SYGNUM

Notes from a cloud security journey

Olivier Busolini

January 2023

Agenda

1 **Sygnum**
Who we are

2 **Key (security) concepts of the cloud ecosystem**
Key areas of interest and risk of any cloud journey

3 **Notes from a cloud security journey**
Sharing lessons learned, key enablers and pitfalls in this journey

SYGNUM

The world's first digital asset bank.

Securely store, trade and manage your digital assets along with traditional banking services.

Bank	Custodian	Broker
CHF – EUR – USD – SGD accounts	Segregated wallets	24/7 Spot Trading
Loans	Staking	Options Trading
Asset Management (incl. DeFi)	SOC-1 certification	Forex
B2B Banking Services	DeFi Access (coming soon)	Best Execution
~ CHF 2Bn in AUC	> 1,250 clients globally	> 40 countries served

Investors and Strategic partners

SBI Holdings, BitRock Capital, TATA, Singtel innov8, SBI Digital Asset Holdings, SCB 10X, 新鴻基有限公司 SUN HUNG KAI & CO. LIMITED, animoca BRANDS, WEMADE, SIX, swisscom, GALAXUS, Gruppo Azimut AZIMUT, DFINITY, bordier 1844

Key concepts of the cloud ecosystem

Balance cloud(s) agility, real time evolution and larger attack surface with trust and security

“Commodisation” of advanced, innovative, agile IT for all

- IT as a Service
  - On prem servers -> On prem / Cloud VMs -> Cloud containers…
- Application modernization to support business improvements
- Multi clouds, hybrid cloud
- Diverse services: IaaS / PaaS / SaaS – it’s often “and” and not “or”

Only a tech choice ?

Competences & beliefs are driving the choices

- People preferences & culture:
  - ExCo, IT mgt, Dev & Ops teams, Infrastructure support, security teams, etc.
  - Microsoft ? Amazon ? Google ? Oracle ? Local ? National / “Sovereign” ?...
- Skills and experience
  - Market dryness - Multi-cloud = people challenges ^ number of clouds

Cost reduction objectives

Shared Responsibility Model (SRM)

- Security *of* the cloud and security *in* the cloud

https://sysdig.com/blog/26-aws-security-best-practices/
https://www.pwc.com/us/en/tech-effect/cloud/enterprise-cloud-transformation-strategy.html
https://aws.amazon.com/compliance/shared-responsibility-model/

Key security concepts of the cloud ecosystem

Managing “usual” IT risks in a fundamentally different IT ecosystem

- Threat model
  - Wider exposure than traditional on prem
- Security requirements are similar as with on-prem IT
- However, risks, controls and governance need to be refactored
  - e.g. recertification of accesses defined in a Terraform file
  - Differences in security controls across different CSPs
  - NIST SP800-53: ~1200 controls ⇔ M365 ~ 5000 technical settings
  - IT asset inventory
    - Dynamic and ephemeral nature of infrastructure and assets being spun up and spun down.
- Observability: visibility and compliance
- Support model from the cloud(s) provider(s)
  - RACI, Proximity, Quality, Size CSP

- An IT ecosystem with probably much more Third Party risks
  - Shadow IT
  - Third party / open source code

Key steps in the Cloud security journey

- Evaluation: certifications and assurance reports - CSA STAR
- Adoption: competences to migrate / spawn in the cloud(s)
- Use and Expansion: auditability
- Termination: data portability - data deletion - exit strategy

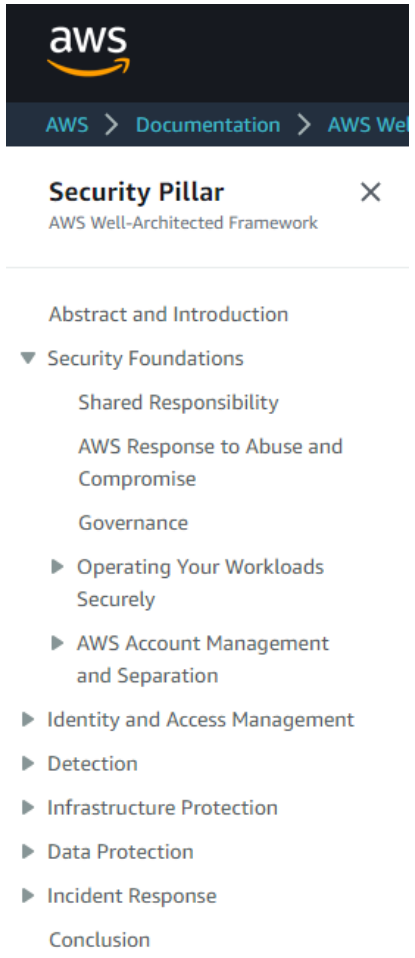
Notes from a cloud security journey (1)

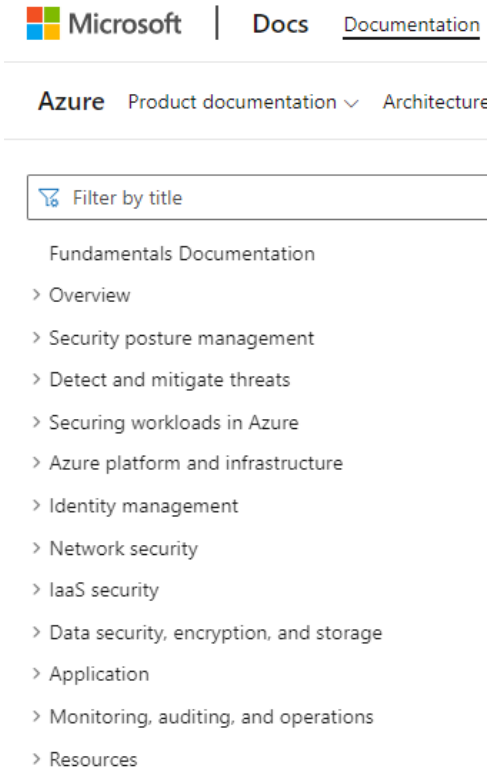
1. People

- New organisational and operating models
- Talent-to-risk-reduction strategy
  - Diversification of cybersecurity talent sourcing, including IT to cybersecurity careers upskill
  - Growing importance of partners and MSSPs
- Role of cloud security architects and engineering (SRM)
  - Advise, explain, train, control and monitor
  - For the migration to cloud and then “run the clouds”

2. Governance

- Identify security risks and drive the security strategy from there
  - Aligned with the enterprise operational and IT risk appetite
  - Architecture blueprint and Operating models
- Cloud security by default and design
- Contractual setup, e.g.
  - Microsoft: M453 (FINMA amendment), DPA, M329 (Swiss standard amendment), Professional secrecy amendment, Confidentiality provision M 744, Product terms…
  - AWS: Enterprise Agreement, Switzerland Financial Services add., GDPR Data Processing add., Professional Secrecy add., supplementary Addendum to the AWS GDPR DPA, Mutual Nondisclosure Agreement…





Sources: https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/welcome.html
https://docs.microsoft.com/en-us/azure/security/fundamentals/best-practices-and-patterns

Notes from a cloud security journey (2)

3. Core cloud security principles

- Defense in depth
  - Enforce, monitor and maintain controls (SRM) across edge of network, network infrastructure, every instance and compute service, tenant and account, container and orchestrator, operating system, application, and code…
- Simplification of cybersecurity stack - Unified & integrated security services
  - Cloud providers tools, in multi clouds
- Automation & Scalability
  - Security Orchestration (Automation and Response, SOAR): Third party tools ?
  - Automated security mechanisms to securely scale rapidly and cost-effectively
  - ML
  - Secure architectures blueprints (as code in version-controlled templates)
- Comprehensive coverage
  - Multi-cloud
- Cost-effectiveness
- Continuous compliance
  - Log and metrics collection across cloud(s)
  - Monitor, alert and audit actions and changes
- Security event and incident monitoring and response

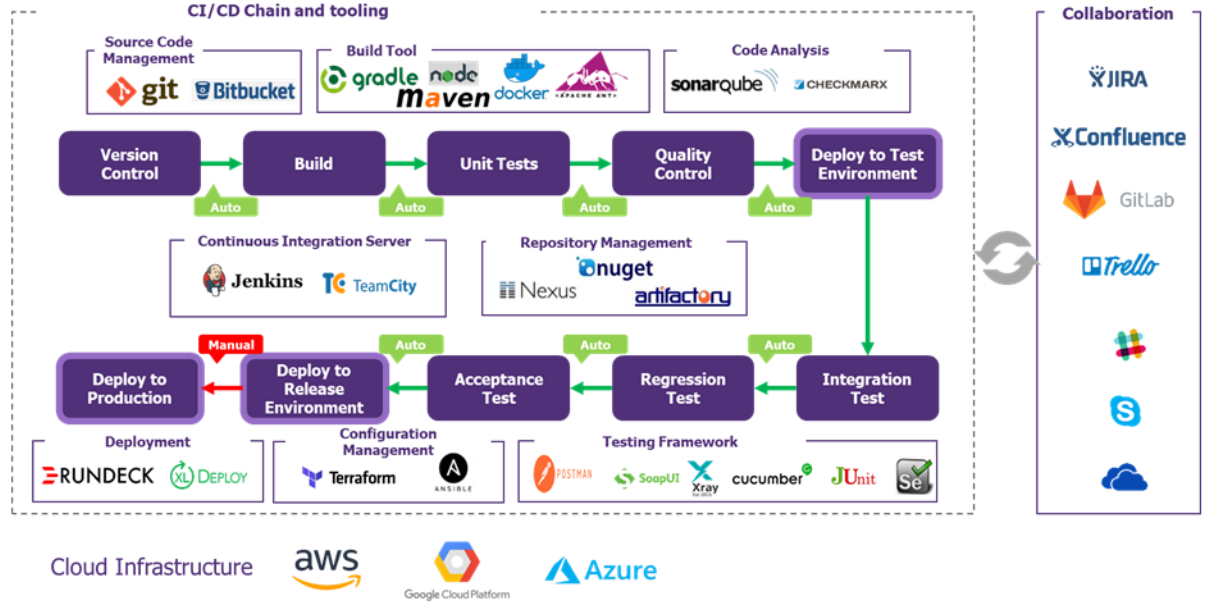
Notes from a cloud security journey (2)

4. Technology

Underlying infrastructure is secured by the cloud provider (“of”)

Application and workload security must be built on top of the cloud infrastructure security (SRM, “in”)

- **Security by default and design**
  - Evaluate and implement new security services and features regularly
  - Secure development and collaboration platforms use
  - An incremental journey
- **S-SDLC – DevSecOps - CI/CD Shift left security**
  - Automate testing and validation of security controls in CI/CD pipelines
  - Assessment of machine images and infrastructure as code templates for security vulnerabilities, irregularities, and drift from an established baselines at each stage of build and delivery
- **Abstraction from cloud specific tech stack**
  - Myth or reality ?
  - E.g. Infrastructure as code, Terraform
- Complexity of **consistent change and configuration management across multi-cloud**



Sources: https://www.riskinsight-wavestone.com/en/2022/09/security-in-agility-and-devsecops-linked-fates/

Notes from a cloud security journey (3)

4. Technology (cont.)

Cloud Access Security Broker (CASB)

- Identify the **reality of the consumed cloud services, Shadow IT** may increase significantly
- Identify **high-risk services** and **data** getting uploaded into those high-risk cloud services
- Identify **cloud services outside of IT control**

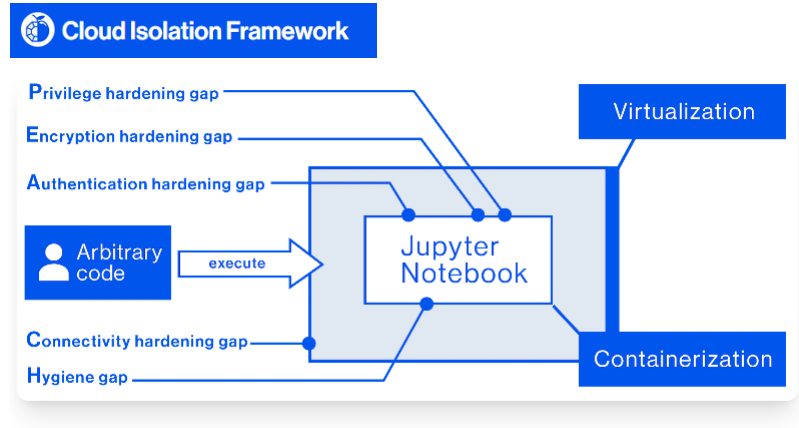
Published: 5/18/2022

Ebook on how Microsoft Defendr for Cloud reduces cloud security risk with unified security control.

Sources: https://azure.microsoft.com/en-us/resources/understand-how-unified-security-control-can-help-reduce-multi-cloud-security-risk/

Cloud Security Posture Management (CSPM)

- Simplifies and automates **configuration management**
  - Continuously monitoring SaaS applications against pre-built policy profiles
  - Can also fix risky configurations
- **Cloud workload protection**
  - Container Security
  - Application programming interfaces (APIs) security



Estimated isolation scheme of Cosmos DB-embedded Jupyter Notebook at the time of ChaosDB's discovery

Sources: https://www.wiz.io/blog/introducing-peach-a-tenant-isolation-framework-for-cloud-applications

Notes from a cloud security journey (4)

4. Technology (cont.)

Identity and Access Management (IAM)

Identity is the new perimeter, specifically in the cloud

Identification

- Centrally managed identities of humans and machines
  - User accounts
  - Privileged accounts, e.g. from “PAM” to “PIM” ☺
- New / more important access control topics
  - program source code
  - API access integration for third-party applications
  - Workload access: separate accounts and group accounts, based on function compliance requirements or a common set of controls

Authentication

- SSO and federation to integrate cloud accounts
- Strong / Multi-Factor Authentication and temporary credentials
- Secure the management of secret authentication information
- Legacy solutions
- Adaptive access management based on risk

Authorisation

- Principle of least privilege
- Identity-based policies from the CSP or the organisation

Notes from a cloud security journey (5)

4. Technology (cont.)

Data protection

Business and legal requirements, including localisation of data centers, data and services that are consumed

Data threat modelling and risk assessment

- What are the threats from those actors we want to prioritise ?
  - Employees ?
  - Cloud provider ?
  - Third parties ?
- What are the risks on data that we want to take into consideration beyond confidentiality ?
- Encryption
  - Data, DB, application, file, disk level ?
  - Cloud provider or non-cloud provider based encryption ?
- Keys / Secret mgt
  - Customer managed vs. cloud provider managed encryption process and key ?
  - Double Key Encryption, BYOK, etc. : Reduced data risks vs business process

Cloud breaches and cloud model

For a second year in this report, we've taken a close look at the impact of cloud model and maturity of cloud security on the cost of a data breach. The research found that 45% of breaches occurred in the cloud, but those in the public cloud cost considerably more than breaches at organizations with a hybrid cloud model. However, analysis of the research also shows that organizations still need a mature cloud security posture, regardless of cloud model.

43%

Share of organizations that were in early stages or had not started applying security practices to safeguard their cloud environments

Meanwhile, 34% were at the midstage and were applying many cloud security practices, and 23% were in the mature stage and were applying security practices consistently across all domains. Another 26% of organizations said that they were in the early stage, meaning that they had begun applying a few cloud security practices. Finally, 17% of organizations said that they had not started their journey in securing their cloud environments.

Source: https://www.ibm.com/uk-en/security/data-breach July 2022

Notes from a cloud security journey (6)

Zero trust cloud objective

- Opportunity to protect **data during processing not just in storage and communication**
- Encrypt data **as close as possible to data golden source** and **decrypt as late as possible before business use**
  - Some technologies enable to inject an encryption/decryption stage between cloud or legacy applications and the presentation to customers or employees while providing searchability and usability
- **Some technologies are at maturity** (Key Management System (KMS) and HSM as a service (HSMaaS), Searchable Symmetric Encryption (SSE), Attribute Based Encryption…) with a variety of providers
  - Technology solutions to strengthen cloud provider data encryption
  - Privacy management from database out: clear text data in DB is protected / sanitized while being consumed
  - **Privacy management from business process in**: **data level encryption that maintains (partially) business usability of data**, such as
    - Search (fuzzy)
    - Service interoperability

- Some insights on data encryption and keys management
  - **Data privacy/confidentiality risks** of using cloud(s) service(s) must be documented, clearly understood, and **accepted by the data owner, legal and risk** management teams
  - Data will probably be **no less secure** than it was prior to adoption of the cloud service
  - **Privacy obligations** are also supported by the **cloud vendor certifications**
  - **Data will probably not be exposed** (in readable/intelligible form) **to cloud service human personnel on their daily activities**

- Future of encryption
  - **Homomorphic Encryption**: encryption of data while in-use while still allowing operations on the data
  - **Privacy-Enhancing Cryptography**: minimize the amount of personal or sensitive data collected by systems while still maintaining functionality
  - Confidential Computing: secure enclaves
  - Post-Quantum Cryptography: NIST Internal Report (IR) 8105 from 2016 called out that quantum computers capable of breaking 2000 bit RSA in a matter of hours *could* exist by 2030

Conclusion

Is there an option not to go to the cloud ?

This journey can be tricky, and it can be secured with the right focus

Balance cloud agility, real time evolution and larger attack surface with security

People and governance

- Understand the Shared Responsibility Model and its consequences
- Develop and retain skilled people
- Strengthen the contract(s)

Process

- IT asset management and securisation of the cloud stack: secure, monitor and maintain controls
- Understand and secure third party resources / services: cloud providers, SaaS providers, Third Party and Open-Source code…

Technology

- Unified & integrated cloud security services - Automation & Scalability is key
- Workload security built on top of the cloud infrastructure security
- IAM
- Data Protection
- Monitoring and response

SYGNUM

Thank you

References

Special thanks to

- Philippe Le Berre, https://www.stacksciences.com/
- Philippe Tarbouriech
- Rémi Pactat, https://ch.wavestone.com/en/

- "SaaS Governance Best Practices for Cloud Customers", Cloud Security Alliance

https://cloudsecurityalliance.org/research/working-groups/saas-governance/

- Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions

https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/sse-1.pdf

- AWS security

https://docs.aws.amazon.com/prescriptive-guidance/latest/aws-startup-security-baseline/welcome.html

https://docs.aws.amazon.com/whitepapers/latest/overview-aws-cloud-adoption-framework/security-perspective.html

https://docs.aws.amazon.com/wellarchitected/latest/financial-services-industry-lens/security-pillar.html

https://cloudsecdocs.com/aws/defensive/checklists/maturity_roadmap/

https://blog.lightspin.io/the-complete-guide-to-aws-kms

https://sysdig.com/blog/26-aws-security-best-practices/

- Cloudsecdocs

https://cloudsecdocs.com/#the-structure

https://roadmap.cloudsecdocs.com/

https://www.marcolancini.it/2022/blog-cloud-security-infrastructure-review/

- Zero Trust

https://zerotrustroadmap.org/

- Microsoft Azure security

https://docs.microsoft.com/en-us/security/compass/compass

https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/secure/

https://docs.microsoft.com/en-us/microsoft-365/compliance/office-365-encryption-in-the-microsoft-cloud-overview?view=o365-worldwide

https://azure.microsoft.com/mediahandler/files/resourcefiles/understand-how-unified-security-control-can-help-reduce-multi-cloud-security-risk/ESG-eBook-Microsoft-Defender-May-2022%20(1).pdf

https://docs.microsoft.com/en-us/azure/governance/policy/samples/nist-sp-800-53-r5

- CI/CD security

https://www.cidersecurity.io/top-10-cicd-security-risks/

Characterizing the Security of Github CI Workflows: https://www.usenix.org/system/files/sec22-koishybayev.pdf

- Legal references

https://www.vischer.com/en/knowledge/blog/swiss-banks-in-the-cloud-this-is-how-it-works-and-how-not-39215/

https://www.rosenthal.ch/downloads/VISCHER-Swiss-Banks-Cloud.pdf

https://iapp.org/resources/article/transfer-impact-assessment-templates/

- Other

https://www.riskinsight-wavestone.com/en/2022/10/compliance-in-the-cloud-a-new-paradigm/

OWASP Kubernetes Top 10: https://owasp.org/www-project-kubernetes-top-ten/

McKinsey "talent to value": https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/securing-your-organization-by-recruiting-hiring-and-retaining-cybersecurity-talent-to-reduce-cyberrisk

Introducing PEACH, a tenant isolation framework for cloud applications: https://www.datocms-assets.com/75231/1671033753-peach_whitepaper_ver1-1.pdf