451 Research

Business Impact Brief

The Emergence of Identity and Access Threat Prevention

The 451 Take

There are a number of compelling reasons why modern enterprises are embracing the cloud: the ability to easily scale to meet spikes in demand, the ease of rolling out new features, and also the potential to lower IT costs, both up front and over time. Despite all of the potential benefits of cloud, however, not all workloads are created equal. While most firms are moving more workloads to the cloud, some are surprisingly moving workloads and services back to on-premises datacenters or private cloud environments, for a variety of reasons.

The upshot of this phenomenon is that it's becoming clear that hybrid IT is more than a temporary transitional phase – for many firms, it's actually an end state in itself. This can present substantial challenges for most IT organizations, which must look for ways to manage security across both legacy on-prem and cloud environments to be truly effective. Said otherwise, cloud computing offers many tangible benefits, but it can also add a new layer of complexity that many firms are ill equipped to handle, particularly when facing a scarcity of security talent and internal resources.

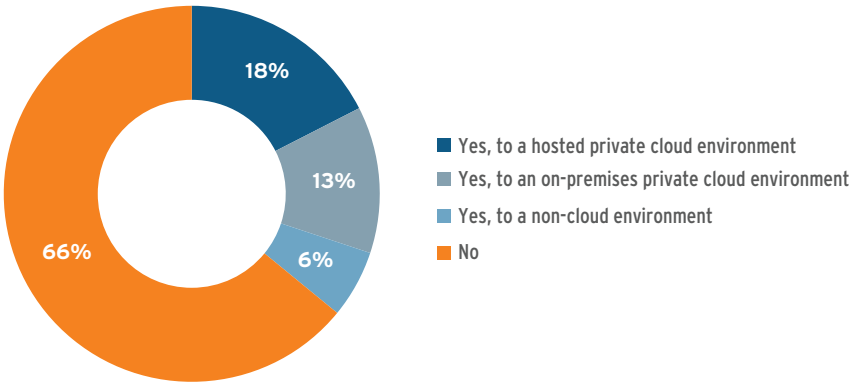
The steady progression of applications and workloads from on-premises deployments toward cloud-based architectures is no secret. In fact, recent research from 451 shows that, on average, 17% of workloads are currently running in public cloud (IaaS, PaaS and SaaS), with 30% expected to run in public cloud within the next two years, while hosted and on-prem private clouds are also expected to increase. Conversely, workloads running in 'traditional' on-prem IT infrastructure are expected to decline sharply, from 46% to 21% over the same period.

Still, there are valid reasons why not all workloads and applications should move to the cloud. Indeed, 451 survey data has shown that roughly one-third of respondents (34%) have shifted workloads from public cloud to either private cloud or on-prem datacenters in the past 12 months. Security has historically been a primary objection to adopting cloud, and not surprisingly it remains one of the biggest reasons to 'repatriate' cloud workloads. Compliance is another big obstacle, particularly with new regulations like GDPR. The number one reason for repatriating workloads, however, is performance concerns, combined with improvements in the performance capabilities of on-prem environments, perhaps due to new developments such as containers and microservices.

Despite Its Benefits, Organizations Are Shifting Workloads Back From the Cloud

Source: 451 Research's Voice of the Enterprise: Cloud Transformation, Organizational Dynamics 2017

Within the past 12 months, has your organization migrated any applications or data that were primarily part of a public cloud to a private cloud or non-cloud environment? (n=249)



Business Impact Brief

Business Impact

BEST EXECUTION VENUE. The survey data lends support to the concept of 'best execution venue' – the idea that applications and workloads should reside in a location that makes the most sense for their specific requirements, whether public cloud, private cloud or even a combination of both. While this may seem straightforward, from a security perspective the implications of such a scenario are nontrivial.

ELIMINATE SECURITY SILOS. As much as cloud is expected to make our lives simpler, the reality for most firms is that we are stuck between legacy IT infrastructure on one hand and 'modern' architectures like cloud, mobility and IoT on the other. Today, access to these distinct environments is managed separately, creating more silos and inefficiencies that place demands on already scarce security resources and leave potential security gaps that attackers can exploit.

HYBRID IT MEANS MORE 'STUFF' TO MANAGE. In the pre-cloud world, most firms were already dealing with a proliferation of security tools to manage, and injecting cloud into the mix results in two sets of infrastructure to maintain. In simple terms, most firms are dealing with way too many security vendors and platforms, and maintaining visibility across all of them is a growing problem for enterprises that are looking to embrace the cloud, as well as IoT or other new architectures.

SECURITY POLICIES NEED TO BE CONSISTENT ACROSS ALL ASSETS. In a hybrid scenario, complexity can increase, which increases the need for context across all assets, as well as visibility across all platforms, both cloud-based and non-cloud. To avoid gaps in coverage, security policies also need to be consistently applied, which implies automated, contextual processes as opposed to manually 'stitching' together legacy policy frameworks.

Looking Ahead

If hybrid IT will be the reality in which most firms operate in the future, a holistic approach to both managing access to resources and addressing threats (internal and external) can allow organizations to take a major step toward abstracting away the underlying complexity of their diverse environments and improving their overall security posture. But as applications, identity stores, users and devices are increasingly 'scattered' outside the corporate network, identity becomes a focal point of any security strategy – 'who' you are becomes more important than 'where.'

Yet historically, identity management and threat protection have been treated as separate domains. Further, identity alone is not sufficient. Identity-based systems have their own limitations, including complexity, a potentially onerous user experience, the challenge of integrating with legacy resources and, perhaps most importantly, identity systems are typically static in nature. For example, there are many resources or applications that do not readily accept MFA without substantial customization, if at all. Further, most MFA offerings are completely blind to what happens post-login, and are thus susceptible to man-in-the-middle attacks or stolen credentials.

To maximize the benefits of identity-based approaches, a new approach called Identity and Access Threat Prevention (IATP) combines elements of identity, behavior and risk principles to help address any security gaps that remain between a heterogeneous mix of resources. A central feature of IATP is continuous monitoring of user behavior to assess the riskiness of certain actions in order to provide more accurate and timely responses to potential threats, without placing an undue burden on users and requiring constant reauthentication, and without requiring extensive changes to existing architectures.

preempt

To learn more about Identity and Access Threat Prevention, download Security Evolved – Why It's Time To Bring Together Identity, Access and Real Time Threat Prevention. IATP allows enterprises to gain holistic visibility of all user activity on-premises or in the cloud; preempt security threats; and enable security operations teams be more effective. This ensures that both security threats and risky employee activities are responded to with the right level of security at the right time.