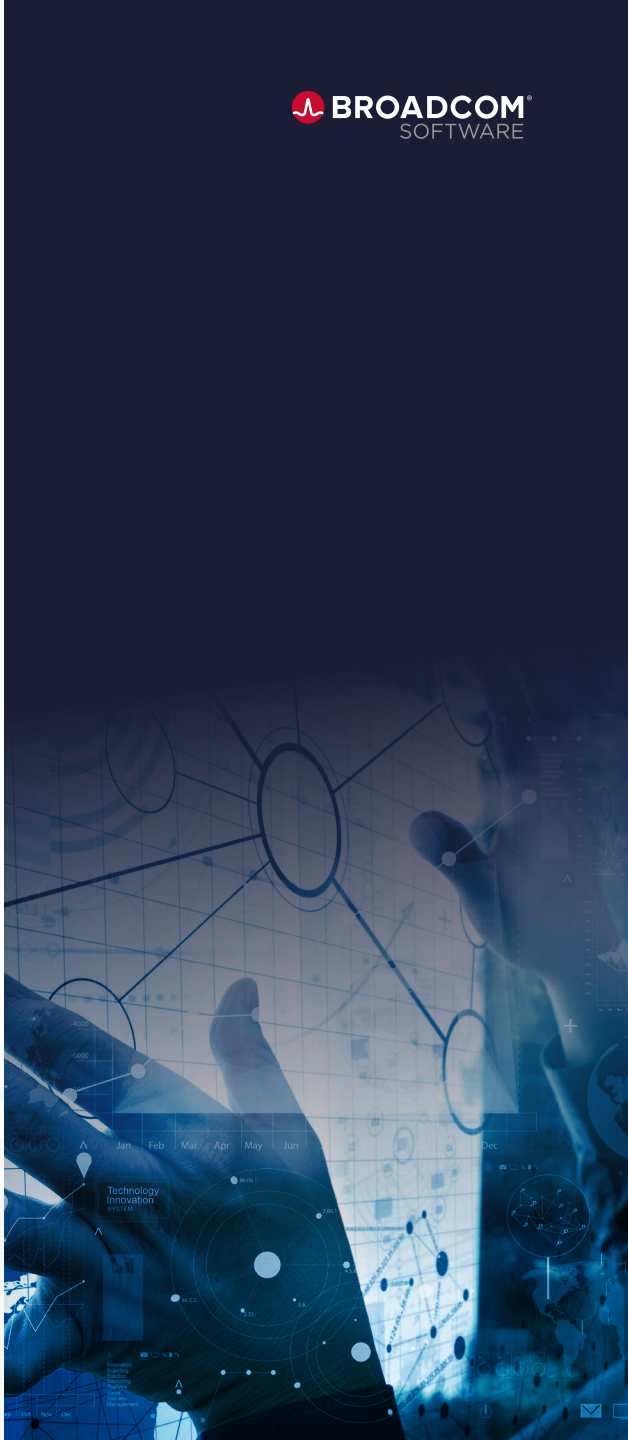
Make Strategic Product Decisions

An effective hybrid cloud strategy fits the unique needs of your Federal agency, the constituents you serve, and the compliance frameworks that apply to your mission.

There's no one-size-fits-all approach to cloud adoption in the Federal industry. You should base cloud investments on each mission's functional and performance requirements rather than guidance from cloud software providers. Your agency should also leverage strategies and design patterns implemented by other Federal agencies as part of its research.

To start, assess your IT infrastructure to determine the value and feasibility of bringing certain products to the cloud. Some applications and infrastructures will always remain on-premises, while others could benefit from cloud computing capabilities.

If your ideal state informs the destination of your hybrid cloud roadmap, your product-level requirements inform the route you take to reach it.



Pick core capabilities that will always stay cloud-independent

Before you invest in new cloud solutions or restructure your technology ecosystem, conduct a business case analysis to identify which areas of your operations would benefit most from the cloud versus where you should continue to leverage on-premises systems.

Evaluate your agency's capabilities, applications, and management systems to determine which ones should remain on-premises and which should move to the cloud.

In some cases, a workload's short-term operational costs won't decrease following a cloud migration, but the cloud-based version may offer you new efficiencies or capabilities. As part of your strategy, consider each application's total cost of ownership, not just the investments you've already made or what it would cost to bring them over to the cloud.

You'll also need to account for enterprise scaling and hardening commercially licensed software versus custom GOTS built from free, open-source software. These solutions often scale poorly and incur high expenses over their entire lifecycle. FOSS-based solutions may work well for small one-off projects, but they are near impossible to integrate into a zero-trust framework.

Keep future state in mind

Once you know which applications need to move to the cloud, it's time to determine how you'll migrate them—and maintain them—successfully.

Cloud lock-in restricts an agency's cloud operations to a single private environment by making it difficult and costly to transfer assets to another provider's environment. Lock-in leaves agencies dependent on a single provider for all on-cloud operations.

Operating in a private cloud doesn't just make it hard to move to a new environment; it also limits an agency's cloud capabilities to those of one specific provider.

If your agency gets locked into a single cloud solution, you'll need to pay extensive transfer fees to regain ownership of your cloud-hosted assets. Alternatively, you might move to a new environment, doubling the time, effort, and expenses associated with your cloud-based operations.

Beyond the risk of cloud lock-in, **agencies that go "all in" on one cloud have no choice but to follow the associated provider's technology roadmap.** And if your mission evolves more quickly than your cloud provider's solution, you'll have to make costly, time-sensitive infrastructure changes to keep up.

As you plan for hybrid cloud operations, mandate cloud portability and avoid using CSP-specific services that undermine it. Instead, leverage the industrial base's diverse software vendor ecosystem since vendors are inherently incentivized to ensure their solutions are compatible with multiple cloud providers.

Address Zero Trust Security

Federal agencies rely on an array of legacy installs to further their missions, which can create barriers to adherence with the White House's Federal **zero trust architecture (ZTA) mandate.** Most legacy solutions aren't inherently zero trust, and they aren't going away anytime soon. The cloud extends across multiple infrastructures and requires unique considerations that don't apply to perimeter-based security.

Rather than looking for a "rip and replace" solution that instantly solves for zero trust, your agency should plan its long-term transition to zero trust by implementing the right applications, platforms, processes, and training across environments and departments.

Make considerations for compliance and scalability

Federal compliance is an essential milestone toward more sustainable operations, and achieving it will pave the way for long-term mission success. When you develop a hybrid cloud strategy, your agency must account for zero trust mandates in each environment individually and your IT infrastructure as a whole.

Many agencies manage an intricate patchwork of staff, citizens, and contractors, all of whom leverage data from multiple sources. Zero trust's comprehensive, continuous access control guidelines help security teams **standardize and implement risk management solutions at scale across environments and user groups.**

Zero trust naturally increases your agency's resiliency and security across on-premises and cloud operations. It extends beyond the government perimeter to the industrial base, accelerating your agency's time to mission and securing your ecosystem from threats.

BROADCOM SOFTWARE

... your agency should plan its

long-term transition

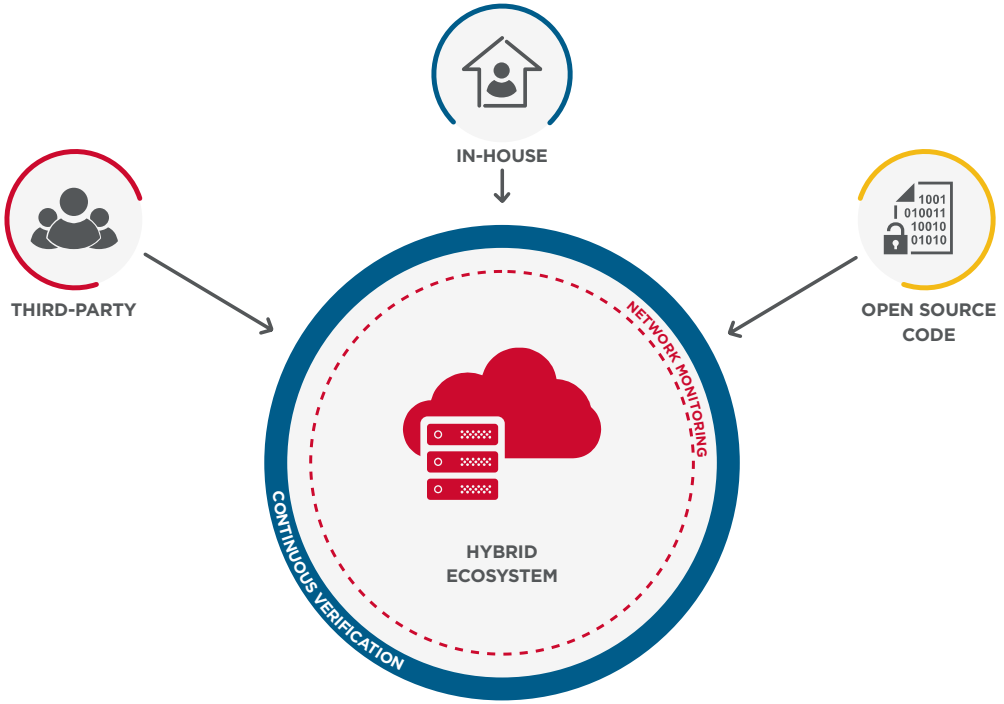
to zero trust by implementing the right applications...

Adopt hybrid zero-trust strategies

Your agency's hybrid cloud operations are dynamic and distributed, making them reliant on zero trust's perimeter-less approach to security and authentication. The zero-trust principle of "never trust, always verify" enables your security teams to identify every user across environments and understand what resources are being used.

Attempting to achieve zero trust with point solutions drives integration complexity and creates risk vulnerability in the seams between the point products. If your agency relies on disjointed point products, you'll end up with Frankensteined solutions that necessitate high costs and diffused accountability.

To successfully implement zero trust in the hybrid cloud, your agency needs **strategic zero trust providers with the breadth, depth, and scale to support all environments.**



In a hybrid workspace, users build some parts of an application in-house, while other elements rely on third-party technology, and others may be composed of open source code. A zero-trust security solution should continuously authenticate users and monitor the entire network. It should allow your security team to vet all third-party or open source technologies before granting them access to your ecosystem.

Evaluate Your IT Infrastructure

The hybrid cloud requires solutions that effectively service your agency's entire ecosystem. For this reason, it's essential to adopt cloud models that enable your workforce to use services from different sources without compromising governance or performance.

Procurement

Federal budgets are typically rigid and constraining. It often feels impossible to support cloud investments amidst the recurring costs associated with on-premises maintenance and the fluctuating expenses of vulnerability remediation.

While it's not feasible to transfer the bulk of your legacy budget to cloud spending in a single instance, reframing your approach to procurement allows your organization to **consolidate and standardize on-premises systems so you can re-allocate a portion of your budget to the cloud.**

Cloud procurement doesn't require an inflated budget or on-premises sacrifices. Instead, it's all about using the existing funding in a new way. Asking questions like, ***"Are there ways we can free up budget from legacy software and allocate it to the cloud?"*** can help you root out inefficiencies and enable strategic cloud growth.

Governance

Zero trust requires that organizations **maintain records of security processes and procedures.** This documentation clarifies how your system validates users, resources, and practices before granting access, which helps employees uphold established security protocols and protect your ecosystem from threats.

The best way to create a practical cloud governance framework is to start simple and grow as your cloud needs expand. Look for opportunities to **reuse processes and best practices across clouds.** Then, establish robust documentation to support your teams and improve your agency's cybersecurity posture.

A hybrid IT infrastructure requires more than new technologies or software investments. Agencies should evaluate their entire IT lifecycle to ensure they're solving for hybrid cloud at every step.

Implementation

An attainable hybrid cloud strategy requires more than deploying a new software solution. To ensure successful implementation, your agency will need to navigate the full breadth of users, partnerships, devices, and applications across on-premises and on-cloud operations.

Here are several critical considerations to keep in mind as you plan for hybrid cloud implementation:

1 Take an incremental approach to adoption

Rather than overhauling your systems, implement zero-trust solutions in phases. Start with one high-priority technology domain and follow a learn-as-you-go strategy to roll out additional implementations. Your first implementation will likely dictate the pace and complexity of additional ones, so prioritize a slow, methodical approach over a fast and furious system redesign.

2 Keep user experience in mind

Zero trust doesn't have to come at the expense of user experience. Work with stakeholders and leadership teams to align your agency's user experience needs and network security requirements, then work together to identify monitoring software that solves both.

3 Align your workforce behind your mission

Collaborate internally to identify zero-trust implications, direction, and roadmap. Your roadmap should enable secure implementations without sacrificing agility or disrupting day-to-day operations. You'll also need to establish training programs and documentation to champion zero-trust rust adoption across your workforce.

Paving the Way for Hybrid Cloud Adoption

Cloud adoption impacts people, processes, and technology across your organization and the industrial base.

Each new software deployment, protocol change, or workflow adjustment can have a ripple effect on your agency's mission, which is why you need an ecosystem of trusted software partners with the breadth, depth, and scale to span the zero trust framework in a hybrid cloud environment.

Find Software Partners That Enable Hybrid Cloud

Federal cloud enablement relies on a strategic mix of on-cloud and on-premises operations. Agencies that rely on cloud-only software vendors to manage their cloud operations and develop in-house data centers to manage on-premises operations will face costly IT redundancies and increased security risks across environments.

Rather than contracting cloud-native vendors and managing your on-premises operations separately, seek out partners that understand on-premises and cloud and can support your hybrid cloud strategy across environments and operating systems.

Hybrid software partners will be able to support your on-premise and cloud systems in tandem, with custom solutions you can adopt at various phases of transition to the cloud.

Broadcom Software's portfolio of enterprise-level software is built for security and scalability from silicon to software. Our solutions are cloud-portable and enable customers to seamlessly combine on-premises data centers with modern, agile cloud technologies.

Leverage our dynamic software to maximize your existing on-premise IT investments, operate in multiple clouds, and remain partially on-premises to support your mission, constituents, and Federal workforce.

BROADCOM SOFTWARE

Cloud adoption impacts people, processes, and technology across your organization and the industrial base.

READY TO UNLOCK THE FULL POTENTIAL OF THE HYBRID CLOUD?

Connect with our Federal sales team today to discover how we can support your hybrid cloud strategy with software that modernizes, optimizes, and protects at scale.

GET STARTED NOW

BROADCOM SOFTWARE

About Us

USA-based Broadcom Software is a world leader in mission-critical software that modernizes, optimizes, and protects—at scale. With its engineering-centered culture, Broadcom Software continues to build a comprehensive portfolio of leading infrastructure and security software, including AIOps, Cyber Security, Value Stream Management, DevOps, Mainframe, and Payment Security. Our software portfolio enables scalability, agility, and security in support of your shared mission.

For more information, please visit our website at: software.broadcom.com