

## IMPRES Technology Solutions

### Moving to the Cloud with a Non-Hackable, Simplified Overlay Infrastructure



Robert Osborne

Federal agencies face many challenges when modernizing their technology infrastructure, particularly when transitioning to the cloud. This includes understanding the types of cloud services available, various levels of cloud security, and providers. Cloud computing has become synonymous with federal IT modernization, emerging as a necessity for agencies to bring their mission-critical operations into the 21st century. Yet the level of success achieved is often impaired by learning curves, misconceptions, and institutional barriers. To successfully implement cloud services, agencies must understand and address diverse issues that complicate their decision making and deployment strategy. Data security and protection are crucial prerequisite for government organizations considering new technology adoption. Agencies in the federal space are often hesitant to “take things off-premise”; and when they do decide to modernize, their preferences tend to toward hybrid solutions. “Customers in the federal space know that they need to move to the ‘cloud’ but fail to note that not all clouds are created equal and that they all come with their own idiosyncrasies, frailties, and benefits,” says Robert Osborne, CTO at IMPRES Technology Solutions. He recalls instances where IMPRES, by

white-boarding and micro-segmenting their clients’ roadmap upfront, was able to deliver solutions at prices that amounted to a fraction of their allocated budgets. As a vendor agnostic solution provider, IMPRES works in tandem with multiple vendors, OEMs, and cloud providers, and delivers a single set of tools and integration services to enable their clients to ensure security and full control of critical data.

#### Connecting and Protecting Applications and Data Across On-Premises and Separate Cloud Providers

Using native security controls to connect and micro-segment workloads and containers between local resources, availability zones, regions and across cloud providers is not only ineffective and inconsistent, but too complex to maintain at scale. The result? All too often we’ve seen teams inadvertently expose workloads to the public Internet by a simple security group error or Internet gateway change. This inability to quickly micro-segment and peer workloads across AWS and Azure zones, regions, and between our on-premises environment force customers to consider writing their own control plane at considerable time and cost.

#### Simple Software Defined Segmentation for Hybrid Cloud Deployments

Our customers have eliminated the complexity, attack vectors, and costs associated with traditional security controls by adopting a unified identity-centric model for cloud and on-premises environments that is simpler and more secure. By deploying zero trust networking infrastructure as code, the security and network perimeter is moved from the network edge to the host,



making policy orchestration explicit and programmable. With Software-Defined Segmentation, protection is automated, and workloads are made invisible to unauthorized machines, giving DevOps the agility and peace of mind, they seek.

Customers can securely isolate and peer their internal network and across multiple distributed AWS VPCs and Azure VNETs. DevOps can follow a typical build, test, and release workflow with all members requiring discrete remote access from anywhere. Functions like cloaked micro-segmentation would be impossible without developing a custom network data and control plane.

Key to setting IMPRES apart from its competitors is their employees, most of whom are former operators in IT for Federal agencies thus bring with them actual experience as to the needs of this sector. In his 30 years of experience in the IT landscape, Osborne himself has notably served in the US Army and worked for organizations such as IBM, Microsoft and DELL in a variety of positions from Senior Architect to Director Enterprise Technologist. He leads the IMPRES’ mission to deliver Cloud and other IT solutions to fit the best interest of the client. “Our biggest differentiator is we are not beholden to anyone except the customer,” adds Osborne. IMPRES has proven their expertise in leveraging ‘resources’ from well-known OEMs and combining them with a vast amount of government contract experience to provide solutions for cybersecurity and the cloud. GC