

HOW THE RAPID ADOPTION OF PUBLIC CLOUDS IS AFFECTING CYBERSECURITY

Security Concerns Need to Be Front and Center



EXECUTIVE SUMMARY

Companies are increasingly moving data and applications to public cloud platforms. Sometimes these transitions happen with IT's approval and guidance; sometimes they don't. Regardless, a company that stores data and uses applications in multiple public clouds creates a challenging environment for the security architect. It's difficult to gain visibility and control of the security posture when the organization relies on an assortment of disparate cloud platforms that all take different approaches to security and offer different tools. And it's hard for a small security staff to stay on top of disparate solutions that fail to integrate.

EXPLOSION OF THE ENTERPRISE CLOUD

As the popularity of public cloud platforms like Amazon Web Services (AWS), Microsoft Azure, and Google Cloud increases, more and more companies are moving their data off-premises for two key reasons. First, the pay-as-you-go cost structure is easier to justify, at least up front, than the large capital expenditures required to stock an in-house data center or build a private cloud. And second, companies appreciate the operational agility that comes with ramping up capacity at a moment's notice or shutting off unnecessary features on demand.¹

One recent study finds that 80% of companies expect to have more than 10% of their workloads on public cloud platforms within three years.² This is borne out by spending forecasts as well. IDC recently projected that over the course of 2018, worldwide spending on public cloud services and infrastructure will reach \$160 billion—a 23.2% increase over 2017. And by 2021, public cloud spending is forecast to reach \$277 billion.³

These investments are enabling companies to make crucial applications easier and more cost-effectively available to employees, customers, suppliers, and other stakeholders around the world. But public clouds demand particular attention from IT security managers for the following three reasons:



23.2%
projected growth in worldwide
spending on public cloud
services and infrastructure
in 2018.⁴



1. FAST ROLLOUT MAY LEAD TO FORGOTTEN OR NEGLECTED APPS

The ability to leverage rapid rollout and scaling of resources as offered by public cloud providers are key reasons why companies—and employees within those companies—choose to deploy applications in public clouds. Deploying Software-as-a-Service (SaaS) solutions does not typically entail a lengthy requisition and setup process. The cloud enables people who are not tech savvy to shop for and provision IT services,⁵ and they can often deploy these services in a matter of minutes.⁶

The upside is an accelerated timeline to get important functionality in the hands of end-users. A company can easily try new solutions, and if they don't work as intended, it can move on to other options. This enables organizations to give employees access to a wider range of applications and the ability to ultimately choose the best application for the business. The result is that these applications are made available much faster than happens in traditional, on-premises data centers.

One downside of the rapid-rollout approach, however, is that application administrators often do not take the time to decommission applications due to the fact that decommissioning a cloud application is often more time-consuming than launching it. Thus, if one application turns out not to work as planned and the company moves on to try other solutions, it may inadvertently leave data in the cloud or fail to turn off permissions and functionality for applications that it is no longer using. It is also a matter of motivation, as people are less motivated to spend the time to clean up behind them.

Months or years down the road, hackers might breach the once-tried but long-forgotten application. Cloud-based software that is not properly decommissioned can present security vulnerabilities that linger indefinitely below the radar of the network and security teams.

2. DECENTRALIZATION HAMPERS ACCOUNTABILITY

A manager or employee with Internet access and a credit card no longer needs IT approval, recommendations, or even guidance to build new applications. As a result, business units are able to deploy cloud resources on their own without requesting IT assistance. However, some of the applications they deploy may not support required business policies and procedures. In many cases, the IT department may not even be aware of new cloud services or applications being utilized by various business units and that business units are moving corporate data into the public cloud until after the fact—and sometimes not at all.

This is a widespread challenge in companies of all sizes. Studies show that “shadow IT”—deployed and used outside the company's standard IT requisition processes—accounts for anywhere from 30% to 50% of total IT spending in large companies.⁷

For the security architect who is charged to design security architectures that provide comprehensive coverage of the entire attack surface and visibility across each cloud infrastructure and application, this is often a serious problem. Solutions set up by users who aren't IT savvy are unlikely to be well protected. In fact, security misconfiguration is one of the top 10 security risks for web applications that were identified by the Open Web Application Security Project (OWASP).⁸ Configuration errors led to a massive data breach at National Credit Federation in December 2017, which resulted in the loss of 111 GB of sensitive data on 40,000 customers.⁹

“We are fast moving away from IT deployments which concentrated IT decision-making in the hands of a few. With the rise of the digital ecosystem, workloads have become diverse, complex, and difficult to understand by the traditional IT teams.”¹⁰



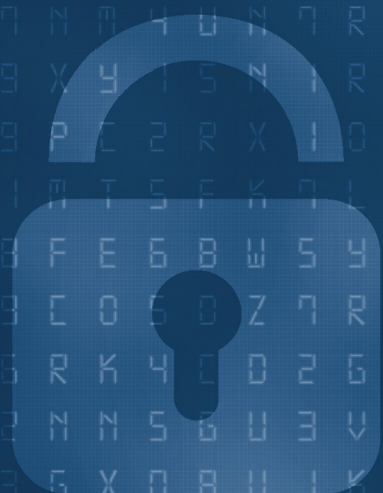
3. CLOUD HETEROGENEITY ADDS TO COMPLEXITY AND WORKFLOWS

A company with a significant number of cloud services and applications must manage a broad set of heterogeneous technology infrastructures. Employees who can deploy applications themselves to solve a variety of different problems inevitably choose different solutions, from different providers, for different areas of the company.

Security capabilities and management interfaces vary across different cloud services, so diversity of solutions further complicates the challenge to create a security architecture that is all-encompassing. Add to that the perpetual disorder caused as business groups are trying and deploying new cloud services and applications, and the challenge of the security architect increases further. Thus, even if shadow IT was not an issue and the cybersecurity team was aware of every application in the company's cloud infrastructure, this constant churn in cloud applications creates an information security dynamic that is hard to track and manage. Further, maintaining a consistent security policy across all a company's public cloud resources, inventorying security options, and selected settings within each application requires an extraordinary amount of manual effort and expertise.

But cybersecurity teams are already stretched and there is an acute security skills shortage—1 million unfilled openings today that is expected to reach 3.5 million in a few years.¹¹ Indeed, more than half of organizations indicate they have a shortage of cybersecurity skills right now.¹²

Still, most companies can't effectively block their employees' use of applications and data in the public cloud. Here, the security architect needs to deploy tools and develop processes that facilitate the collection of complete information about the location and security of corporate data assets, whether on-premises or in a private or public cloud.



WHO'S RESPONSIBLE FOR SECURITY IN THE CLOUD?

Some users, and even some security and networking staff, incorrectly believe that data in the public cloud is secured by the cloud provider. The major providers, such as Amazon, Microsoft, and Google, have security capabilities and practices in place for protecting the availability and integrity of the services they offer. But other security responsibilities are owned by the end-user. The onus for protecting the confidentiality of data as well as the availability and integrity of applications resides with the end-user.¹³

Common problems when security of cloud-based applications is mismanaged include unsecured directories, deployment of insecure non-production applications in the same security environment as a production server, failure to patch known vulnerabilities, and misconfigured firewalls.¹⁴ End-user credentialing and passwords also continue to cause headaches for security teams. Some employees use the same credentials for an assortment of applications. They may use the same password for critical internal applications, such as finance systems, for the software they access in the public cloud. This security practice means that if the public cloud is breached, the company would be vulnerable to direct attacks of internal systems or indirect attacks using social engineering. A recent study finds that 81% of hacking-related data breaches leveraged passwords that were either weak, stolen, or simply the software's default.¹⁵

Unlike providers of public cloud infrastructure, SaaS providers are responsible for securing both the application and infrastructure. Still, content permissions are the responsibility of application users.¹⁶

But this approach can open up the organization to new vulnerabilities. Line-of-business employees may set overly permissive read privileges and give the wrong people access to sensitive information. Dow Jones, as an example, lost millions of customer records last year due to poor permission management in the public cloud.¹⁷ Similarly, business users might fail to properly lock down write privileges, which can open the door to hackers changing corporate files.

Customers who run applications on Infrastructure-as-a-Service (IaaS) platforms are also taking on significant security responsibilities. While IaaS providers are responsible for keeping cloud services running, the customer is fully responsible for security of the operating systems and software running on the platform. This requires attention not only to upfront security settings, but also to ongoing patching and updates.¹⁸

“It is up to the enterprise—not the cloud provider—to properly configure certain cybersecurity settings. Improperly configured cloud security settings were at fault for the recent massive breach of voter data mined by a data analytics company that had been hired by the Republican National Committee.”¹⁹



MULTIPLE CLOUDS EXPONENTIALLY INCREASE THE ATTACK SURFACE

With statistics like these hanging over their heads, security architects are trying to secure a nebulous and ever-expanding public cloud environment. Corporate security is only as strong as the weakest link, and in a diverse cloud infrastructure, each provider has different vulnerabilities.

In this case, different public cloud providers have different policies for connecting elements of different applications. Others offer different security solutions. For example, some offer only a network firewall and make customers responsible for any security beyond the perimeter gateway. Others also provide web application firewalls and security information and event management (SIEM) technologies.

This is problematic because when applications use application programming interfaces (APIs) or other connectors to share data, a vulnerability in one public cloud application puts the interconnected applications at risk as well. A hacker need only breach one of the cloud-based applications to attack applications throughout the enterprise IT infrastructure. Thus, sharing corporate data in the public cloud dramatically expands the organization's attack surface.



CLOUD SECURITY CHALLENGES START WITH ARCHITECTURE

The Cloud Security Alliance identifies the top 12 threats to cloud security as:

- Data breaches
- Insufficient identity, credential, and access management
- Insecure interfaces and APIs
- System vulnerabilities
- Account hijacking
- Malicious insiders
- Advanced persistent threats
- Data loss
- Insufficient due diligence
- Abuse and nefarious use of cloud services
- Denial of service (DoS)
- Shared technology vulnerabilities²⁶

These are the threats that keep security architects up at night. Integration among different public clouds is difficult. The ever-expanding corporate attack surface reduces visibility into threats and vulnerabilities for both the IT team and its internal customers. And lack of integration leads to an unnecessarily large number of manual workflows, which presents resource challenges for security teams facing tight budgets and staffing.

In addition, sharing of threat intelligence among solutions cannot be automated, so proactive risk management may be nearly impossible. To overcome these challenges, the security architect needs a cloud-centric mindset and the help of cloud security technologies that integrate tightly and automate as many processes as possible.

- ¹ Alex Lesser, "[The Cloud Vs. In-house Infrastructure: Deciding Which Is Best For Your Organization](#)," Forbes, July 25, 2017.
- ² Arul Elumalai, James Kaplan, Mike Newborn, and Roger Roberts, "[Making a secure transition to the public cloud](#)," McKinsey & Company, January 2018.
- ³ "[Worldwide Public Cloud Services Spending Forecast to Reach \\$160 Billion This Year, According to IDC](#)," IDC, January 18, 2018.
- ⁴ Ibid.
- ⁵ Sally Johnson, "[Cloud providers can enable 'self-service' IT with a cloud portal](#)," TechTarget, accessed Sept 13, 2018.
- ⁶ Paul Korzeniowski, "[Following both sides of the decentralized vs. centralized IT debate](#)," TechTarget, accessed Sept 13, 2018.
- ⁷ Peter Bendor-Samuel, "[How to eliminate enterprise shadow IT](#)," CIO, April 11, 2017.
- ⁸ "[OWASP Top Ten Cheat Sheet](#)," OWASP, accessed September 14, 2018.
- ⁹ Malena Carollo, "[National Credit Federation exposed 40,000 customers' finance data](#)," Tampa Bay Times, December 6, 2017.
- ¹⁰ Girish Sharma, "[Why More than 50% of Cloud Deployments Today are Hybrid](#)," Netmagic Solutions blog, September 6, 2017.
- ¹¹ Steve Morgan, "[Cybersecurity Jobs Reports 2018-2021](#)," Cybersecurity Ventures, May 31, 2017.
- ¹² Jon Oltsik, "[Research suggests cybersecurity skills shortage is getting worse](#)," CSO, January 11, 2018.
- ¹³ Michael Kassner, "[How to manage cloud security when providers and customers share responsibility](#)," TechRepublic, August 19, 2018.
- ¹⁴ Robert Bond, "[25% of Public Cloud Users Experienced Data Theft](#)," SecureOps, June 15, 2018.
- ¹⁵ Torsten George, "[Compromised Credentials: The Primary Point of Attack for Data Breaches](#)," SecurityWeek, January 24, 2018.
- ¹⁶ David Egts, "[Public cloud security doesn't end with the cloud provider](#)," GCN, February 20, 2018.
- ¹⁷ Ibid.
- ¹⁸ Ibid.
- ¹⁹ Alex Lesser, "[The Cloud Vs. In-house Infrastructure: Deciding Which Is Best For Your Organization](#)," Forbes, July 25, 2017.
- ²⁰ Robert Bond, "[25% of Public Cloud Users Experienced Data Theft](#)," SecureOps, June 15, 2018.
- ²¹ Adam Marre, "[Shadow IT: Every Company's 3 Hidden Security Risks](#)," Dark Reading, August 7, 2018.
- ²² Robert Bond, "[25% of Public Cloud Users Experienced Data Theft](#)," SecureOps, June 15, 2018.
- ²³ Adam Marre, "[Shadow IT: Every Company's 3 Hidden Security Risks](#)," Dark Reading, August 7, 2018.
- ²⁴ Debasish Pramanik, "[What is Shadow IT? Necessity & Its Impact on Enterprise Security](#)," CloudCodes, October 25, 2017.
- ²⁵ Ibid.
- ²⁶ Bob Violino, "[The dirty dozen: 12 top cloud security threats for 2018](#)," CSO, January 5, 2018.



GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
8 Temasek Boulevard #12-01
Suntec Tower Three
Singapore 038988
Tel: +65-6395-7899
Fax: +65-6295-0015

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990