Security Best Practices & Case Studies

Tristan Woerth – Cloud Architect

Basel 11.07.2019

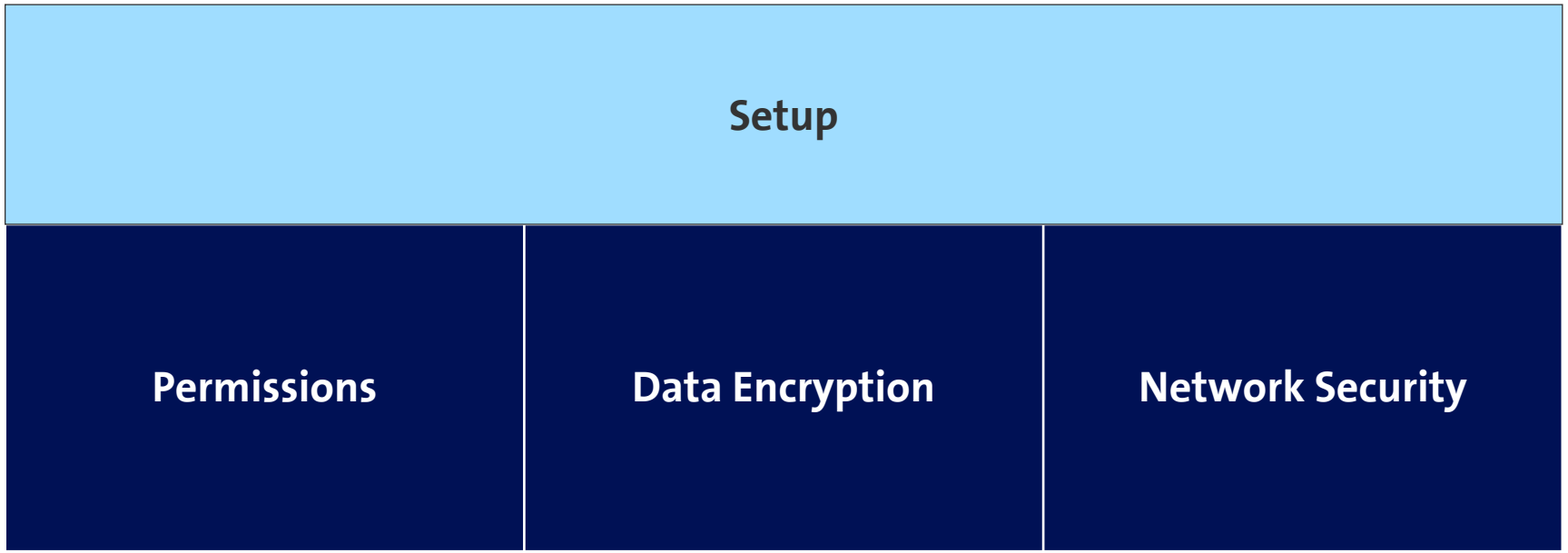
swisscom

Shared Responsibility Model

The **provider** is responsible for the security **of** the cloud.
The **customer** is responsible for the security **in** the cloud.

On-Premises	IaaS	CaaS	PaaS	SaaS
Users	Users	Users	Users	Users
Applications	Applications	Applications	Applications	Applications
Data	Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Containers	Middleware	Middleware
O/S	O/S	O/S	O/S	O/S
Virtualization	Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking	Networking
Facility	Facility	Facility	Facility	Facility

3 Main Areas, 1 Pre-Requisite



Well-Architected Framework

The Well-Architected Framework consists out of 5 pillars and documents a set of foundational questions that allow you to understand if a specific architecture aligns well with cloud best practices.

Benefits

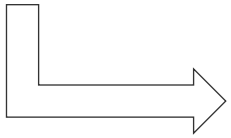
- Evaluate workload against best practices
- Independent assessment
- Identifying gaps
- Get recommendations
- Benefit from broad expertise

Well Architected Framework - Security

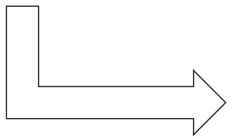
Enable traceability

Implement a strong identity foundation

Automate security best practices



Apply security at all layers

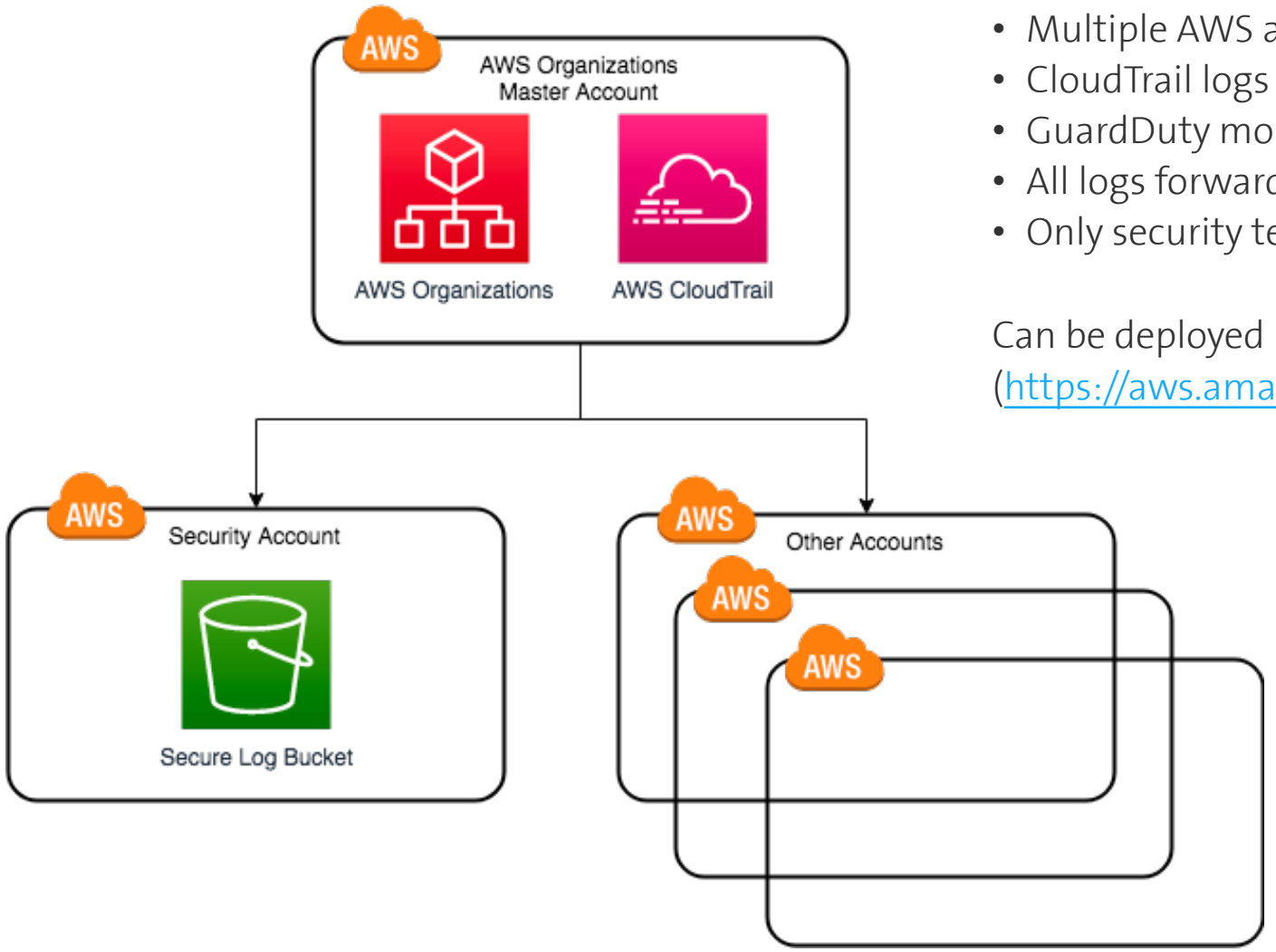


Protect data in transit and at rest

Keep people away from data

Prepare for security events

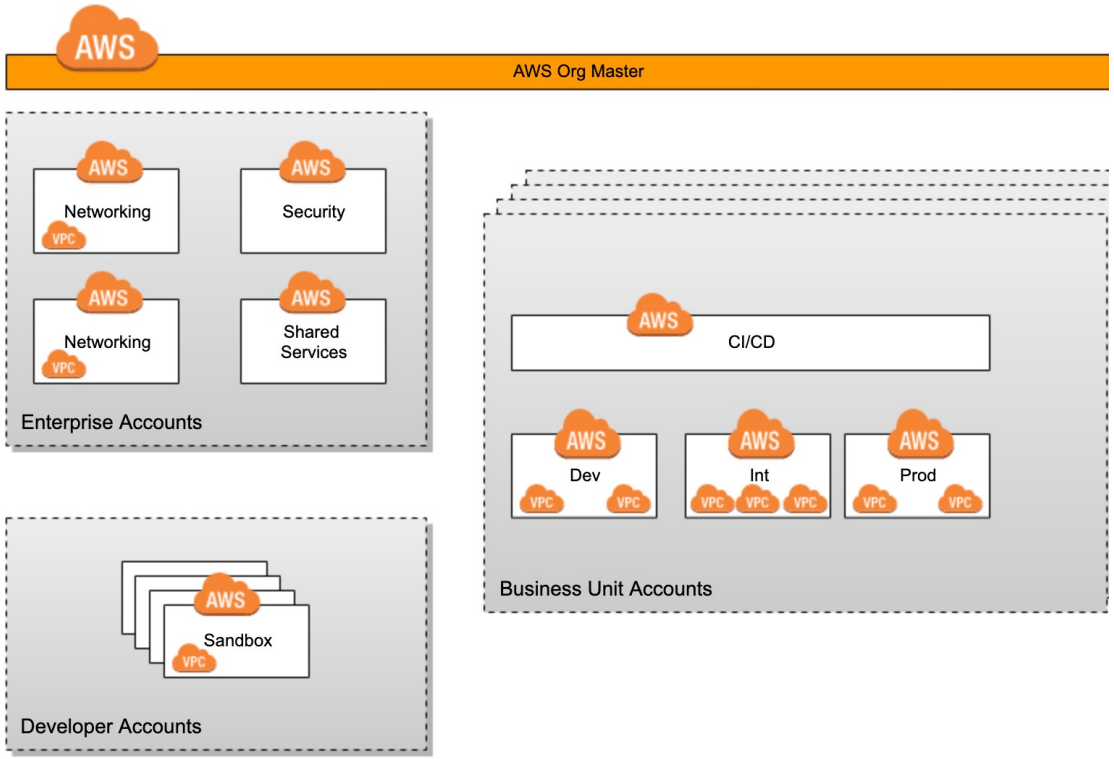
Best Practice – Data Bunker



- Multiple AWS accounts part of an Organization.
- CloudTrail logs enforced, going into Master Account.
- GuardDuty monitoring events across all accounts.
- All logs forwarded to Security Account.
- Only security team has access to Security Account.

Can be deployed by AWS as part of Control Tower (https://aws.amazon.com/controltower/features/)

Extended version



Enterprise Accounts	
Networking	• Direct Connect • Networking Services
Log / Mon	• Cloud Trail Logs • Security Logs • Guard Duty

Shared Services	• DNS / LDAP
	• Golden AMIs
	• Availability- / Service Monitoring
	• Scanning Infrastructure
	  • Snapshot Life Cycle
	  • Improper tagging
	  • Inactive Instances

Security	• Security Tools and Audits • Key Management • Cross-Account read/write

Best Practice – IAM

Secure Root Account with MFA, aim to never use it.
(exceptions at https://docs.aws.amazon.com/general/latest/gr/aws_tasks-that-require-root.html)

Any account with access to the console should be under MFA.

MFA should be enforced, not merely enabled. AWS Config Rules can help enforce.

Federation can be used to reduce the amount of manual operations as well as the latency until changes are implemented.

Fine grained authorization should be used to follow the Principle of Least Privilege by reducing the permissions to both services and resources. (https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_actions-resources-contextkeys.html)

Fine grained policies are easier to maintain through CloudFormation. The AWS Managed Policies are useful, but too coarse for real life use.

CloudFormation Drift Detection will then be able to detect manual changes.

Best Practice - Monitoring

Tooling will help, but success is highly dependent on the right culture.

- Real-time alerts.
- In high usage channels (email is typically not enough).
- Culture of acknowledging and investigating alerts.
- Playbook on when to escalate, who needs to be informed, in which channels, etc.
- Continuous improvement mindset rather than finger pointing.
- Regular drills can help.

Customer Case: Insurance

Scenario

Company transitioning to a Cloud first strategy. Need to enable wide use of AWS services while maintaining their Compliance & Security standards.

Components

Helped with Strategic consulting, designed and implemented account on-boarding, IAM Federation concept, etc. Monitoring and Alerting, , CIS-benchmark checks implementation

Benefits

Compliance & Security stakeholders are satisfied. Company is able to benefit from AWS services with high degree of automation.

Shared Responsibility Model

Provider and consumer share the task of securing the workload.

Understanding your responsibilities will help you focus on what matters most.

Framework

Frameworks such as the Well-Architected Framework help to continuously improve your practices.

Security greatly benefits from this.

Partner

A competent and trustworthy partner can be vital for success.

Partnering can take many forms.