Rethinking security for the cloud

Richard Bartley

Gartner®

Through 2023, at least 99% of cloud security failures will be the customer’s fault.

Overview

- Redefining Security Architecture for Cloud
- A deeper look at IaaS Security capabilities

Redefining Security Architecture for the Cloud

Business Challenges

Elasticity, Flexibility and Scalability

Continuous Improvement and Continuous Development

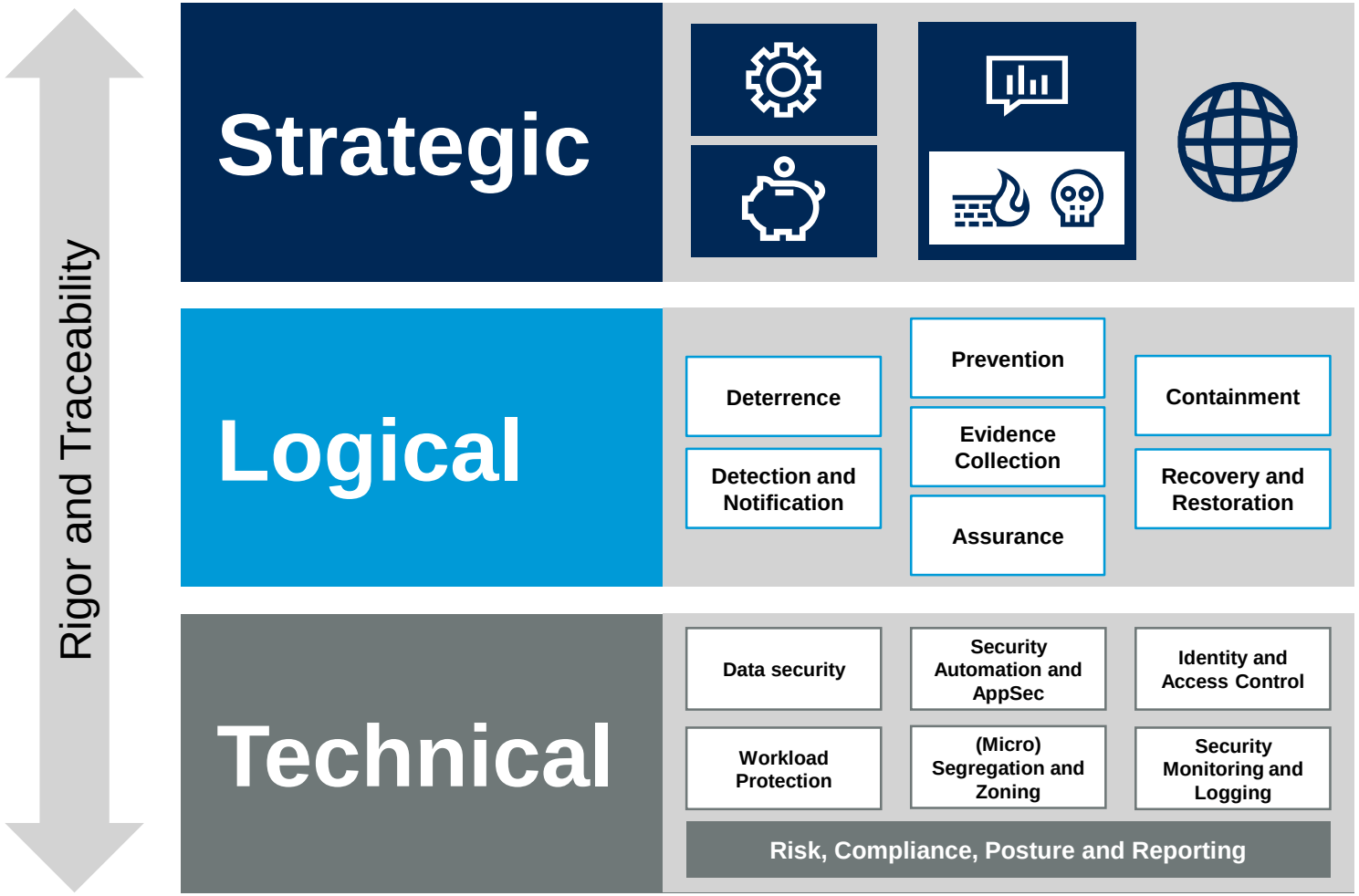
Automation and DevSecOps

Business Transformation

Technology Enablement

Creating Architecture to Respond to New Challenges

- Moving from business needs to logical security capabilities
- Cloud realities for security
- Design principles and cloud security decisions
- Assuring layered defenses



PUBLIC

Gartner

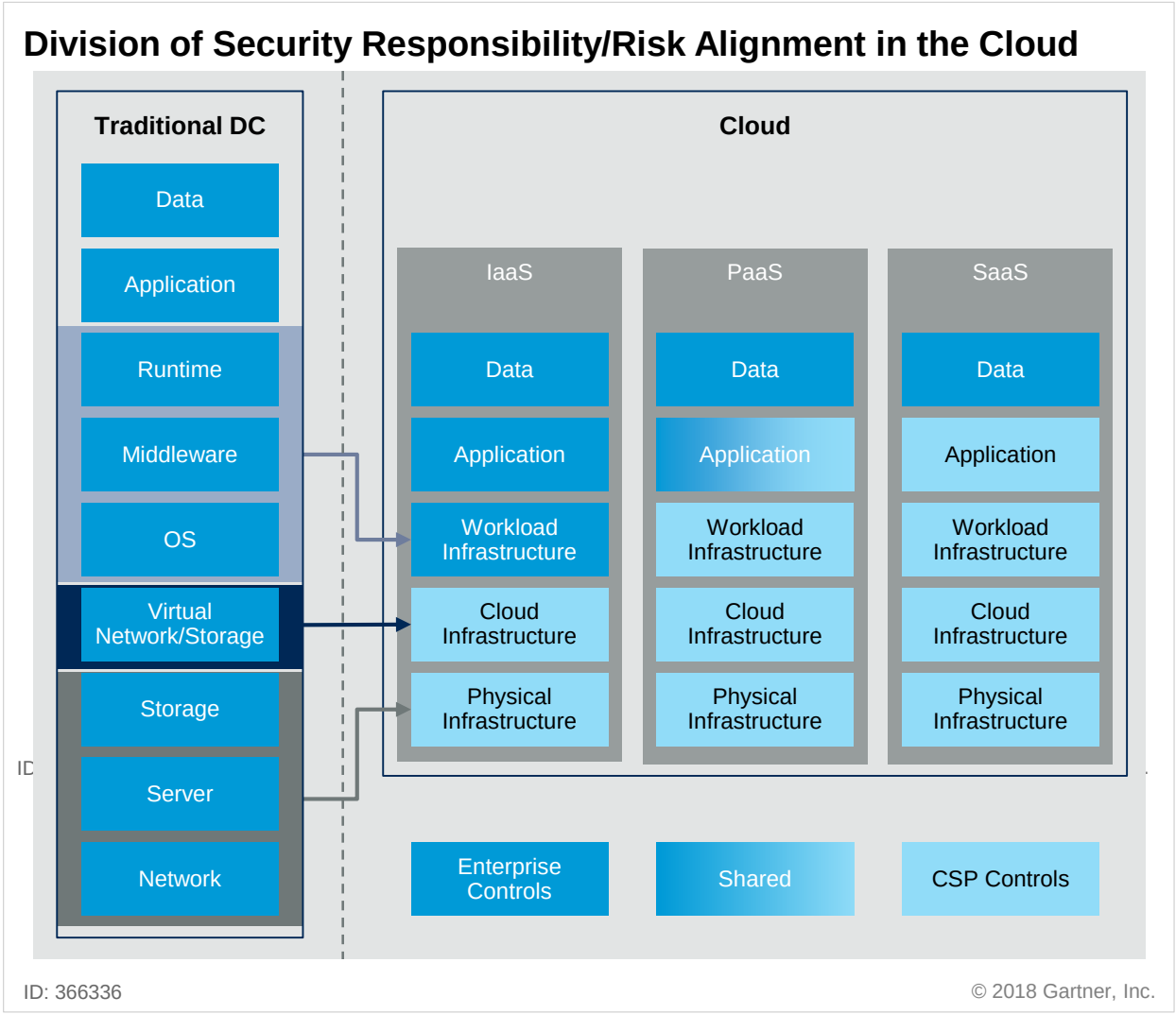
Cloud Realities Architects Must Navigate

- Logical security architecture and business context lay down the requirements for the security services and components we need to deploy.

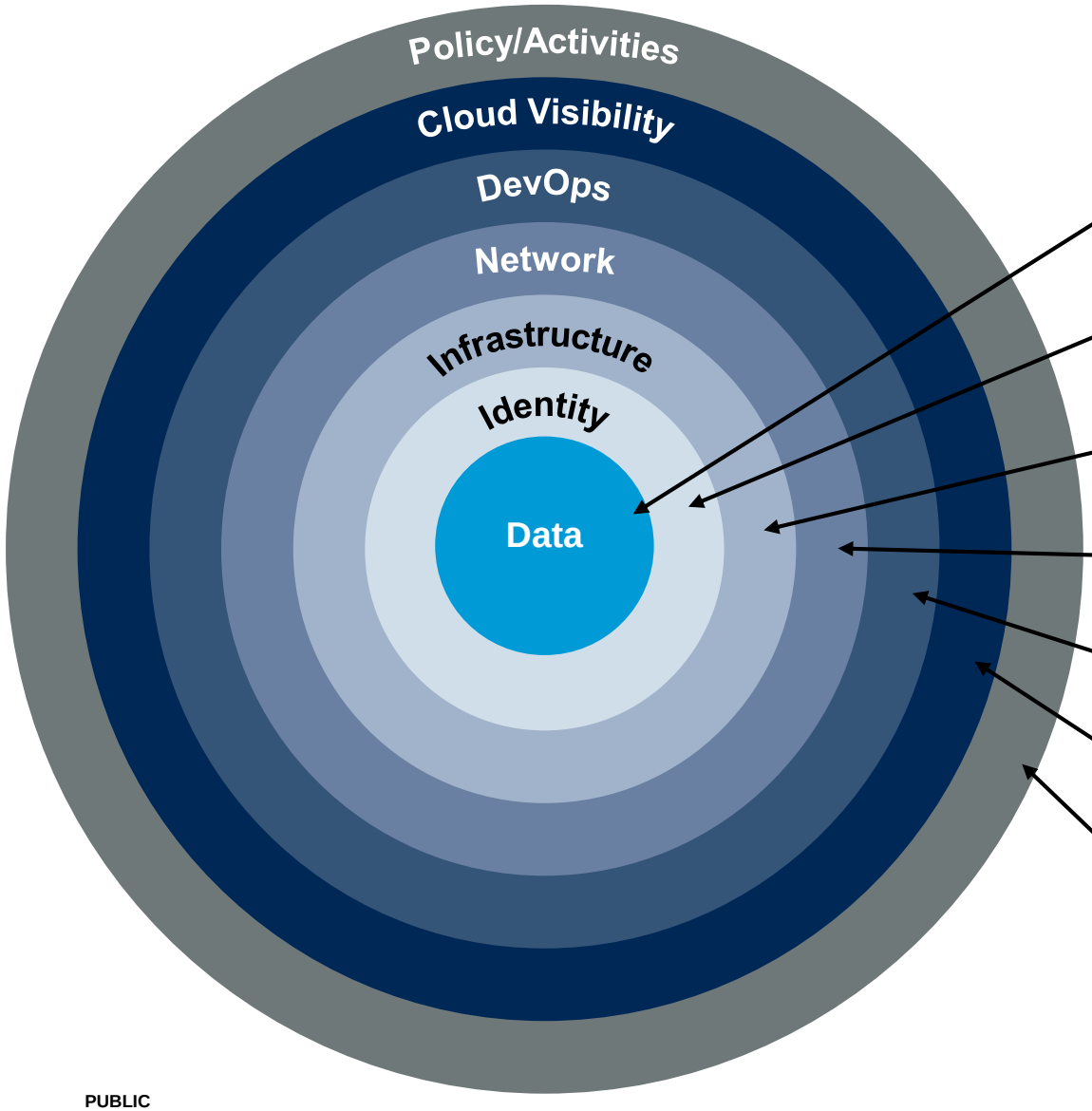
Existing controls brought into the cloud	Cloud provider native tools	New cloud third-party vendor controls
• Firewalls • IPS • Endpoint protection • Server monitoring • EDR • SIEM	• Threat monitoring • Workload security • User behavior monitoring • Compliance • Risk management	• CWPP • CSPM • CASB • Micro-segmentation • CDN

- But how do you work out what is best for you?

Understand Separation of Responsibilities



Stacking Your Technical Defenses



Data security — Encryption, Masking, Data Loss protection, Behavior, CASB

Privileged Identity Management, Cloud Access Control, Behavior Monitoring and Analytics

Infrastructure and Workload Security, CWPP

Native Network and Zoning, Interconnect, Micro-Segmentation Tools, WAF

Security Automation, Application Security Controls and Testing

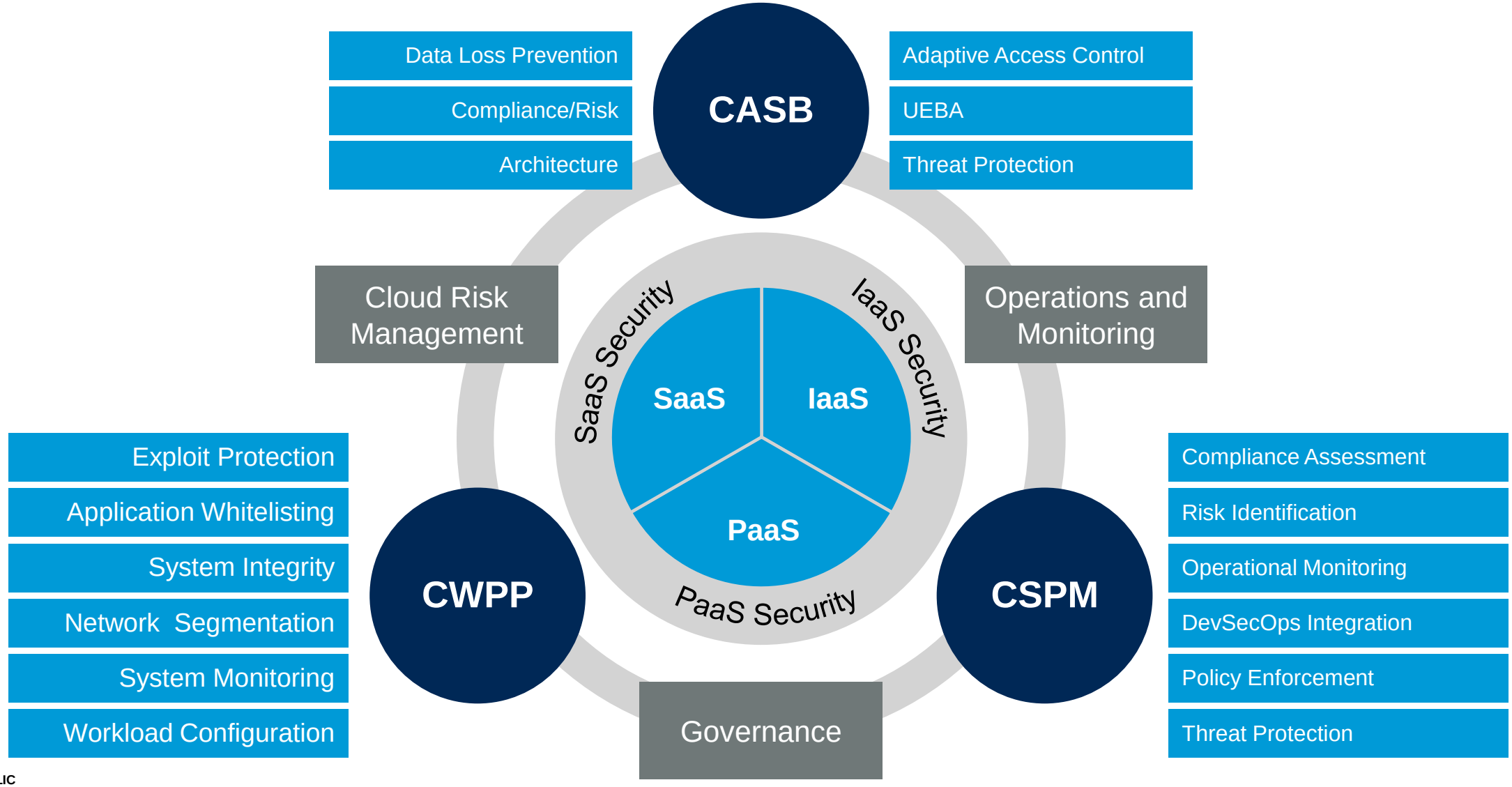
Native Monitoring and Logging, CSPM, SIEM

Native Compliance tools, CSPM — Posture and Reporting

PUBLIC

Gartner

Augmenting Native Controls With Vendor Products



PUBLIC

Key Cloud Technical Security Architecture Principles

- You should assemble a set of design principles to help with assigning security components, tools and services.

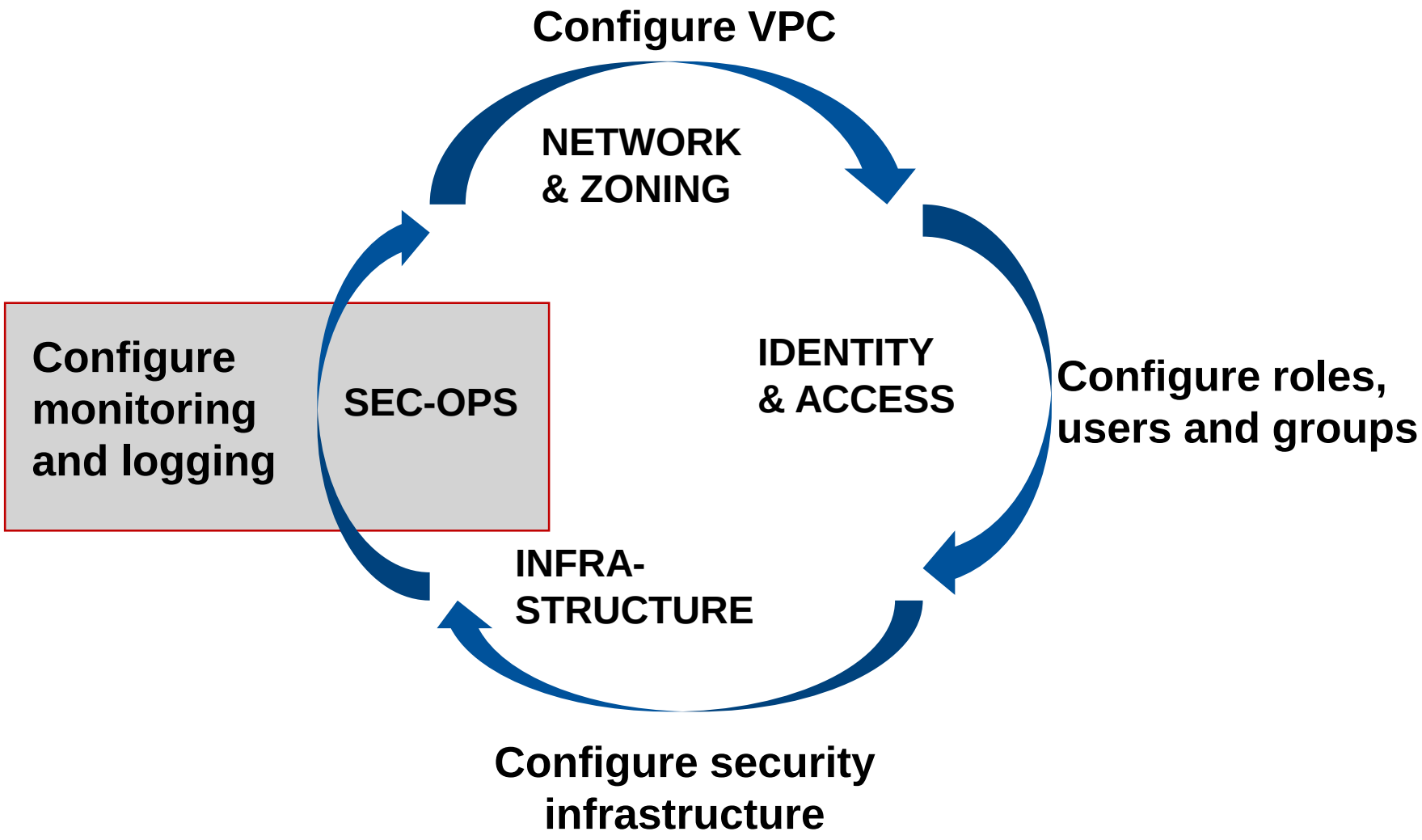
Use on-prem. capability?	Only select where the vendor has explicitly implemented tools fully compatible with your cloud.
Use cloud native tool?	Take a native-cloud security tools-first approach
Use cloud security vendors?	Choose these when native-cloud doesn't meet your requirements.
Do you have multicloud needs?	Choose vendor tools covering all your cloud environments over numerous point solutions.
Can we automate?	Maximize all opportunities to automate security component deployment and operation.

Recommendations

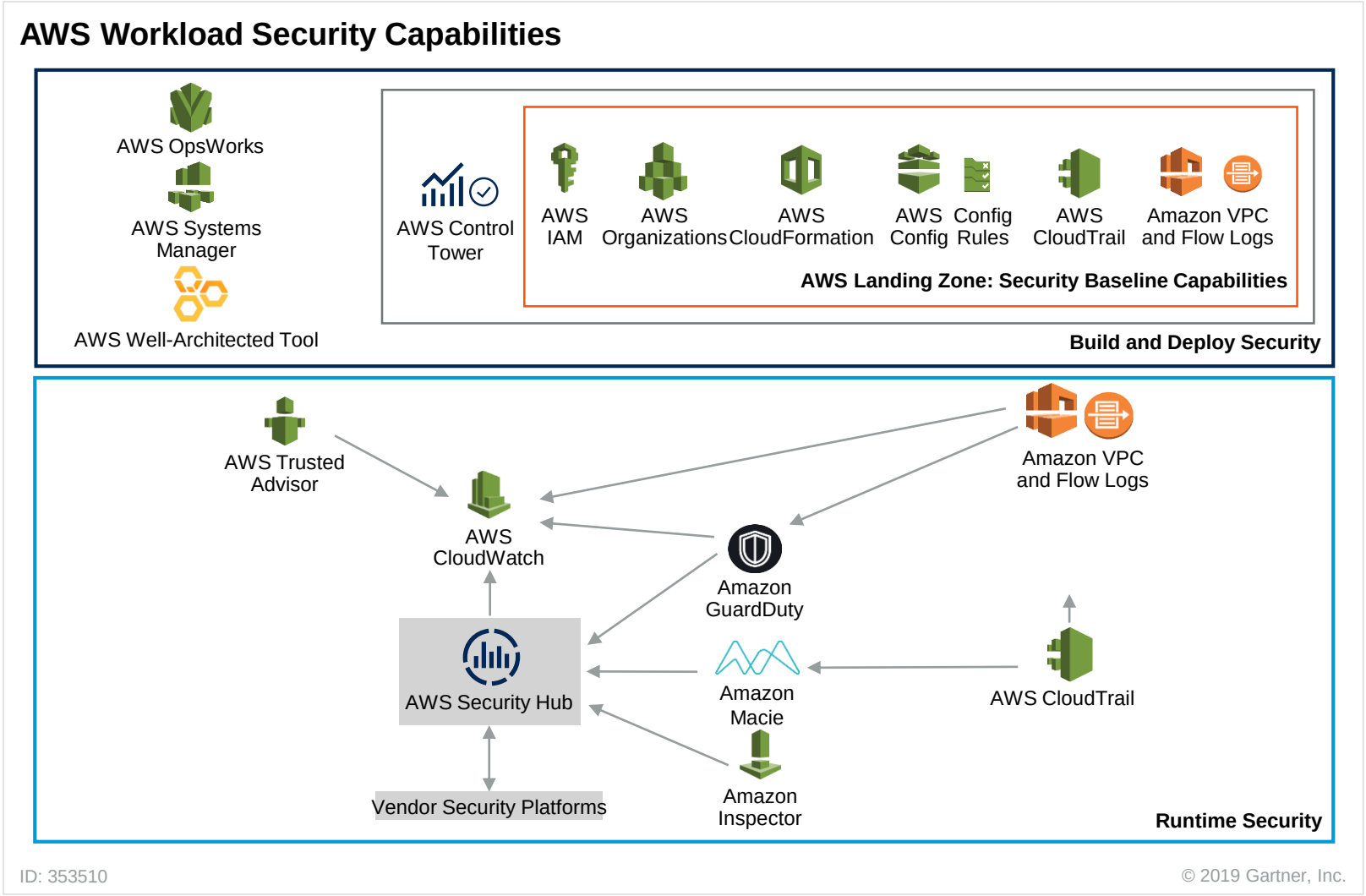
- Develop an enterprise cloud strategy, including guidance on what data can be placed into which clouds and under what circumstances.
- Implement and enforce policies on cloud ownership, responsibility and risk acceptance by outlining expectations for control of cloud use.
- Build processes to review security architecture, beginning periodically and moving to continuous review, to ensure that emergent risks because of changes to business, technology or the threat landscape are addressed.

A Deeper Look at IaaS Security Capabilities

Steps towards cloud security implementation

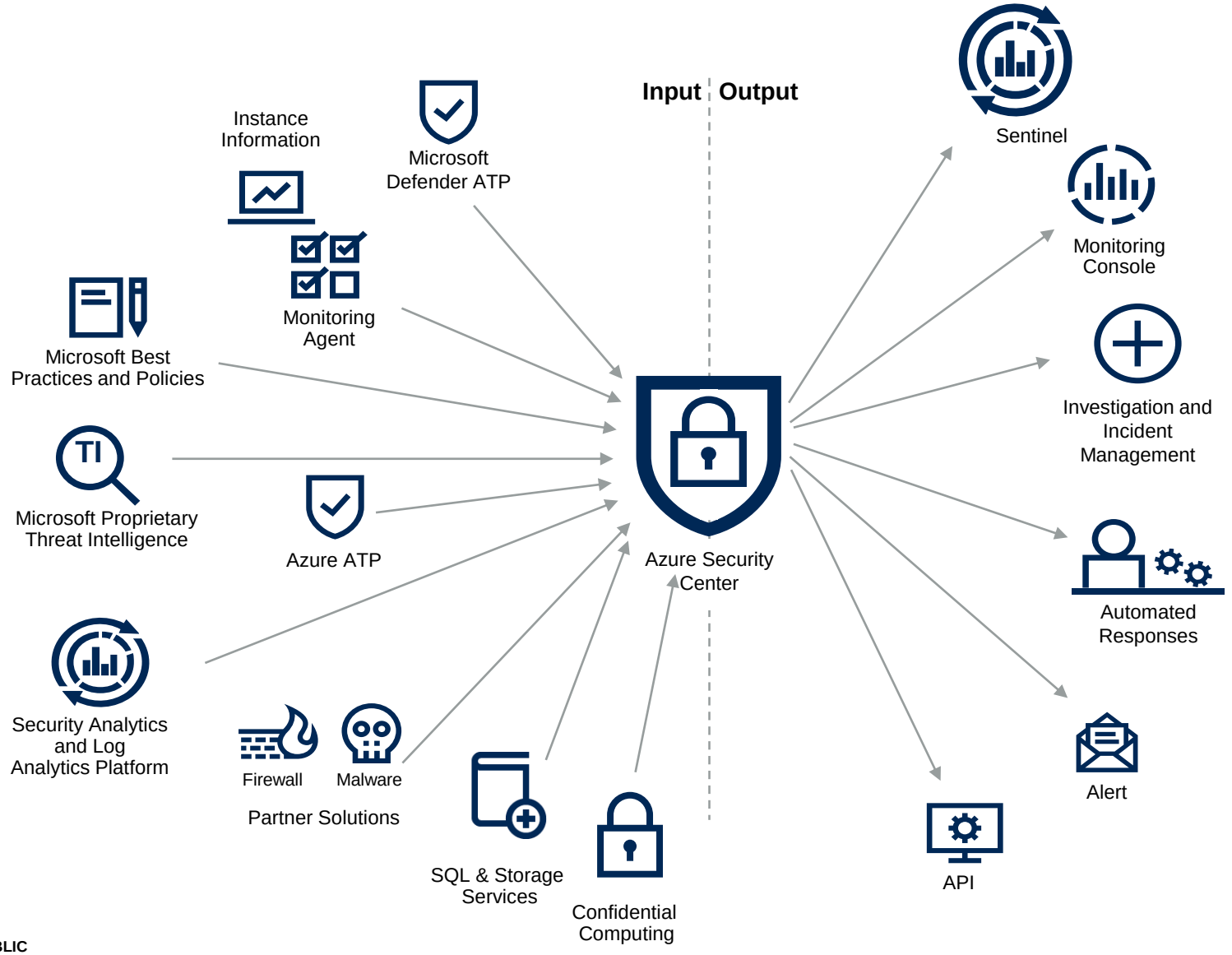


AWS Monitoring & Deployment



- AWS Landing Zone & build tools help deploy securely and repeatedly.
- AWS Security Hub fronts sensors for:
  - System vulnerabilities
  - Discovering and monitoring sensitive data
  - Monitoring for threats

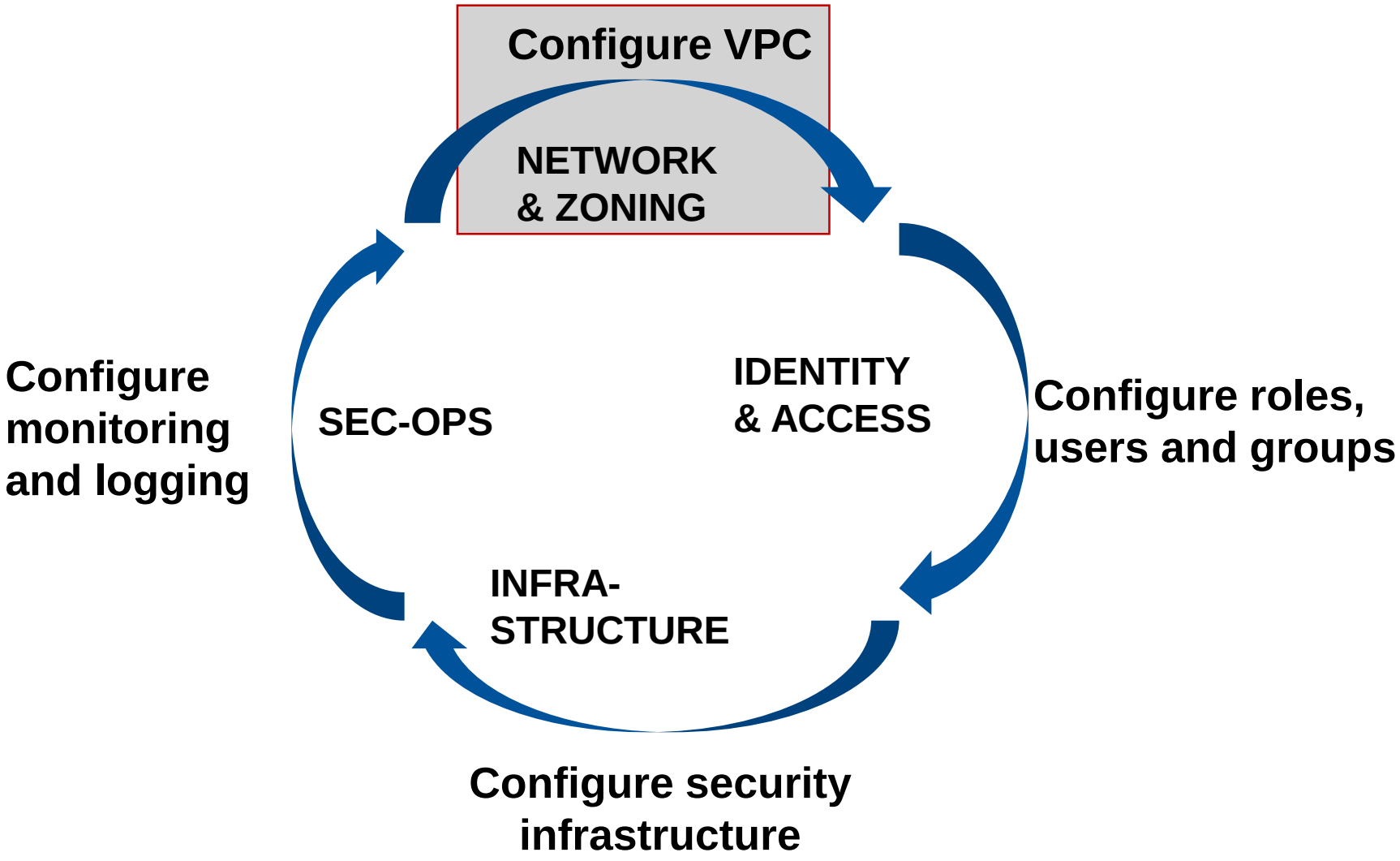
Microsoft Azure Security Monitoring



- Build securely with Azure Blueprints and Automation
- In-workload protection with Microsoft Defender ATP
- Threat monitoring
- Compliance and monitoring services through Azure Security Center

Gartner

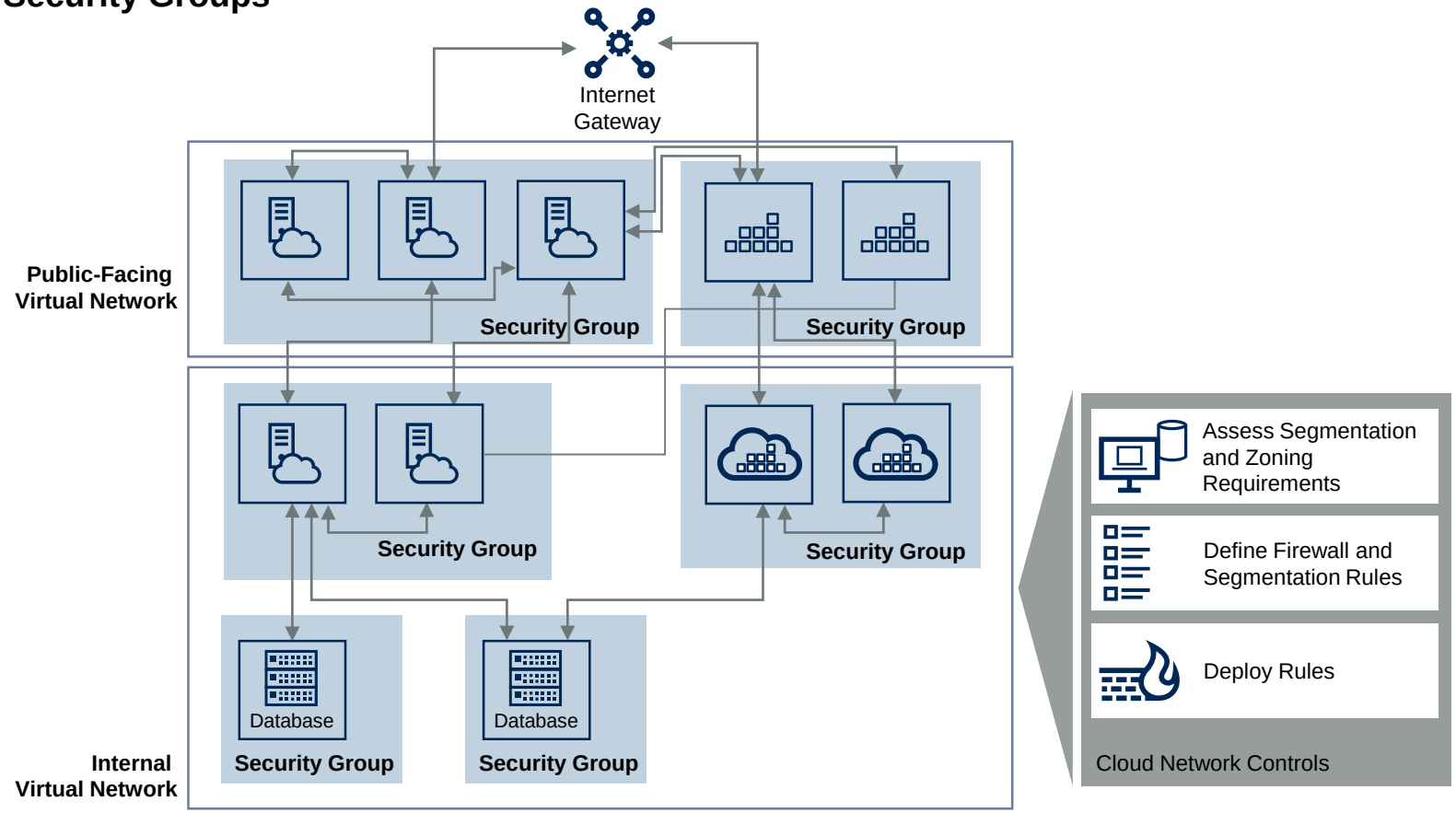
Steps towards cloud security implementation



Network Firewalling

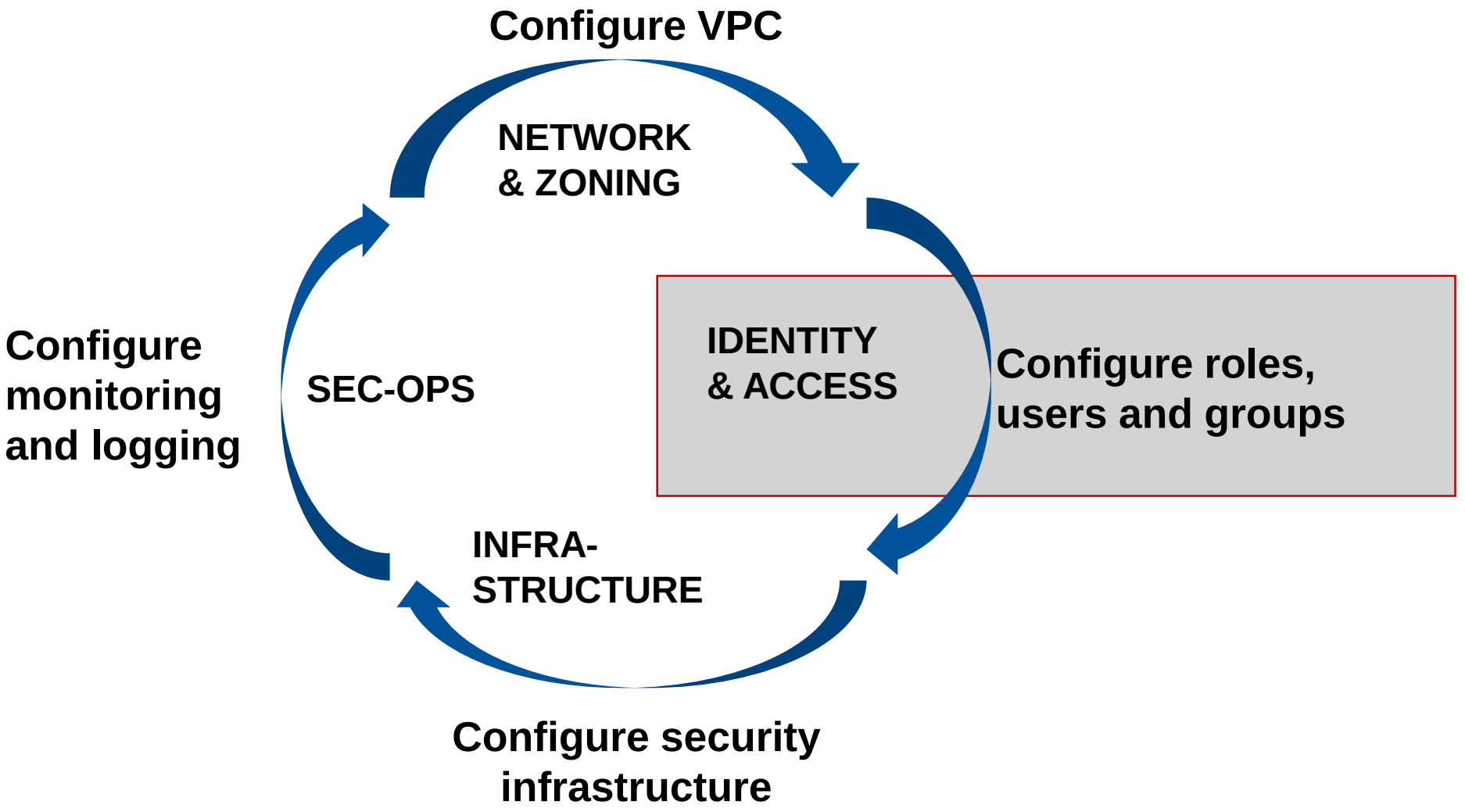
- VNets & VPCs provide coarse controls.
- (Network) Security Groups and Firewall rules provide much finer grained.
- Some cloud providers offer Layer 7 - type controls

Network Firewalling and Segmentation Example Using Virtual Networks and Security Groups



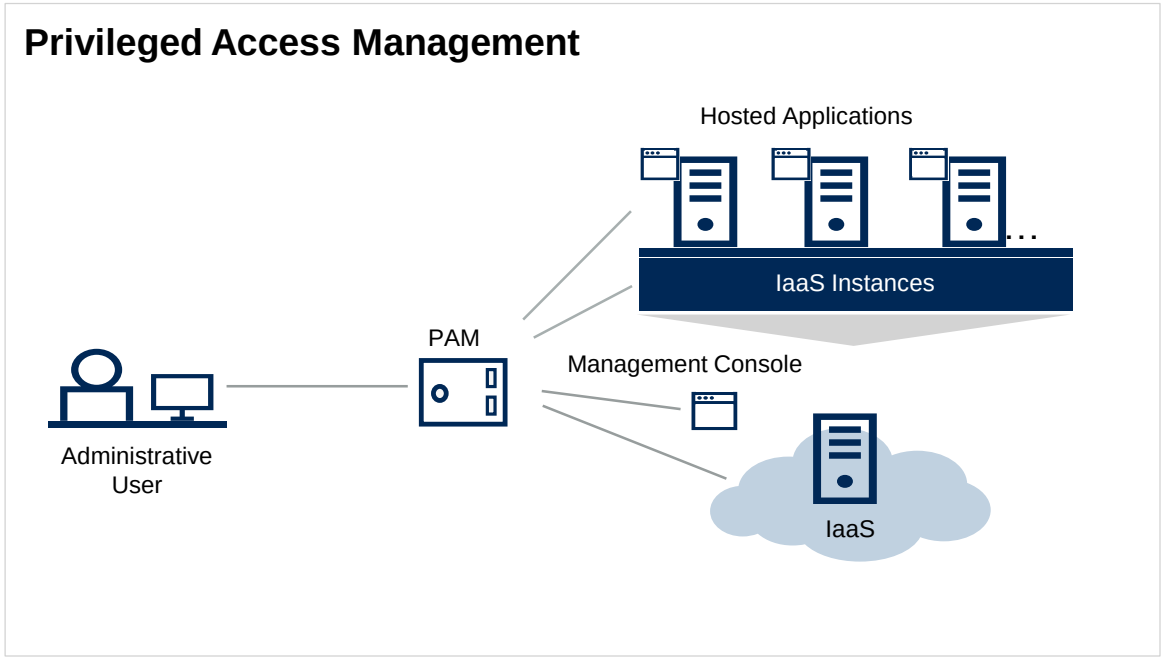
PUBLIC

Steps towards cloud security implementation



Cloud Identity and Access Controls

- Use native IAM tools to ensure privileged accounts are highly secured (e.g., hardware MFA etc.).
- Use curated IAM roles with services like AWS Landing Zone, and Azure Security Blueprints, to help you get off the ground securely, and repeat!



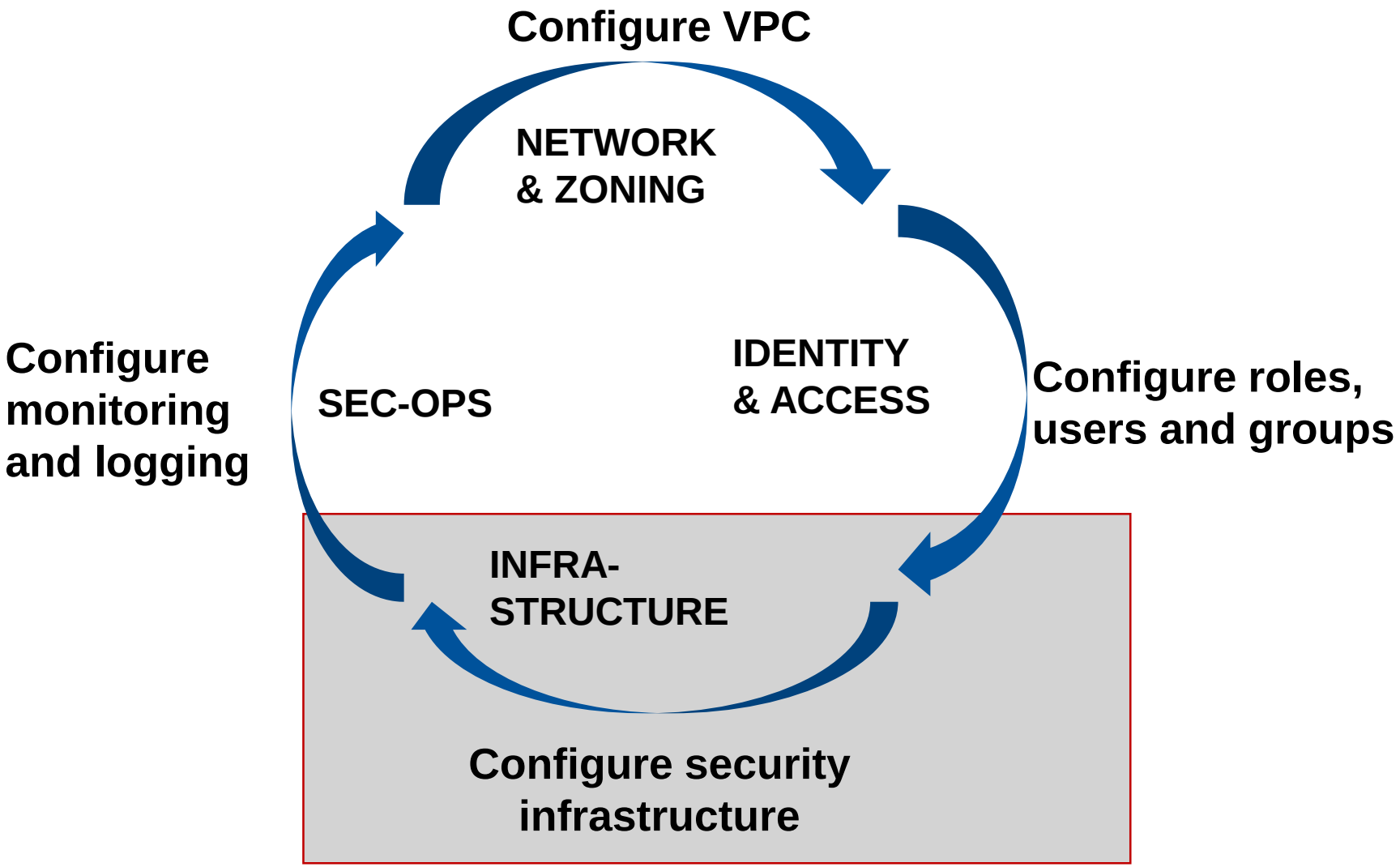
AWS IAM

AWS Organizations

Google Cloud Platform IAM

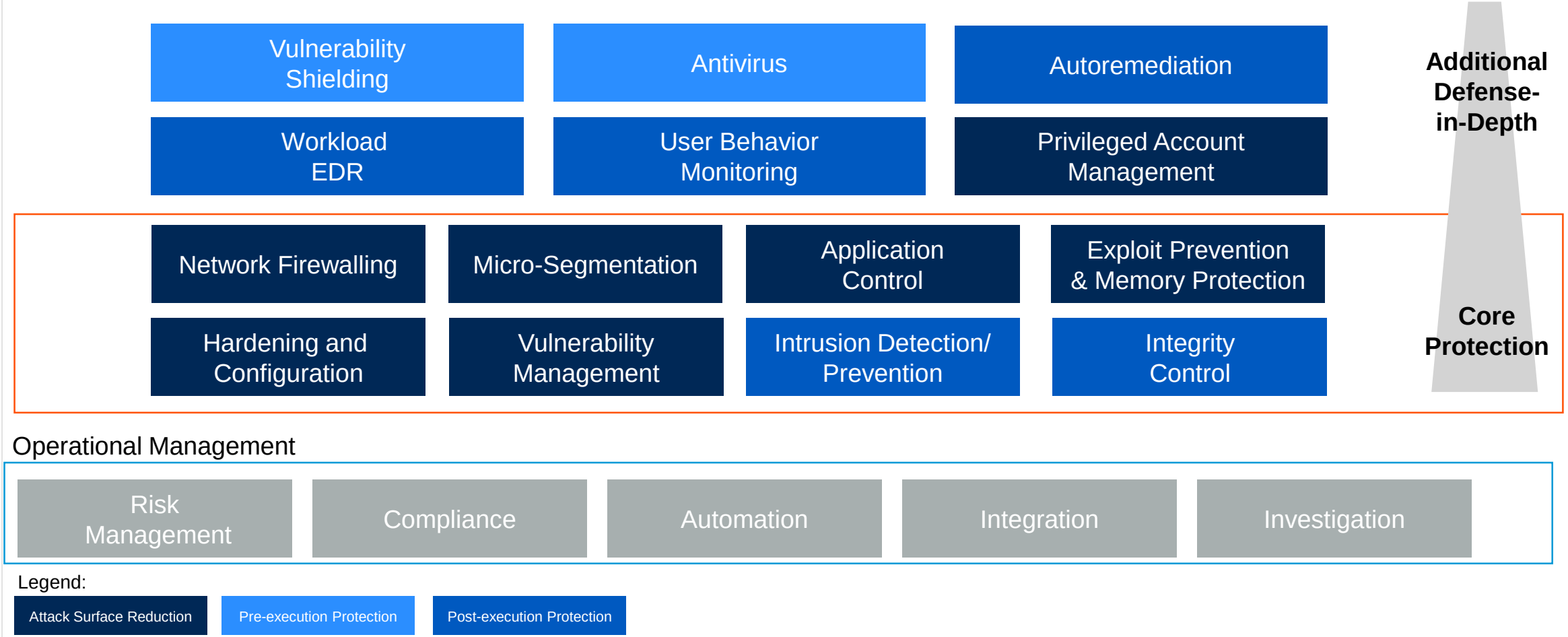
Azure Active Directory

Steps towards cloud security implementation



Workload security capabilities

Core and additional defense-in-depth controls



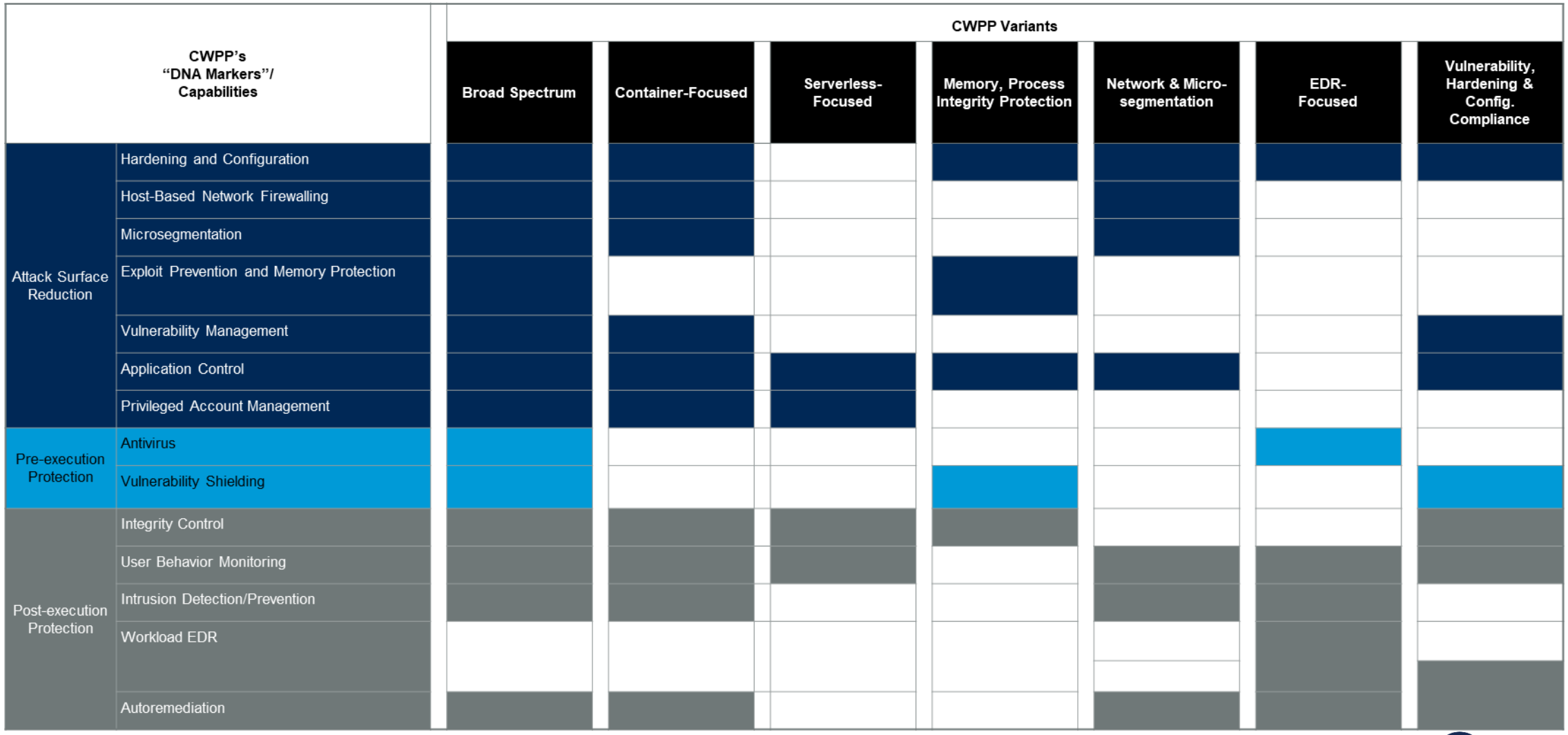
PUBLIC

Why use a third party CWPP tool?

- When cloud / hosting providers do not provide workload protection
- Tighter control over workloads than the cloud providers offer.
- Increased workload visibility and behavior monitoring
- Reduce unauthorized east-west traffic
- Richer set of defense-in-depth capabilities

CWPP Variants and their “DNA”

“DNA Marker” Analogy Diagram Showing CWPP Variants and Their Minimum Capabilities



Gartner®

CWPP Vendors in Variant Categories

Key strengths of vendors, but keep in mind many vendors have additional value added capabilities.

Broad Spectrum
Atomicorp
Bitdefender
Carbon Black (Protect)
CloudPassage
Kaspersky Lab
McAfee
Microsoft (Defender ATP)
Qingteng (China only)
Sophos
Symantec
Trend Micro
VMware

Memory & Process Integrity Protect
Morphisec
Palo Alto Networks TRAPS
Polyverse.io
Virsec

Container Focus
Aporeto
Aqua Security
Qualys (Layered Insight)
NeuVector
Twistlock
StackRox
Sysdig

Serverless Focus
Nuweba
Protego Labs
PureSec

EDR based
Capsule8
Carbon Black (Defend)
CrowdStrike
Lacework
ThreatStack

Network & Micro-Segmentation
Alcide
Aporeto
Cisco
Edgewise
Guardicore
Illumio
Truefort
Zshield (China only)

Vuln, Config & Hardening
CloudAware
Cloud Raxak
HyTrust
Security Code
Tripwire
Turbot

Gartner®

Why buy a third party CSPM service?

- Multicloud demands, single management console.
- Compliance requirements – demonstration of continuous compliance to specific standards / frameworks.
- Coverage of more tests than native services offer.

Gartner

Cloud Security Posture Management Capabilities

Cloud Security Posture Management

- Identification & Discovery
- Compliance Assessment
- Operational Monitoring
- Visibility & Policy Enforcement
- DevOps Integration
- Threat Protection
- Risk Identification
- Risk Assessment vs. Frameworks
- Verifying Operational Security

AWS Security Hub	Google Cloud Security Command Center	Azure Security Center
Cloud Subscription	**Cloud Subscription**	**Cloud Subscription**

CSPM Vendorspace

CASB vendors with CSPM

bitglass

ORACLE

netskope

McAfee

Symantec

paloalto NETWORKS

CWPP vendors with CSPM

Cloudware

SOPHOS

CloudPassage

CROWDSTRIKE

threat stack

CLOUDVISORY

CSPM Only Vendors

ALERT LOGIC

bmc

Caveonix

cavirin

Check Point SOFTWARE TECHNOLOGIES LTD.

Cloud Conformity

cloudneeti

LACEWORK

Cloud Checkr

CLOUDNOSYS

sonraí SECURITY

SAVIYNT

vmware

turbot

Fugue

DivvyCloud

Outpost24

Gartner

Where can native tools support DevSecOps?

Cloud Workload Security and CI/CD Activities

Deploy

Automated Secured Configuration for Runtime and Cloud Native Security Agent Deployment

Runtime

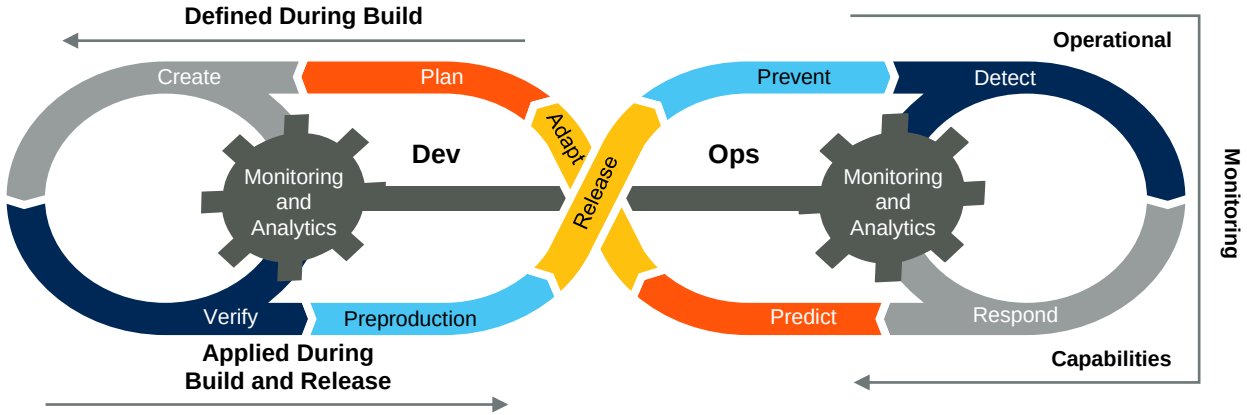
Workload Protection Services in Place:

- Integrity Control
- Configuration
- Application Control
- User Behavior Monitoring
- Workload EDR
- Intrusion Detection/ Prevention
- Exploit Prevention/ Memory Protection
- Vulnerability Shielding
- Anti-Virus

Build

Workload Image Scanning — Seeking to Identify Possible:

- Malware
- Vulnerabilities
- Nonhardened Configurations



Remediate

Automated Remediation Is Generally Customized Configuration, but Can Be:

- File Removal/Isolation
- Network Traffic Isolation
- Process/Application Isolation

Response

Automated Behavior Detection Initializes Alerts to Cloud Security Center Management Services

Investigate

Automated Support for Investigation Can Include:

- Security Center-Type Services to Provide Drill-Down Into Issues
- Tools for Decision Support for Mitigation Options

Gartner

Recommendations

- Follow your architectural principles – Cloud tools first, only bring on-premises tools if they suit your requirements and are compatible
- Remember cloud service providers new tools are disrupting these markets. Test out the native security management and workload security tools to see whether they can meet your requirements.
- Use 3rd party vendor CWPP to augment workload security above native control capabilities to fulfill enhanced requirements for visibility and protection.

Client Case Studies

Alert Logic used Cloud for their Security-as-a-Service

Opportunity

- Alert Logic wanted a powerful and secure cloud system to store and analyze data for their Security-as-a-Service Solutions.

Cloud Business Actions

- Alert Logic moved its Security-as-a-Service solutions to AWS.
- Alert Logic used Amazon S3 for its security-as-a-service solution and migrated all of their user data from their data centers to AWS centers.
- Alert Logic tested the scale of AWS with 100 times more than the current production load of the company.

Results

- Reduced cost of footprint by more than 50%.
- Performance of applications and data security improved as per customers.

Increased Productivity & Engagement	NexGen Products and Services	New Business Model	New Competitors	Reduce Capex

Use Case Publish Date: 06 Mar 2018

Gartner

Vodafone Italy enhanced Top-up functioning and secured client data using cloud

- Opportunity
  - With increasing client base Vodafone Italy wanted to deploy a secure and reliable system to facilitate Credit and Debit Card top-ups.
  - Required Flexible infrastructure to scale to meet demand.
- Cloud Business Actions
  - Used Amazon EC2, Amazon Virtual Private Cloud, Amazon Elastic Book Store, Amazon Simple Email Service to introduce Topup without Login.
  - Amazon S3 was used to store approximately 25 GB of log copy and static web content.
- Results
  - Full compliance of PCI-DSS rules for online payment system.
  - Reduction of Capital Expenses by 30%.
  - 99.99% increase in availability, leading to greater satisfaction level of customers.

Increased Productivity & Engagement	NexGen Products and Services	New Business Model	New Competitors	**Reduce Capex**

University of New Hampshire uses cloud to support network Demand & Security

University of New Hampshire

vmware

Business Challenge

- UNH IT Team wanted a scalable solution for their growing demand for network and security. They also wanted to reduce power and cooling needs.

Business Actions

- UNH chose VmWare NSX network virtualization platform for their software defined networking.
- University consolidated 500 physical servers to 80 and runs several thousand virtual machine workloads.
- Echostor Technologies helped UNH to understand the virtualization technologies. UNH now deploys all new networks and security services with VmWare NSX.

Business Impact/Results

- Reduced deployment time from months to days.
- Reduced Spending cost on network infrastructure, power and cooling.

Increased Productivity & Engagement	NexGen Products and Services	New Business Model	New Competitors	**Reduce Capex**

Use Case Publish Date: Oct 2016

Gartner