maximus

The Cloud and Zero Trust: Finding the Right Balance

IS YOUR AGENCY struggling to make Zero Trust a reality? If so, you're not alone.

While it's never been more crucial to bolster cyber defenses, the struggle to incorporate Zero Trust into agency environments is proving daunting for many agency IT and security teams. This is particularly poignant as agencies search out ways to continue tapping into the cloud to modernize legacy applications, systems and data to enable new, innovative ways to meet the mission. Moreover, with the recent **Executive Order** requiring agencies to implement new Zero Trust security models, agencies are at a crossroads regarding how to balance their journey to the cloud while also establishing new security models that go from traditional perimeter security to a perimeterless security architecture.

At a glance, Zero Trust is a security framework that requires all users in an agency's network to be authenticated, authorized and continuously monitored. This requires agencies to not only fully understand their IT environment so that they can protect it, but incorporate the necessary tools to authenticate and monitor users.

With all this, Zero Trust can certainly seem like a tall order for agency IT teams, many of which are already working with constrained resources. And while many agency leaders understand the need for **Zero Trust** and acknowledge it is crucial to preventing unauthorized access to data, services, networks, applications, and identity, many struggle with understanding how to successfully implement a fully mature Zero Trust framework, even with the plethora of guidance from the **OMB**, **CISA**, **GSA**, **NIST**, and the **Defense Department**.

Agency leaders are now challenged to understand where they currently are with their security postures, where they want to go with their modernization efforts and Zero Trust requirements, and how these two initiatives can come together cohesively.

By tapping into Zero Trust, organizations can enable the modern workplace, support digital products and services, reduce and manage risk, sustainably reduce cost and enhance agility. And everyone is taking notice: the global Zero Trust market is **expected** to skyrocket in coming years, growing from $19.6 billion in 2020 to $51.6 billion by 2026.

As agencies work toward the goal of Zero Trust, it will be key to incorporate Zero Trust principles as workloads are moved to the cloud—not afterward—and to chart out a strategy to do so in advance. In other words, Zero Trust must be part of the plan, no matter what agency IT environments look like. Read on to learn more about the importance of incorporating Zero Trust principles into your agency's cloud strategy in order to keep government data and systems secure, and how agencies can effectively make Zero Trust a reality in any cloud environment.

The global Zero Trust market is expected to skyrocket in coming years, growing from $19.6 billion in 2020 to $51.6 billion by 2026.

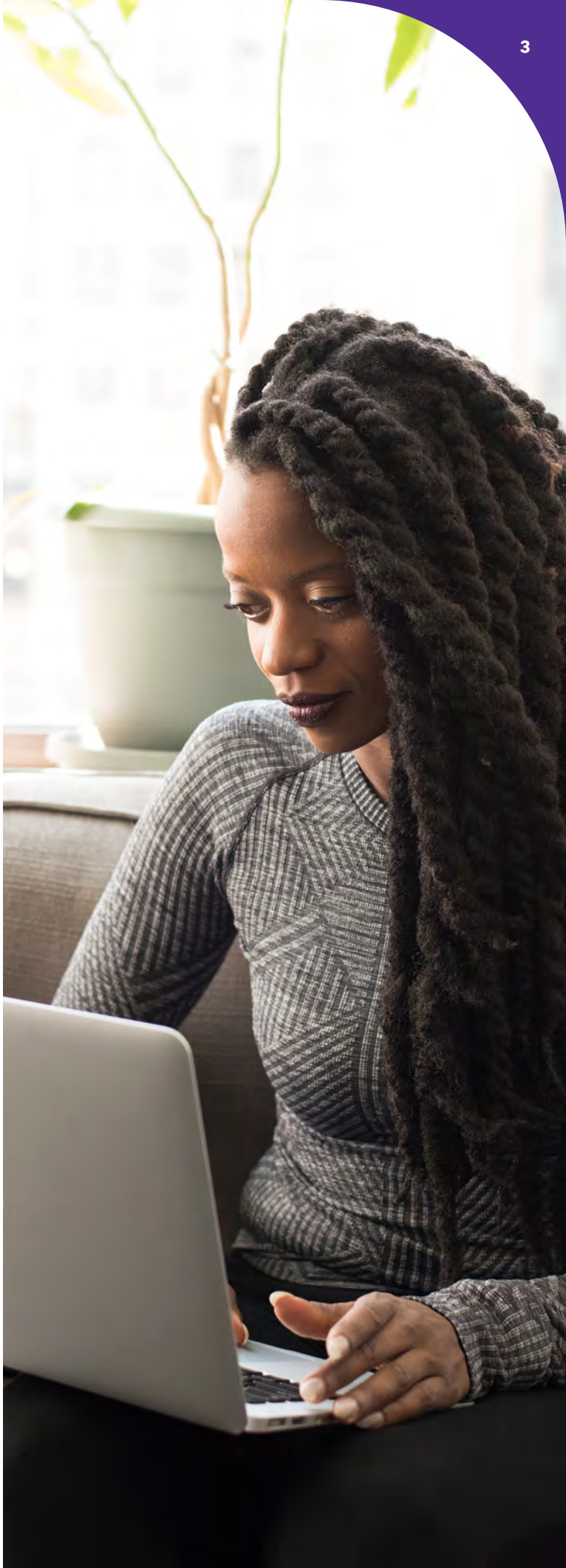
Taking an All-In Approach to Cloud

DESPITE HOW DAUNTED many agency IT teams may feel when it comes to Zero Trust, moving to the cloud is actually the simplest way for an agency to progress towards their Zero Trust goals. This is because most cloud providers have already "baked in" Zero Trust-friendly architecture into their platforms and continue to add new tools to strengthen security. The three major cloud platform vendors have a long history of compliance with federal security requirements and, in fact, already provide vital elements of Zero Trust architectures, such as tools that can help agencies to identify users' identities and dynamic policies to limit data access.

"Since cloud providers tend to keep up with security, the cloud can offer a ready-made solution, at least in part, toward Zero Trust," said Kynan Carver, DoD Cyber Lead at Maximus, a systems integrator and technology solutions provider to the federal government. "It's a far easier path than modernizing your on-premises hardware and then buying software to handle the change to Zero Trust."

Even agencies that have migrated many of their resources to the cloud can benefit. While original cloud environments may not have had many Zero Trust-friendly features, cloud platform vendors have worked diligently to update capabilities over time to comply not only with federal IT and security mandates but also to accommodate the user-friendly security necessary to keep data safe while moving the mission forward.

It's important to note, however that not all cloud instances are entirely Zero Trust-compliant, particularly for highly



classified information, Carver said. While existing cloud environments are likely to satisfy some Zero Trust requirements, they may not meet them all. The good news, however, is that experienced companies like Maximus can help agencies retrofit requirements where necessary. Carver gave the example of one defense agency that adopted the cloud early. Given the early adoption, the platform they had wasn't fitted with the right tools to meet today's Zero Trust requirements. Carver's team partnered with the agency to inventory the security features the cloud had and then identify and retrofit with the necessary elements to meet the agency's current Zero Trust needs.

Moreover, agencies should think carefully about the workloads they are thinking of migrating when adopting cloud environments in order to ensure existing resources are a good option for the cloud. In some cases, such as when legacy applications that may not port well to the cloud are still heavily incorporated into the agency IT environment, it may make more sense for an agency to wait to delay a cloud migration by a few years and, in the meantime, apply Zero Trust principles to the existing environment instead.

Further, as workloads, missions and work environments evolve, not every IT environment is the best match for every workload, which is why agencies also need to consider their Zero Trust approach for hybrid cloud environments.

Since cloud providers tend to keep up with security, the cloud can offer a ready-made solution, at least in part, toward Zero Trust.

Kynan Carver, DoD Cyber Lead
Maximus

The Hybrid Cloud Approach

WHILE SOME AGENCIES are more or less "all in" with the cloud, the vast majority have feet in both the on-premises and cloud worlds. The move to the cloud environment has grown significantly in the past two years, as the pandemic demonstrated, illuminating the importance of having some resources in the cloud. In a recent study, two-thirds of public sector leaders said the pandemic **accelerated their agencies' hybrid strategies** by a year or more. The moves are paying off. Many said it has increased flexibility and agility and boosted data availability and interoperability. The study also said **92 percent of federal IT managers** see hybrid cloud as the ideal operating environment for a resilient government.

The same survey also found that the top strategy for adopting a hybrid model was improving security. With more resources in the cloud, agencies can take advantage of the built-in security capabilities that cloud vendors have implemented, including biometrics and multifactor authentication, application policies, and networking redundancies. They can also be ready to add more capabilities necessary to achieve Zero Trust.

It's not as simple as moving on-premises workloads to the cloud. Sometimes, existing hardware or software is not cloud-compatible or cloud-ready. This is often the case with legacy systems and applications that are still mission critical. In other situations, moving workloads to the cloud requires changing the network structure or the need to add more tools. That's why it's critical to carefully analyze the existing on-premises environment to determine what's possible to shift to the cloud and what should remain on-premises, at least for the time being.

To do this effectively, Carver advises agencies to analyze on-premises workloads layer by layer, beginning with the current identity management system. From there, agencies should decide whether moving it to the cloud would create a mature, Zero Trust-compliant identity management set-up. Next, agency IT and security leaders should evaluate whether all applications, data, and networks are suitable for the cloud based on performance, security and cost factors. In addition, IT teams may need to

consider regulatory requirements like the Health Insurance Portability and Accountability Act (HIPAA) for healthcare or DoD classified information, which require some resources to remain on-premises.

In some cases, as with one agency that Maximus currently partners with in which many of its mission critical systems would prove costly and resource-heavy to move to the cloud, that might mean that a portion of a system is in the cloud, while some remain on-premises.

But not all workloads can be shifted even partially to the cloud, and thus agencies must also think through Zero Trust for entirely on-premises environments, as well.

The Basics of Zero Trust

While security has always been a top priority for federal government, events of the past few years like the Colonial Pipeline ransomware attack prompted the White House to issue an **executive order** calling for strengthened security, centered on principles of Zero Trust. A recent survey found that more than 80 percent of public sector organizations rely on a Zero Trust approach to cybersecurity, and that number continues to rise.

The basic idea of Zero Trust is that no person, system, network, device or service is trusted without verification. As NIST explains it, Zero Trust is an evolving set of cybersecurity practices that move defenses from static, network-based perimeters to focus on users, assets and resources. More specifically, Zero Trust requires:

- Denying users, devices, data flows and requests for access by default
- Authenticating and authorizing each of these to the least privilege required using dynamic security policies
- Encrypting and authenticating all traffic as soon as possible, including internal traffic
- Terminating every connection so that all traffic (even encrypted traffic) can be inspected in real time before it reaches its destination
- Protecting data using granular context-based policies
- Enabling users to connect directly to the resources they need instead of directly connecting to networks

One of the most effective ways to move toward Zero Trust is by embracing software-based micro-segmentation, which creates a secure perimeter around each workload, preventing attackers from moving laterally once inside the network perimeter. It does this by enabling agencies to establish tailored security policies and controls. As a result, it's easier to verify the identity of devices, users, data and applications across the network.

For more information on the federal government's approach to Zero Trust, reference these documents:

CISA's Zero Trust Maturity Model **NIST's SP 800-207** **NSA's Zero Trust Security Guide**

The On-premises Option

WHILE THE TREND is cloud-forward, there are plenty of reasons why federal agencies need to keep all resources on-premises. Regulatory requirements, privacy and data sovereignty – especially when it comes to highly classified workloads or those that include personally identifiable information (PII) like financial records or health information—are just a few reasons. In these cases, on-premises solutions can provide greater data control because they never leave the premises.

In other cases, it's about survivability. While cloud vendors put a lot of effort and resources into hardening their data centers, they often do not go as far as hardening these environments against truly catastrophic events like nuclear attacks or massive earthquakes. Agencies that need that kind of security often resort to their own fortified data centers, typically part of a Continuity of Operations (COOP) plan for continuous operation in the event of a natural disaster.

While it's more challenging to get on-premises environments and resources to a state of Zero Trust, it's possible to do so, despite typically older technology and fewer available resources. It may require major changes to everything from how you configure your Active Directory schema and networking to how you label your data.

Sometimes, challenges arise when existing technologies aren't readily adaptable to the principles of Zero Trust. If the infrastructure relies on older networking devices that don't allow for the micro-segmentation Zero Trust requires, for example, the agency might have to consider replacing the hardware to make it work.

There will eventually be a bar you will need to meet in Zero Trust, so it pays to take the time to analyze everything to see what you can do now.

Kynan Carver, DoD Cyber Lead
Maximus

It is possible to achieve full Zero Trust compliance on-premises, but requires essentially peeling an onion: going layer by layer and seeing what works and what doesn't, what needs to be done now, and what can wait.

"There will eventually be a bar you will need to meet in Zero Trust, so it pays to take the time to analyze everything to see what you can do now," Carver said.

When looking for upgrades to Zero Trust-compliant technologies, Carver recommends looking at **FedRAMP** and other industry-approved standards to see what products have already been vetted. "If you can go with something that has been approved and has been labeled by the government as Zero Trust-compliant, you'll be ahead of the game," he said.

The good news, however, is that no matter which approach an agency takes, there is always a path toward Zero Trust as long as agency IT and security teams are willing to take the time and approaches necessary to vet and understand their IT environments—and put the necessary security measures in place.

It all Comes Down to Data

While Zero Trust includes many other important aspects, it all comes down to protecting data. Not only are data stores throughout the government growing rapidly, but that data is being used more often for advanced analytics, predictive modeling, and decision-making. In other words, data is the government's most important asset—a point made clear by the **Federal Data Strategy**.

That's why Zero Trust mandates have put data protection front-and-center. A core principle of Zero Trust is protecting data by using granular, context-based policies. The Federal Zero Trust Strategy requires federal security teams and data teams to work together to develop data categories and security rules to automatically detect and block unauthorized access to sensitive data. It also requires developing a comprehensive approach to categorizing and tagging data—even loosely structured or unstructured data generated by the growing number of Internet of Things (IoT) devices agencies use today.

Zero Trust can go a long way toward better securing data and creating further visibility into who or what is using or accessing it and where it's going. But that requires knowing what data you have, where it's located, what risks might affect it, as well as how data travels between systems and applications. Answering these questions is critical to understanding what security products and processes exist and what may need to be changed or added.

"You don't want to just start subscribing to or buying identity management solutions without understanding how that Word document with a security classification needs to be routed to users," Carver said. "You need to know as much as possible about the data and what the end state should be to formulate the right strategies to protect it."

At a minimum, it's important to ensure that data can't be modified, deleted or encrypted by any non-authorized person, device or service. One way to do that is by employing a solution that inspects and logs traffic and creates a secure data layer where data is always encrypted, both at rest and in-flight across clouds or sites.

Endpoint Security in a Zero Trust World

Securing endpoints—not only handheld mobile devices, but laptops and PCs, printers, servers, medical devices, handheld scanners and IoT devices—is critical for meeting Zero Trust requirements. That's especially true in today's environment when so many employees are working remotely.

Because Zero Trust assumes that endpoints aren't secure until proved otherwise, remote work presents a big challenge, even with cloud-based resources. As more agencies enable employees to log into their desktops and other resources from home-based devices and networks, they must make sure that data never lives on the device and that networks are secure and governed.

It's a simpler proposition in cloud environments, Carver explained, because desktops accessed via the cloud are subject to the policies agencies have prescribed. By combining those policies with endpoint protection solutions like Windows Defender onto employee workstations, agencies can maintain full control over users' devices. It's a little more complicated in hybrid or on-premises environments, requiring more visibility and monitoring tools.

In all cases, the key is ensuring that the same securities are applied to all environments, regardless of whether the devices are agency-owned or privately owned by employees. Policies can be configured to apply to any type of endpoint device, not only laptops and desktops. It's also important to require that all endpoints be registered with agencies and cloud identity providers, that all devices are fully encrypted, and that access is granted only to compliant endpoints.

The Road to Zero Trust

IT'S IMPERATIVE FOR agency and IT leaders to understand that Zero Trust is not just a solution an organization can buy—it's a fundamental shift in how agencies harden their cybersecurity infrastructures. Moreover, that shift takes time, planning and resources. Depending on where agencies start and what's needed, that can mean anywhere from a few months to a few years.

While it can be difficult to determine when and what to move toward Zero Trust, it's well worth making the effort to understand, even if it takes working with outside partners to help shape the Zero Trust journey.

> Zero Trust is a fundamental shift in how agencies harden their cybersecurity infrastructures.

maximus

moving people forward

https://maximus.com/federal