FloCon 2022

Using Data to Defend

Sensing in Hybrid Clouds

Timothy Shimeall, Ph.D.

CERT Situational Awareness Group

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM21-1098

FloCon 2022

An Architecture for Situational Awareness

Carnegie Mellon University
Software Engineering Institute

Overview

Why this isn't a vendor issue

Security in hybrid clouds

Three

Four

Why This Isn’t Just a Vendor Issue

Cloud hosting services are dedicated to provision

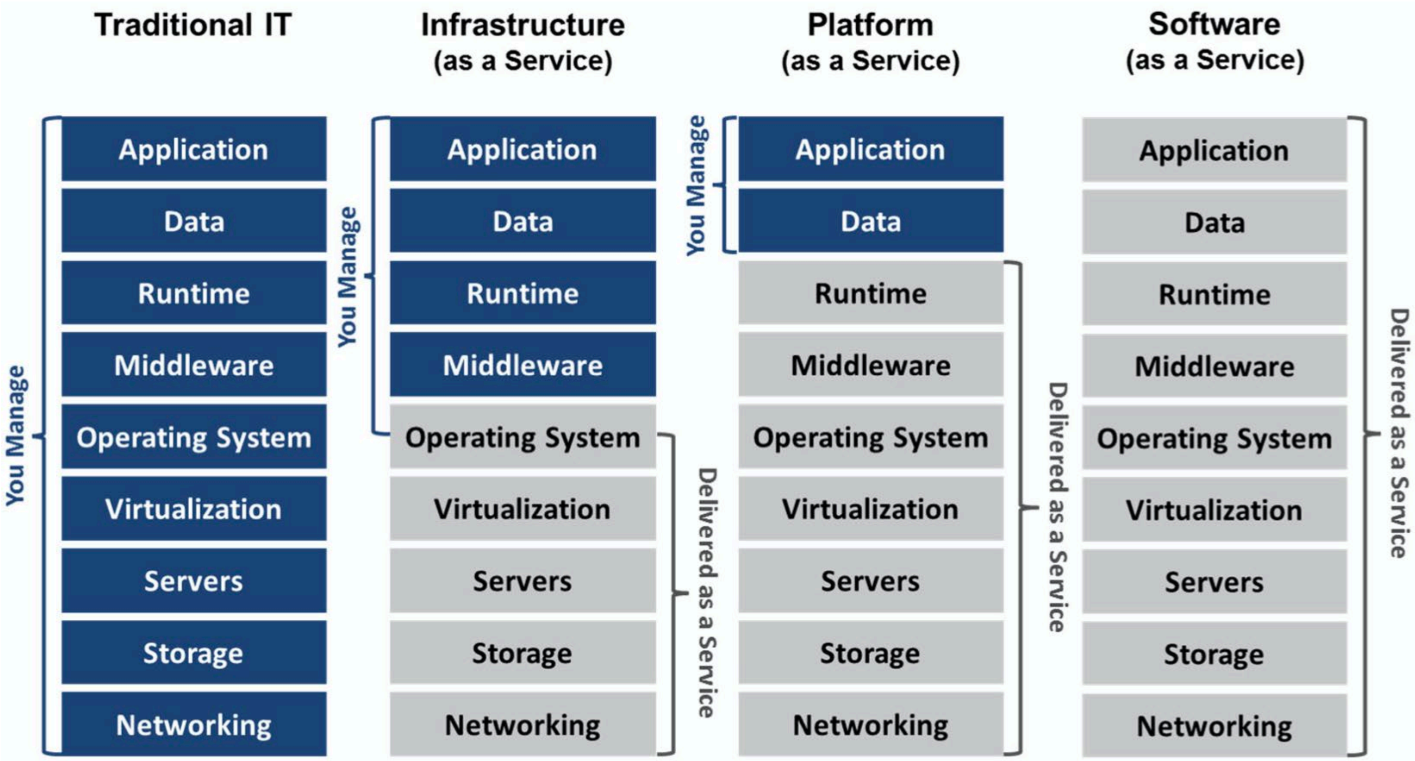
The organization that uses cloud services is responsible for security

- Provisioning and monitoring is done jointly with cloud service provider (CSP)
- Identify requirements and expectations, compare with contract statements
- Content, not infrastructure
- Abuse, not activity

A using organization may host services on more than one vendor

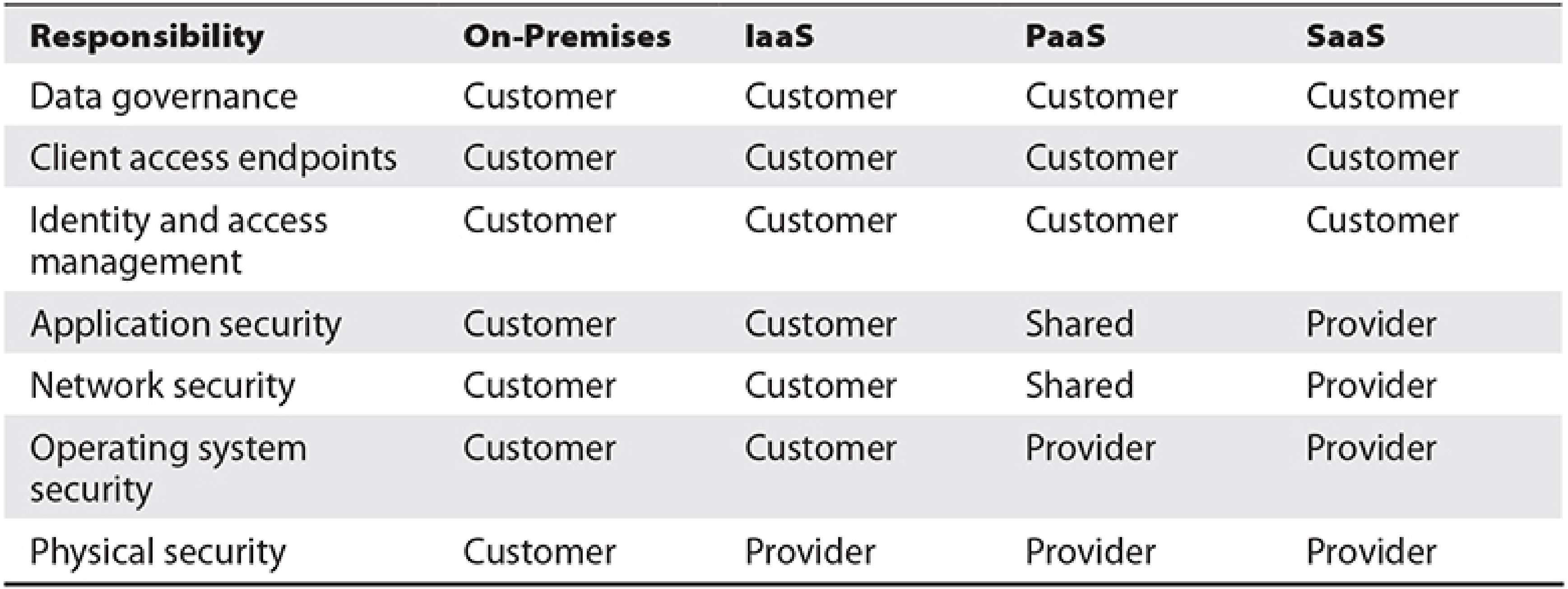
Understand trade-offs and risks

Shared Responsibility Model – 1



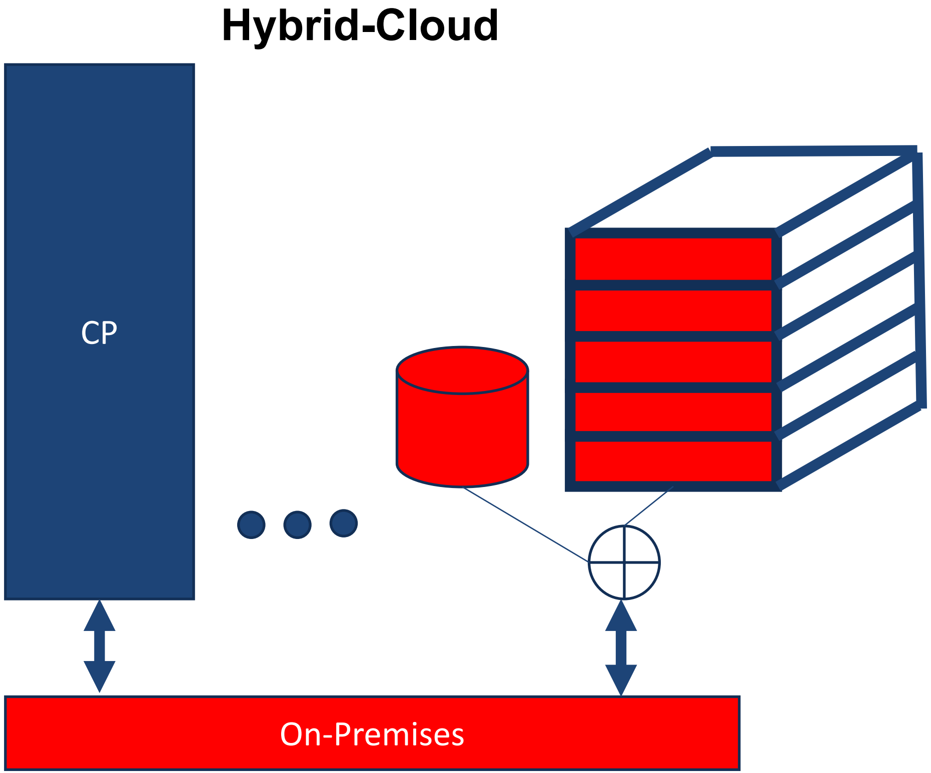
Traditional IT	Infrastructure (as a Service)	Platform (as a Service)	Software (as a Service)
Application	Application	Application	Application
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
Operating System	Operating System	Operating System	Operating System
Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking

Shared Responsibility Model - 2



Responsibility	On-Premises	IaaS	PaaS	SaaS
Data governance	Customer	Customer	Customer	Customer
Client access endpoints	Customer	Customer	Customer	Customer
Identity and access management	Customer	Customer	Customer	Customer
Application security	Customer	Customer	Shared	Provider
Network security	Customer	Customer	Shared	Provider
Operating system security	Customer	Customer	Provider	Provider
Physical security	Customer	Provider	Provider	Provider

Security in Hybrid Cloud



Deploy services across both public and private clouds, in cooperation with on-premises services

You manage:

- Previous shared responsibilities
- Local administration
- Mission and load between on-premises and cloud hosting
- On-premises security
- Interaction between on-premises and cloud assets

Storing Security and Other Information

Security data (traffic capture and service logs) is high velocity

Need to make conscious decision where to store data

- Blob “hot” storage is more expensive than “warm” or “cold” storage.
- Warm and cold storage are slower and can get expensive if data is accessed too often.
- Data warehouse (e.g., Redshift) adds complexity to storage questions (similar to in-house, but not identical).

Need to properly control access to security data.

Security Issues: Dealing With Mixed Security

Detecting issues:

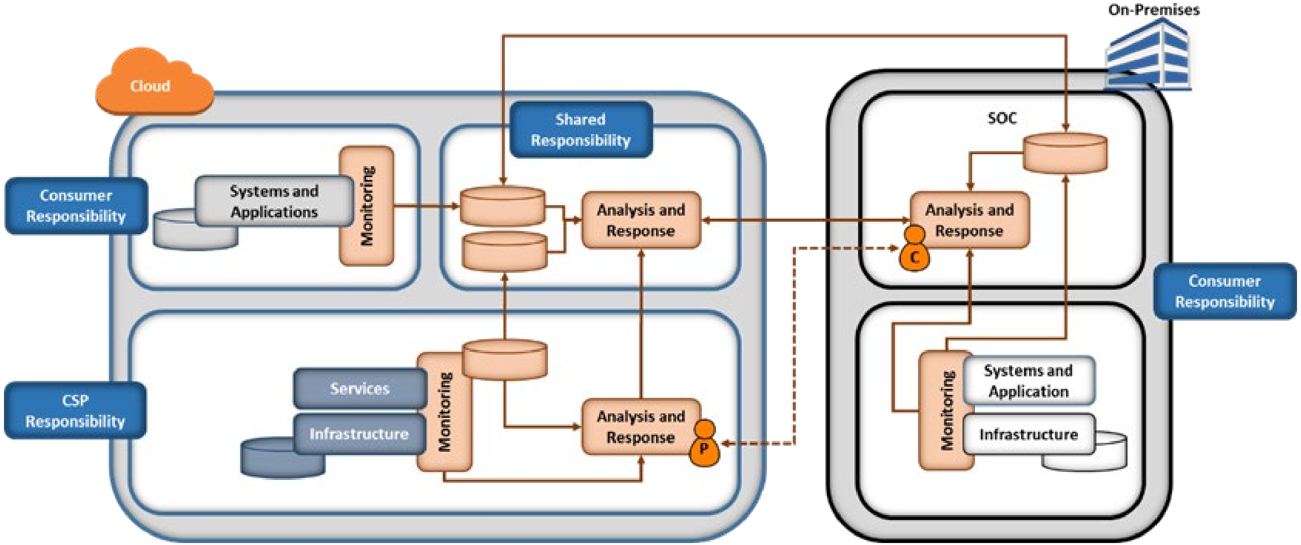
- Events
- Identities

CSP shared responsibilities:

- Monitor infrastructure and services
- Sensing infrastructure for backend

Client shared responsibilities:

- Profiling system, services, usage
- Incident response
- Coordination



Security Issues: Turning Data Into Information

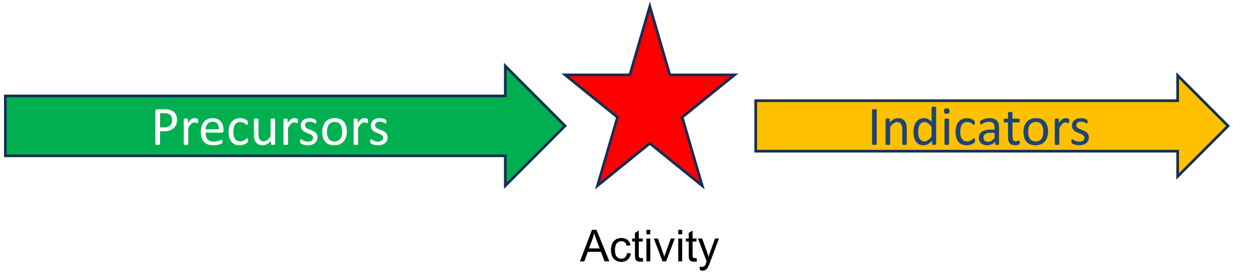
Context

Precursors vs. Indicators vs. false alarms

Microanalysis

Macroanalysis

Reporting



Monitoring Capabilities

Bridging:

- Address spaces
- Traffic volume differences
- Port/Protocol differences (due to gateways, tunneling)
- Timing differences (clock drift and traffic delays)

Varying views of events

- Proxies and retransmission
- Traffic view vs. service view
- De-interleaving traffic
- Partial capture

Summary

Hybrid clouds are increasingly with us

Need to address monitoring and analysis challenges

Mix of commercial, academic, and governmental efforts

Questions?

Tim Shimeall

Software Engineering Institute

Carnegie Mellon University

Pittsburgh, PA

tjs@cert.org