



Information Security Systems International

An introduction for consultants to cloud security

October 6, 2022

Agenda

- Introductions & objectives
- The business context for cloud security
- The shared responsibility model
- The AWS well architected security model
- Cloud vulnerabilities
- Cloud threats
- Cloud vs on prem security – the approach
- Why is cloud security different to on prem?
- Security questions to ask your MSP/cloud supplier
- Contact details

Barry Turner

25 years service creation experience working with cloud service providers and telco's across EMEA on behalf of ISSI, AWS, Microsoft, Cisco, Mitel & Agile Programmes. AWS Solution Architect (associate), ITIL V4 Foundation, ISO27001:2013 lead auditor certified, PMP qualified with specialisation on marketing and go to market planning.

[Linkedin Profile](#)

David Pool

David is an experienced Cloud and Managed Services specialist and business strategy advisor with more than fifteen years of experience in the Telecoms industry. For the past 8 years David has focused on helping Businesses to benefit from the adoption of Cloud and Managed Services.

[Linkedin Profile](#)

Cloud MSP Best Practices Experience:

Consultants for ISSI

About ISSI

- Founded in 2006 in the USA
- Multi-cloud MSP consulting and auditing company
- Consulting and auditing services for the world's largest hyperscale cloud platform providers
- Best in class practices from over 500 next generation hyperscale cloud MSPs and 75+ Partner Transformation consulting engagements

Website: <http://www.issi-inc.com>

Sources

ISSI
Best Practices and IP
(Consulting/Audits)

Cloud Providers
Best Practices in
Business Process
and Architecture

Cloud Providers
MSP Certification
Programs

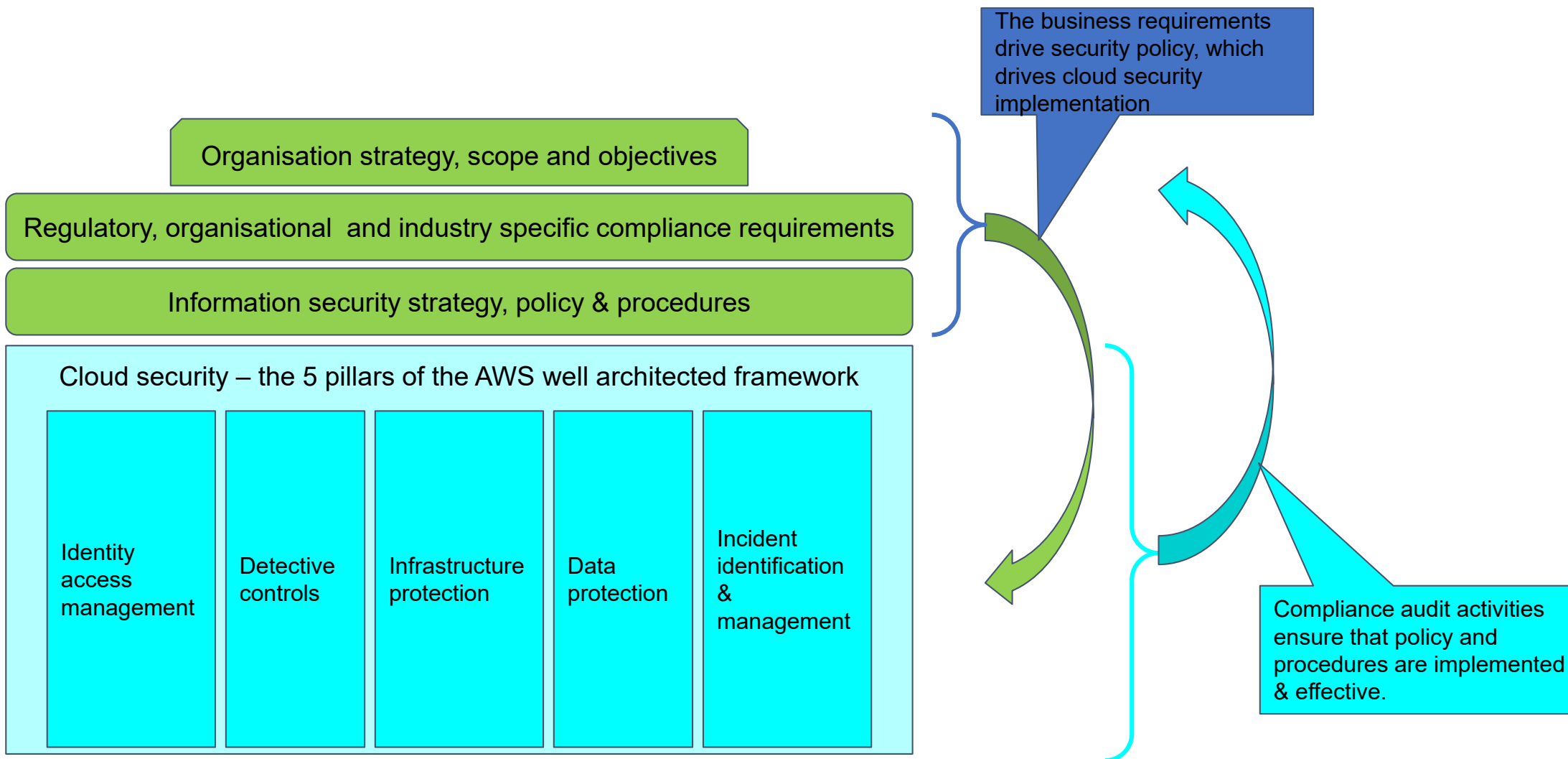
Industry Research
Reports – Gartner,
Forrester, IDC and
451

Best Practices

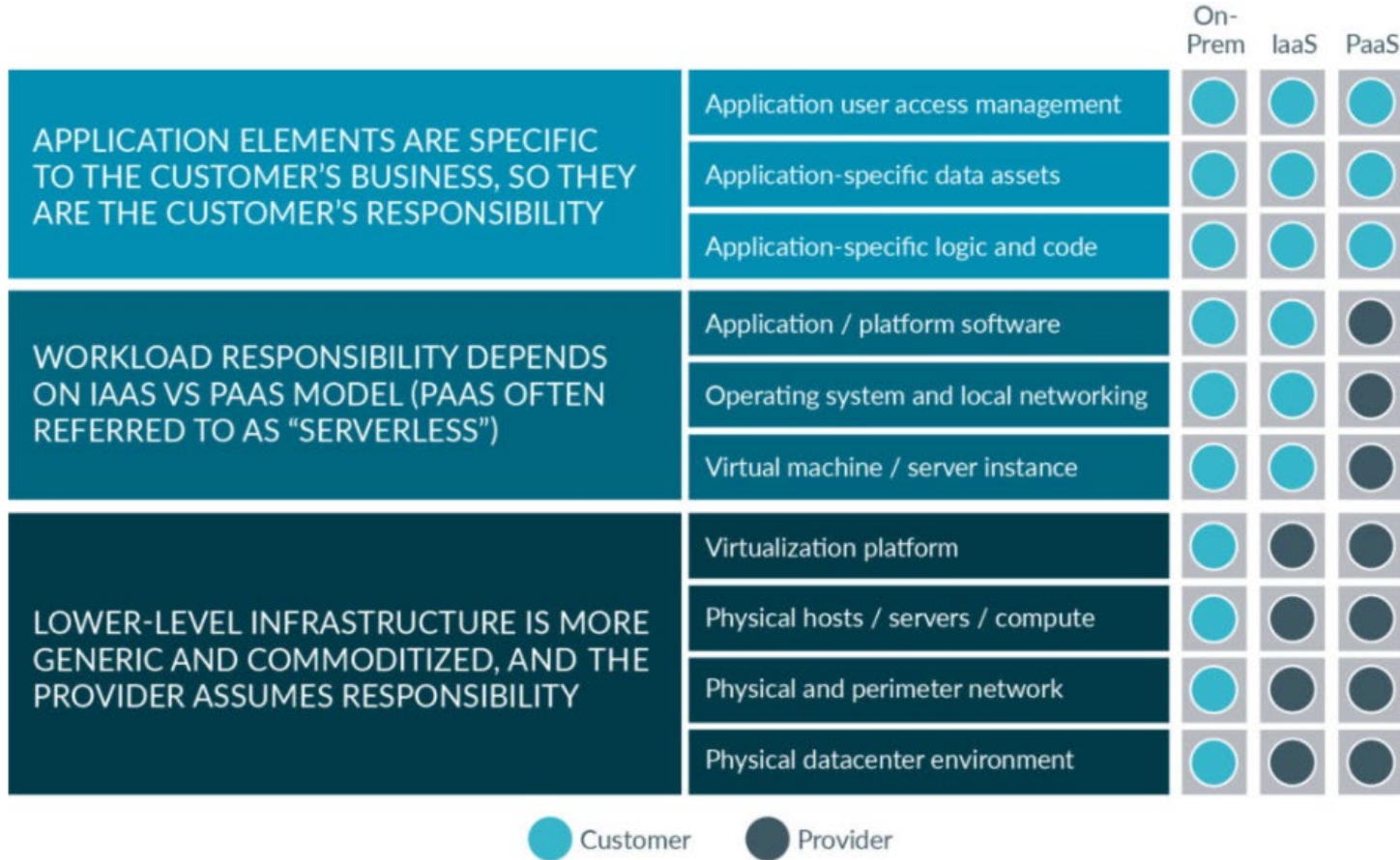
Business	Cloud Strategy
	Business Planning
	Talent Management
	Go to Market
Process	Service Offering Design
	Assessment and Migration Planning
	Design and Deployment
	Service Operations Management
	Monitoring Services
	Customer Lifecycle Management
Tools	Security and Governance
	Automation / DevOps
	Lifecycle Tooling

- ▶ Understand the cloud security landscape
- ▶ How cloud security is different from tradition on prem security
- ▶ Be able to engage in conversation with a potential supplier on how to secure your cloud environment

Setting the context of cloud security



The shared responsibility model



The diagram is provided by the cloud security alliance. This can be found at:

<https://cloudsecurityalliance.org/blog/2020/08/26/shared-responsibility-model-explained/>

Figure: A vendor-agnostic view of the division of responsibilities in the shared responsibility model

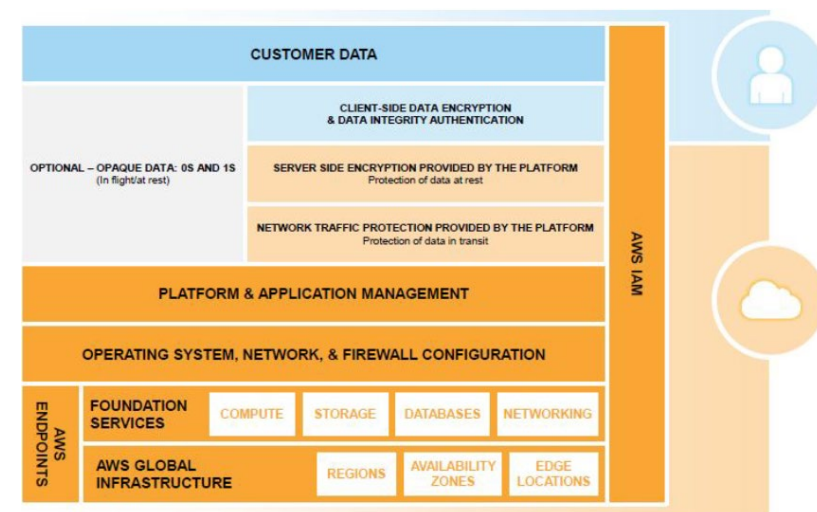
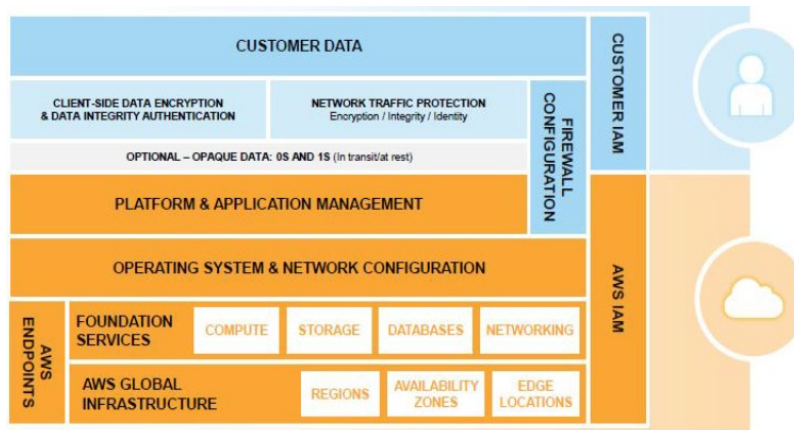
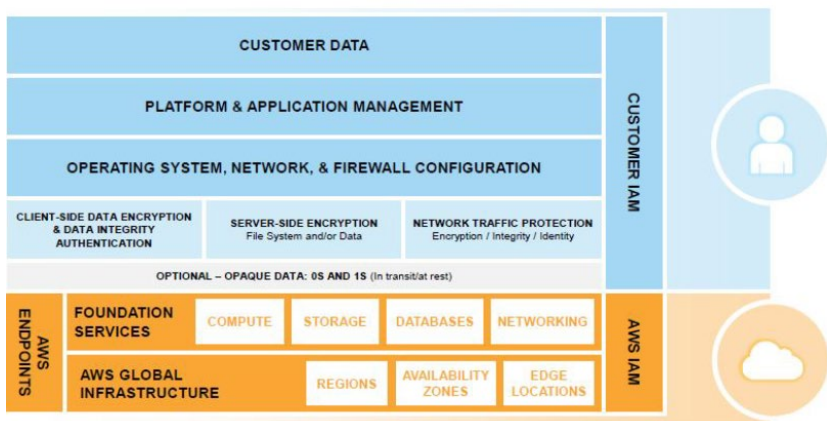
Shared Responsibility Model is not Static

It can shift based on technology, business purpose and architecture

Infrastructure Services

Container Services

Abstracted Services



AWS Well-Architected Framework Security Overview

Organizing security

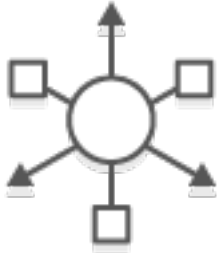
4 Categories of Security Controls



Core security topics
Identity and Access Management
Detective Controls
Infrastructure Protection
Data Protection
Incident Response

Augmenting the Core 5				
Secure CI/CD: DevSecOps	Compliance Validation – automated via policy as code	Resilience	Configuration and Vulnerability Analysis	Security Big Data and Analysis

Identity & access management



- ▶ Centralize access management
 - ▶ Federation (ADFS/other) or IAM for authentication
 - ▶ Leverage roles and policies extensively
 - ▶ Avoid “credential fatigue”
- ▶ Leverage Least Privilege –policy
 - ▶ Users and services should have only minimal necessary rights to perform their tasks
- ▶ Applies to processes & VM’s etc as well as people
 - ▶ API access
 - ▶ Application key management
- ▶ Logging
 - ▶ Trail logs to central place
 - ▶ Build capability to monitor and follow up on deviations

Usage Policy – Enable, do not deny

- Support the users, do not limit them
- Make rules easily findable
- Make rules easily understandable
- Allow users to decide themselves – but make clear what is supported and what they need to support themselves
- Be extra careful not to suffocate everything that is good in the cloud – agility, elasticity, platform services
- Consider both Human and machine identities
- Centralize identity control

If the easy way is the correct way, you have the best chances to succeed.

Detection - Service and application Logging



**AWS
CloudTrail**

AWS Cloudtrail

- Used to record all API requests 'who did what and when from where'



**AWS
Config**

AWS Config

- AWS account configuration



**Amazon
GuardDuty**

AWS GuardDuty

- Is a threat detection service that continuously monitors for malicious activity.



AWS Security Hub

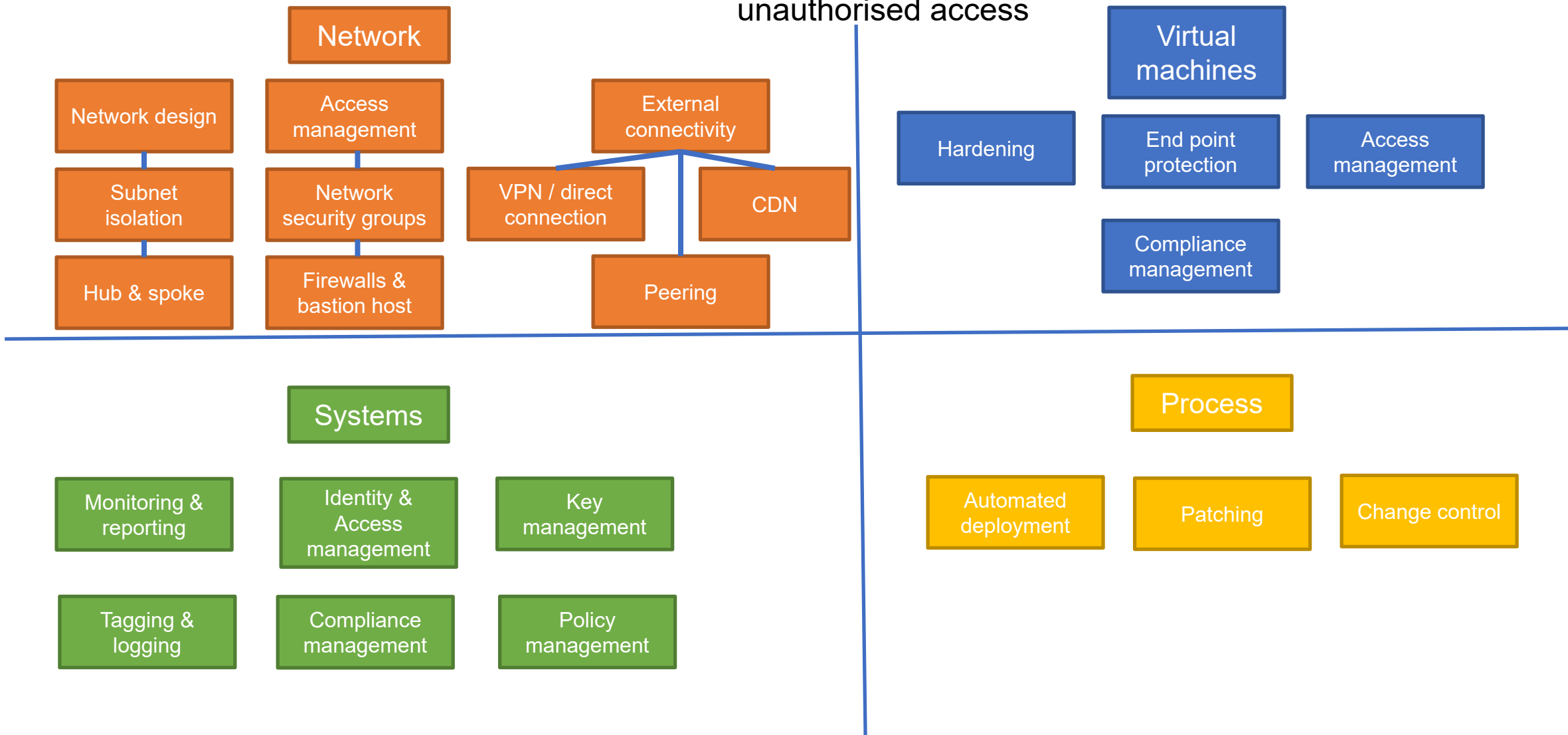
- Organises and prioritises security alerts or findings from multiple AWS services and third party products to give a comprehensive view of security alerts and compliance status

Tagging

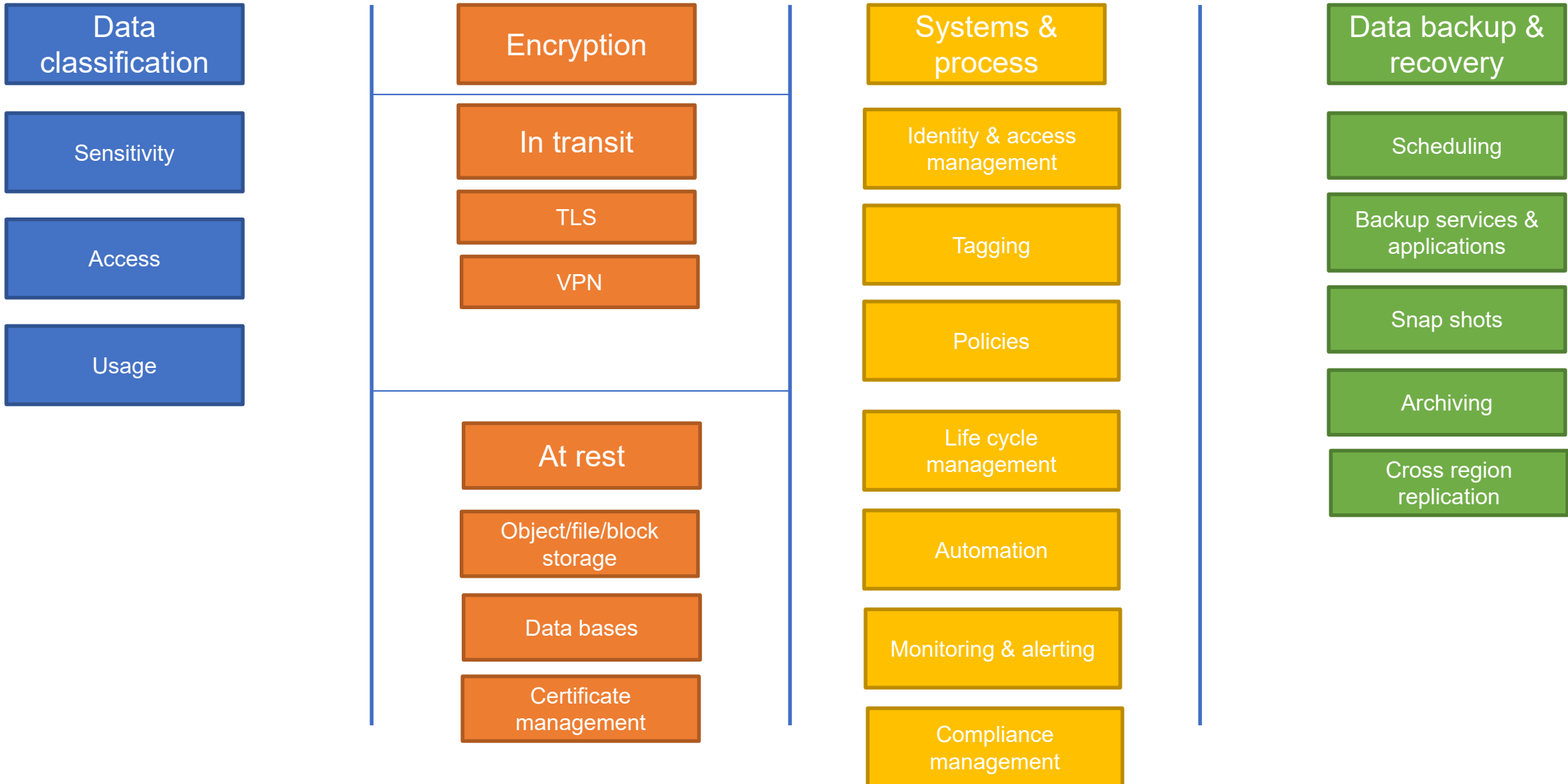
- Helps & enables the performance of all these functions

Infrastructure protection

preventing unauthorised access

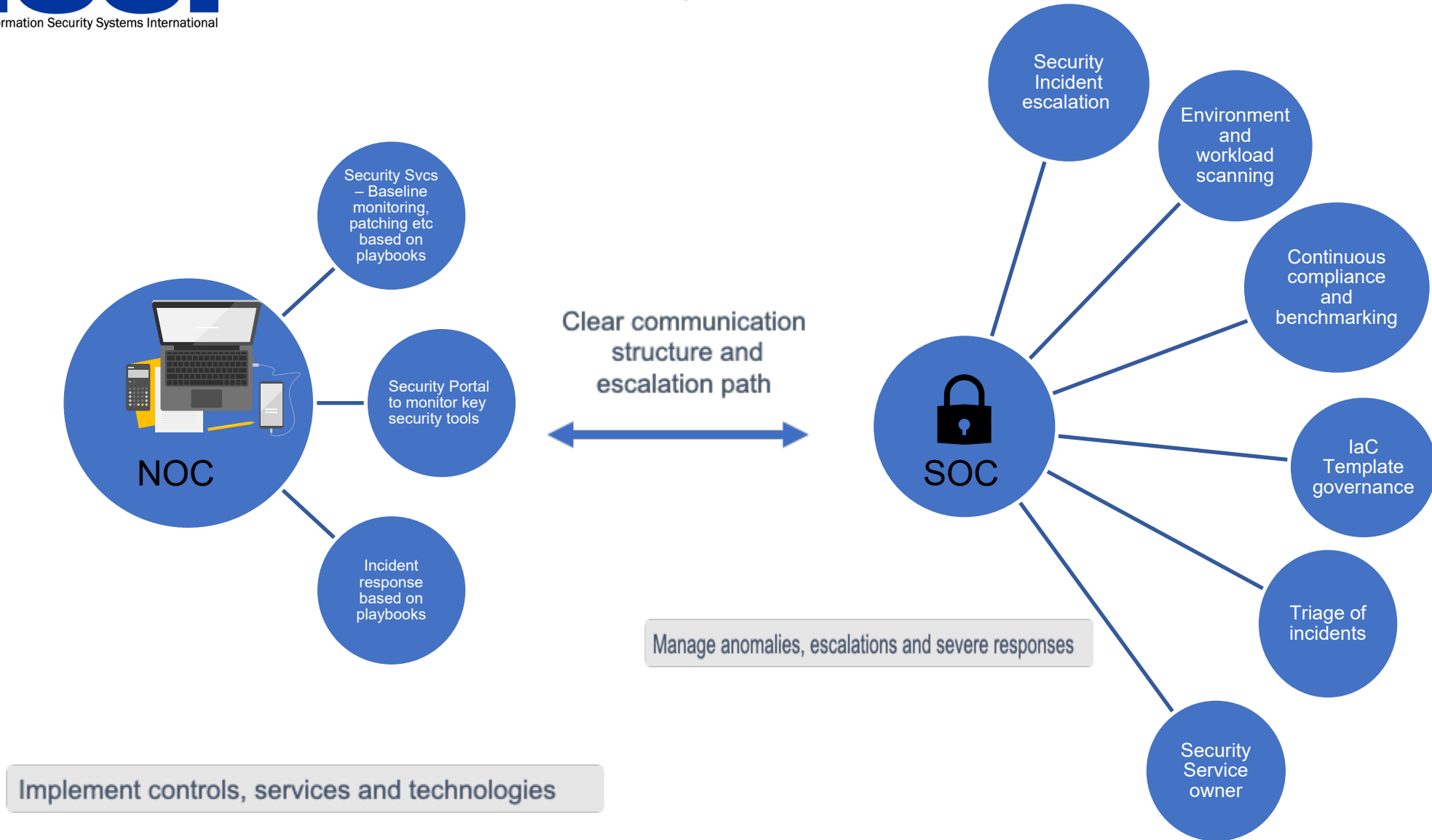



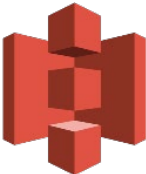
















Data protection



- ▶ Data classification drives the overall control requirements for confidentiality, integrity and availability.
- ▶ As data is created or acquired, it must be classified, for example:
 - ▶ by confidentiality (e.g. public, internal, confidential, strictly confidential)
 - ▶ by loss impact (e.g. no impact, medium impact, business-critical)
 - ▶ by external requirements (e.g. regulatory needs, legal holds, cardholder data)
- ▶ Example policy: strictly confidential, business-critical data in S3
 - ▶ Server Side Encryption must be active (confidentiality)
 - ▶ MFA authentication required before deletion (availability)
 - ▶ S3 bucket versioning must be enabled (integrity)
 - ▶ S3 reduced redundancy storage must not be used (availability)
 - ▶ Access must be for authorized users only (confidentiality)

Incident management



Item					
Data Protection	 Amazon EBS	 Amazon S3	 Amazon RDS	 AWS KMS	
Identity and Access Management	 IAM	 MFA token	 permissions	 role	
Infrastructure Security	 Amazon VPC*	 AWS WAF	 AWS Shield	 Amazon CloudFront	 Amazon Route 53
Detective Controls	 AWS CloudTrail	 AWS Config	 Amazon CloudWatch	 Amazon GuardDuty	 Amazon Security Centre

Incident management & Governance

Quickly assess your high-priority security alerts and security posture across all your accounts and regions

AWS Security Hub



AWS Systems Manager



AWS IAM access Analyzer



Amazon GuardDuty



AWS Config



Amazon Inspector



AWS Firewall Manager



AWS Health



Amazon Macie

Integrated APN solutions

Continuously aggregate and prioritize based on highlighted emerging trends or possible issues

Conduct automated security checks



Take action

Use cases:

- Conduct automated security checks based on common frameworks
- Integrate systems and automate workflows
- Correlate findings to discover new insights

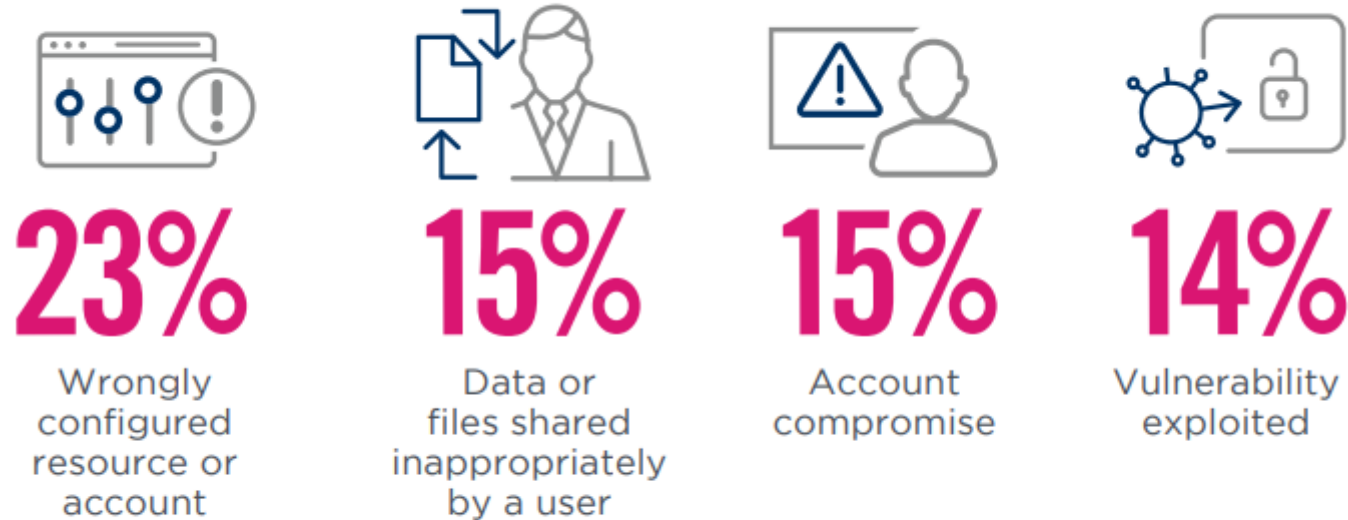
Vulnerability	Description
Poor access control vulnerabilities	This includes people, groups, cloud objects & API's
Misconfiguration vulnerabilities	The dynamic nature of the cloud increases the probability of mis configuration resulting in a vulnerability. This is particularly relevant when DevOps and /or containers are being used to frequently make releases. The ease of access to make changes increases the probability of this happening.
Shared tenancy vulnerabilities	Vulnerabilities created by shared compute resource such as hypervisor, shared kernel in containers, serverless compute.
Supply chain vulnerabilities	The shared responsibility model splits this across either 2 or 3 parties. The customer, the hyperscale vendor and potentially an MSP/partner
Attack vector changes	The extensive use of APIs, complexity of the architecture, and exposure to the internet, ease of access extends the attack vector.
Process	Failure to adapt processes for public cloud creates security vulnerabilities.
Lack of visibility	The lack of cloud specific tools for security reduces visibility.
Lack of cloud security strategy and architecture	The dynamic nature of cloud means that the lack of a strategy & architecture results in a growing number of vulnerabilities and poor governance.
Data Sovereignty/residence	It is not always obvious where data is stored, and therefore who has access to it.

Threats	Description
Malicious insiders	A trusted individual with access to cloud assets that initiates an attack.
Hijacking of accounts	A form of identity theft in which a criminal or other attacker obtains control over a user's online account (normally but not exclusively a financial account)
Denial of service / distributed denial of service attacks	An attempt to shut down a website by targeting it with high volumes of traffic.
Advanced persistent threat groups	Professional cyber criminal groups that work in an organised way to launch attacks.

These are not necessarily cloud specific. The cloud vulnerabilities provide a different set of opportunities to hackers & cyber criminals.

Which incidents are most common

► If yes, what type of incident was it?



Of the 8 listed, 7 are attributed to vulnerabilities

Data or files uploaded to an unsanctioned cloud resource 12% | Malware infection 9% | Data or files downloaded to an unsafe device 9% | Other 8%

This chart is taken from the Checkpoint/Cybersecurity Insiders 2022 Cloud Security Report

Cloud vs on prem security - approach

pillar	Cloud	On prem
IAM	Granular, accounts, landing zone, credentials	Microsoft AD or similar
Detective controls	Tagging, api log, event log, threat & vulnerability detection e.g SIEM	Logs, SIEM
infrastructure protection	security groups, Cloud services	Firewall, appliances, IPS / IDS
data protection	Encryption, backup, availability, Web application firewall,	Encryption, backup, availability,
incident management	Monitoring and incident management	Monitoring and incident management
Process	designed in, automated, auto compliance, IAC, "shift left", devsecops	components added in, manual, manual audit,

Why is cloud security different to on prem?

Vulnerability	Description
Access control	Significant increase in the number of users and components requiring access to an increased number of applications and services.
Misconfiguration vulnerabilities	The ease of access to make changes, the increased complexity and the dynamic nature of cloud services such as microservices increase the probability of misconfiguration.
Shared tenancy vulnerabilities	Does not exist with on prem or private cloud. A successful attack against a client account can be used as a door to other accounts & subscriptions.
Supply chain vulnerabilities	The nature of the vulnerability changes from the hardware and software components to include the hyperscale and other suppliers such as the MSP. The security, deletion and disposal of data is no longer within the total control of the user.
Attack vector changes	Increased complexity is introduced with multiple cloud providers, hybrid architectures, a mix of IaaS, PaaS and SaaS services, the use of microservices and the extensive reliance on APIs. The “perimeter” is considerably extended with this complexity. An increased number of applications are accessed from the internet. This additional complexity, increased application internet access and perimeter extension extend the the potential attack vector.
Skills and processes	These need to adapt and change to accommodate all of the above.
The shared responsibility model	Responsibility for security is shared between user, cloud vendor and any third-parties providing consultancy and managed services.
Ever changing workloads	Cloud workloads are typically highly dynamic being deployed, taken out of service and scaling at a high velocity. This renders traditional security management tools ineffective.
Wide spread adoption of DevOps	Use of DevOps to automate releases creates the need to design security in the code and processes.

Security questions to ask your MSP

	Question
1	How many certified cloud security specialists do you employ?
2	What security accreditations does your organisation hold?
3	What cloud security education and enablement services can your organisation provide?
4	What governance discovery processes do you run?
5	How does your organisation run a cloud security gap analysis?
6	How does your organisation utilise the well architected framework to implement cloud security?
7	What security monitoring and incident management services does your organisation provide?
8	How does your company build security into the DevOps processes?
9	What governance services does your organisation provide?
10	What security services does your organisation provide?
11	What is your strategy for securing for more advanced application design such as containers and functions
12	What elements of the shared responsibility model will you manage?

Key take aways

Implement the 5
pillars

Use the 12
questions

Educate your
people

Think about security
differently

Work with cloud
security certified
experts

Make use of the
cloud specific
security tools

Use your vendors
well-architected
framework

Cloud can, and
should be, as
secure, if not more
so than on prem

Source	content	URL
AWS	Well Architected Framework - Security Pillar	https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/welcome.html
NSA	Mitigating Cloud Vulnerabilities	https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF
BSI	Why your organization needs a Cloud security strategy and how to adopt one	https://www.bsigroup.com/en-US/our-services/cybersecurity-information-resilience/resources/whitepapers/cloud-security-strategy-and-how-to-adopt-one/
National Cyber Security Centre	Cyber Security Consultancy Standard	https://www.ncsc.gov.uk/information/ncsc-certified-cyber-security-consultancy
Tufin	Cloud security white paper	https://www.tufin.com/resources/white-papers
Cloud Security Alliance	Security Guidance	https://cloudsecurityalliance.org/research/guidance/
Cloud Security Alliance	Shared Responsibility Model	https://cloudsecurityalliance.org/blog/2020/08/26/shared-responsibility-model-explained/
Paloalto	Public Cloud Security Overview	https://www.paloaltonetworks.com/resources/guides/public-cloud-security-overview
Software Engineering Institute	12 risks, threats, & vulnerabilities in moving to the cloud	https://insights.sei.cmu.edu/blog/12-risks-threats-vulnerabilities-in-moving-to-the-cloud/
Christophe Tafani-Dereeper Personal tech and security blog about things I like, use, dislike and misuse.	Summary of 2021, information on the danger of static credentials	https://blog.christophetd.fr/cloud-security-breaches-and-vulnerabilities-2021-in-review/
CSRC NIST	NIST framework identify, protect, detect, respond, recover	https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final#
CSRC NIST	NIST framework assessment tools	https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/collaboration-space/focus-areas/risk-assessment/tools

Source	Content	URL
Cloud Security Alliance	CSA cloud controls matrix	https://cloudsecurityalliance.org/research/cloud-controls-matrix/
Cloud Security Alliance	CSA Star levels	https://cloudsecurityalliance.org/star/#tab_levelTwo
CREST	Various white papers & blogs on CREST accreditations & certifications	https://www.crest-approved.org/index.html
CSO online	Top 10 cloud security threats	https://www.csoonline.com/article/3043030/top-cloud-security-threats.html?page=2
Checkpoint	Top cloud security threats	https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-issues-threats-and-concerns/
Secureworks	Cloud security solutions guide	https://www.secureworks.com/blog/cloud-security-guide-to-platforms-threats-solutions
Splunk	Top security threats	https://www.splunk.com/content/dam/splunk2/en_us/gated/ebooks/top-50-security-threats.pdf
2022 state of cloud security report	synk	State of 2022 Cloud Security Snyk