AWS Summit

Berlin

amazon web services

Mapping traditional security technologies to AWS

Dave Walker – Specialised Solutions Architect
Security and Compliance
Amazon Web Services UK Ltd

amazon web services

AWS' Compliance "Display Cabinet"

Certificates:

Programmes:

PCI DSS Level 1	HIPAA
SOC 1/ ISAE 3402	FedRAMP (SM)
SOC 2	DoD CSM Levels 1-2, 3-5
SOC 3	DIACAP and FISMA
ISO 9001	ISO 27001
IRAP (Australia)	MTCS Tier 3 Certification
FIPS 140-2	ITAR
CJIS	MPAA
CSA	G-Cloud
FERPA	Section 508 / VPAT

Why a Mapping of Security Controls?

- 2 primary reasons:
  - Dealing with Standards
  - Introducing the new, through the concepts of the familiar
- Also:
  - Tracking the state of the art
  - Enrico Fermi and Donald Rumsfeld

amazon web services

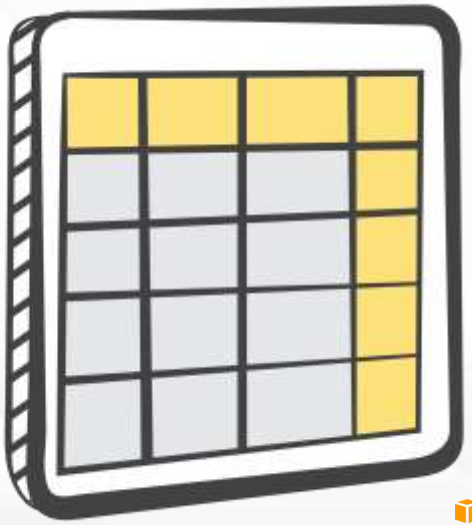
Why a Mapping of Security Controls?

- PCI-DSS
  - standards for merchants which process credit card payments and have strict security requirements to protect cardholder data. A point-in-time certification.
- SOC 1-3
  - designed by the “big 4” auditors as an evolution of SSAE16 etc, and to address perceived shortcomings in ISO27001. A continuous-assessment certification, covering process and implementation.
- ISO 27001
  - outlines the requirements for Information Security Management Systems. A point-in-time certification, but one which requires mature processes.

amazon web services

Standards, Controls and Commonality

- Controls overlap between standards
  - see eg https://www.unifiedcompliance.com
- AWS master control list and mappings
  - 1800+ internal controls
  - Mappings to external standards
  - Engage auditors, and…



amazon web services

“Principles Rarely Change, but Implementations Do”

- Zeno’s Paradox: Achilles and the Tortoise
  - Technology (almost) always leads standards
  - In 2014, AWS made 516 feature updates (including new service launches)…
  - ISO27001, ISO9001, SOC1-3, PCI-DSS (and lots of others) are covered by various AWS services at the infrastructure and container layers – others aren’t
  - The AWS Marketplace is growing…

amazon web services

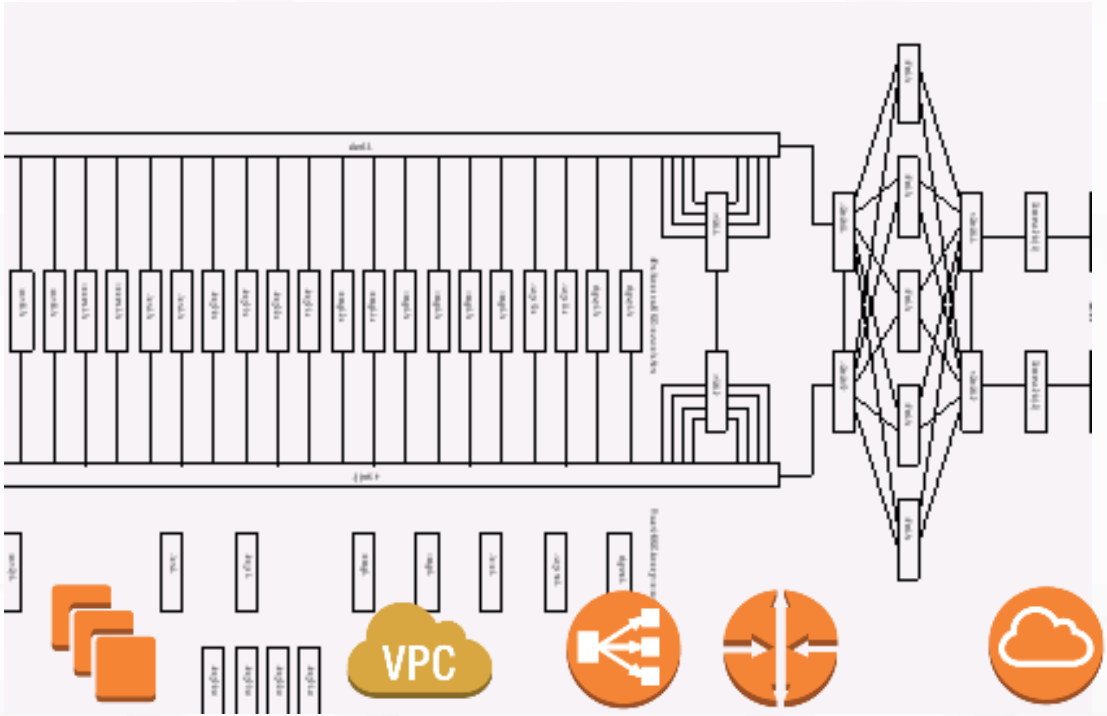
AWS Marketplace: One-stop shop for security tools

Advanced Threat Analytics	Application Security	Identity and Access Mgmt	Server & Endpoint Protection	Network Security	Encryption & Key Mgmt	Vulnerability & Pen Testing
ALERTLOGIC	IMPERVA	CIPHERGRAPH networks	TREND MICRO	FORTINET	SafeNet	tenable network security
ALIEN VAULT	FORTINET	SECUREAUTH	intel Security	SOPHOS	Vormetric	QUALYSGUARD
	Barracuda	M-Pin SSO		Check Point We Secure the Internet.	HYTRUST	
				paloalto networks.		

amazon web services

“When I were a Lad…”: Traditional Controls

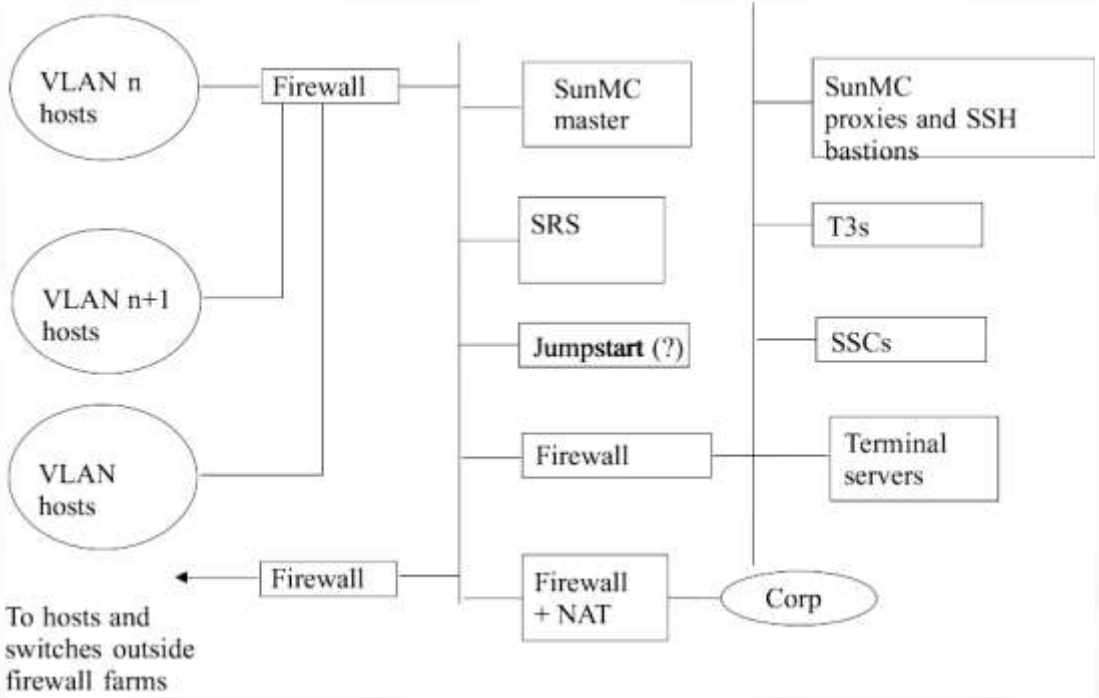
Service networks looked like:



amazon web services

“When I were a Lad…”: Traditional Controls

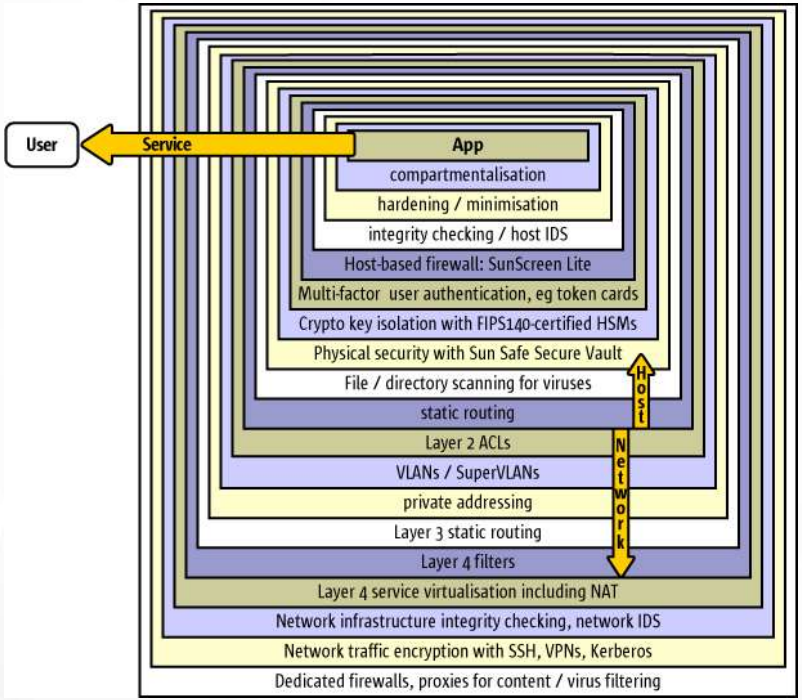
Management networks looked like:



amazon web services

“When I were a Lad…”

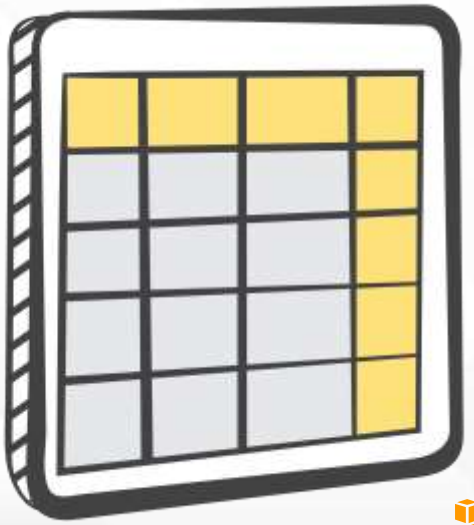
Security technologies looked like:



amazon web services

But:

- AWS security controls are rather more extensive
  - Can't readily be reduced to a 2D "onion"
    - (5 dimensions might about do it…)
- So, we have a table
  - And it's not small (circa 110 rows…)



amazon web services

Start Here:

- Infrastructure meta-security
- Host security
- Network security
- Logging and Auditing
- Resilience
- User Access Control and Management
- Cryptography and Key Management
- Incident Response and Forensics
- “Anti-Malware”
- Separation of Duty
- Data Lifecycle Management
- Geolocation

amazon web services

“Can our current Security Functions be mapped onto AWS?”

AWS Environment Management

amazon web services

“Can our current Security Functions be mapped onto AWS?”

Network

AWS to Customer Networks →	Internet and/or Direct Connect
Layer 2Network Segregation →	Amazon VPC
Stateless Traffic Management →	Network Access Control Lists
IPsec VPN →	VPC VGW, Marketplace
Firewall/ Layer 3 Packet Filter →	Security Groups
IDS/IPS →	AWS CloudTrail, CloudWatch Logs,SNS, VPC Flow Logging
Managed DDoS Prevention →	Included in Amazon CloudFront

amazon web services

Brand New DDoS Whitepaper:

- http://d0.awsstatic.com/whitepapers/DDoS_White_Paper_June2015.pdf

amazon web services

“Can our current Security Functions be mapped onto AWS?”

Encryption, Key Management

Data-In-Flight	→	IPsec or TLS or your own
Volume Encryption	→	Amazon EBS Encryption
Object Encryption	→	AmazonS3 Encryption (Server and Client Side)
Key Management	→	AWS Key Management Service
Dedicated HSMs	→	AWS CloudHSM
Database Encryption	→	TDE (RDS / Oracle EE)
	→	Encrypted Amazon EBS (with KMS)
	→	Encrypted Amazon Redshift

amazon web services

“Can our Current Security Functions be mapped onto AWS?”

Data Management

Hierarchical Storage	→	Amazon S3 Lifecycle
Deletion Protection	→	Amazon S3 MFA Delete
Versioning	→	Amazon S3 Versioning
Archiving	→	Amazon Glacier

amazon web services

“Can our Current Security Functions be mapped onto AWS?”

Host / Instance Security

Traditional Controls	Traditional Controls (mostly)
Instance Management	Delete-and-promote
Incident Management	More alternatives!
Asset Management	“What the API returns, is true”
Instance Separation	PCI Level 1 Hypervisor
	Dedicated Instances

amazon web services

“Can our Current Security Functions be mapped onto AWS?”

- For some functions, AWS architecture will take you in a particular direction – for other functions, AWS architecture allows you to do more interesting things than on-premise.
- Some examples:

amazon web services

“Familiar functions, made Cloud scale”:

- IAM: “RBAC writ large”
  - Fine-grained privilege
  - Further access controls
    - Source IP
    - Time of day
    - Use of MFA
    - Region affected (a work in progress; works for EC2, RDS)
- Data Pipeline: “Cron writ large”

amazon web services

Asset Management, Logging and Analysis:

- “What the API returns, is true”
- CloudTrail, Config, CloudWatch Logs
  - “Checks and balances”
  - S3 append-only, MFA delete
  - SNS for alerting
  - Easy building blocks for Continuous Protective Monitoring

AWS CloudTrail

AWS Config

CloudWatch

amazon web services

IDS / IPS / WAF:

- Host vs network
  - Everything preventative needs to be inline
    - IPS / WAF in particular
    - Unless you wanted to have fun with RST packets
  - Dealing with autoscaling
  - Separation of Duty / managed service?
- VPC Flow Logging

amazon web services

Immutability and Mandatory Access Control:

- S3 cross-account sharing
- SELinux on EC2
  - SELinux enforcing policy can be complicated to write – see eg http://www.tresys.com

amazon web services

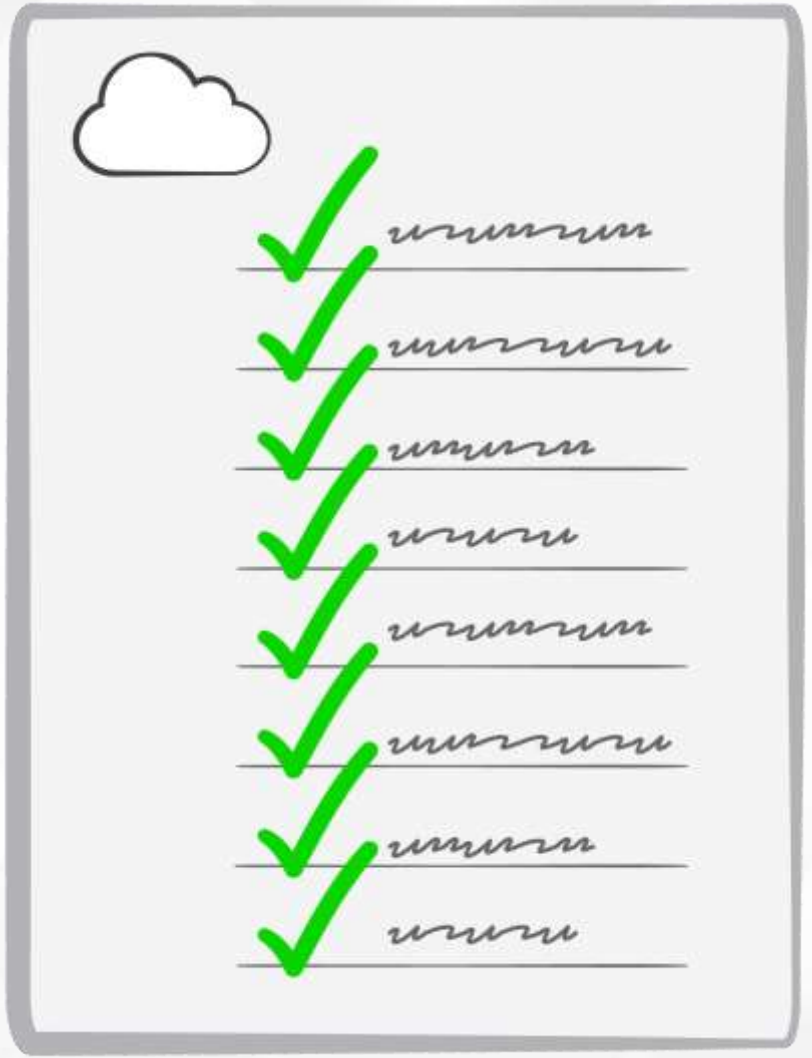
Incident Management:

- Traditional infrastructure:
  - Manage and Mitigate?
  - Pursue and Prosecute?
- Cloud gives you a third option:
  - Replicate, repair, ringfence and redirect
  - You’re back up and running, with previous environment isolated for forensic examination

amazon web services

Regulatory Compliance:

- Deutsche BaFin, UK FCA
- French ASIP Santé
- …



Thank You

amazon web services

Mapping traditional security technologies to AWS

Dave Walker – Specialised Solutions Architect
Security and Compliance
Amazon Web Services UK Ltd

amazon web services

AWS Summit

PLACE

amazon web services