InquisIT

TOP 5 CLOUD SECURITY CHALLENGES FOR FEDERAL AGENCIES

& CLOUD SECURITY BEST PRACTICES CHECKLIST

www.inquisitllc.com

June, 2020

InquisIT

INTRODUCTION

The Federal Government is moving to the cloud at a rapid pace, fueled by the desire to modernize and consolidate IT infrastructure. Amazon AWS alone states that over 2000 federal agencies[1] are making use of their FedRAMP certified services, while Microsoft's Azure offerings are poised to encompass the Department of Defense via the JEDI Program. Simultaneously, a daily onslaught of news is emerging across the world about compromised cloud infrastructure, spilling millions of records containing sensitive information due to misconfiguration, lack of visibility, or neglect to adhere to industry best practices. It is obvious why the topic of cloud security has garnered so much attention!

At InquisIT, we have the privilege of working with a variety of agencies towards resolving their security concerns. As a result, we have identified the top five challenges we regularly solve with our customers. Common themes range from highly technical to administrative in nature, but with one goal in common - to keep the bad guys out!

With each challenge is a solution, helping you to mitigate your apprehension towards the cloud and allowing you to custom-tailor each for your own organization.

> *Successfully managing cloud adoption risks requires collaboration between agency leadership, mission owners, technology practitioners, and governance bodies...Cloud Smart encourages agencies to approach security and privacy in terms of intended outcomes and capabilities...*
>
> *Cloud Smart operates on the principle that agencies should be equipped to evaluate their options based on their service and mission needs, technical requirements, and existing policy limitations. Computing and technology decisions should also consider customer impact balanced against cost and cybersecurity risk management criteria.*[2]
>
> — Office of the Federal Chief Information Officer, Office of Management and Budget

1. Fedramp. Amazon Web Services (AWS). (n.d.). https://aws.amazon.com/compliance/fedramp/
2. *From Cloud First to Cloud Smart*. Federal Cloud Computing Strategy, Office of Management and Budget. (n.d.). https://cloud.cio.gov/strategy/

CHALLENGE 1 COMPATIBILITY

We find that agencies are most often trying to find a path to migrate their on-premises technology stacks into the cloud. For many Commercial-off-the-Shelf (COTS) products this is not an issue. Many technology brands have embraced cloud-native implementations years ago when the trend towards the cloud began.

However, we find that many agencies are reliant on proprietary, home-grown applications which may be two-to-three tiered in nature, and with data flows that do not adhere to a simple "lift and shift" approach. There are often many software dependencies which add even more complexity to the mix.

Understandably, the availability of mission systems is so critical that it can pose a difficult added challenge to finding a path forward for migrating these workloads safely into the cloud.

CLOUD NATIVE DEFINITION

"Cloud native technologies empower organizations to build and run scalable applications in modern, dynamic environments such as public, private, and hybrid clouds. Containers, service meshes, microservices, immutable infrastructure, and declarative APIs exemplify this approach.

These techniques enable loosely coupled systems that are resilient, manageable, and observable. Combined with robust automation, they allow engineers to make high-impact changes frequently and predictably with minimal toil."[3]

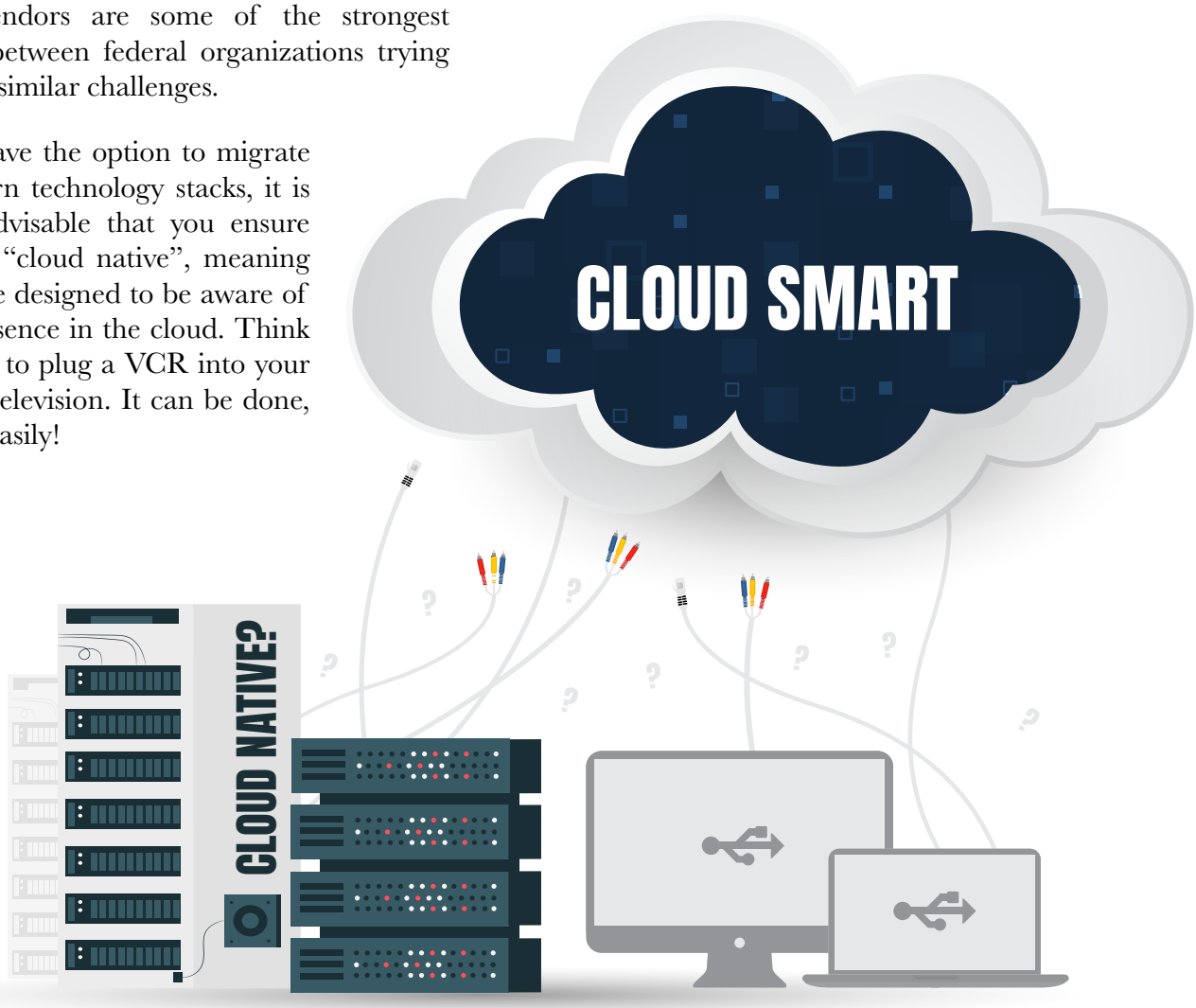
3. *CNFC Cloud Native Definition*. Github. (June, 2018). https://github.com/cncf/toc/blob/master/DEFINITION.md

Fortunately, these issues are not insurmountable. It requires careful diligence and an in-depth examination into the target system and its dependencies. Dig into your network architecture and documentation to get a full understanding of the system and its information flows ahead of time. If you have the option, migrate less critical workloads first, allowing for sufficient time to test the resilience of your cloud enclaves.

Engage your IT teams with your cloud vendor of choice and set up a solutioning meeting to discuss in detail what you are trying to accomplish. Come prepared with the strategic goals you are looking to achieve, the challenges you foresee, and the technologies you believe are most relevant towards success. We find that cloud vendors are some of the strongest liaisons between federal organizations trying to tackle similar challenges.

If you have the option to migrate to modern technology stacks, it is highly advisable that you ensure they are "cloud native", meaning they were designed to be aware of their presence in the cloud. Think of trying to plug a VCR into your 65" 4K television. It can be done, just not easily!

> *Cloud Smart operates on the principle that agencies should be equipped to evaluate their options based on their service and mission needs, technical requirements, and existing policy limitations. Computing and technology decisions should also consider customer impact balanced against cost and cybersecurity risk management criteria. Additionally, agencies need to weigh the long-term inefficiencies of migrating applications as-is into cloud environments against the immediate financial costs of modernizing in advance or replacing them altogether.*[4]



4. *From Cloud First to Cloud Smart*. Federal Cloud Computing Strategy, Office of Management and Budget. (n.d.). https://cloud.cio.gov/strategy/

CHALLENGE 2 CONFIGURATION MANAGEMENT

As many are aware from watching the news, managing how you configure cloud infrastructure has serious ramifications if done improperly. Services which took weeks to configure can suddenly be spun up in seconds. This is fantastic! But it requires some foresight.

Changes that seemed innocuous on-premise now have a very real cost associated with them which can be difficult to estimate. Something as simple as a click in the wrong place could expose your data, resulting in some heavy hand-slaps at a minimum. Visibility into these changes may not exist out of the box, and could mean a misconfiguration can go for long periods of time without being noticed. Cloud services can be highly atomic in nature, which means unless you configure a service to do something, it won't do it!

> *As agencies implement the Cloud Smart strategy, they should execute communication plans that help employees understand the changes that will occur. For example, migration to the cloud may require decommissioning legacy systems that have been in use for many years. Employees may feel reluctant, especially if positions will be redefined, to learn to operate new systems in a cloud environment. Agencies can ease workforce concerns by clearly articulating how the current workforce will align once cloud adoption is complete. Socializing a technology roadmap to include systems that will be migrating to the cloud, either completely or partially, and an outline of the change management process to include reskilling opportunities is strongly recommended. Agencies should also feel comfortable leveraging vendors involved in cloud migration activities to provide or support training for current employees.*[5]

The solution to this challenge may be in front of you already. Applying a systematic change management process with integrated roll-back plans, risk assessments, peer review, and formal approval will help you get a handle on change in the cloud. Integrations with your SIEM, CASB, or cloud native configuration monitoring tools can give your team near real-time alerting to changes in your cloud tenants, intended or otherwise.

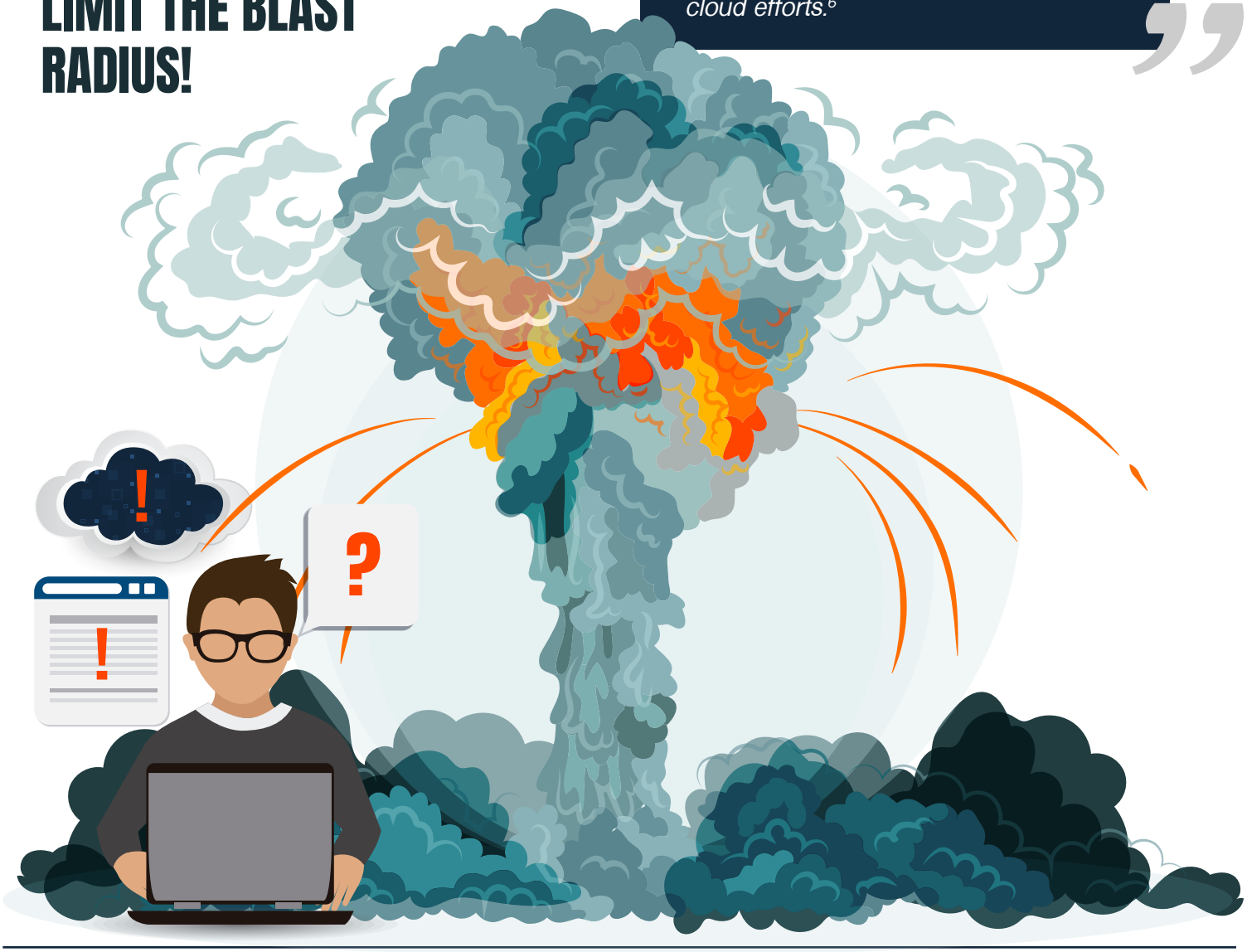
5. Ibid.

Professional training is key. Gaining access to training materials to refresh your team's skill-sets are no longer a nice-to-have, but a hard requirement. Embrace role-based access control through federation early for your administrators.

In cloud, the term "blast radius" is used frequently, referring to the range of consequence any single administrator can make accidentally when performing a change. Limit the blast radius!

> *[P]roviding staff with training and other educational resources is essential to fostering maturity in the areas of privacy, security, and procurement. Agency IT staff should become familiar with lean product management, agile development, continuous delivery, and automated infrastructure at the team and program level as part of any modernization plan. Additionally, non-IT staff supporting privacy, security, and procurement should receive training in the multiple core disciplines outlined above. Sustained progress in these areas of staff training is foundational to the successful implementation of new cloud efforts.*[6]

LIMIT THE BLAST RADIUS!

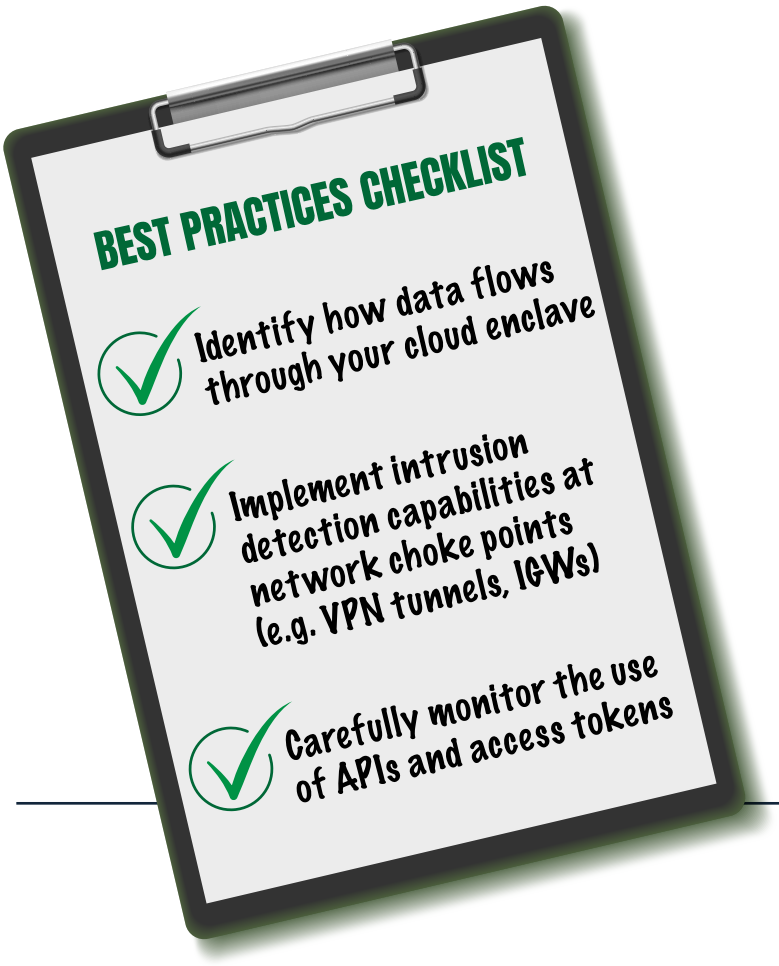


6. Ibid.

CHALLENGE 3 VISIBILITY

When agencies approach the cloud, we find that taking age-old networking paradigms and transposing them can present new questions. Whether it is relevant to security, operations, or administrative teams, the primary question usually becomes *"How do I monitor inbound and outbound traffic at the perimeter?"* No matter who you ask, the answer will be "It depends." That is a frustrating answer to deal with!

Cloud for the enterprise is limitless given infinite funds, meaning that you can connect your tenant to any site across your infrastructure to do as much or as little as you want. The service model was literally designed for optimal accessibility, the flexibility to accommodate the largest and smallest organizations, and with the widest a-la-carte menu of technology offerings. ***This means that if you want visibility, it is on you to define where and how to get it!***



From Cloud First to Cloud Smart[7]

"Released in 2007, OMB Memorandum M-08-059 established new requirements for Federal agencies with the intent to reduce the Federal-wide number of external network connections while standardizing their security. Since the policy's release, agency network traffic in compliance with OMB requirements has flown exclusively through a limited number of external connections, known as Trusted Internet Connections (TICs). While this initial architectural concept served an important purpose at its inception, at a time when networking was constrained by physical limitations and agency approaches to network security were not standardized and highly fragmented, the technology landscape has evolved to provide agencies with more tools, technologies, and approaches to secure their data, leaving the once-useful TIC construct now relatively inflexible and incompatible with many agencies' requirements. With the proliferation of private-sector cloud offerings, the emergence of software-defined networks, and an increasingly mobile workforce, the TIC model must compete with newer, more flexible solutions that provide equal or greater security, or it must evolve as well.

Electing the latter option, the Department of Homeland Security (DHS) is working with various agencies to pilot agency-specific approaches that meet the objectives and intent of M-08-05 while minimizing technical constraints posed by the policy's one-size-fits-all TIC model. These newer, less rigid approaches will be incorporated into updated TIC Reference Architectures to highlight use cases wherein security objectives can be met without routing all traffic through a prescribed set of physical access points. The TIC Reference Architectures will also demonstrate how different use cases that do not require traffic to be routed through a TIC can address the requirements for government-wide intrusion detection and prevention efforts, such as the EINSTEIN Program while also incorporating DHS-designated controls, which have been designed to ensure a baseline level of security across the Federal enterprise.10v

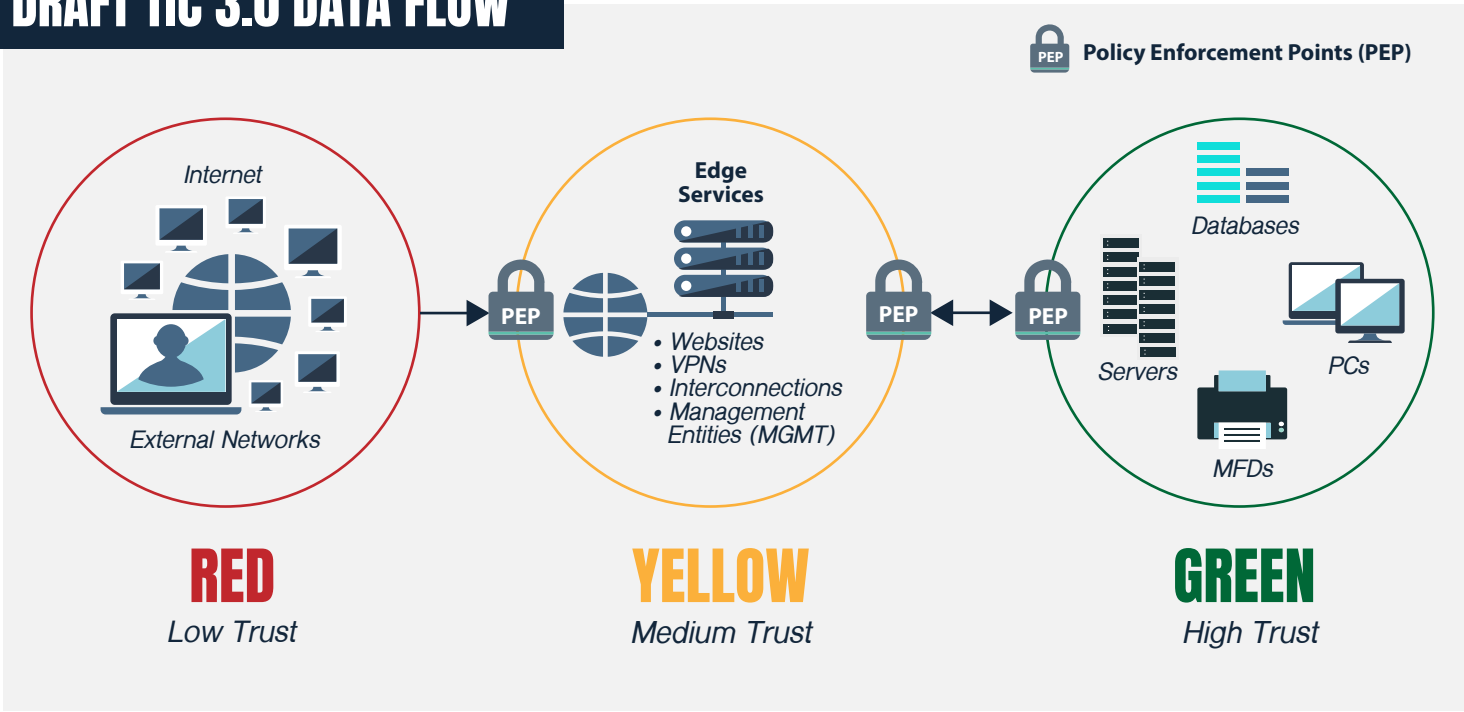
By taking these actions to expand the options available to agencies to secure their networks and data, the collective ability of the Federal Government to take advantage of new paradigms, such as zero trust networks, is heightened, as its effectiveness in managing risk." [7]

7. Ibid.

The perimeter is ultimately where you define it. Asking yourself how data flows through the enclave may seem straight forward, but when you break out the whiteboard and begin to catalogue the API keys, VPN tunnels, and Internet Gateways, you may be in for a surprise. For core network traffic, VPN tunnels into the cloud will be your choke-points with which to monitor from. Apply your intrusion detection technologies to inspect traffic traversing these connections. Going in and out to the Internet directly from your cloud tenant becomes difficult specifically due to the ongoing development of TIC 3.0[9] and TIC-in-the-Cloud efforts. If managed solutions are available, architect your cloud presence to utilize them. Otherwise, we advise you to replicate such infrastructure with a firewall-based solution that can perform the necessary traffic inspection. Placement of services behind these barriers is essential to enable visibility. Finally, be mindful of access tokens! Any set of credentials can punch a hole through your defenses. Protect API keys through CASB tools, carefully tailored permissions (limiting the "blast radius"!), and recurring credential resets.

> *Critical to the success of this security strategy in the context of Cloud Smart is the assurance of confidentiality, integrity, and availability of Federal information as it traverses networks and rests within systems, regardless of whether those environments are managed locally, off-premises, by a Government entity, or by a contractor. Additionally, it is essential that agencies perform continuous monitoring to detect malicious activity and dedicate effort to improving systems governance.*[8]

DRAFT TIC 3.0 DATA FLOW[9]



8. Ibid.

9. *Trusted Internet Connections 3.0.* Cybersecurity and infrastructure Security Agency. (Dec, 2019). https://www.cisa.gov/sites/default/files/publications/Draft%20TIC%203.0%20Vol.%202%20Reference%20Architecture.pdf

CHALLENGE 4 RISK MANAGEMENT

A recurring theme we encounter with many federal agencies involves challenges in adhering to legacy frameworks and practices. These frameworks were effective when developed, but must be updated to keep with the times.

Risk Management in particular is one of those areas. We see many agencies struggle to apply RMF to their newly-expanded infrastructure, or have difficulty adapting security controls around their respective clouds. As mentioned earlier, these service offerings were designed to be accessible first, which does not necessarily coincide with traditional "Defense in Depth" architectures. Performing point-in-time ATOs and control assessments are not efficient uses of the team's time, and often no longer accurately depict the security posture of the organization.

> *Agencies should take a risk-based approach to securing cloud environments. As recommended by the Report to the President on Federal IT Modernization, agencies should emphasize "data-level protections and fully leverage modern virtualized technologies."6 This requires that agencies place an emphasis on protections at the data layer in addition to the network and physical infrastructure layers, transitioning to a multi-layer defense strategy, otherwise known as defense-in-depth.*[10]

The solution here is three-fold:

(1) carefully define your authorization boundaries
(2) lean heavily on Continuous Monitoring
(3) embrace agile methodologies

In regard to boundaries, optimizing your cloud systems for control inheritance is a force multiplier. Most organizations do not have sufficient man-power to complete reauthorization activities with their current staff, and adding more work is that much more daunting. We advise you don't re-invent the wheel. Carefully review the security package provided by your CSP to identify controls that are covered, and where your existing General Support Systems make up the difference. Operationally, this consists of extending your technical controls, including identity and access management, audit and accountability, and incident response capabilities, into the new cloud system. Begin to analyze how you can identify deficiencies in these gapped controls in as close to near real-time as possible. Finally, think about how to facilitate Ongoing Authorization in the cloud by approaching common SA&A tasks such as control assessments and policy updates into smaller, distributed sprints. Doing so can provide a more accurate portrayal of your organization's posture, as opposed to a snapshot in time.

10. *From Cloud First to Cloud Smart*. Federal Cloud Computing Strategy, Office of Management and Budget. (n.d.). https://cloud.cio.gov/strategy/

CHALLENGE 5 COMPLIANCE

How agencies operate is the sum of a wide variety of directives, memorandums, and guidance designed to protect the data they process. Adding local policy into the mix, the end result can lead to what we call "compliance confusion".

Specific to cloud, questions are frequently raised around how to funnel these policies into an all-encompassing solution which makes use of the FedRAMP program. This ends up most commonly being a discussion about how to balance cost, compliance, and functionality into a technical approach that meets the organization's needs while not incurring undue administrative burden. Not an easy task!

To begin tackling this, you must identify the "high water mark" for the data your agency will process in the cloud. This is important because despite a cloud offering being FedRAMP certified, regulations around certain types of data (e.g. CJIS, IRS 1075, ITAR) may have additional implications. This can include US data sovereignty and citizenship status of the CSP staff which support you. As an example, some commercial offerings may provide "follow-the-sun" support models which may not be compatible. Additionally, select CSPs may only support FedRAMP in select regions. Perform your due diligence when selecting services in the cloud relative to the data being processed there.

Next when it comes to the build-out, you need a configuration baseline. The Center for Information Security (CIS) is slightly ahead of the curve as opposed to the DISA STIG, and can give you extra assurance that your tenant is adequately hardened. By implementing such benchmarks on your tenant, you will be reinforcing the controls needed to acquire and maintain a cloud ATO. Next, be mindful of your CSP's responsibilities with your data. We find that asking the simple question "What happens to our data if we decide to leave?" or other previously assumed processes can often unravel some hidden "gotchas" and help align your desired state configuration to a fully featured, compliant offering.

CONCLUSION

You will be flying high when you embrace the cloud! There is no denying it. From a security perspective, the cloud natively mitigates more challenges than it presents. Physical security, availability, scalability, and redundancy can all be a simple checkbox click away. At the same time, exposing the wrong bucket, instance, or port to the outside world can also be just a click away as well. By taking a mindful approach to cloud security, you can rest assured that your modernization goals are underway while keeping adversaries at bay!

CLOUD SECURITY BEST PRACTICE CHECKLIST

COMPATIBILITY

- ☑ Carefully review existing network architecture to identify dependencies
- ☑ Engage with a cloud solutions architect to discuss your challenges
- ☑ Embrace cloud-native technologies as much as possible throughout the migration

CONFIGURATION MANAGEMENT

- ☑ Integrate Change Management processes to your cloud infrastructure.
- ☑ Implement automated monitoring to alert you to configuration changes.
- ☑ Emphasize cross-training and professional development with your team.
- ☑ Limit the "blast radius" of bad configurations through role-based access controls.

VISIBILITY

- ☑ Identify how data flows through your cloud enclave
- ☑ Implement intrusion detection capabilities at network choke points (e.g. VPN tunnels, IGWs)
- ☑ Carefully monitor the use of APIs and access tokens via your SIEM, CASB, or native features

RISK MANAGEMENT

- ☑ Define your cloud authorization boundary with an emphasis on control inheritance
- ☑ Perform a gap analysis between your GSS and the CSP's security package
- ☑ Integrate Agile methodologies towards your cloud ATO

COMPLIANCE

- ☑ Identify regulations around your data and how it aligns to your target cloud offering
- ☑ Apply a configuration baseline to your cloud tenant (e.g. CIS)
- ☑ Carefully review your CSP's security responsibilities