FORTRA

The Security Dangers Lurking in Your Hybrid Cloud Environment

The Good News: Cloud Capabilities Enable Expansion Like Never Before

Businesses everywhere seek new ways to grow and expand. Whether your company has put forward a concerted effort to increase sales, or is lucky enough to enjoy a naturally burgeoning interest in your product or service, success is welcome.

IT teams are often among the first areas in the organization to feel the change. There's more data to store and manage across all lines of the business, and more users to onboard.

These teams often turn to the cloud for its promises of agility. In fact, in the last quarter of 2017, Microsoft Azure® saw 90 percent growth and category leader Amazon Web Services (AWS®) grew by 45 percent[1]. According to customer segmentation data announced during 2017's AWS re:Invent conference, the company has also captured 50 percent of all cloud deployments for small to midsized businesses in the U.S.

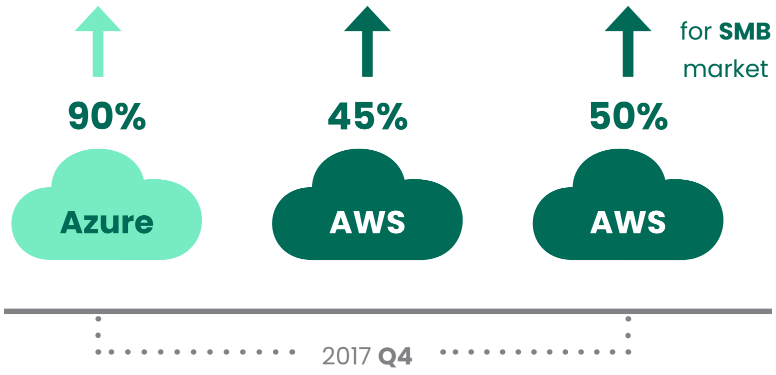
Clearly, the cloud has become an integral part of today's business and IT operations toolkit.

The beauty of the cloud is that it's possible to expand capabilities like short-term capacity or long-term backups quickly and without the costly infrastructure and additional employees associated with onpremise equipment.

For example, media companies can host events during which they need to scale up their capacity to a massive extent for just a few days. However, they still need to protect their IP at all times. Or, a company may want to sell a live product in real time while recording how the audience interacts with it.

The problem is that when it comes to the security of the data being pushed to the cloud, everyone assumes it's on someone else's list.

But it's not.



[1] https://cloudtweaks.com/2018/02/smart-data-approach-environment/

The Bad News: Security Policies in Hybrid Environments Are Lax or Nonexistent

Already in the first six weeks of 2018 there have been 124 data breaches reported[2].

The sad fact of the matter is data stored on any server with poor security controls is at risk—from opportunistic employees digging into areas they shouldn't and malicious external hackers seeking information ripe for black market sales or ransom.

124
data breaches
Jan
Feb
2018

This is to say nothing of the accidents—those situations when an employee causes an outage from misconfiguring a setting or leaves sensitive documents containing passwords, employee records, or business strategies completely open to anyone who stumbles across them online.

As often happens during periods of growth or change, safeguards and standard operating processes fall by the wayside in the mad dash to scale up operations, infrastructure, and employees. What usually starts as a great idea to use the cloud to increase capabilities can turn quickly into confusion if you're lucky, and a data breach if you aren't. Security can become a second or even third thought to the person spinning up a new server in the cloud to meet an important deadline.

Digging into the details of how security is being handled is equally important for on-premise servers and those deployed in the cloud. These two infrastructures need to be in lock-step with one another when it comes to critical defenses such as user identities, roles, and privileges. Your cloud environment can disintegrate into the new Wild West if you're not careful. It happens every day.

> **Internally, most companies have established solid security controls and practices, but they don't really know what's happening with their cloud data.**

Oftentimes, vulnerabilities come to light during routine audits. Many an auditor has uncovered poor security controls when evaluating businesses for adherence with regulations such as Sarbanes-Oxley, PCI DSS, HIPAA, or GDPR. A lack of attention to securing important information becomes materially relevant to the audit and is detrimental to your organization.

Security Is Up to You—Not Your Cloud Provider

Big-name brands use well-known cloud computing vendors such as AWS, Microsoft Azure, and Google Cloud Platform™, so the default security settings must be good, right? **Wrong**.

Every day IT staff miss the fine print in cloud agreements that they're the ones responsible for aligning cloud security with their defined protocols.

It's not the cloud vendor's responsibility. It's also not the responsibility of the application or operating system vendor whose pre-built systems you can drag and drop easily from the cloud portal store into your own cloud environment.

The big cloud infrastructure providers focus their efforts on providing a seamless onboarding process for new customers. Likewise, application or OS vendors clearly state their lack of business liability in their "Right to Use" legal agreements—which IT staff normally do not review.

While security information and robust controls are certainly available with these vendors, they want companies to get up and running first and foremost.

Aligning the Security Profiles of Your On-Premise and Cloud Environments

Sometimes it's difficult to develop a clear view of what your full hybrid security model looks like.

Technologists frequently expect security policies in cloud and onpremise environments to be mirror images of one another, because they should be. However, many discover they are actually managing two completely different models. Because of this there are probably even different tools and software solutions involved as well, which makes for a lot of extra work and can lead to the formation of separate security teams.

Overall, organizations with multiple models increase the chance they will overlook a key component or have their security policies drift out of sync, which auditors will likely detect.

Without a dedicated approach to bringing security policies in sync, they typically aren't even close. Operating systems, databases, and data connectors should be aligned. These are available in the public cloud and can hook up to your internal tools.

Your ultimate goal is to centralize the management of accounts, access, and privilege across all users to control your entire security landscape and protect your organization.

It's up to you and your project team to complete the due diligence needed on everything from how user access is handled to the security of multi-tenant boundaries and whether the vendor has the auditing capabilities you need to achieve regulatory compliance.

Righting the Security Ship

If there are red flags going up in your mind regarding the security of your hybrid cloud environment, you're not alone. The good news is you can now take a fresh look at your security program and bring cloud and on-premise servers into alignment, with the right protocols in place going forward.

The first step is to define your security processes internally in preparation for extending them to the cloud. You may be surprised to discover during this phase that your internal policies and tools aren't cloud ready.

If you determine you'll need to evaluate new options to bring your infrastructure up to speed, this is well worth the investment and an ideal time to explore the advances in functionality available.

> **Companies typically account for 20 percent of their existing technology to roll onto new platforms each year, and your security effort is a good candidate for this budgeted expense.**

You'll also want to investigate your procurement policies. Many larger organizations have dual-source procurement requirements in place that require two cloud vendors be used due to the criticality of the data involved. Some require even more. Make sure you understand if this is a base requirement at your company as you evaluate your overall cloud deployment strategy.

The Role of Identity and Access Management

With the right security technology in place it doesn't matter if you have eight servers or 80,000. You're able to manage security and user access seamlessly from a central location and rest assured that information stored both on premise and in the cloud is secure. You can also scale out quickly as you grow or address short-term needs for additional cloud services.

Leveraging an identity and access management (IAM) solution that can scale with your business means you don't have to overhaul your security profile just a few years after you implement it. The right solution will evolve with you, keeping training and reporting consistent over time for ease of use.

With an IAM solution, your goal is to effectively manage user privileges and access, because **many cyberattacks are carried out by company insiders.**

You also want to limit the exposure of sensitive information by giving the smallest number of users elevated privileges to the most sensitive systems, which is called privileged access management (PAM). This is particularly important if credentials become compromised.

Get Control of Security in Your Hybrid Environment with Powertech Identity & Access Manager (BoKS)

Powertech Identity & Access Manager (BoKS) can help you transform your multi-vendor Linux and UNIX server environment into one centrally managed security domain. It simplifies your organization's ability to enforce security policies and control access to critical systems and information.

With full control over accounts, access and privilege, your IT and security teams can proactively prevent internal and external critical system attacks.

Drive efficiency

Simplify administration with role-based groupings of people and systems with tools to increase productivity and quickly extend security to the cloud with your existing staff.

Increase security

Centralize access and privileged security for better control, visibility, and scalability.

Meet compliance requirements

Meet compliance regulations such as PCI DSS, HIPAA, and Sarbanes-Oxley by architecting security into your deployment from the start.

Conclusion

The cloud is a great at-the-ready option whether you need to scale up capabilities quickly for a short period of time or require long-term backups and information storage.

Unfortunately, many organizations have discovered their cloud environments have been left untended from a security standpoint, putting their organization and end-customers at risk.

Bringing security policies into alignment for on-premise and cloud servers allows for centralized control of how users interact with your sensitive information.

Tools such as Identity & Access Manager can enable you to reduce the burden on your internal teams while enforcing strong security measures and meeting compliance requirements. Having a welldefined and enforced security strategy will set the stage for the ongoing growth and success of your business.

Get a Demo of Identity & Access Manager

Learn more about how Identity & Access Manager can support your security initiatives no matter how extensive your hybrid IT environment. Request a demo at www.fortra.com/cta/request-livedemonstration-identity-access-manager

FORTRA

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.