451 Research

Business Impact Brief

# The Emergence of Unified Access Management

## The 451 Take

Modern enterprises are embracing the cloud for various reasons: scaling to meet spikes in demand, quickly rolling out new features or lowering IT costs. Most firms are actively moving more workloads to the cloud. But all workloads aren't created equal, and not all will shift to cloud, for a range of reasons. Thus, it's becoming clear for many that hybrid IT is more than a temporary transitional phase – it's actually an end state in itself. To manage this hybrid reality, IT professionals must seek solutions that can unify application access across both legacy on-premises and cloud environments to be truly effective.

In recent years, we have seen a steady progression of applications and workloads from on-premises deployments toward cloud-based architectures. In fact our research shows that 62.8% of overall workloads are currently running in the cloud, with more than two-thirds (67.5%) expected to be there within two years. Despite all the advantages, there are valid reasons why not all workloads should move to cloud. Security remains one of the biggest hurdles. In many ways this is unfounded, since most cloud providers are arguably more secure than the average enterprise will ever be. Compliance is another big obstacle to cloud deployment, particularly with new regulations like GDPR looming.

### Hosted IT Infrastructure – Inhibitors

Q: What is stopping you from using more hosted IT infrastructure? [Select top three] (n=1503)


Source: 451 Research

Another major adoption hurdle is complexity. In the pre-cloud world, most firms were already dealing with a proliferation of security tools to manage, and injecting cloud resources into the mix adds even more overhead in terms of security concerns, staffing requirements, etc. In simple terms, most firms are dealing with too many security vendors and need to start exploring ways to streamline the number of vendors they engage with on a day-to-day basis.

Enterprises do not operate in a binary world. Hybrid IT is defined as the use of multiple deployment models to deliver a single workload or application. And while the term 'cloud' is often presented as a

# Business Impact Brief

## The 451 Take (cont)

homogeneous entity, in reality firms will pursue a variety of cloud models – including on-prem and hosted private clouds, virtual private clouds, IaaS, PaaS and SaaS – and will also leverage new services such as containers, serverless computing and microservices. In other words, a one-size-fits-all approach to workload execution venue is likely to yield suboptimal results.

Regardless of the particular flavor of cloud adopted, the reality is that we are living in a 'netherworld' between the old and new, which will likely persist indefinitely. Decisions around deployment models and 'best execution venues' will remain dynamic, based on individual application profiles and requirements. And one of the main criteria for success will be how well security – and specifically access management – will be applied to each of these scenarios.

## Business Impact

**HYBRID IS MORE THAN A TRANSITION STRATEGY.** Hybrid IT is not just a transitional phase on the path to 'cloud nirvana.' The general idea of hybrid IT is to serve applications and workloads across heterogeneous environments – across both legacy on-prem and cloud resources, but also across multiple clouds.

**ELIMINATE SECURITY SILOS.** As much as cloud is expected to make life simpler, the reality for most firms is that we are stuck somewhere between legacy IT infrastructures and 'modern' architectures like cloud, mobility and IoT. Access to each of these distinct environments is often managed separately, creating more silos and inefficiencies that place demands on already scarce security resources, and also create potential security gaps that attackers can exploit.

**A UNIFIED APPROACH CAN RELIEVE EXISTING PAIN POINTS.** Historically, access to traditional on-prem applications such as ERP from SAP or Oracle has been managed discretely from SaaS applications. A unified access management approach can help enterprises address pain points that result from managing not only a mix of on-premises and cloud apps, but also various directories (AD, LDAP, Google G Suite, HR systems) and a wide range of users (employees, partners, contractors and customers) across a mix of network access solutions (VPN, Wi-Fi) and devices (PC, Mac, iOS, Android).

## Looking Ahead

If hybrid IT is the reality in which most firms will operate going forward, a holistic, unified approach to managing access can enable organizations to take a major step toward abstracting away the underlying complexity of their diverse environments. Specifically, unified access management can help address the operational pain points arising from this heterogeneous and fast-changing mix of applications, users, networks and devices.