Cloud Security

Adopt best-practice standards and guidelines for Cloud Security

- Growth in Cloud computing can come at the expense of security
- Unmanaged sensitive data in SaaS platforms is an increasing risk
- Adopt best-practice standards and guidelines for Cloud Security

As a business, you must know precisely where your data is stored and ensure that you comply with all legislation that governs that data storage and transfer in the countries in which you operate. When it comes to Cloud data, you also need to make sure that your cloud provider offers tight security and has protocols to follow in case of a data breach, or in case you need to destroy any data. This is where your choice of cloud technology and cloud service provider can make a huge difference in the life of your business—and your data.

- The standard is a shared responsibility model meaning that cloud providers will provide security of the cloud and the client is responsible for security in the cloud
- There is no such thing as the “right” cloud, it is all about the line of sight
- Ensure that security is considered at each layer of the cloud stack

Cloud computing is seeing an ongoing explosion in growth, with Cisco claiming as high as 94% of all workloads are now being processed via cloud data centres. According to Gartner, "Global end-user spending on public Cloud services is expected to exceed $480 Billion next year". The COVID-19 pandemic has pushed the hybrid working model to the point where remote work and collaboration is the norm rather than an exception, with cloud services at its core. Gartner also predicts that public cloud spending will exceed 45% of all enterprise IT spending by 2026. To put that into perspective, current levels are at 17% for 2021.

Whilst the move to the Cloud is rapid, security concerns and the emphasis thereof are equally growing. Check Point reports that 94% of organisations surveyed say that they are "moderately to extremely concerned" about cloud security. Cloud cybersecurity incidents now surpass the on-premise ones for the first time, and by a lot. This is according to the annual report from Verizon Data Breach Investigations report (DBIR). Incidents involving cloud assets accounted for 73% of the total, compared to just 27% in the prior year. IBM, in their annual report of 2021 say that businesses face as much as $4.24 million per typical data breach incident.

The challenge for CISOs is to understand how cloud providers differ in their approach and practice to securing and ensuring resilience on their respective platforms, particularly the best-known 3 (Microsoft Azure, AWS and Google). There’s no argument that these big players don’t do a decent job in securing and protecting the cloud itself, with the occasional issue like a database vulnerability promptly dealt with by their extensive security teams, but they do also form a rather large target.

Whilst the Physical security and Technical or Infrastructure security is the cloud vendor's responsibility, access and encryption of data and control of that access is primarily the responsibility of the data owner or customer in the shared responsibility model. According to Gartner, they predict that up until 2025, 95% of cloud security failures will be due to a fault attributed to the customer. As we author this piece, at this very moment, millions of android users' personal data remain exposed due to various misconfigurations of third-party cloud services, even after Google was alerted by researchers, according to Check Point Research.

The recent DoControl report, "Quantifying the Immense Risk of Unmanaged SaaS Data Access," highlights how "vast amounts" of sensitive data in enterprises is at risk, with 40% of data in Cloud (SaaS) platforms unmanaged. Along with the rising adoption of SaaS applications, the threat of related data leaks is "growing exponentially" and "To date, security practitioners have focused on enabling SaaS access in a secure manner, but now is the time to prioritize the relevancy of this data access internally and externally."

Popular Cloud Services

Whilst every cloud provider has a slightly different approach, the core principles, security control objectives and best-practice advice remains the same. Each of the providers have amalgamated service specific guides that cover the exact settings to be managed to achieve a secure cloud within their particular platform:

Microsoft Azure

Microsoft offer an in-depth introduction to securing their Azure cloud platform.
Azure security | Microsoft Azure
Microsoft have also teamed up with the Center for Internet Security (CIS) to provide a number of preconfigured secure operating systems as ready-to-go packages.
Microsoft Azure Marketplace

Google Cloud

Google's contribution to the security of their cloud services comes in the form of a document catering towards enterprise organisations.
Best practices for enterprise organisations | Documentation

Amazon Web Service

Amazon offer a number of comprehensive guides for securing Amazon Web Services (AWS) distributions. They also provide the ability for users to purchase and share additional security modules through the AWS Marketplace.
AWS Marketplace Resource Hub
Security solutions in AWS Marketplace

Cloud Computing Standards

The National Institute of Standards and Technology (NIST) Cloud Computing Standards Roadmap (NIST-SP 500-291) along with the technology- and implementation-agnostic Cloud Computing Reference Architecture (NIST SP 500-292) identifies the main cloud Actors, their roles, and the main architectural components necessary for managing and providing cloud services.

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) joint committee on Cloud Computing and Distributed Platforms also developed a reference architecture standard, derived from NIST SP 500-292: International Standard ISO/IEC 17789 | Recommendation ITU-T Y.3502 "Information technology - Cloud computing - Reference Architecture", which outlines security components as part of multi-layer functions.

These reference architecture standards provide a common language and model with which to design, manage and communicate cloud solutions, including high level recommendations on how security should be dealt with. Specific configuration details for different platforms require the translation of these standards into guidelines and procedures.

Cloud Security Hardening - Configuration Guidelines

The Center for Internet Security has maintained carefully curated and up to date guides for a large number of operating systems and services. The security guides cover the big cloud players and go into detail on how to secure each instance to an acceptable level.
CIS Benchmarks™ https://www.cisecurity.org/cis-benchmarks/
Despite the different platforms that they cover, the CIS hardening benchmarks share a number of similar key areas and points:

Identity and Access Management:
Ensuring that there is always a way to gain access to the service, a number of different communication methods and redundancies must be implemented.
Secure passwords and authentication procedures must be enforced and when combined with Multi-Factor Authentication (MFA) produce an extremely difficult service to gain unauthorised access too.
Maintaining strict access rights for all users, whether they are required for business purposes or just as guests is critical.

Logging and Monitoring:
Logging must be turned on for all service features and monitoring with alarms must be enabled for all logs.

Storage:
Encryption must be utilised when data is at rest or being transferred to ensure the safety of the contents.

Networking:
External RDP or SSH access from the internet must be disabled along with HTTP access. If a connection is needed it should be done through HTTPS or with an encryption key pair.

Assessing cloud computing security
Establishing appropriate security controls as cloud solutions are designed and implemented is vital, but how can we assess existing solutions and configurations? The Cloud Security Alliance provides a set of sector-specific controls for cloud service providers in their Cloud Control Matrix (CCM). There is also a set of questions a cloud consumer and auditor may wish to ask a cloud provider to ascertain their compliance to the CCM called the Consensus Assessment Initiative Questionnaire (CAIQ).
The CAIQ offers an industry-accepted way to document what security controls exist in cloud services, providing security control transparency and to some extent assurance.
https://cloudsecurityalliance.org/blog/2020/04/04/why-use-the-caiq-for-vendor-analysis-vs-other-questionnaires/

Key Consideration
No matter what cloud platform is being used, visibility is key, and it should form the foundation of any cloud security strategy. Whether security revolves around compliance, policy governance or risk remediation, visibility into infrastructure security is one of the most pressing cyber security challenges within cloud security. As businesses grow, merge and acquire, visibility gaps widen due to the implementation of a variety of deployment processes and technologies. Being able to accurately see and comprehend your organisation's cloud footprint is the first crucial step in defending it.

References

- Microsoft Azure cloud vulnerability is the 'worst you can imagine'
- Cloud Trends -Learn What You Need To Know in 2021 | VNT
- Gartner Says Four Trends Are Shaping the Future of Public Cloud
- 2021 DBIR Master's Guide
- Cost of a Data Breach Report 2021
- Is the Cloud Secure? - Smarter With Gartner
- NIST-SP 500-291, NIST Cloud Computing Standards Roadmap
- NIST Cloud Computing Program
- ISO/IEC 17789:2014(en) — Cloud computing — Reference architecture
- Why use the CAIQ for cloud vendor analysis?

How can Tannhauser assist?

In Assess we review your existing cloud and its alignment with your business risk. We also consider:

- Governance review for support of function and long-term objectives
- Do policies define access to critical data?
- Risk assessment and assurance services
- Cloud security posture maturity
- Does the Cloud strategy align well with the organisation that delivers this policy?

Based on the results of the Assess phase, Tannhauser will build and Enhance your cloud security operations:

- Cloud infrastructure configuration hardening
- Identity and Access Management for cloud services
- Logging and monitoring
- Gain visibility into how your data and systems are accessed

To understand what cloud security means for you and your business, we are on hand to help address any questions and assist in the implementation of improved controls.