CLOUD SECURITY

Risks, remediation & resilience

Ramkaran Rudravaram

2019

Global Azure BOOTCAMP

VALUEMOMENTUM.AZUREBOOTCAMP.NET

APRIL 27, 2019

Cloud security

Agenda - RISKS, REMEDIATION & RESILIENCE

Security issues

threat modeling

threat Profiles

Steganography

Security controls

compliance

privacy protection

cloud governance

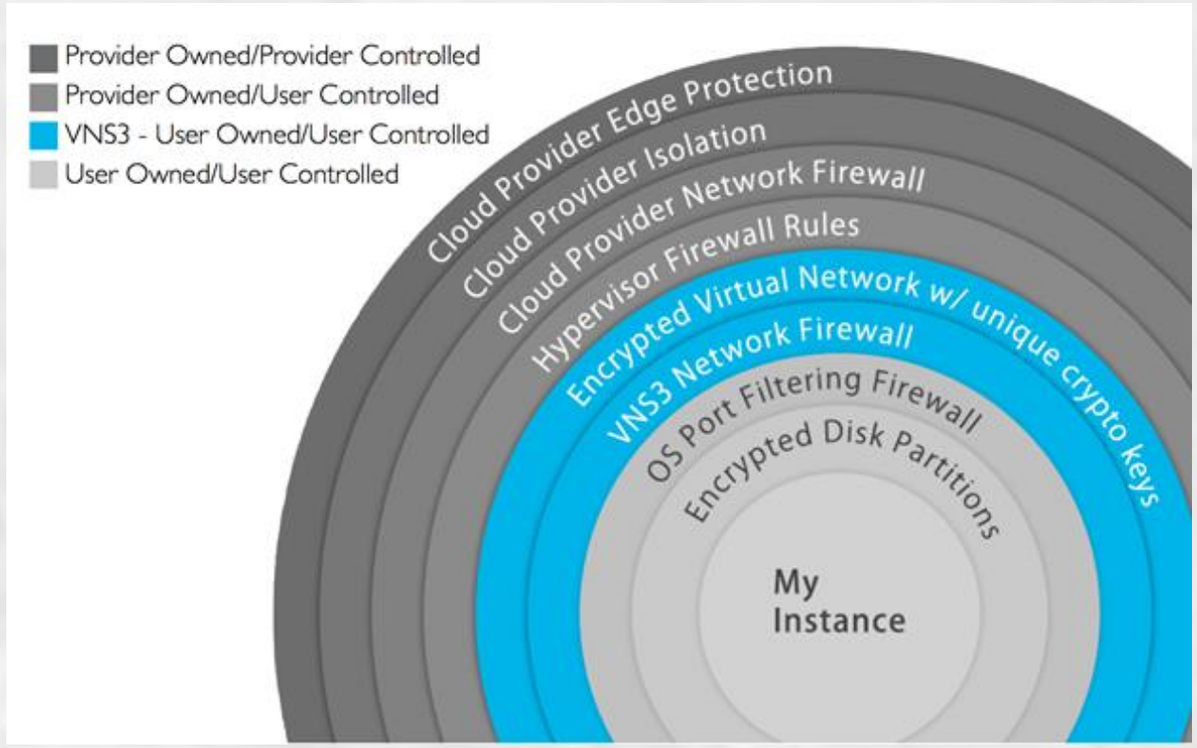
Encryption

Cloud security

RED PILL or BLUE PILL

VISION FOR a Cloud security model

Feeling secure



being Secure

Holistic Model

Harmony..Proportion..Synthesis..

Credits: Bruce Schneier

Cloud security

Agenda - RISKS, REMEDIATION & RESILIENCE

Security issues
threat modeling
threat Profiles
Security controls
compliance
privacy protection
cloud governance

- Application
- Network & System Security Tiers
- Secure Operations
- Data Security
- Cloud Security Optimization
- Security Metrics
- Governance
- Identity & Access Management

Cloud security

KEY CONCEPTS

CONFIDENTIALITY

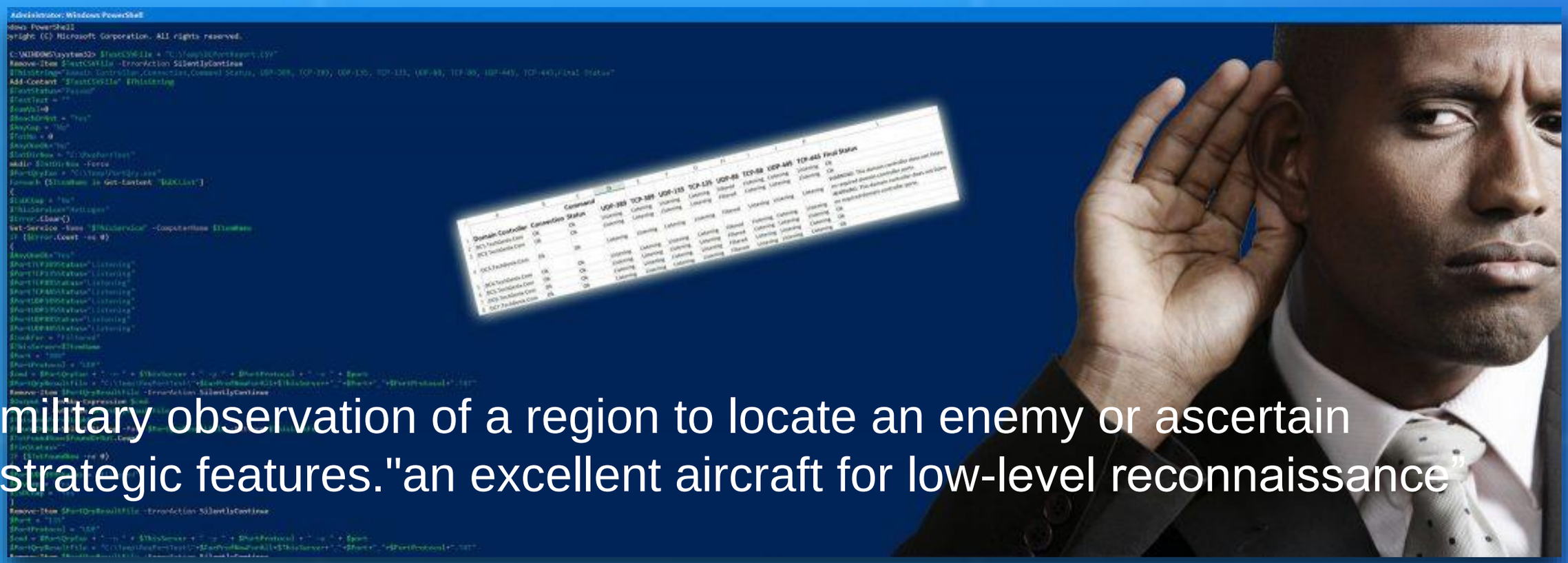
INTEGRITY

AVAILABILITY

" IT'S A FINE LINE BETWEEN SECURITY AND PARANOIA."

Cloud security

Reconnaissance



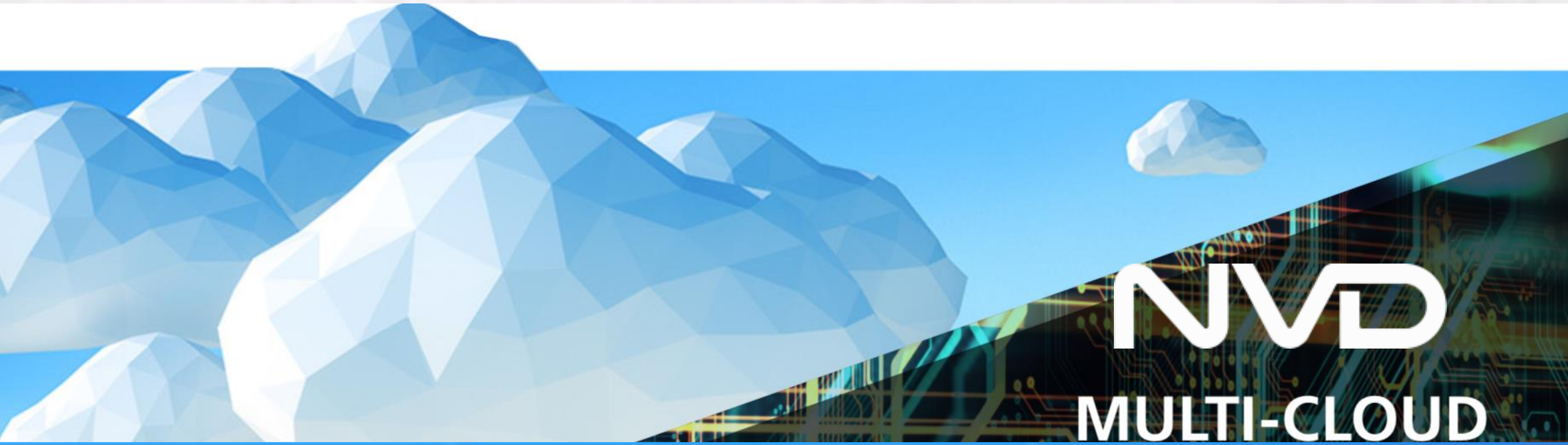
Credits: Techgenix

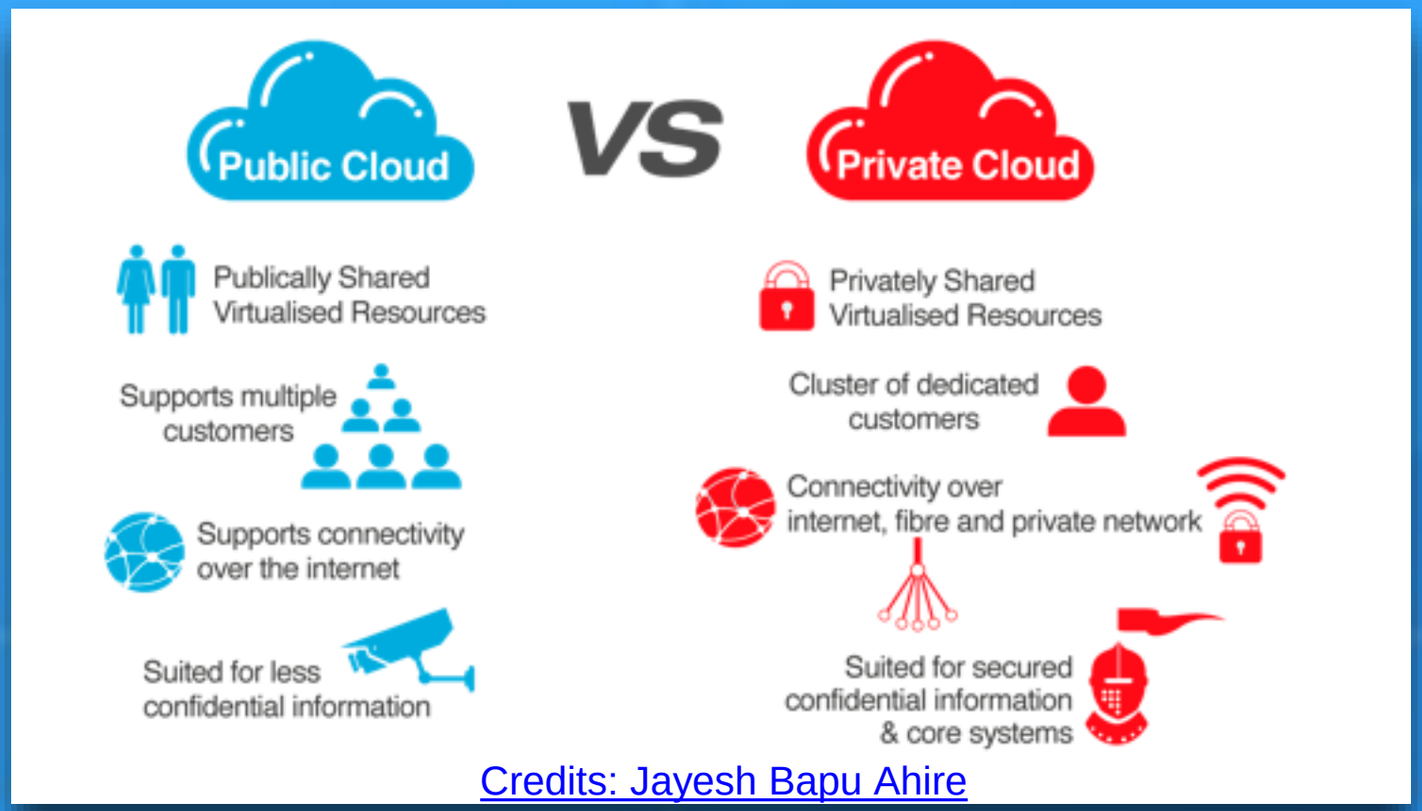
1. preliminary
   survey, survey, exploration, observation, investigation, examination, inspection, probe, scrutiny, scan; patrol, search, expedition; reconn oitring, scouting (out), spying out; informal: recon, recce, shufti
2. ”He took some marines to make a reconnaissance of the island”

OBSERVE.. RECORD.. TRACE…

Cloud security

Keep an Eye on VULNERABILITies





Credits: Jayesh Bapu Ahire

National Institute of Standards and Technology
U.S. Department of Commerce

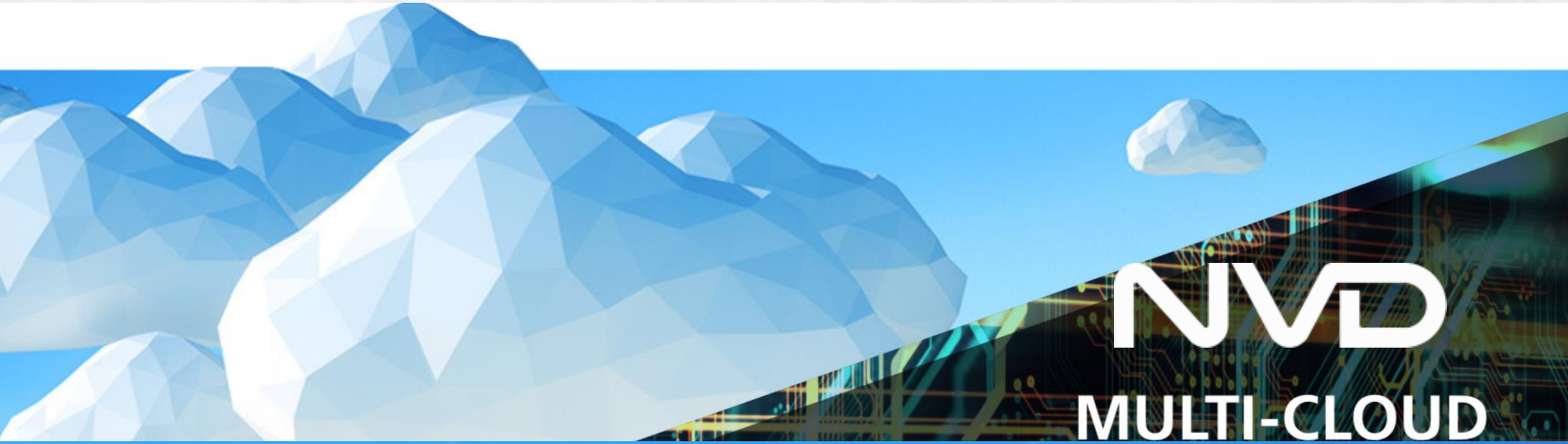
TRUST {PROVIDER}

TRUST {USERS}

TRUST {API/SaaS}

Cloud security

Protect ASSETS



National Institute of Standards and Technology
U.S. Department of Commerce

PROTECT ASSETS

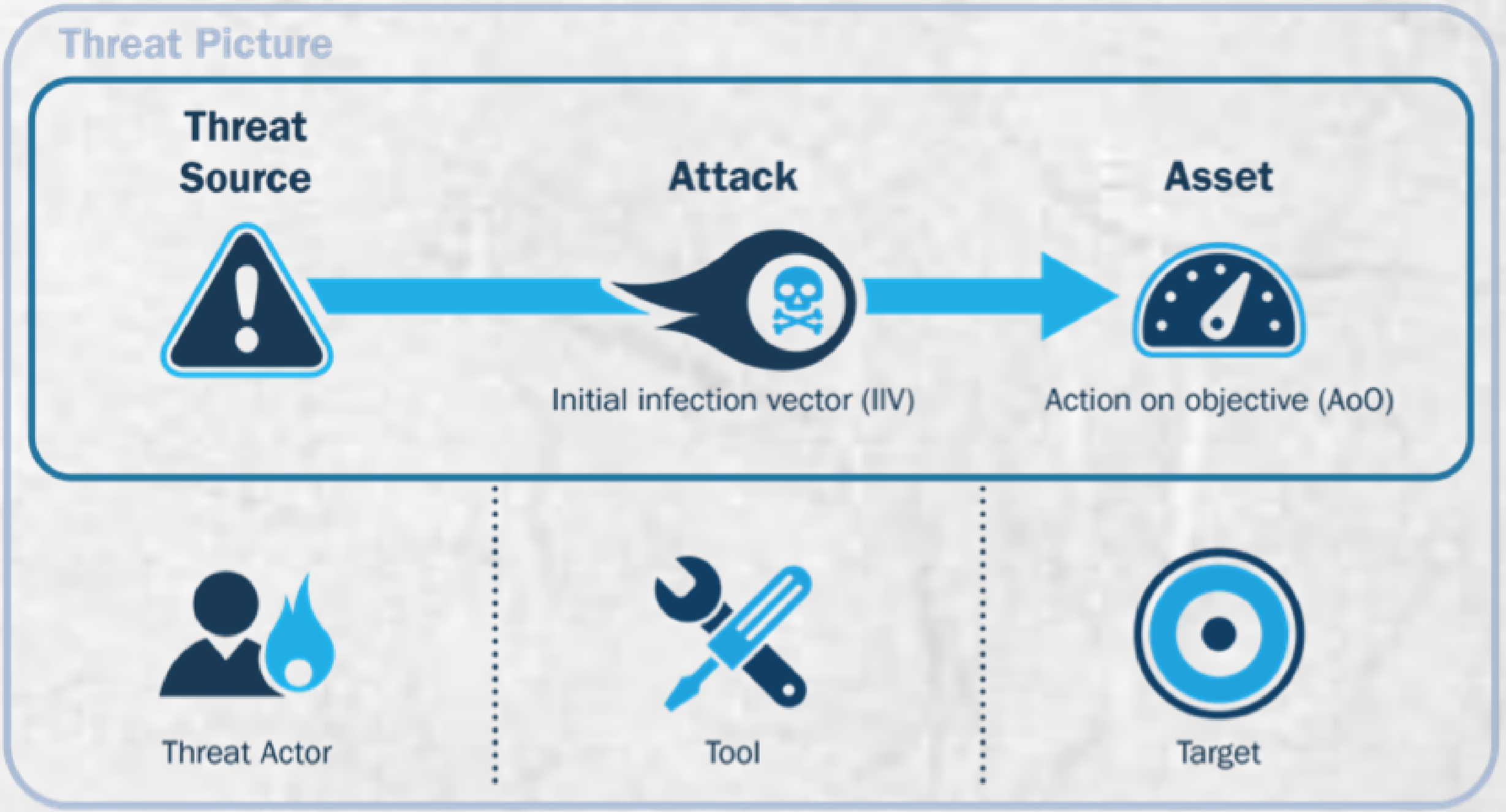
Encrypt

ENCAPSULATE

ENFORCE ACCESS policy

Cloud security

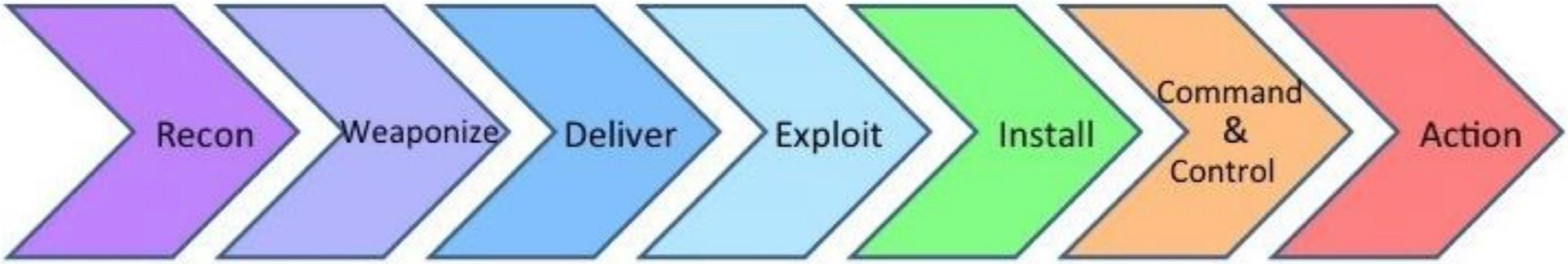
Anatomy of threat



Credits:Timothy Morrow-CMU

Cloud security

Intrusion KILL CHAIN



Source: Lockheed Martin

Recon - observe, Record, TRACE

Weaponize - create dangerous payload & Entice..

Deliver - Drop it in Target environment

Exploit - take advantage of known Vulnerabilities

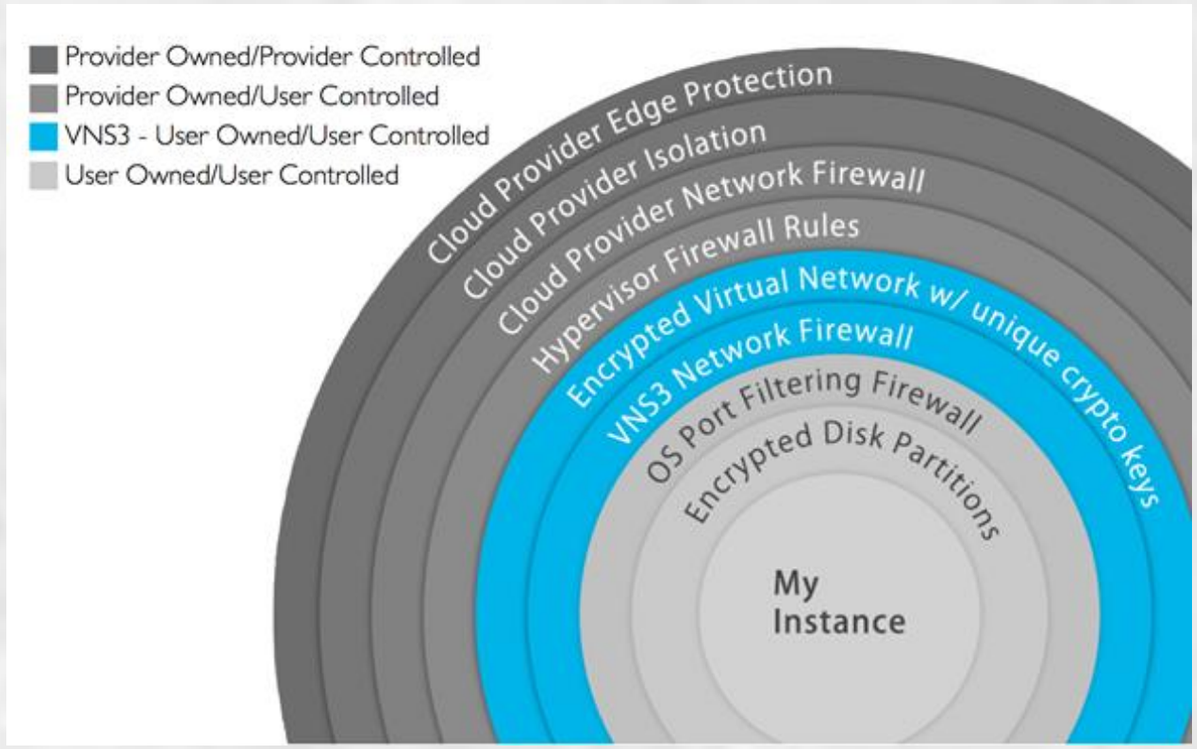
Install - payload operational on threat source

C & C - Two-way Comms with command & Control Infra

Action: Exfiltrate Assets - Data, Programs etc..

VISION FOR a Cloud security model

Feeling secure



being Secure

PROMOTE CLOUD ADOPTION

BACK TO SCHOOL: Cloud??

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 500-291

3 - Service Models - SaaS, PaaS, IaaS

4 - Deployment Models - Pvt, Public, Community & Hybrid

5 - Essential Characteristics

Network Access, Elasticity, Resource Pooling, Metering, Self-Service

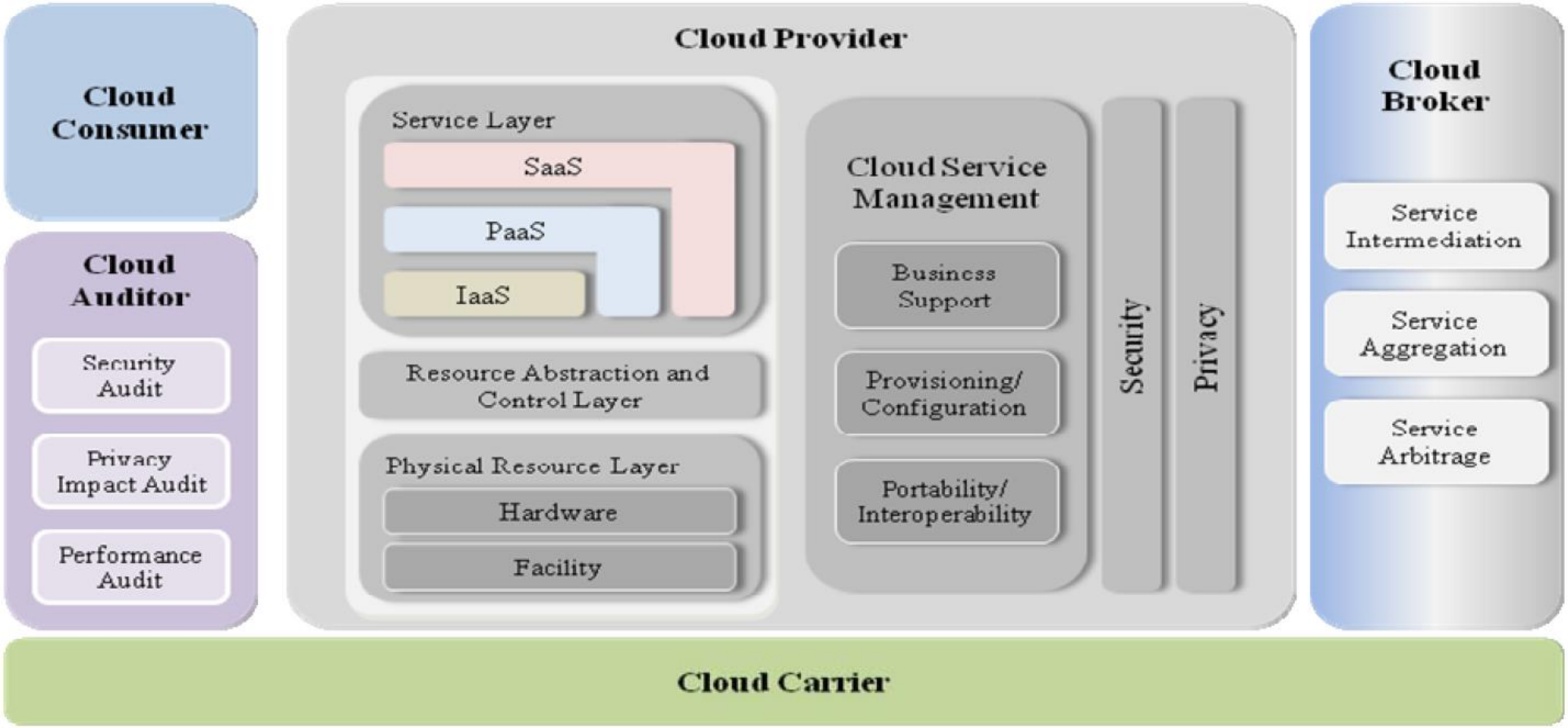
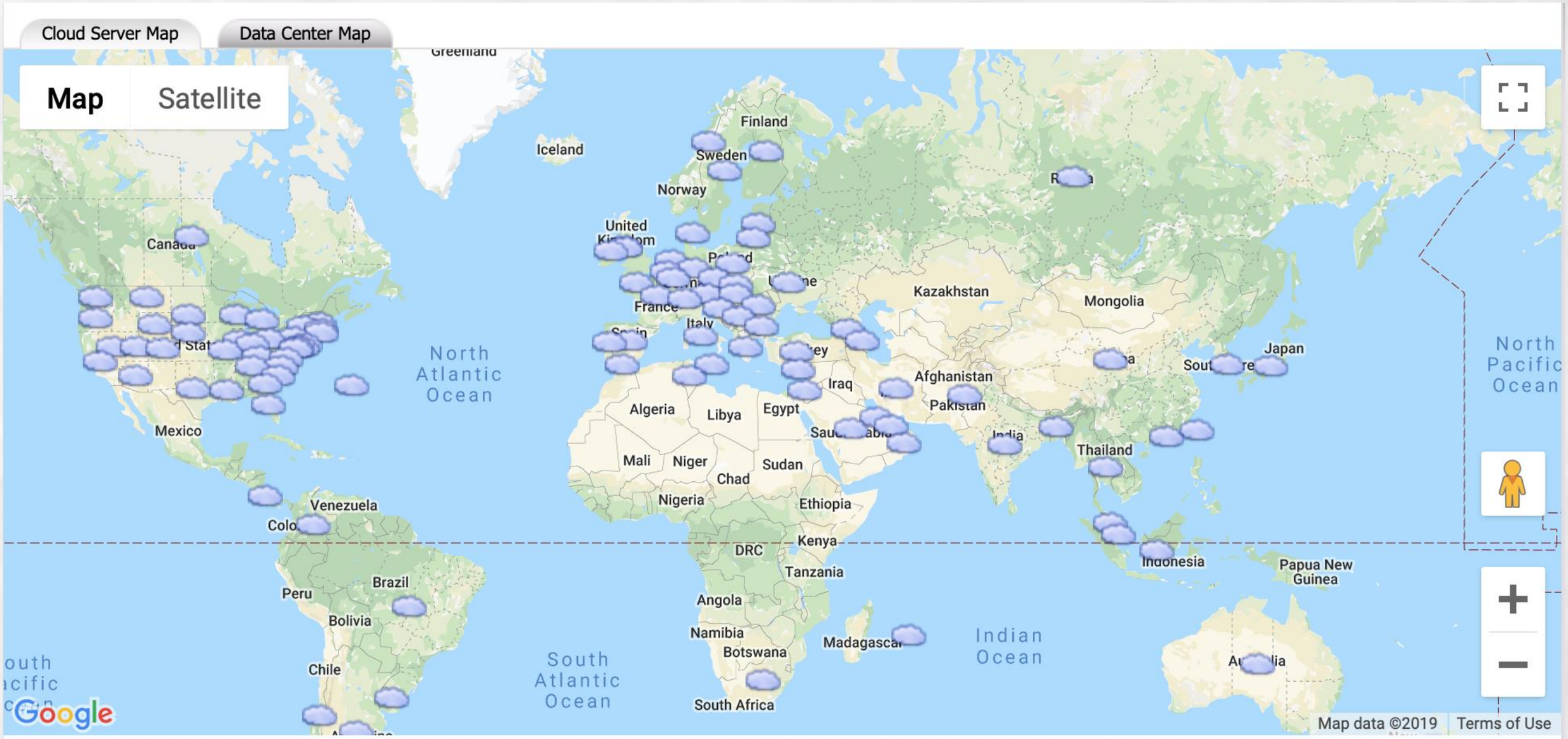


Figure 12 – The Combined Conceptual Reference Diagram

WHERE IS MY CLOUD



Cloud Infrastructure

Feeling Secure

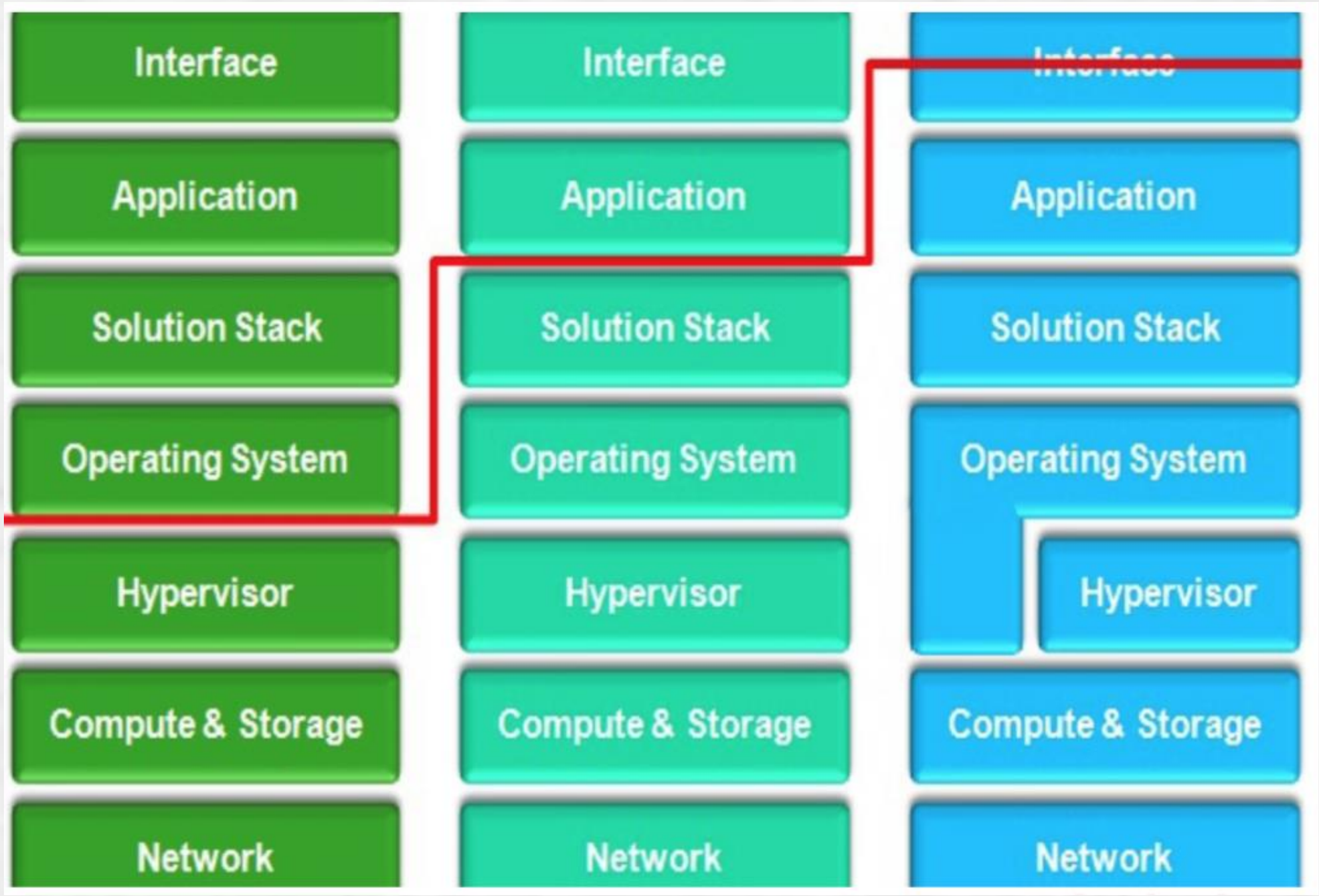
Cloud security

Inhibitors for Cloud Adoption

Credits:IBM Security

Cloud security

SCOPE of Shared RESPONsIBILIty



Subscriber

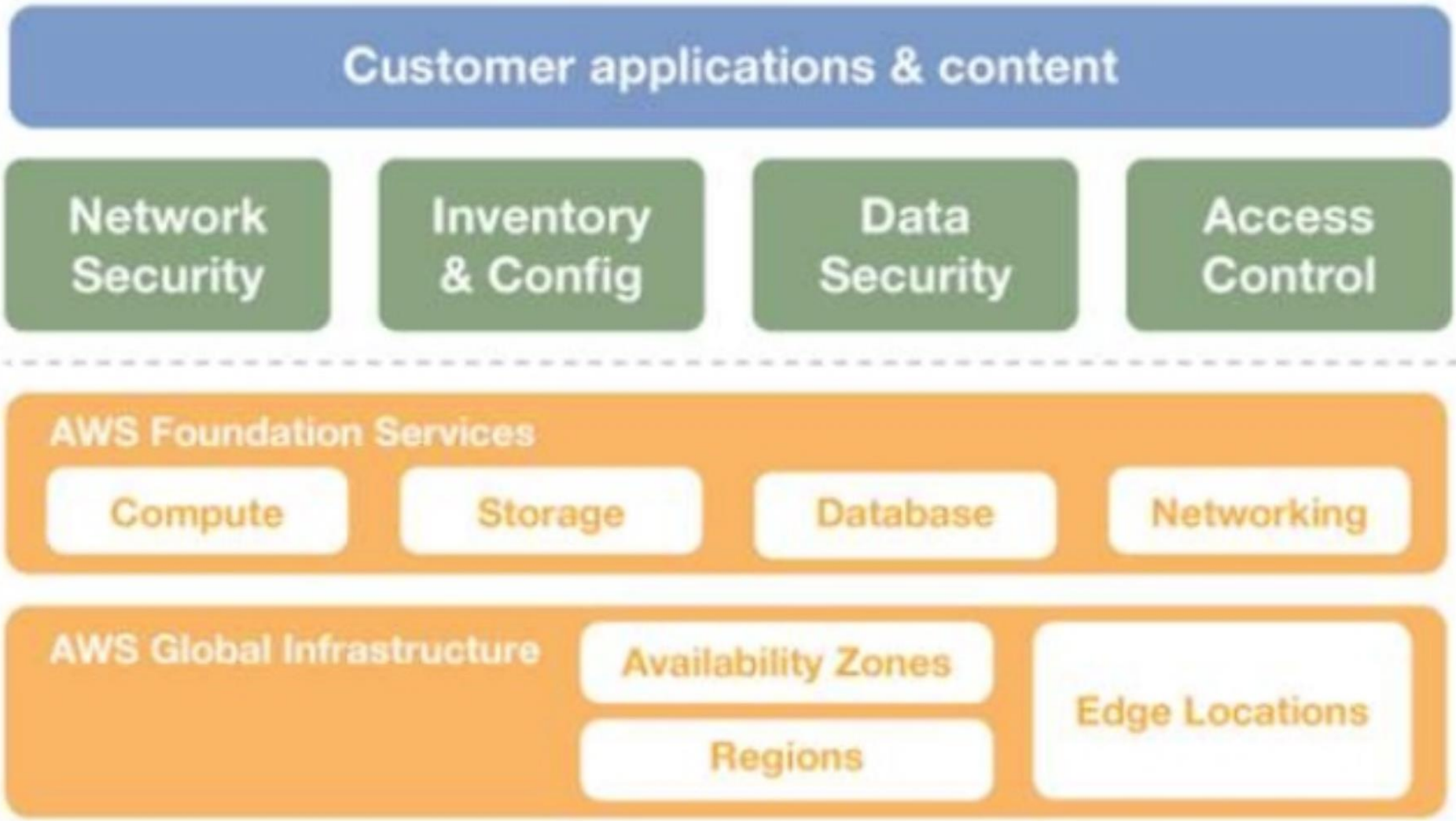
Provider

Credits:IBM Security

Cloud security

Shared Responsibility - AWS VIEW

https://aws.amazon.com/security/sharing-the-security-responsibility/

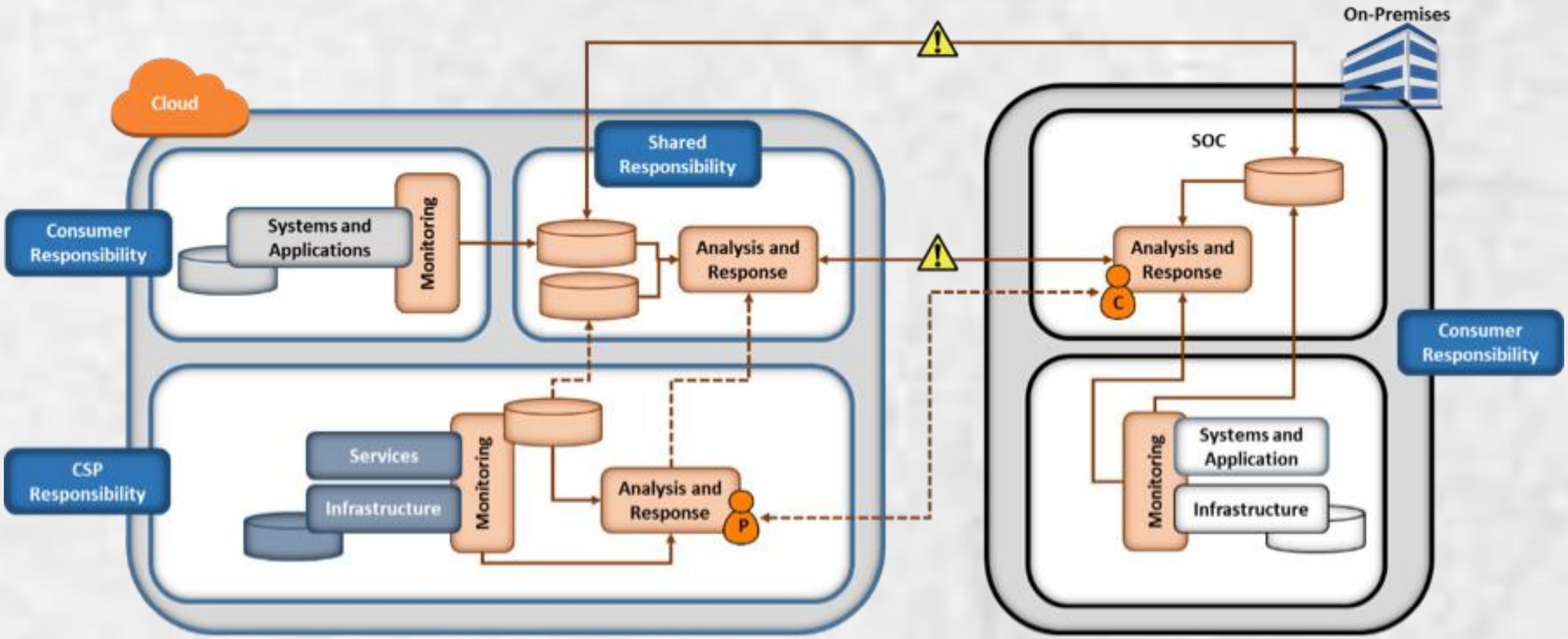


You
define your controls **'in'** the Cloud

AWS
takes care of the security **'of'** the Cloud

Cloud security

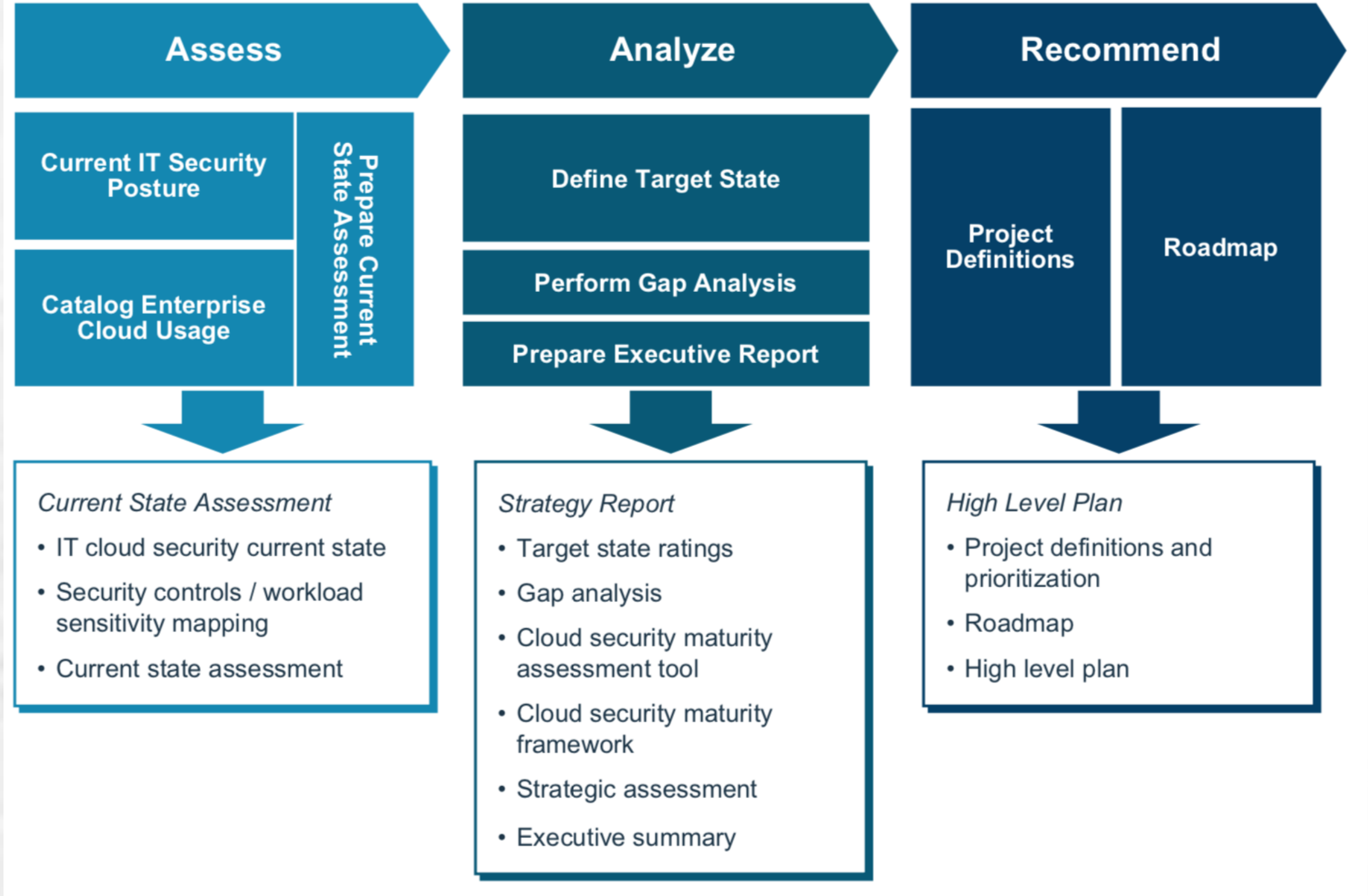
Shared Responsibility



Credits:Timothy Morrow-CMU

Cloud security

Being Secure needs A Strategy



Credits:IBM Security

cloud security alliance®

EXECUTION

Feeling secure

STARWatch is a SaaS application to help organizations manage compliance with CSA STAR (Security, Trust and Assurance Registry) requirements. STARWatch delivers the content of the Cloud Controls Matrix (CCM) and Consensus Assessments Initiative Questionnaire (CAIQ) in a database format, enabling users to manage compliance of cloud services with CSA best practices.

STARWATCH

Assurance on Demand

NEED FOR REMEDIATION

Source: Ponemon Institute 2014 Cost of Cyber Crime study

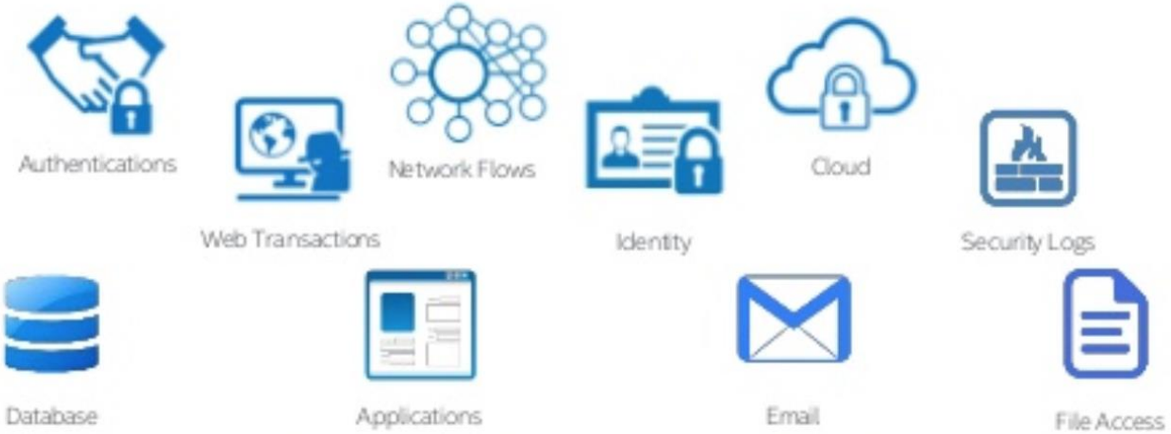
SITUATIONAL AWARENESS IS CRITICAL FOR REMEDIATION STRATEGY

Increasing Complexity

Time Imperative

Resource Constraints

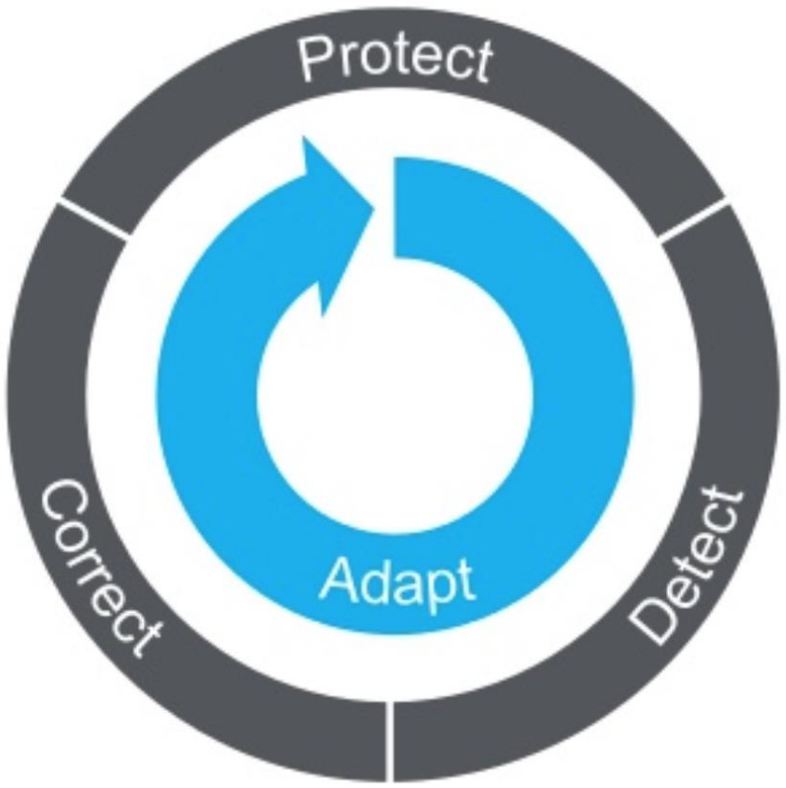
Data Sources



Context Enrichment

REMEDIATION WITH SIEM & SOAR

Continuous, Automated, and Shared Threat Intelligence

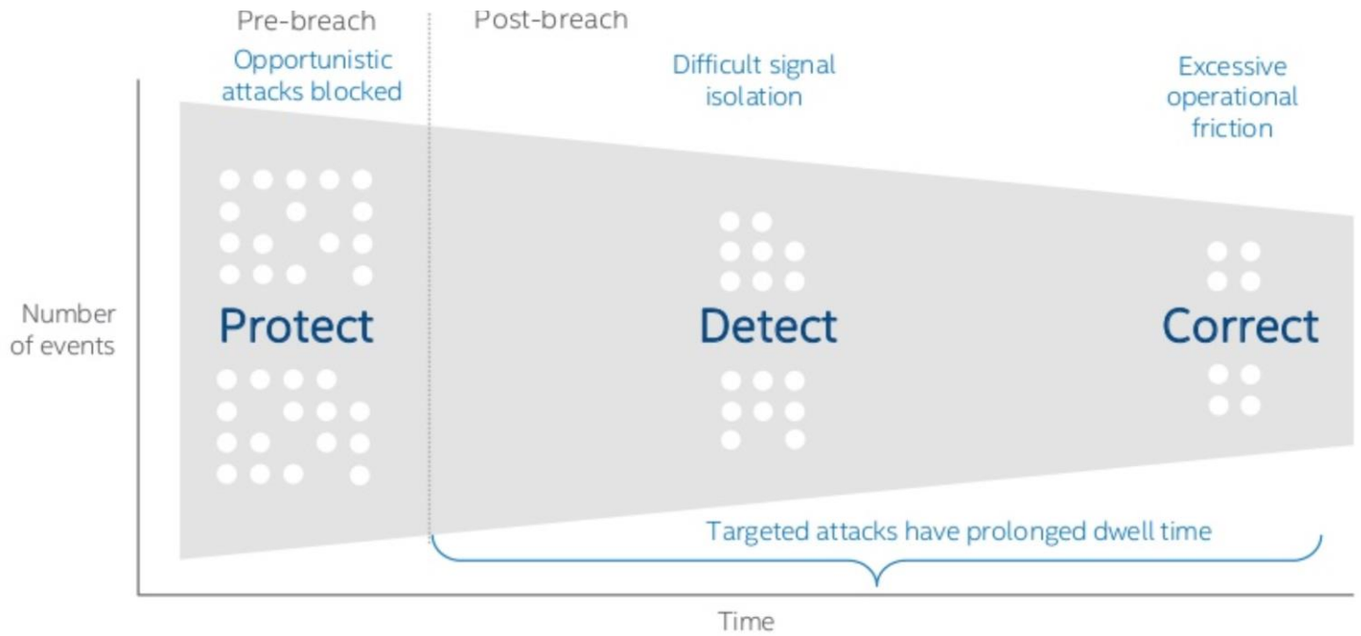


Protect – Stop pervasive attack vectors while also disrupting never-before-seen techniques and payloads.

Detect – Illuminate low-threshold maneuvering through advanced intelligence and analytics.

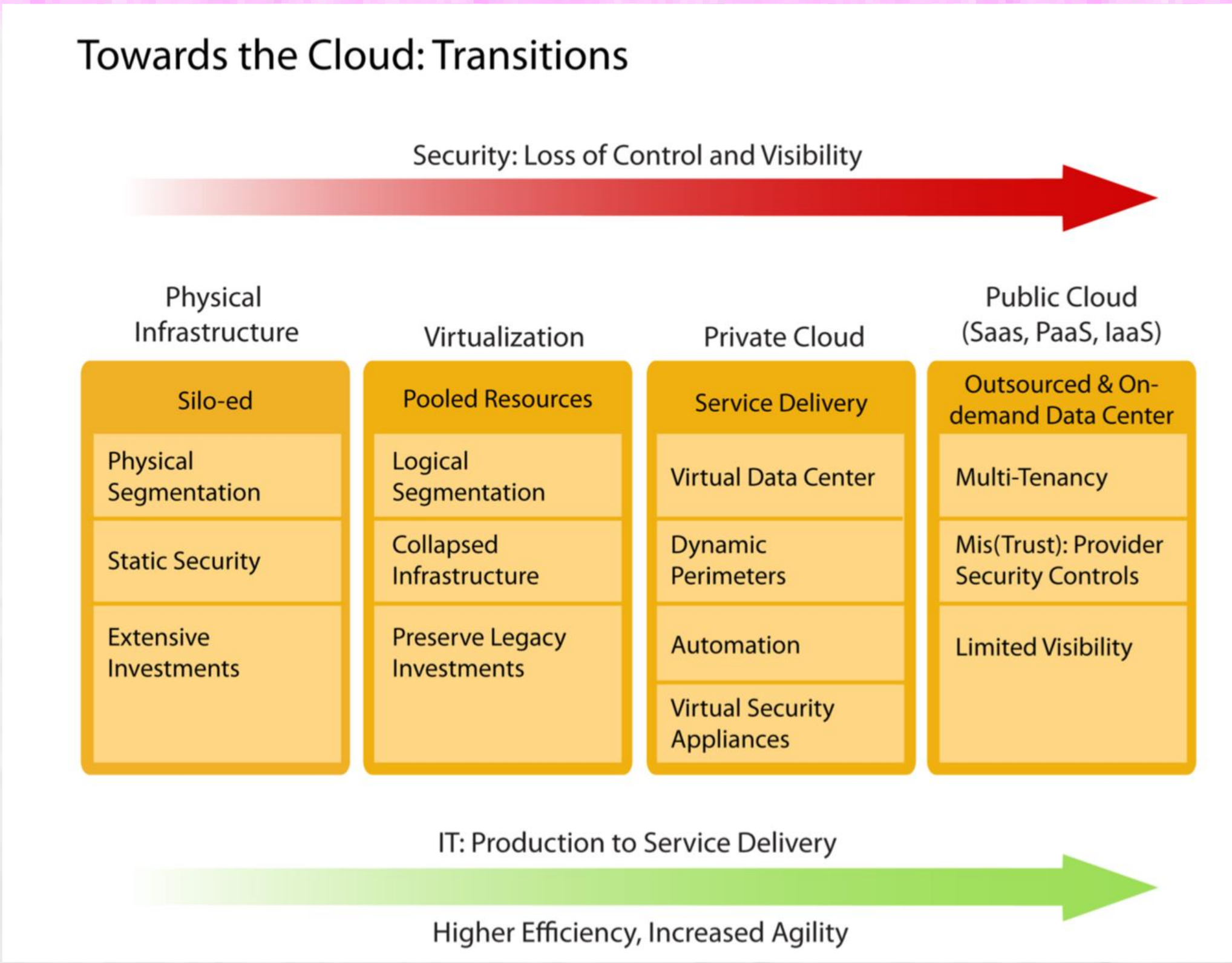
Correct – Improve triage and prioritize response as part of a fluid investigation.

Adapt – Apply insights immediately throughout an integrated security system.



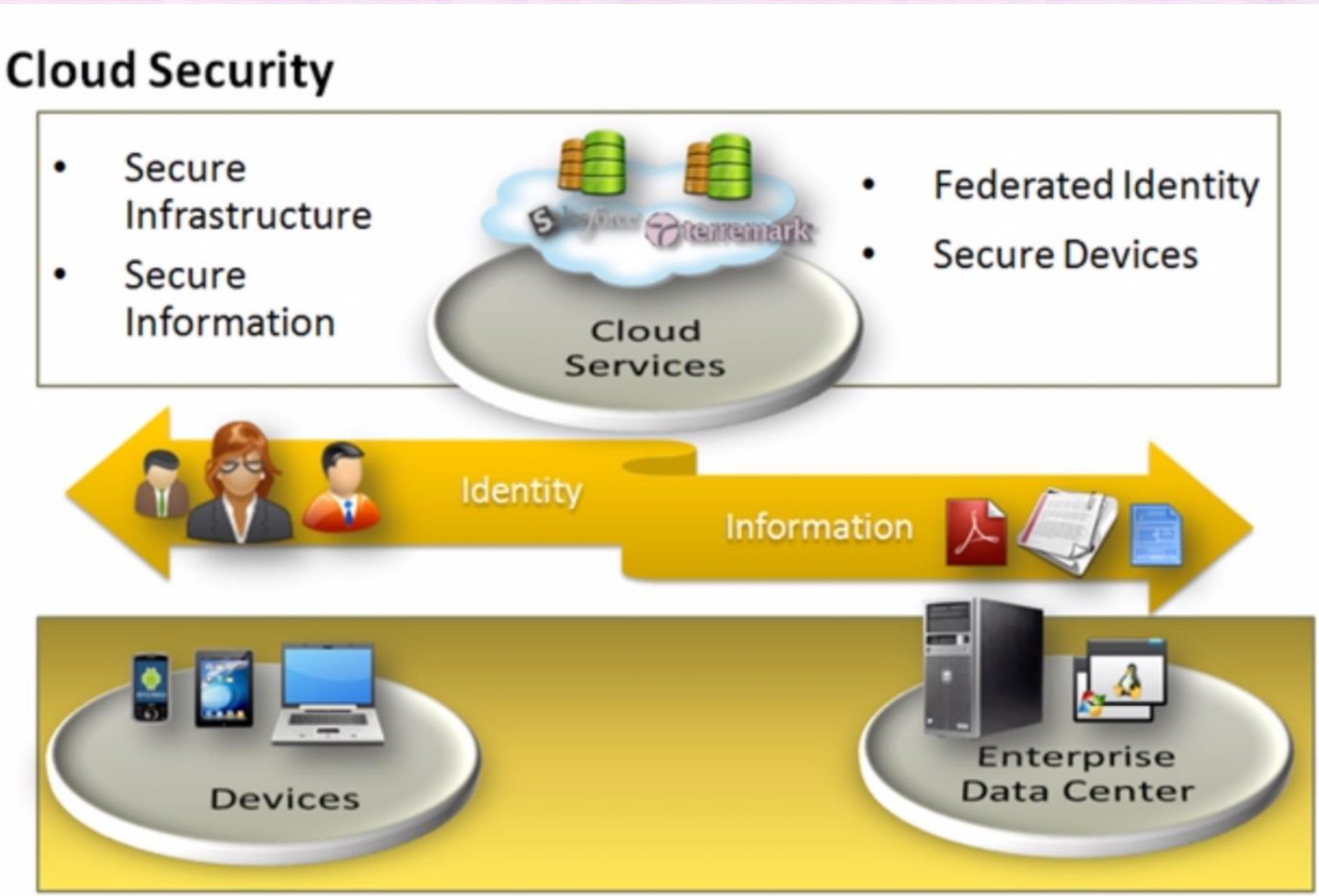
PLANNED REMEDIATION STRATEGY

REIMAGINE CLOUD SECURITY



Credits:VMware & Symantec

REIMAGINE CLOUD SECURITY



Credits:VMware & Symantec

REIMAGINE CLOUD SECURITY

Towards the Cloud: Security Recommendations

Security: Regains Control and Visibility

Virtualization	Private Cloud	Public Cloud (Saas, PaaS, IaaS)
Infrastructure Security	Elastic Security for Elastic Workloads	Secure Information, Audit Infrastructure Security
Secure Virtualization Layer	Virtualized Security Controls	Identity and Access Management
Virtual Network Security	On-Demand Security Deployment and Configuration	Secure Information Transmission and Storage with Encryption
Configuration and Change Management	Dynamic Perimeter Controls	Control Compliance Assessment
Image Management	Integration with Workload Automation	

IT: Production to Service Delivery

Higher Efficiency, Increased Agility

Credits:VMware & Symantec

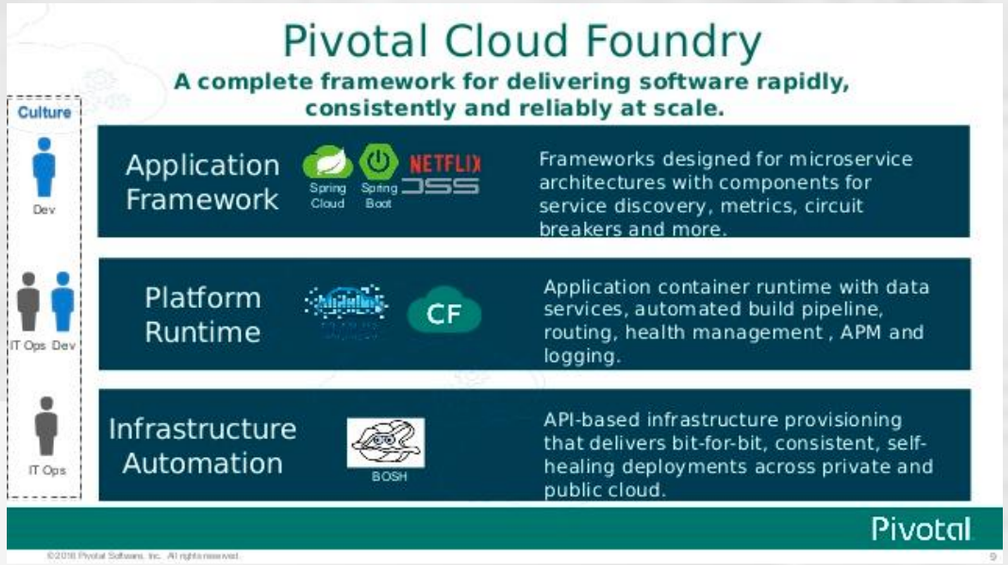
INTRINSIC SECURITY

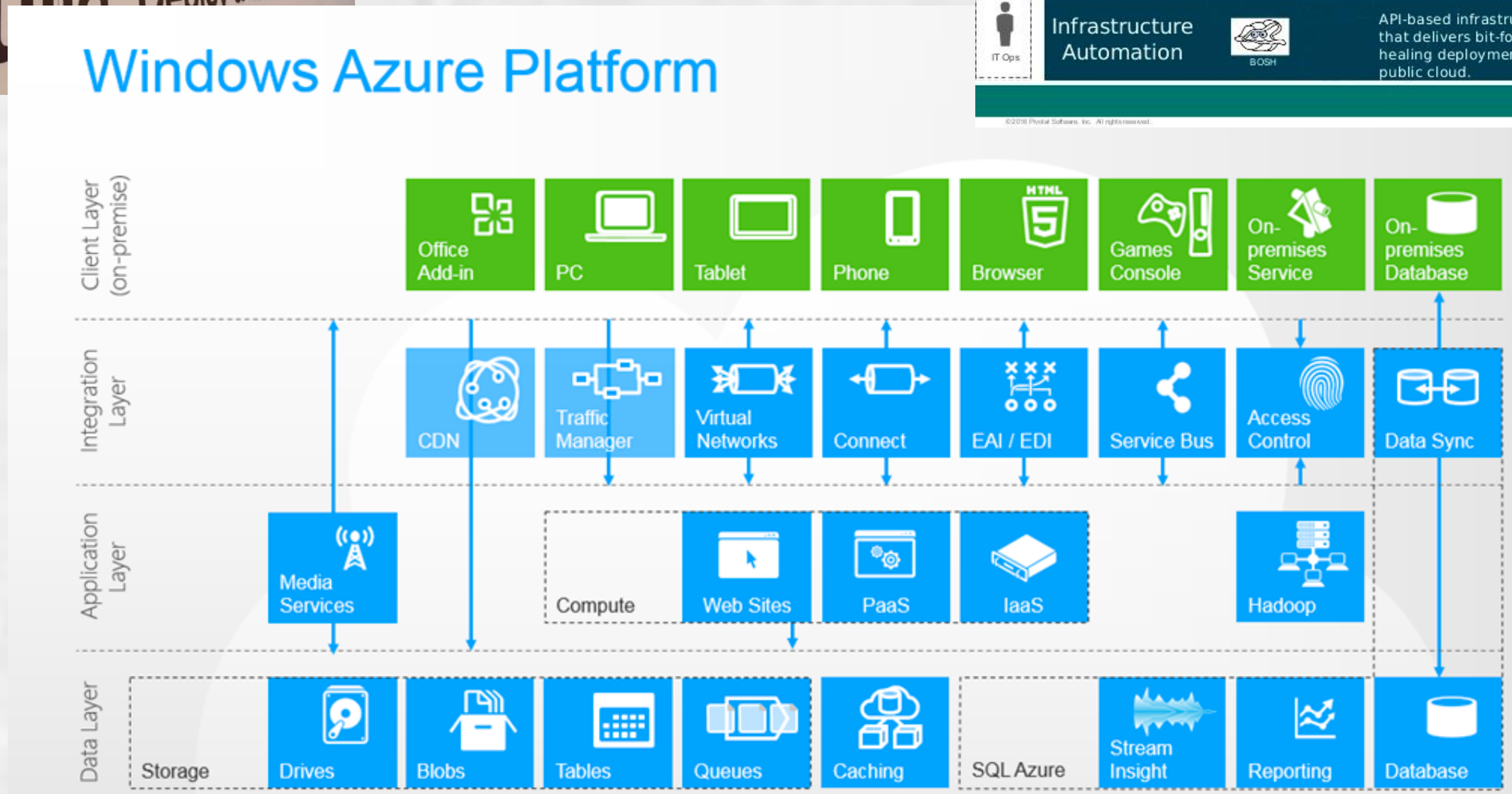
BUILT-IN SECURITY - BETTER RESILIENCE

APP SECURITY

SECURE THE PLATFORM SERVICES

ADOPT SECURE PLATFORM SERVICES





RESILIENCE

KUBERNETES

CONTAINERS

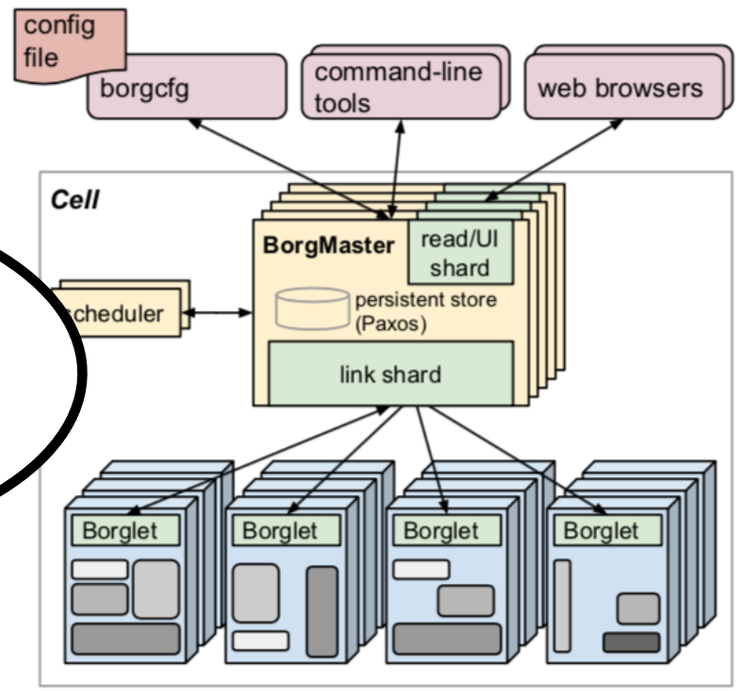


Figure 1: The high-level architecture of Borg. *Only a tiny fraction of the thousands of worker nodes are shown.*

Driven by Software

INNOVATIONS

RESILIENCE

KUBERNETES

CONTAINERS

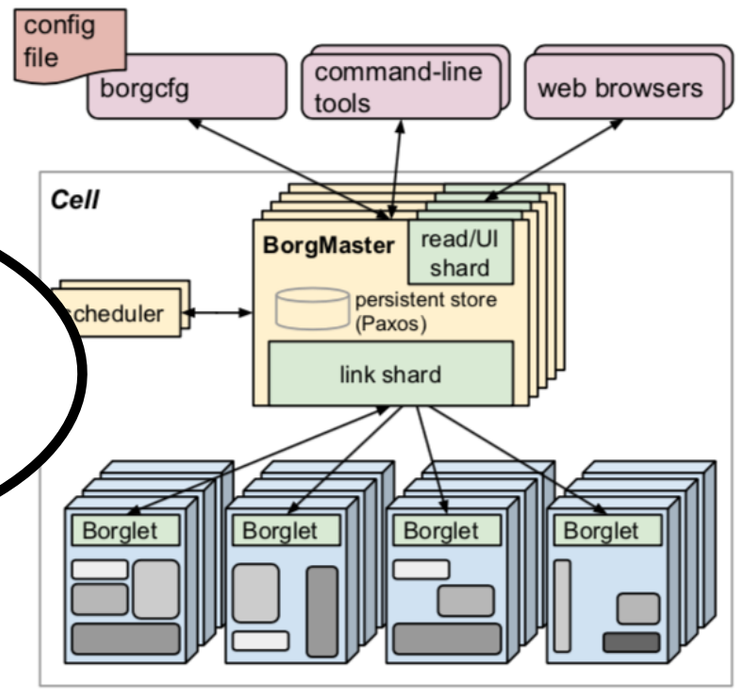
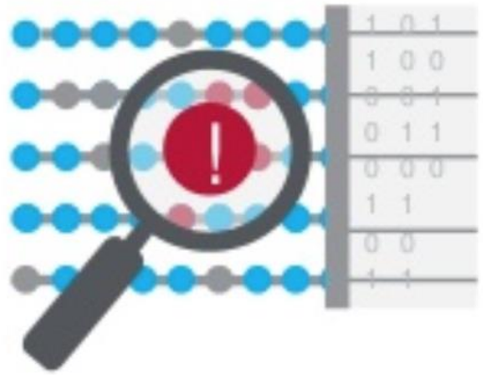


Figure 1: The high-level architecture of Borg. *Only a tiny fraction of the thousands of worker nodes are shown.*

INNOVATIONS

RESILIENCE

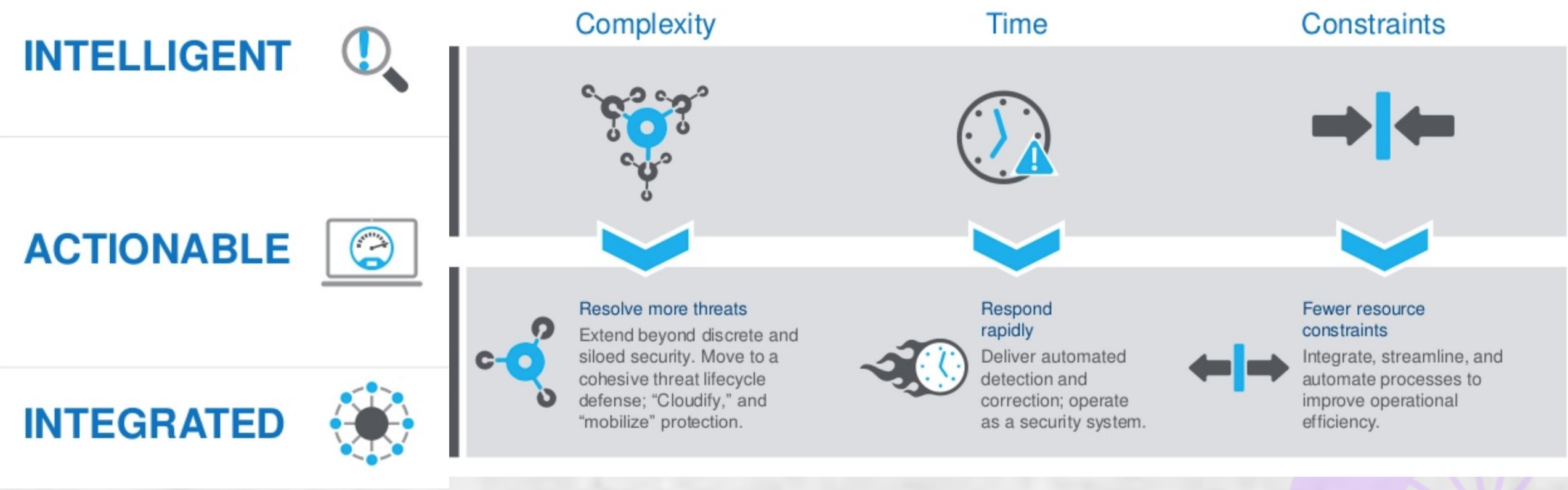
Orchestration & Automation



Credits:Intel Security

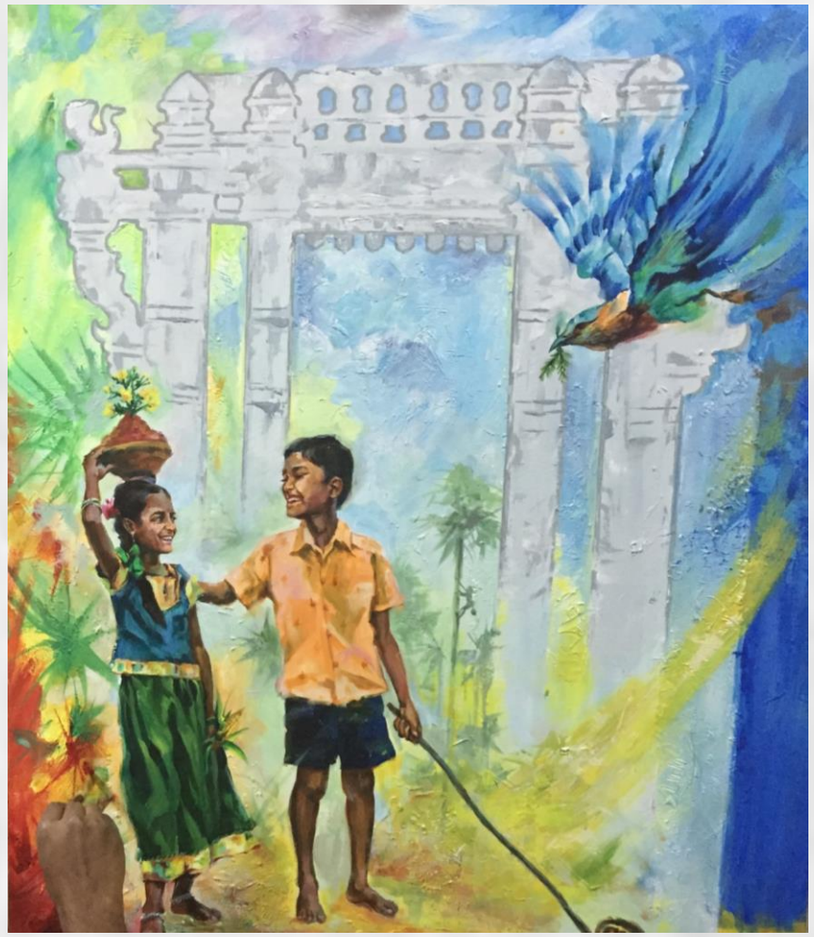
RESILIENCE

SECURITY Orchestration & Automation



Credits:Intel Security

Thank you…



2018