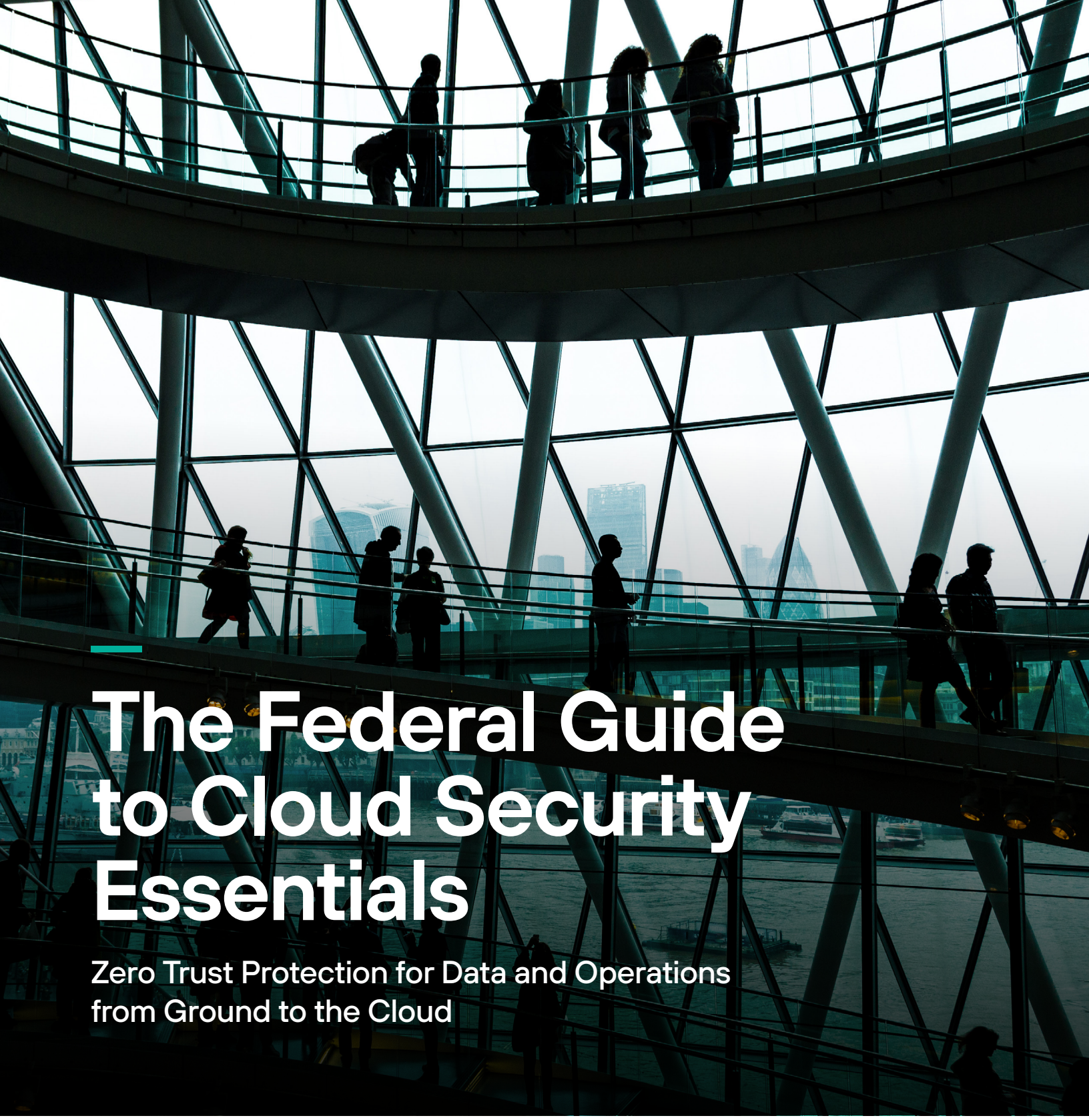

The Federal Guide to Cloud Security Essentials

Zero Trust Protection for Data and Operations from Ground to the Cloud

Forcepoint

Brochure

Landscape Overview: Cloud Security and Cloud Migration

The 2021 Executive Order 14058 on *Improving the Nation's Cybersecurity* calls for U.S. Federal agencies to accelerate movement to secure cloud and adopt a Zero Trust approach to mitigate increasingly sophisticated threats.

Migrating to the cloud can bring costs savings, efficiency, and scalability to IT Departments. But it's also a modern expectation of how agency employees now access and consume resources.

How people consume cloud every day drives how agencies adopt and secure cloud.

- **Cloud security is people-driven.**
- **Cloud is instant access.**
- **Zero Trust and cloud is an expectation.**

With constant access to content, apps, devices—all seamlessly connected to each other, all the time, without disruption—cloud is an inextricable part of our everyday lives. Deeply woven into the fabric of how the modern person unconsciously functions and operates. So in agency environments, the expectation is the same.

You want to use what you need, when you need it, and you want a fluid experience that doesn't hinder your productivity, but instead does the opposite. How do you increase your productivity with cloud? How do you do more with less? How do you embrace Zero Trust in the cloud? Because really, cloud is convenience that also supports modern infrastructure needs. But it also presents its own vulnerabilities if not properly secured.

Ultimately, workers are consumers. How agencies secure their organization and protect their data and people needs to match that same expectation and experience in our day-to-day. And security needs to evolve to allow for that fluidity while also securing the ever-expanding threat landscape accompanying that freedom and convenience.

This is the general culture of cloud. But there are many reasons the government has had to rethink their approach to cloud and security as a whole. They include:

- → Zero Trust mandates
- → The journey of digital transformation, starting with adoption and implementation of O365
- → Moving legacy and custom apps to the cloud, like EHR or ERP systems
- → People working beyond the confines of an office, off the corporate network or behind other defenses
- → Agencies are operating within and across highly distributed environments, encompassing sites that need the same level of security as HQ—without the need to recreate an expensive, hardware-heavy footprint at each location with backhauled traffic
- → Optimization efforts—whether it's consolidating security stacks, streamlining teams' workflows or just reducing CapEx/OpEx
- → Moving infrastructure to public clouds like AWS or Azure

The Right Way to Cloud

Cloud security means something different to everyone. And it's constantly and rapidly changing. So how do you keep up? How do you ensure your approach is holistic and effective and aligns with your Zero Trust strategy? In order to successfully protect your agency, cloud security needs to be inclusive.

Let's think about the key components of cloud:

Data
in the cloud

Users
in the cloud

Apps
in the cloud

Connectivity
in the cloud

Infrastructure
in the cloud

Zero Trust Security
in the cloud

At its core, this is what cloud security is all about. Cloud service providers are only responsible for the core infrastructure, not the apps and resources running on that infrastructure, nor the data being stored. Cloud shared security agreements require agencies to properly configure and reinforce agency specific policies. And Zero Trust requires all components of the cloud to be considered, governed, and protected in a unified manor to on-premis resources in order to avoid security gaps and keep users and data safe. While cloud security doesn't have one static definition, there is a right way to "cloud."

So, what does this look like?

To protect and connect to the cloud, agencies must:

- → Apply Zero Trust access to web content and cloud apps for any user, anywhere, and on any device
- → Have visibility and control across the organization to drive a consistent cloud security strategy
- → Safeguard data as it moves to and from the cloud
- → Enable direct-to-cloud connectivity for users and sites without backhauling
- → Optimize infrastructure and workflows
- → Protect against advanced threats, including zero day exploits

Great, so now that you know what you have to do, how is it actually achieved? Many agencies have existing products that can perform some key capabilities that enable this modernization, or employ different teams that are responsible for certain elements of cloud security or Zero Trust. But what every security organization wants to avoid is overwhelming their already-tapped security teams by implementing multiple point products that aren't integrated and that don't talk to each other.

What agencies truly need is a singular approach reinforced with a simplified solution that supports zero trust methodologies — not a concoction of vendor-diverse products. Yes, dependencies do exist — like the need to have visibility in order to have control, or the need to migrate on-premise web security to the cloud in order to protect off-network users. In its optimal state, cloud security is a unified solution wrapped around data, web access, cloud access and cloud data, and connectivity. It serves to alleviate any and all pain points across your security team, avoids security gaps, and aligns with your Zero Trust goals. Whether that's achieved with one vendor or three, enterprises must ensure that what they have, what they want, and where they want to be all align to achieve key agency outcomes.

Addressing Cloud Concerns

Moving data to the cloud is a significant undertaking—and if you feel some anxiety about it, you're not alone. How do you maintain ownership and control? How do you continue to keep threats at bay? How do you ensure performance?

Let's resolve some of the most common pain points.

Security
Cloud data security becomes increasingly important as we move our devices, data centers, processes, and more to the cloud. Cloud security is a shared responsibility model, where the cloud providers are only responsible for the security of the infrastructure they are providing. This means the accountability is incumbent on agencies to security data in their cloud environments. Ensuring quality cloud data security is achieved through comprehensive security policies, an organizational culture of security, and cloud security solutions.

Latency
Coverage is critical to reducing latency. An expansive footprint with abundant PoPs a will deliver low latency as well as other productivity-boosting benefits like content localization. **Tier 1 networks and Tier 4 data centers** help to ensure a high level of reach, redundancy, connectivity and quality ideal for latency-sensitive applications.

Visibility
You can't protect what you can't see. And you can't make changes or set policy without knowing what it will affect. Pairing a **cloud-delivered web gateway** with a **firewall** offers consistent visibility and enforcement across users and locations, including policy enforcement and control of shadow IT. And **CASB** functionality helps secure enterprises by providing visibility into what users of both sanctioned and unsanctioned apps are doing in the cloud to understand risks and protect users and data.

Aligning Cloud and Zero Trust Goals
It is important when embracing the cloud and hybrid IT that your Zero Trust strategy is at the forefront of your cloud planning and not an after thought. Moving to the cloud means that many of your Zero Trust security controls will likely need to be cloud native. Segmenting applications run from the cloud is also important. At the very least, agencies need to ensure that policies are consistent and manageable across environments and adopt technologies that enable this.

Driving change to the Federal Cloud Infrastructure
There are many policies and programs that are impacting Federal agencies' move to the cloud. The following programs are major elements of the Federal security strategy that must evolve alongside technological progress to allow agencies to take such a holistic and outcome-driven approach, including:

- → Cloud Smart encourages agencies to move to the cloud with the approach that security and privacy should be considered in terms of intended outcomes and capabilities.
- → FedRAMP stands for the "Federal Risk and Authorization Management Program." It standardizes security assessment and authorization for apps and infrastructure hosted in the public cloud and for SaaS based apps used by U.S. federal agencies. But FedRAMP does not apply to every solution, has limited approved services, and lags in keeping up with innovation cycles.
- → The Trusted Internet Connections (TIC) 3.0, a robust program that sets guidance and an execution framework for agencies to implement a baseline boundary security standard. It has evolved from simply reducing external network connections to protecting agency enterprise perimeters, mobile, and cloud connections with a focus on increasing the use of boundary protection capabilities to protect agency assets from an evolving threat landscape.
- → 2021 Executive Order 14058 on *Improving the Nation's Cybersecurity,* calls for Federal agencies to accelerate movement to secure cloud and adopt a Zero Trust approach to mitigate increasingly sophisticated threats.
- → Federal Information Security Modernization Act (FISMA) and Federal Information Technology Acquisition Reform Act (2014) (FITARA) also impact the Federal cloud strategy and Zero Trust and may require updates to support effectively measuring progress as agencies move to the cloud and adopt Zero Trust.

Data Sovereignty
While the cloud itself has no concrete confines, it's not exempt from the legal consequences of geographical borders and boundaries. Digital data is subject to the laws in which that data resides. Utilizing government cloud data centers located in the regions where your enterprise operates and is supported by US citizens is essential for Federal agencies data sovereignty, as well as performance.

Data Loss
A unified approach is the most successful approach. With integrated **data protection solutions**, you can extend your security measures from on-premises to the web, email, endpoint, network and cloud. Following Zero Trust best practices, you must ensure that access to data is determined by dynamic policy and granted on a per session basis. Risk Adaptive Protection (RAP) is built by combining UEBA and DLP technologies. The RAP combines the power of the DLP and UEBA technologies by ingesting the DLP event and incident data into the UEBA platform which performs modeling and analytics to determine a user profile risk. Leverage RAP to extend dynamic data policies to protect data at rest in the cloud and data in transit.

Planning for Unmanaged Devices and Remote Work
Today's workforce relies on a multitude of sanctioned and unsanctioned cloud applications, on both managed and unmanaged devices. When securing remote and roaming users, network perimeter defenses and endpoint protection don't cut it. You must distinguish between managed devices and BYOD and enable **granular security policies** that ensure employees using their own devices do so following agency policy and do not present additional risk. **Expanded controls** offer security for remote users who use agency devices for both work and personal use.

Settling for Good Enough
Eager to become more agile, efficient, etc., agency users frequently want to take a "figure it out later" approach when it comes to the cloud. But just checking the box often sacrifices both security and efficacy. For example, URL filtering alone is not security—the same way a recursive DNS solution is not a replacement for a full web gateway. You can't get full protection with just one element of a solution. Moreover, the bare-minimum approach puts security in a position to have to react, rather than pro-act. Make sure traditional silos like **security and networking teams work together and have a seat at the table** as your enterprise creates its roadmap to digital transformation and Zero Trust—that way they're working in lockstep with agency objectives and can avoid playing catch up.

Achieving Success in a Zero Trust Cloud-connected World

We established at the beginning that cloud security is people-driven, which is why it must be people-centric.

Thanks to the cloud, humans are **the new perimeter**. As users, partners, and customers access your organization's data from virtually anywhere, the artificial wall that protects the data is no longer enough. Legacy, infrastructure-centric security that groups trusted users on the inside and untrusted individuals on the outside is no longer relevant. Inherent trust can't be part of your security stack. And your security stack is integral—not ancillary—to your digital transformation.

To accelerate and safeguard it, here are some core principles to keep in mind:

Cloud at Your Own Pace
Rome wasn't built in a day. And your cloud migration isn't going to happen overnight. Most agencies are operating in hybrid IT/multi-cloud environments—and will continue to for the foreseeable future. Ensure your secure web gateway has flexible deployment options that enable you to migrate based on what is right for your agency today, and tomorrow. This will allow you to migrate on your own terms, as you're ready, while maintaining across-the-board security.

Extend Alongside Your Edge
Secure your cloud, network and endpoints to meet your ever-changing agency needs. A low-hardware, converged platform with modular security capabilities offers highly distributed agencies the extensibility and agility they need to take advantages of new advances, prevent blind spots and connect across locations—securely and manageably.

Zero Trust, Absolute Insight
"Never trust, always verify" is a key tenant of the Zero Trust framework—meaning the way to protect your agency's data is by evaluating access to that data throughout the user and device interaction. This helps you understand the "who" and "how." Understanding the "why" is what will help you move beyond awareness and into prevention. Layer on behavioral analytics to understand intent.

Are you ready for what's next on the journey to scalable cloud security?

Check out our eBook

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, Twitter and LinkedIn.