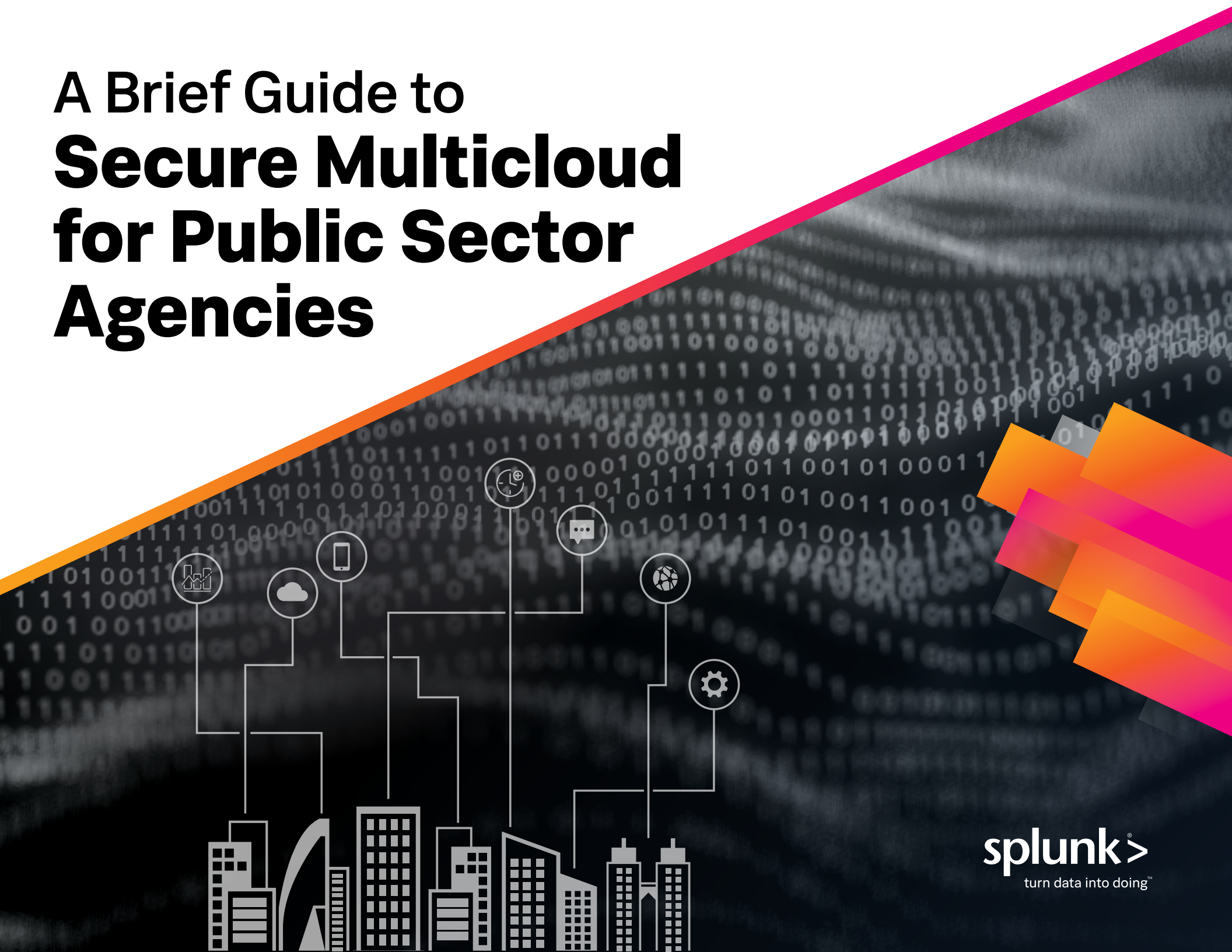
A Brief Guide to **Secure Multicloud for Public Sector Agencies**



splunk>
turn data into doing™

A Brief Guide to **Secure Multicloud for Public Sector Agencies**

As more public sector organizations are shifting infrastructure and services to the cloud, more are adopting a multicloud strategy.

Why?

In this brief guide we will explain what multicloud is, the benefits of embracing a multicloud strategy and lastly — and we would argue most importantly — how government can secure multicloud with the right security solution.

What Is **Multicloud?**

Adopting a multicloud strategy is not a difficult concept to understand. It simply means a government organization that leverages at least two cloud services in a single architecture to solve various challenges.

There's some nuance here that's important to understand. Specifically, there are different types of cloud services that can make up multicloud. Let's start with the public cloud. Think Amazon Web Services, Microsoft Azure or Google Cloud Platform. And then there is the private cloud, which is similar to the public cloud but access is exclusive to a specific organization or hosted privately on premises by a company. Lastly, multicloud often includes all the software as a service (SaaS) solutions public sector organizations are now using. Think of services such as G Suite, Workday, Salesforce, Adobe Creative Cloud and Office 365. And the list goes on and on.

A multicloud strategy is not the same as a hybrid cloud strategy, which instead refers to multiple cloud deployment models ranging from public, private or both. For example when an organization builds its infrastructure with both an on premises private cloud and a third party public cloud. Organizations sometimes need to take this approach for its infrastructure for compliance or to segment different parts of the business like finance, for example.

Six Benefits of a **Multicloud Environment**

There are more than six benefits to embracing a multicloud strategy but for the sake of brevity, we have come up with a top six list:

1. Cost savings
2. Flexibility and agility
3. Improved reliability
4. Performance optimization
5. Avoiding vendor lock-in
6. Lowered risk of DDoS attacks

In the continued spirit of brevity, let's quickly add context to the list.

There are several ways a multicloud strategy can ensure **cost savings**, especially because of the **flexibility and agility** it offers. For instance, it can make it more difficult for hackers to take down all of an organization's services if they are distributed across multiple clouds. Additionally, multicloud strategy can vastly **improve performance**. Passive clouds can be the fallback solution when primary clouds are taken down or have performance issues (whether it's caused by a bad actor or a change in operations). This **improved reliability** of services as a whole can help reduce and/or eliminate downtime until the primary cloud is brought back online.

To put it into real-world context think about **distributed denial-of-service (DDoS)** attacks, where hackers use several computer systems or connected devices to attack and overwhelm a server, website or cloud provider. A successful attack means networks go down while costs go up for the target organization.

The results can have a range of repercussions, from dollars lost for businesses to lives at risk in healthcare services. A recent survey put a dollar amount on it. It found that 98% of organizations say a single hour of downtime costs on average over $100,000, while 33% or enterprises reported downtime could cost them upwards of $5 million.

A multicloud strategy can help reduce the effect of DDoS attacks by spreading traffic and services over multiple clouds, in turn, eliminating the risk of having one point of failure.

A multicloud strategy also means avoiding **vendor lock-in**. Instead of going all-in on one provider, multicloud organizations can evaluate analogous offerings and select whichever one serves them best, regardless of who provides it. On their end, vendors have to compete harder for an organization's business when they know organizations have multiple options and clouds available. It requires vendors to stay competitive with services and cost knowing their multicloud customers could switch to another vendor for their SaaS or cloud architecture needs.

The Challenges of Securing a **Multicloud Strategy**

For all the benefits of a multicloud strategy, there are some challenges that come with it as well. For instance, it can be difficult to secure a multicloud strategy because of a lack of visibility across hosts and services. In such an environment, hackers can find exploitable vulnerabilities within an organization's infrastructure that may have been overlooked by those managing it.

More than a lack of visibility, initial mismanagement and misconfigurations can have costly outcomes down the road. When setting up multicloud environments, proper identity and access management (IAM) is key and fundamental to the overall security of an organization's infrastructure. It can effectively grant access to cloud resources without leaving it exposed to malicious actors or unfortunate accidents.

There is also the question of complexity. While the cloud make infrastructure management simple, it also introduces complexity in the form of dozens of new services, some loss of control over the data once it's in the cloud and a lack of visibility, as mentioned above.

How to **Secure Your Multicloud**

But luckily there is a solution. A multicloud ecosystem is diverse — spanning across multiple vendors, applications and systems. Organizations who adopt a multicloud strategy need visibility and change controls across it all to better understand who is doing what and where across a myriad of cloud services to prevent downtime, or worse.

The Splunk Cloud Platform deliver this visibility, providing instant security and operational insights into the most popular cloud services such as AWS, Azure and the Google Cloud Platform.

The Splunk platform helps organizations with a multi-cloud strategy monitor the uptime and availability of multiple cloud services in a single view, ensure the security and compliance of a multi-cloud environment. The platform can also help deploy third-party cloud services with confidence.

The Splunk Cloud Platform meets the FedRAMP security standards, and helps U.S. federal agencies and their partners drive confident decisions and decisive actions at mission speeds. Splunk Cloud Platform has additionally achieved U.S. Department of Defense Provisional Authorization at Impact Level 5.

Get Started.

Ready to learn more about how to gain greater visibility and security across your multicloud? Learn how to achieve mission success **with Splunk**.

Learn More

splunk> turn data into doing™

21-13388-Splunk-PUBSEC-Brief-Guide-to-Securing-Your-Multi-Cloud-101