Securing the cloud — the next chapter

How today's cloud-based solutions are unlocking business benefits — and threats

KPMG International

home.kpmg/securingthecloud

Foreword

The migration to cloud solutions continues unabated and the COVID-19 crisis has simply accelerated the race to innovate using an array of services that dramatically enhance productivity, capabilities and efficiencies. These outweigh the disadvantages of adopting such solutions but working in the cloud does not relieve your organization of data privacy and security concerns.

As technology and cloud solutions become more sophisticated, so do the efforts of hackers endlessly crafting creative new ways to access your sensitive data. With businesses turning to the cloud, now is the time to ensure these services are governed and monitored by corporate IT, risk and cyber security professionals who understand today's emerging threats and regulatory requirements.

Andreas Tomek
Global Cyber Security Cloud Lead
KPMG

Highlights

- The rapid adoption of cloud services during the pandemic has spotlighted the critical need for strategic vision during every cloud adoption.
- Today's new reality and threat landscape requires security teams to move beyond traditional approaches to effectively manage security and protect vital business assets.
- If your business is not enacting crucial steps that are designed to govern cloud security solutions, you could be opening the door to new attacks.

Contents

New solutions — increased benefits

Cloud has gone mainstream and, as the crucible of the new digital economy, innovative cloud services, platforms and infrastructure are delivering unprecedented scalability, flexibility and resilience for businesses of all sizes. For organizations pursuing workforce productivity gains, enhanced efficiency and new ways to meet rapidly evolving consumer expectations, cloud solutions are unlocking breakthrough capabilities.

Many organizations are still in the early stages of their migration to cloud Infrastructure as a Service (IaaS), grappling with issues that include stubborn legacy architecture, data privacy compliance and the role of cloud providers versus the organization. Others may be more advanced in their adoption of increasingly popular Platform as a Service (PaaS). Meanwhile, almost every organization today relies on some form of cloud Software as a Service (SaaS) for standard office productivity tools, online training, enterprise wide HR management platforms and more.

Increased threats

As businesses migrate to various cloud services, security professionals have anxiously witnessed the increasingly sophisticated efforts of cyber criminals to exploit cloud technology that inherently broadens enterprise security challenges. Do you have a shadow IT issue? Well, your shadow cloud problem may be more extensive. Has your IT development team missed a few security controls on a product that's due to go live in a week? Well, in that week your cloud DevOps team is planning dozens of product releases, and all of them need to be right. Challenges of this nature often arise from a false sense of security.

Major cloud service providers offer a formidable suite of security controls and cyber defenses that normally outperform typical network and application controls. But unless those controls are configured correctly and tuned to an organization's threat landscape and security processes, they will not be effective. And unless security governance adapts to the culture and mindset shift that comes with cloud adoption and agile DevOps, the security team risks rapidly losing control of its estate. Adopting a false sense of security in the cloud can be costly.

What key steps can you take to avoid these risks? And what hard won lessons and insights have KPMG professionals gained from working with clients on their journey to the cloud?

Beware of threats lurking in the shadows

'Shadow cloud' solutions have proliferated, in our experience, and their defining characteristics are often ill-configured security controls and a lack of integration with the security and monitoring processes that the legitimate IT function would employ. These solutions will usually result in an increased risk of exposure for corporate data, personally identifiable information and intellectual property.

Shadow cloud solutions raised security concerns before the pandemic but the forced and disruptive shift in working patterns and rapid infrastructure changes during the pandemic have dramatically accelerated their presence. In organizations whose security and technology teams were slow to adopt collaboration tooling to support remote working, their business teams and individual employees have turned to cloud-based solutions for collaboration, storage and continued productivity.

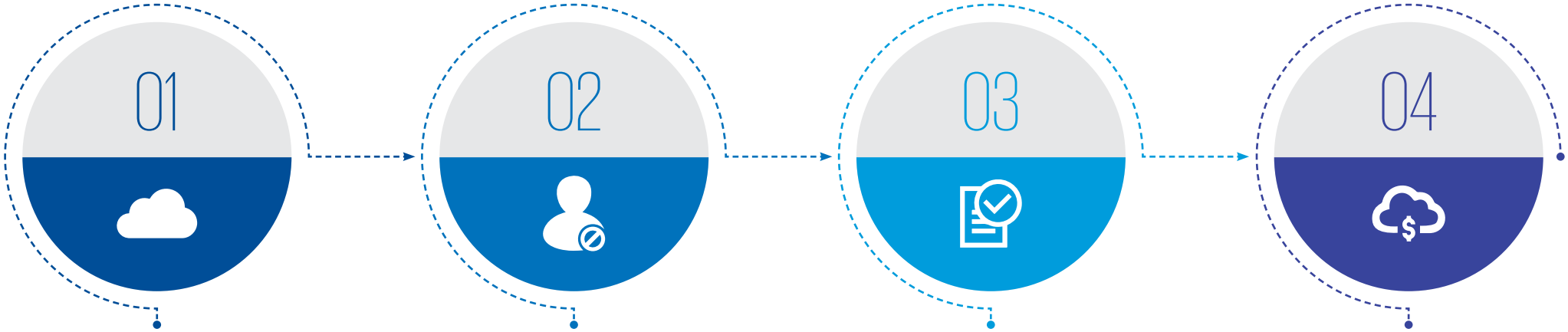
These applications may not be protected by multi-factor authentication or strict password policies and may not meet data localization and retention requirements. Now is the time to ensure these services are governed and monitored by corporate IT and risk professionals who understand the risks they pose and the regulatory requirements they must meet.

When organizations enact efficient oversight and governance of cloud technology, staff and stakeholders will be discouraged from deploying shadow cloud solutions. Eliminating the mindset that propagates shadow cloud usage can be as effective a security control as any.

"92 percent of organizations are concerned that individuals, departments and business lines are in violation of security policies for cloud applications."

— 2019 KPMG & Oracle Cloud Threat Report

Four tips for keeping shadow clouds at bay



Address shadow cloud issues in policies and employee standards. It's not enough to simply ban the use of cloud solutions lacking the permission of the security team. Make business leaders accountable for the control of shadow cloud solutions and implement clear protocols and disciplinary measures as needed.

Consider blocking access to unauthorized cloud-based applications. If cloud-based file sharing is authorized, settle on one platform and govern its use. Implement permission lists including sites or platforms that are approved for access, and block all others lacking approval.

Offer stakeholders a path for approval. It's essential to understand why users may want to 'go rogue.' If employees have difficulty managing their work, collaborating or providing client services via old architecture, a rapid cloud deployment can be a smart solution. But beware! Failure to handle these requests quickly and effectively can lure users into the shadows.

Some cloud services are free or carry minimal costs to employees. But some projects can cost thousands per year. Discourage the use of shadow cloud services by carefully managing expense reports and invoices payable to such services. While this may not limit the use of free cloud applications, shadow cloud deployments that house large or enterprise wide projects will need to seek legitimacy and funding.

Cloud-based email — opening the front door to attacks

Cloud-based email, most notably Microsoft Office 365, has changed the way organizations implement email services, offering much needed flexibility to businesses enduring today's disruptive pandemic. Cloud-based email is available for employees from outside the corporate network, requires no patching and is readily scalable. But the convenience of email everywhere comes at a price: access is also convenient to today's crafty hackers — anywhere, anytime.

The fact that attackers need only credentials to compromise email accounts has given rise to large-scale business email compromise (BEC) attacks. After compromising a single business email account through credential harvesting websites, credential stuffing or password spray attacks, attackers can exploit the trust and familiarity of colleagues and supply chain partners to harvest additional credentials or request fraudulent transactions. Beware. Attackers have become extremely creative, utilizing mailbox rules and scripted searches to streamline their quest for new targets and exploitation opportunities.

Case study

Hackers cash in on email access

A hacker's target organization employed services from a vendor company. A vendor employee entered their email password into a credential harvesting website via a phishing email, allowing the hacker to compromise the email account and email the accounts payable team of the target organization, stating the vendor's banking information had changed. Since the email was sent from the vendor's domain and the email address was familiar, the target organization did not question the 'account change.' As a result, the target organization sent money to a bank account controlled by the perpetrators. The funds were never recovered.

Key steps to help foil attackers

The most common cloud-based email services come with a suite of authentication and monitoring capabilities as add-ons, which can help security teams to be equally creative in foiling attackers. Monitoring rules can effectively detect malicious activity. However, they should be carefully maintained to limit false positives.

Enable multi-factor authentication (MFA). MFA forces the attacker to compromise the second form of authentication. Be aware that some sophisticated attacks are requesting the current token code to log into a fake website that is immediately used to log into the actual Office365 account.

Enforce conditional, IP-based MFA for access to cloud-based email services. We see clients implementing IP-based restrictions suffering far fewer email related compromises. A secondary option is to only allow email access from within the corporate network, while this removes the benefit of a globally accessible email, it still reduces risk.

Set up, monitor and respond to suspicious activity alerts. These can include alerts for impossible travel (a user logging in from two geographic areas within an impossible timeframe); new inbox rules created on a user's account; and excessive failed log ins indicating a potential brute force attempt.

Test your incident playbooks

When organizations 'lift and shift' their applications into the cloud, security teams are often reassured by the range of security monitoring tools offered as standard. They should be, but incident response procedures may need to be adapted to be effective in the cloud.

Speed matters. Incident response procedures look and feel different in the cloud and security teams need to know they work.

Case study | The need for speed

A hacker accessed a cloud-based customer records application by compromising an administrative password. Using an automated script, they extracted large volumes of customer data. The security monitoring tools offered by the cloud provider detected a spike in traffic and highlighted it to the security operations team for review. But because the data was extracted so quickly via the cloud link, the Security Operations Centre (SOC) analyst could not respond before the extraction was complete.

Guidelines to enhance security

Stress test: Stress test your incident playbooks to prove they work for cloud hosted applications. Work with red teaming providers to simulate various types of breaches requiring your security team's response and determine how to intercept attacks and isolate them early.

Automate: If the ability to respond quickly to cloud native application incidents is unclear, automate the early stages of response playbooks with Security Orchestration, Automation and Response (SOAR) tooling, and tune your detective tooling to the early indicators of compromised systems.

Outside the security team: The most useful indicators of compromise can come from outside the security team. Work with your service management, customer facing sales staff, fraud and HR teams to understand what attacks look like at the earliest stages — and how threat actors think. The more time you can buy for your first line of defense to react, the better.

Focusing on the 'now'

The remarkable acceleration of cloud services adoption during the pandemic isn't a temporary trend and our recommendations represent the most practical steps to effectively govern cloud security solutions. In today's reality, holding the threat landscape at bay requires security teams to move well beyond manual asset management and configuration, access reviews and incident playbooks.

Efforts to prevent and detect the pace and volume of cloud-based and cloud targeted cyber attacks must be continuous and seamless, leveraging fraud data analytics to identify and monitor assets, detect suspicious activities and track unfolding kill chains. And when events do escalate into incidents, it will not be SOC analysts receiving alerts from security incident and event management (SIEM) tools. Instead, it will be automated and orchestrated incident containment and eradication protocols, working silently behind the scenes to combat attacks.

How KPMG can help

At KPMG, our global organization of cyber security professionals offers a multidisciplinary view of risk. Helping you carry security throughout your organization, so you can anticipate tomorrow, move faster, and get an edge with secure and trusted technology.

No matter where you are on your cyber security journey, KPMG firms have expertise across the continuum — from the boardroom to the data center. In addition to assessing your cyber security and aligning it to your business priorities, we help you develop advanced solutions, implement them, monitor ongoing risks and help you respond effectively to cyber incidents.

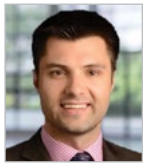
KPMG brings an uncommon combination of deep technical expertise, strong business insights and creative professionals who can help you to envision, build and configure next generation cloud security controls and processes — and position you to govern your cloud estate with confidence. Together, let's create a trusted digital world, so we can push the limits of what's possible.

Authors

David Ferbrache
Global Head of Cyber Futures
KPMG

Anthony Gawron
Principal, Cyber Security Services
KPMG in the US

J Jewitt
Director, Cyber Security Services
KPMG in the US



Konrads Klints
Director, Cyber Security Services
KPMG in Singapore

Ravi Jayanti
Associate, Cyber Security Services
KPMG in the UK

Contacts

Andreas Tomek
Global Cyber Security Cloud Lead
KPMG in Austria
E: atomek@kpmg.at

Andy Yuen
KPMG in China
E: andy.yuen@kpmg.com

Luca Lora Lamia
KPMG in Italy
E: lloralamia@kpmg.it

Koos Wolters
KPMG in the Netherlands
E: wolters.koos@kpmg.nl

Michele Daryanani
KPMG in Switzerland
E: micheledaryanani@kpmg.com

Nicolas Manavella
KPMG in Argentina
E: nmanavella@kpmg.com.ar

Guy Posbic
KPMG in France
E: gposbic@kpmg.fr

Motoki Sawada
KPMG in Japan
E: motoki.sawada@jp.kpmg.com

Michal Kurek
KPMG in Poland
E: michalkurek@kpmg.pl

Sheikh Shadab Nawaz
KPMG in the UAE
E: snawaz1@kpmg.com

Kathy Robins
KPMG in Australia
E: krobins@kpmg.com.au

Markus Limbach
KPMG in Germany
E: mlimbach@kpmg.com

Jee-Hyung Kim
KPMG in Korea
E: jeehyungkim@kr.kpmg.com

Ton Diemont
KPMG in Saudi Arabia
E: antondiemont@kpmg.com

Dimitrios Petropoulos
KPMG in the UK
E: dimitrios.petropoulos@kpmg.co.uk

Diego Freitas
KPMG in Brazil
E: diegofreitas@kpmg.com.br

Pranav Kathale
KPMG in India
E: pranavkathale@kpmg.com

Ubaid Mustafa Qadiri
KPMG in Malaysia
E: ubaidqadiri@kpmg.com.my

Ser Yen Lee
KPMG in Singapore
E: seryenlee@kpmg.com.sg

Steve Barlock
KPMG in the US
E: sbarlock@kpmg.com

Hartaj Nijjar
KPMG in Canada
E: hnijjar@kpmg.ca

Dani Michaux
KPMG in Ireland
E: dani.michaux@kpmg.ie

Eduardo Maldonado
KPMG in Mexico
E: eduardomaldonado@kpmg.com.mx

Daniel De Diego Lopez
KPMG in Spain
E: ddediego@kpmg.es

Juan Manzano
KPMG in Venezuela
E: jmanzano@kpmg.com

home.kpmg/socialmedia

Designed by Evalueserve.
Publication name: Battling economic crime — and winning together
Publication number: 137292-G
Publication date: December 2020