cpl.thalesgroup.com

THALES
Building a future we can all trust

Owning your own Access Security

The key to building strong cloud security and avoiding the risk of vendor lock-in

White Paper

Contents

Executive Summary

The latest cybersecurity incidents affecting government agencies and organizations as well as large enterprises around the world, who have invested heavily in digital and cloud initiatives, have demonstrated the urgent need for a different approach to security. Based on cloud security's shared responsibility model, businesses should segregate their security duties from those of cloud service providers, bring their own security tools to avoid cyber threats and from criminals moving laterally into their corporate networks.

Security duties segregation can also help organizations in meeting and sustaining compliance with an evolving regulatory and jurisdictional landscape, as the "Schrems II" rule proved. The purpose of this white paper is to showcase the tangible benefits of selecting a vendor-neutral cloud security solution to address the evolving security risks and privacy requirements.

What a Shared Security Model is

In a traditional, on-premises data center model, you are responsible for security across your entire operating and computing environment, including your applications, physical servers, user controls, and even physical security.

When you migrate your services, applications, workloads, and data to the cloud, you need to be aware that cloud service providers adhere to a shared security responsibility model, which means that your security team maintains some responsibilities for security, while the provider takes some responsibility, but not all. The key to a successful cloud security implementation is understanding where your provider's responsibility ends, and where yours begins.

- In the AWS Shared Security model[1], AWS claims responsibility for "protecting the hardware, software, networking, and facilities that run AWS Cloud services."
- Microsoft Azure[2] claims security ownership of "physical hosts, networks, and data centers."
- Both AWS and Azure state that your retained security responsibilities depend upon which services you select.

1 Amazon Web Services, Shared Responsibility Model, https://aws.amazon.com/compliance/shared-responsibility-model/

2 Microsoft Azure, Shared responsibility in the cloud, https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

The following diagram provides a high-level, vendor-agnostic, conceptual view of a shared responsibility model:

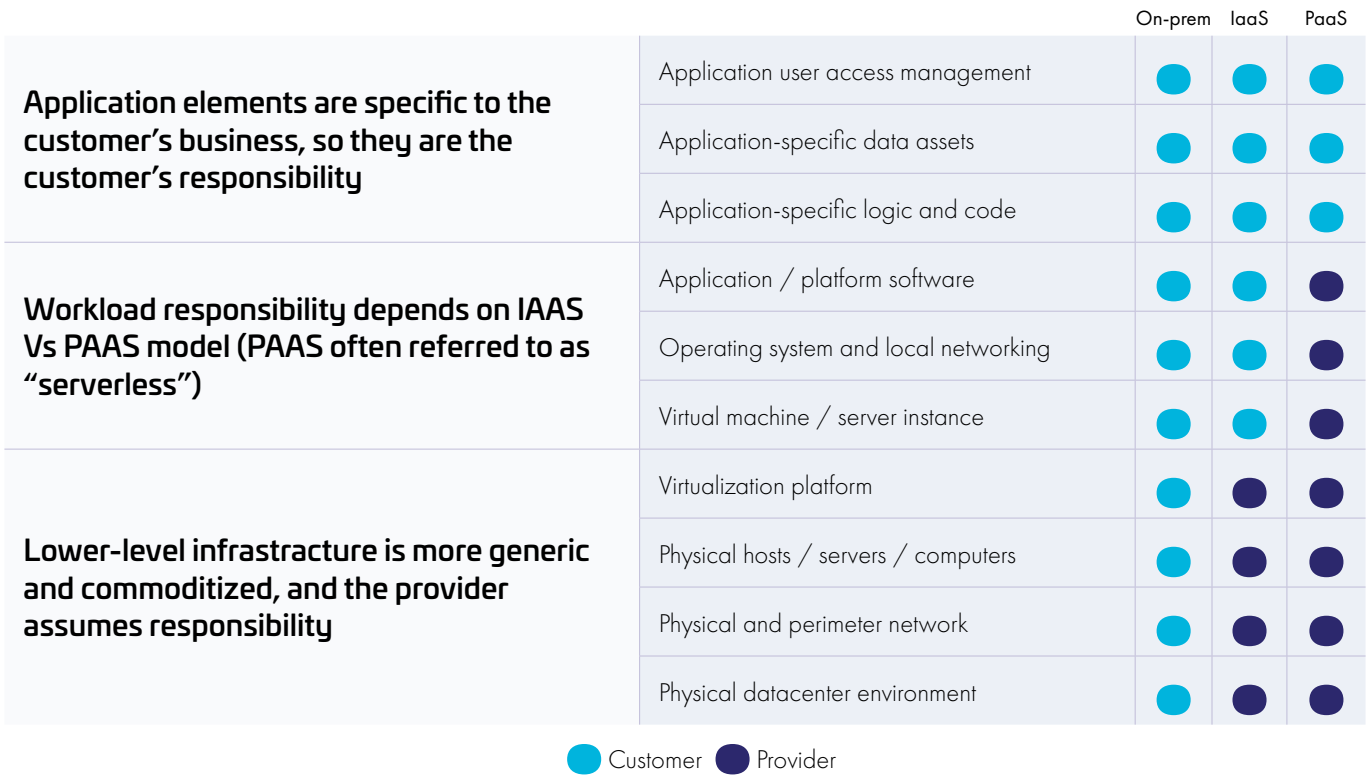

Figure 1: A vendor-agnostic view of responsibilities in the shared responsibility model. Source: Cloud Security Alliance[1].

No matter what your computing environment, whether on-premises, public cloud, private cloud, or just hybrid, you are always responsible for securing what's under your direct control, including:

- **Data**: By retaining control over your data, you control how and when your data is used. The cloud provider has zero visibility into your data, and you maintain all access to your data.
- **Applications**: Your proprietary applications are yours to secure and control throughout the entire application lifecycle – from development to testing and deployment.
- **Identity and Access**: You are responsible for all facets of your identity and access management (IAM) program, including authentication and authorization mechanisms, single sign-on (SSO), multi-factor authentication (MFA), access keys, and credentials.
- **Platform Configuration**: When you deploy cloud computing environments, you control the configuration of the underlying operating environment. Platform configuration varies based on whether your instances are server based or serverless.

1 Cloud Security Alliance, Shared Responsibility Model Explained, https://cloudsecurityalliance.org/blog/2020/08/26/shared-responsibility-model-explained/

Risks and limitations of having everything with a single service provider

Cloud service providers have launched their own security tools to help businesses protect their cloud-based instances and assets. Opting for a vendor-native cloud security solution means trusting the security of your data, applications, encryption keys and credentials to the cloud service provider. Although this seems enticing, can you place such a level of trust to a single provider?

Security and privacy regulations and laws contribute to building trust in your cloud computing environment. However, it is easier to trust if you can trust less[1]. Although you can certainly trust the technologies behind cloud computing, you should decrease the amount of trust you place into the security solutions offered by the cloud service providers.

This is of huge importance, because risks, vulnerabilities, and threats to the service provider are traversing the customers, allowing adversaries to move laterally across corporate networks. Here are three threat vectors you need to consider before selecting a cloud security solution.

1. Human error

Human error and negligence account for a large percentage of cloud security incidents. In fact, according to the 2020 Cloud Security Report[2], misconfiguration of the cloud platform (68%) is ranked as the biggest security threat to cloud deployments. Configuration errors, as well as developers' mistakes, poor source of entropy and accidental loss of keys, create cloud security challenges such as unauthorized data disclosure, loss of data privacy, and accidental exposure of credentials.

2. External attacker

External attackers tend to find the above-mentioned human errors and turn these weaknesses into compromises as a result. Advanced threat actors have been known to attack key management systems (KMS) and weak authentication schemes to gain wider access to data. For example, during the recent SolarWinds supply chain compromise, attackers exploited "systemic weaknesses[3]" in the native authentication mechanism of a cloud service provider to move laterally within the networks of many cloud customers. It became apparent that the model of deploying a vendor native security solution not only did not prevent attackers from launching their attack, but it became the driver for escalating their malicious actions.

3. Insider threat

A rogue or disgruntled service provider employee, having access to keys and/or credentials, may leverage their privileges to access and disclose sensitive data or disrupt cloud-based functions of customers.

1 Anton Chuvakin, Il-Sung Lee, The cloud trust paradox: To trust cloud computing more, you need the ability to trust it less, https://cloud.google.com/blog/products/identity-security/trust-a-cloud-provider-that-enables-you-to-trust-them-less

2 Cybersecurity Insiders, 2020 Cloud Security Report, https://www.cybersecurity-insiders.com/portfolio/2019-cloud-security-report-isc2/

3 https://www.infosecurity-magazine.com/news/crowdstrike-slams-microsoft-over/

Regulatory motivations for a neutral cloud security solution

Besides the above threat considerations, you should pay attention to various developments surrounding data privacy regulations, and especially the concept of data portability and sovereignty. Regional requirements are playing a large role in how organizations migrate to the cloud and operate workloads in public cloud. Regulators in Europe, Japan, India, Brazil and other countries are considering or strengthening mandates for keeping unencrypted data and/or encryption keys within their boundaries.

In addition, the Court of Justice of the European Union issued its decision in "Schrems II" on 16 July 2020. This is a landmark decision that invalidates the EU-U.S. Privacy Shield arrangement. Until July 16, Privacy Shield had served as an approved "adequacy" mechanism to protect cross-border transfers of personal data from the European Union to the United States under the EU General Data Protection Regulation. More than 5,000 organizations participate in Privacy Shield. Many thousands more EU companies rely on Privacy Shield when transferring data to these organizations. With the "Schrems II" rule, the conditions for the lawful transfer of this data have been removed[1].

Considering the major cloud service providers – namely Amazon, Microsoft and Google – are not based in the European Economic Area (EEA) region, raises certain concerns regarding the access of EU personal data. The European Data Protection Board (EDPB) has identified two Unlawful Use Cases:

- Unlawful Use Case 6: Transfer to cloud services providers or other processors which require access to data in the clear.
- Unlawful Use Case 7: Remote access to data for business purposes.

The existence of Unlawful Use Cases 6 and 7 mean that common cloud vendor practices leave corporate officers and boards of directors open to liability risks from the potential for unlawful data access[2].

To meet the new data sovereignty requirements, cloud service providers have modified their Standard Contractual Clauses (SCC)[3] to add guarantees that their services occur entirely within the EU. However, organizations can mitigate the risks for unlawful data access by deploying their own vendor-neutral security solution data pseudonymization and managing access credentials to satisfy the EDPB requirements for lawful transfer of EU pseudonymized data.

A final motivation for opting for a vendor neutral security solution is to address the scenario when cloud providers are obliged by law enforcement agencies to permit access to customer data. If you are the owner of your own security, the provider does not have access to any keys or credentials that would permit any requesting entity to gain access to your data.

The concept of Bringing-Your-Own-Security (BYOS) in the cloud is essential considering both the initiatives by certain countries to introduce "backdoors" into end-to-end encryption, protecting the privacy and confidentiality of personal data, and the terms and conditions for using cloud services and platforms.

For example, the AWS contractual clauses mention the following[4] :

"Disclosing the minimum amount necessary: We also commit that if, despite our challenges, we are ever compelled by a valid and binding legal request to disclose customer data, we will disclose only the minimum amount of customer data necessary to satisfy the request."

1 Brian Hengesbaugh, CIPP/US, What Privacy Shield organizations should do in the wake of 'Schrems II', https://iapp.org/news/a/what-privacy-shield-organizations-should-do-in-the-wake-of-schrems-ii/

2 Gary LaFever, Magali Feys, 'Schrems II': How to protect against liability when using non-EEA vendors, https://iapp.org/news/a/schrems-ii-how-to-protect-against-liability-when-using-non-eea-equivalency-country-vendors/

3 Amazon's Standard Contractual Clauses (SCC): https://aws.amazon.com/blogs/security/aws-and-eu-data-transfers-strengthened-commitments-to-protect-customer-data/, Google Cloud: https://services.google.com/fh/files/misc/gsuite_foredu_whitepaper_gdpr_schremsii.pdf, Microsoft Azure: https://blogs.microsoft.com/eupolicy/2020/07/16/assuring-customers-about-cross-border-data-flows/

4 Stephen Schmidt, AWS and EU data transfers: strengthened commitments to protect customer data, https://aws.amazon.com/blogs/security/aws-and-eu-data-transfers-strengthened-commitments-to-protect-customer-data/

4 Tangible benefits of shared security model

The shared cloud security model is a concept that helps businesses and organizations adopt industry best practices for separating the protection of their data in the cloud from the other services offered by the cloud provider. In fact, the greater the segmentation of duties, the better the security you can offer your data.

Segmentation of duties by adopting a vendor-neutral solution covers both the protection of encryption keys and the authentication and access mechanisms to access corporate data. There are some tangible benefits that stem from separating security in the cloud from the service provider.

Better to be independent from service providers for breach mitigation

During the Congressional hearings for the SolarWinds attack, many participants elaborated that the use of different methodologies or technologies, independent from the cloud service provider, can eliminate a considerable threat vector and introduce greater obstacles for adversaries. Considering that adversaries seek to exploit vulnerabilities to let them into networks and move laterally undetected, increasing the level of difficulty in doing so acts as a deterrent. Cloud service providers provide great infrastructure, services, resources and apps but wrapping BYOS around these is considered to be best security practice in this scary new world.

Tip 1

Use a specialist identity and access management (IAM) solution supporting a wide range of authentication techniques to create a barrier to your networks and data, should your cloud service provide get compromised.

Select the solution that allows you to maintain regulatory compliance now and tomorrow.

The patchwork of privacy and data protection requirements requires businesses to adopt solutions to provide the required flexibility to operate under various jurisdictions. Segregating duties and opting for authentication and key management solutions that meet the specific operating and compliance requirements of your organization is the best practice for mitigating unlawful process of personal data.

Tip 2

Select a neutral IAM solution and a Hardware Security Module (HSM) platform that meet your business needs and your regulatory framework. Pay special attention to data sovereignty and protection contractual clauses.

Control your own security.

Deploying your own, neutral solution allows you to maintain a centralized, flexible control of your access security, keys, and data. Reducing the reliance, and placing less trust on your cloud service provider, results in a reduced threat surface, and decreased potential of lateral damage because of attacks on the provider.

Tip 3

Opt-in for a security solution for authentication and key management that allows you to manage your corporate security centrally and flexibly.

Avoid the dangers of vendor lock in.

Opting for a native security solution entails the danger of vendor lock in. Vendor lock in presents risks from a commercial, regulatory and threat perspective, which may increase the overall risk environment. As businesses are looking to reduce their exposure to business risks and increase resilience, segregation of duties is the best practice for strengthening their security and privacy posture.

Tip 4

Segregate your security duties from your cloud service provider and opt-in for specialist IAM and HSM solutions to increase your overall business resilience.

The benefits of Thales agnostic security

Thales is a world leader in providing vendor agnostic security solutions to help you protect your assets and data wherever they are – on-premises or in the cloud. Thales SafeNet Trusted Access lets you keep control of your access security and averts the risks of vendor lock-in.

- **Maintain flexibility:** IT managers can maintain flexibility by using any user directory, while strengthening business continuity by ensuring interoperability throughout multi-cloud deployments.
- **Reduce your threat surface:** The CISO can reduce the attack surface and strengthen corporate security posture by separating access security from apps and data, limiting the scope of lateral attacks within corporate networks.
- **Future proof against emerging regulations:** Regulations are emerging and changing rapidly. By controlling your access security you will be able to future-proof against emerging regulations on data privacy and data sovereignty and reduce the risk of third parties accessing sensitive corporate data.
- **Ensure commercial leverage:** CFOs gains flexibility and can achieve a strong negotiating position when it comes to renewals and licenses by adopting a multi-vendor strategy.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

THALES

Building a future we can all trust

Contact us

For all office locations and contact information,
please visit cpl.thalesgroup.com/contact-us

> cpl.thalesgroup.com <