Securing the cloud – the next chapter in public services

How governments can secure their journey to the cloud

KPMG International

home.kpmg/cybersecurity

Foreword

As businesses everywhere accelerate their pursuit of game-changing digital capabilities amid the global pandemic's sudden and unexpected disruption, governments are also stepping up their efforts to transform public sector infrastructure in ways that can provide new citizen-centric services and operational efficiencies.

Cloud-enabled technology is playing a crucial role in governments' efforts to achieve this. Cloud adoption can present vast opportunities to help deliver reliable new public-facing services while considerably enhancing data use and decision making, cost efficiency, workforce productivity, scalability and more. But working in the cloud isn't likely to relieve government organizations of data privacy and security concerns and needs.

As technology and cloud solutions become more sophisticated, so can the efforts of hackers endlessly crafting creative new ways to access sensitive data. Now is the time to help ensure that the cloud's leading services are appropriately governed and monitored by IT, risk and cyber security professionals who seek to understand today's emerging threats and regulatory requirements.

Wilhelm Dolle
Global Cyber Security IGH Lead and Partner
KPMG in Germany

Highlights

- Government organizations can face unique challenges and roadblocks to securing their cloud environments.
- Rapid adoption of cloud services during the pandemic has spotlighted a critical need for strategic vision during cloud adoption.
- Today's reality and threat landscape can require security teams to move beyond traditional approaches to manage security and protect vital assets that can include citizen data and confidential government records.
- If your organization is not enacting crucial steps that can be required to govern cloud security solutions, you could potentially be opening the door to new attacks.

Contents

Cloud security in government 04

Leading solutions for the public sector 06

Nurturing a culture that's fit for the cloud 07

Cloud-based email — don't open the front door to attacks 09

Be aware of threats lurking in the shadows 11

Test your incident playbooks 13

Potential opportunities for public services 14

How KPMG can help 15

Cloud security in government

Governments around the world have long been familiar with the advantages that cloud services can unlock for their public-facing services and internal IT infrastructure. Take the UK, for example, which established the G-Cloud initiative in 2012 to enable government organizations to more easily procure cloud-based technology. Other governments have followed suit and become quite sophisticated in cloud technology. Yet, many have been slow to progress along their transformation efforts. While some have moved boldly forward, it seems clear that public sector services and capabilities continue to lag behind the private sector.

Governments can certainly face their own set of challenges surrounding the critical need to enhance security, privacy, data protection and public trust as new technologies like the cloud come onstream. But the need to adopt and capitalize on cloud technology's capabilities is significant. If not implemented carefully and strategically, however, the journey to the cloud can potentially unleash dangerous new threats.

KPMG professionals are helping clients in the public sector navigate the path to progress amid today's regulatory, security, trust and compliance challenges. Governments shouldn't waste any time in their pursuit of new digital capabilities that can provide new public services, resources and efficiencies.

Roadblock to progress

Third-party providers

Government organizations should be able to trust third-party technology providers. They typically hold the key to confidential data and records that, if compromised in the case of governments, could undermine public trust or pose a threat to national security. A 'trust gap' has in many cases prevented governments from migrating critical data to the cloud.

Roles and responsibilities

Successful cloud transformation requires a clear understanding of shared responsibilities, including data security between organizations and their cloud providers. We have seen cloud transformation initiatives fail amid a lack of clarity regarding responsibilities and roles, as well as a lack of new skills needed in-house to manage cloud's capabilities.

Digital sovereignty and data residency

Many nation-states desire digital sovereignty and their reluctance to place infrastructure and data in the hands of outsourced cloud services have only been reinforced to some degree by the pandemic's impact on economic stability and geopolitical tensions. We are seeing cloud providers launch dedicated data centers in more countries to tackle this challenge. Also in play are initiatives such as GAIA-X, an EU proposal to create the next generation of data infrastructure for Europe: a secure, federated system that meets the highest standards of digital sovereignty while promoting innovation. More than 300 organizations are currently involved, and the initiative remains a work in progress.

Regulation

From a regulatory perspective, the EU's General Data Protection Regulation (GDPR) sets high data privacy standards for cloud providers. Others, such as Brazil and India, are following suit with the introduction of their own laws. Standards implemented by governments differ by country — creating new challenges for cloud providers.

Leading solutions for the public sector

Cloud has gone mainstream and, as one of the crucibles of the new digital economy, innovative cloud services, platforms and infrastructure are helping to deliver high levels of scalability, flexibility and resilience. Cloud solutions are helping to unlock leading capabilities for government bodies pursuing workforce productivity gains, enhanced efficiency, and new ways to meet rapidly evolving consumer expectations.

Many organizations, governments included, 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.

Keeping sensitive government data secure

As governments migrate to various cloud services, security professionals have anxiously witnessed the increasingly sophisticated efforts of cyber criminals to exploit cloud technology that inherently broadens and complicates enterprise security challenges. Governments have been understandably cautious, if not reluctant, to simply shift all their data to the cloud — as some of their data is highly sensitive and protects national interests. Governments should first understand exactly what data they hold, and what data is appropriate for the cloud. Some data may be too sensitive and should never leave on-premise data centers. But, aside from this — key questions remain.

Do you have a shadow IT issue? If so, your shadow cloud problem may likely be more extensive. Has your IT development team missed a few security controls on a product/service that's due to go live in a week? Your cloud DevOps team may likely be planning to launch dozens of new products/services to the public at the same time, and each needs to be managed appropriately. Challenges of this nature can often arise from a false sense of security regarding your cloud services.

Major cloud service providers offer a robust suite of security controls and cyber defenses that are designed to 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 may 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 can risk 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? Let's start with some guiding principles followed by some lessons and insights KPMG professionals have gained by working with clients on their journey to the cloud.

Nurturing a culture that's fit for the cloud

Historically, IT has been responsible for infrastructure provisioning, and, before the cloud, was primarily focused on the challenges on the ground. The security team is charged with scanning that infrastructure for vulnerabilities, but they often don't know what to scan due to a disconnect with IT on an updated threat list. Managing infrastructure and related assets has always been demanding, but in the cloud, where everything is faster and more ephemeral, getting security involved early and hardcoded into the provisioning plan is a challenge and struggle for many governments.

In terms of the cloud, government security teams are largely not prepared to enable the business, neither in terms of skills nor talent. In the cloud, the priority is information protection. More and more, we're finding that the way data is being deployed in the cloud is often not necessarily resilient. We're not simply talking about multiple availability zones, but the ability to recover critical assets if there's a major breach.

We also see two camps that seemingly operate at opposite ends of the security spectrum. On one side are the old-school practitioners who have been working in security architecture for 20 years or more but haven't fully adapted to life in the cloud. On the other side, you've got cutting-edge security professionals who fully embrace today's technology and are trying to promote and enable the cloud mindset so security can be embedded by design and at scale. As governments continue their migration to the cloud, getting these factions on the same page is a priority.

Guiding principles to help create a safe and secure life in the clouds

Become a learning organization

One of the things that attracts cloud talent, beyond money, is culture. Prospective employees should know they're not joining a classic, hyper-risk-averse, slow-moving organization. Creating a culture that's open to innovation and experimentation can help attract new talent.

Know your environment

Build an understanding of what data you hold, what can be appropriately stored off-premise versus on-premise, and then implement controls to help ensure this data is classified and stored correctly. More than most organizations, governments can hold the key to highly sensitive data. If this data gets into the wrong hands, it could harm national security.

Think small — act fast

Send the message that you can build things fast, break things faster, and then rebuild based on what you've learned. Most organizations have already proved that they can move fast in reacting to the pandemic, so now is the time to translate any lessons learned into business as usual. Security can enable success through incremental steps. For example, go live with a new container protection strategy in small bites, and enable the business to move fast.

Shift security to the left into the early stages of your software testing cycle

Doing so can help to enhance value to both customers and users. Apply security — again, in small bites — as far left in the process as possible, which can typically involve infrastructure as code. You can help make it happen by empowering developers to hard code the required security measures without the security team's involvement, which the cloud can facilitate.

Have an appreciation of the underlying code

The ability to read and write code can earn the respect of DevOps engineers. Increasingly, we will likely need security professionals with an ability to code, as we continue to move away from that traditional security architecture role of measuring diagrams and handing it over to a solution designer or solution, which then goes to an engineer to stand up physical infrastructure.

Work to understand — and communicate to the entire enterprise

Help the enterprise understand the connection between business enablement, business resilience, and information protection. It's not much of a departure from how you would do it on premises, but it can be a little bit different when you've got critical data in the cloud. Making this part of your DNA can help you weed out the "noise" from an operations perspective so you can focus on bigger security priorities.

We also see several common security challenges faced by our clients along their journey to the cloud. Some of these are not necessarily new but have been exacerbated by the sprint to digitize and adapt to the new reality. We'll explore three of these recurring challenges now.

Cloud-based email — don't open the front door to attacks

Cloud-based email, most notably Microsoft Office 365, has helped change the way organizations implement email services, offering some much-needed flexibility amid today's disruption. Cloud-based employee email is readily available requires no patching and is easily scalable. But the convenience of email everywhere comes at a price: access is also convenient to today's crafty hackers.

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 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. We recommend being vigilant, as 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 in to a fake website that is immediately used to log in to the actual Microsoft Office 365 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 organization's network. While this removes the benefit of a globally accessible email, it can help reduce 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.

Be aware of threats lurking in the shadows

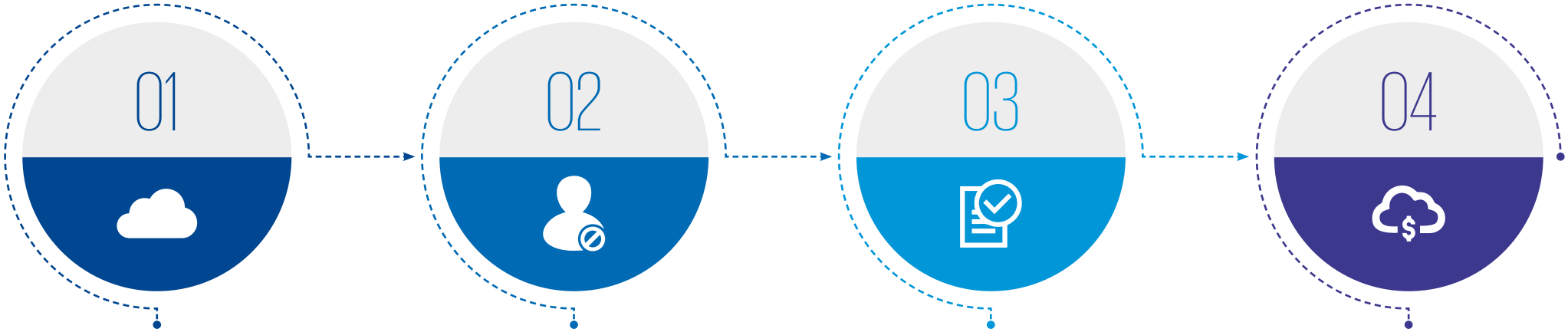
We have seen an increase in 'shadow cloud' solutions, and their defining characteristics are often ill-configured security controls and a lack of integration with the security and monitoring processes that the legitimate IT function would employ. These solutions will usually result in an increased risk of exposure for 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 accelerated their presence. In organizations whose security and technology teams were slow to adopt collaboration tooling to support remote working, 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. These can present both security and regulatory risks. For example, employees based in Europe may be unaware that the application they are using is transferring un-encrypted personally identifiable information (PII) to non-European data centers, which can result in non-compliance with the General Data Protection Regulation (GDPR). Moreover, many government organizations have strict internal policies to ensure their data remains in-country. We believe now is the time to ensure these services are governed and monitored by IT and risk professionals who can understand the threats they pose and the regulatory requirements they must meet.

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

Four tips to help keep shadow clouds at bay



Address shadow cloud issues in policies and employee standards. It's likely not enough to simply ban the use of cloud solutions lacking the permission of the security team. We recommend making 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, we recommend settling on one platform and governing its use. We also recommend implementing permission lists, including sites or platforms that are approved for access, and blocking all others lacking approval.

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

Some cloud services are free or carry minimal costs to employees. But some projects can cost thousands per year. We recommend discouraging 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 likely need to seek legitimacy and funding. Keep a close eye on whether licenses purchased are personal. Monitoring the purchase of licenses can help organizations avoid any fines or compliance issues associated with using the wrong type of license.

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 can matter. Incident response procedures can look and feel different in the cloud and security teams should 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: We recommend stress testing your incident playbooks to prove they work for cloud-hosted applications. You can work with red teaming providers to simulate various types of breaches requiring your security team's response and help determine how to intercept attacks and isolate them early.

Automate: If the ability to respond quickly to cloud native application incidents is unclear, you can 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: Some of the most useful indicators of compromise can come from outside the security team. You can work with your service-management, 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.

Potential opportunities for public services

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

Efforts to prevent and detect cloud-based cyber attacks should be continuous and seamless, leveraging fraud data analytics to identify and monitor assets, detect suspicious activities and track unfolding kill chains. A shared responsibility model should be understood and agreed between government bodies and cloud providers. And if your organization lacks the skills to achieve this, staff should be trained accordingly. When events escalate into incidents, it will likely not be SOC analysts receiving alerts from security incident and event management (SIEM) tools. Instead, it will likely be automated and orchestrated incident containment and eradication protocols, working silently behind the scenes to combat attacks.

How KPMG can help

KPMG cyber security professionals from around the world offer 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 professionals have expertise across the continuum — from the boardroom to the data center. In addition to assessing your cyber security and aligning it to your organization's priorities, we can help you develop advanced solutions, implement them, monitor ongoing risks and help you respond effectively to cyber incidents.

KPMG professionals also have a strong knowledge of how governments work because many have held senior public sector roles and consistently combine our practical, hands-on local experience with insights from our global practice. Through our deep knowledge of the government sector, we can gain insight into current trends as well as future challenges — be they disruptions, opportunities, or innovations.

KPMG brings an uncommon combination of deep technical expertise, strong government insights and creative professionals who can help you to envision, build and configure next generation cloud security controls and processes — and help position your organization to govern your cloud estate with confidence.

Together, let's create a trusted digital world, so you can push the limits of what's possible.

Authors

Wilhelm Dolle
Global Cyber Security IGH Lead
KPMG in Germany

Konrads Klints
Director, Cyber Security Services
KPMG in Singapore

J Jewitt
Director, Cyber Security Services
KPMG in the US

Anthony Gawron
Director, Cyber Security Services
KPMG in the US

David Ferbrache
Global Head of Cyber Futures
KPMG

Ravi Jayanti
Associate, Cyber Security Services
KPMG in the UK

Contacts

Liz Forsyth
Global Head of Government
KPMG Australia
E: lforsyth@kpmg.com.au

Tony Hubbard
Principal, Cyber Security Services
KPMG in the US
E: thubbard@kpmg.com

David Hsiu
Director, Cyber Security Services
KPMG in Taiwan
E: dhsiu@kpmg.com.tw

Ton Diemont
Director, Cyber Security Services
KPMG in the Middle East
E: antondiemont@kpmg.com

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

Richard Krishnan
Director, Cyber Security Services
KPMG in the UK
E: richard.krishnan@kpmg.co.uk

Imraan Bashir
Partner, Cyber Security Services
KPMG in Canada
E: ibashir@kpmg.ca

Rahul Gupta
Director, Cyber Security Services
KPMG in India
E: rahulgupta@kpmg.com

Wilhelm Dolle
Global Cyber Security IGH Lead
KPMG in Germany
E: wdolle@kpmg.com

Ian Gray
Partner, Cyber Security Services
KPMG Australia
E: igray@kpmg.com.au

Paul Sammut
Senior Manager, Cyber Security Services
KPMG in Canada
E: paulsammut@kpmg.ca

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

home.kpmg/socialmedia

Designed by Evalueserve.
Publication name: Securing the cloud — the next chapter in public services
Publication number: 137430-G
Publication date: June 2021