Top-down continuous policy compliance

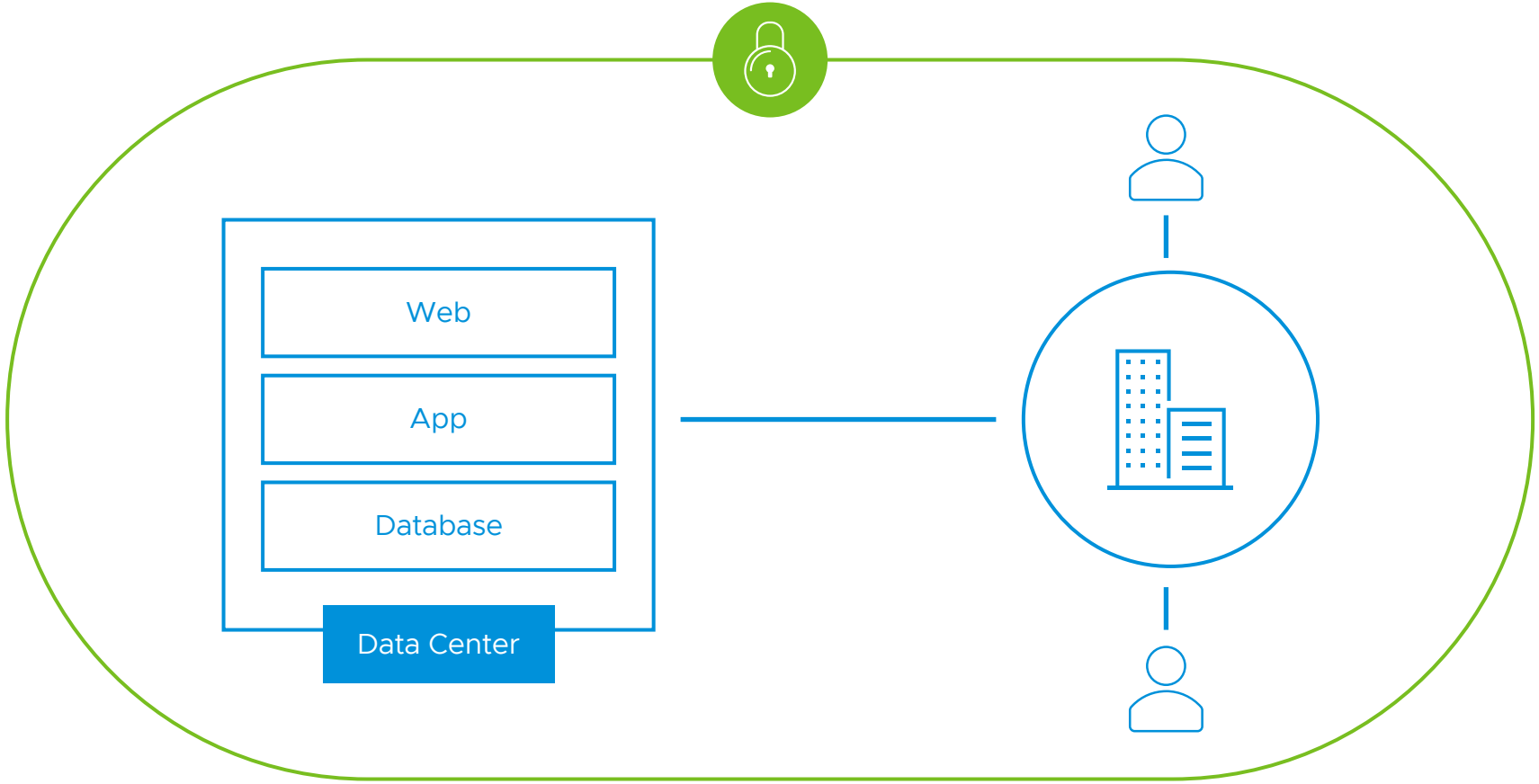
A Zero Trust Architecture

Sergio Pozo-Hidalgo, PhD

Sr. Product Line Manager

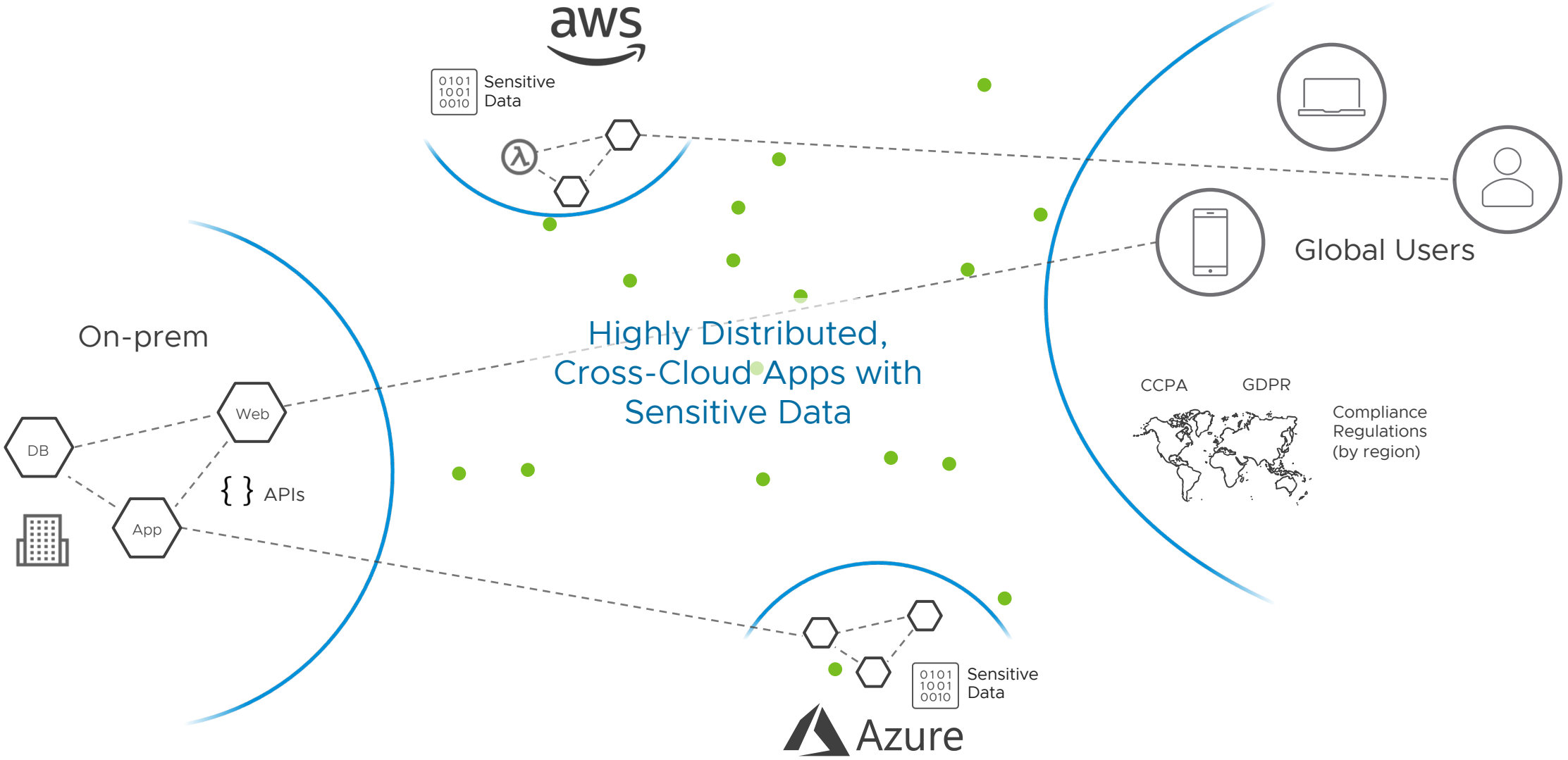
CTO Office, Networking and Advanced Security BG

Where we were



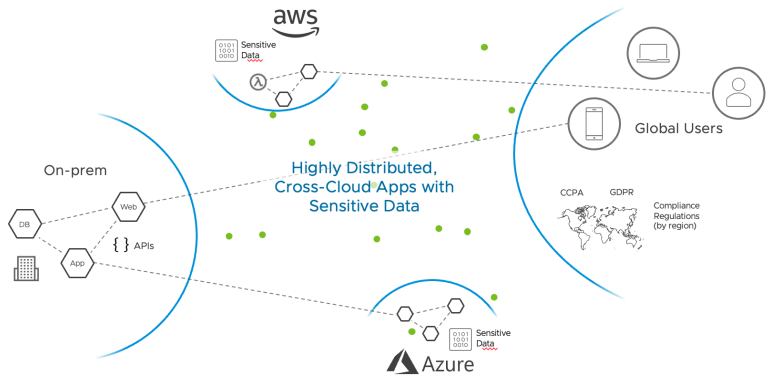
Where we are today

Highly distributed applications with highly heterogeneous connectivity and security



Where we are today

Complexity in infrastructure, security controls, policies, and operational models



Identity models based on ownership as proxy for trust don't work

Heterogeneous infrastructure: edge, multi-cloud and private DC.

Organizations increasingly lose ownership and control of the infrastructure, their users, their applications, and their data.

Composite Applications complicate secure connectivity

They contain components from multiple providers.

Components execute distributed across multiple platforms in different clouds and on the edge.

Risk and Compliance assessment is extremely difficult

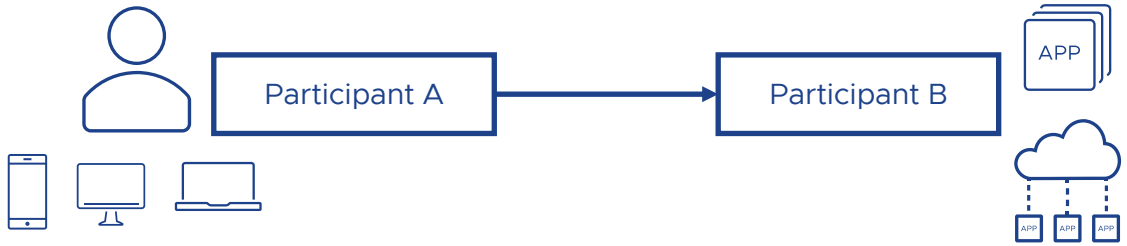
Lack of control of all elements of the environment.

IT has lost visibility as application operations teams have become more self-sufficient.

Increased risk leading to an increased attack surface.

Traditional security approach is showing its age

Risk and compliance management across heterogeneous silos is very challenging



Is the conversation between A and B appropriate?	IDS, IPS, DLP
Is B a reputable entity to talk to?	URL filtering, DNSsec, ATP
Should A access B?	ZTNA, FW, App/API Control
Should A run an executable?	Antivirus, Sandbox
Is the platform where B runs compliant?	CSPM
Is A behaving as expected / Is A compliant?	EDR, UEBA
Does A have all that it need to talk to B?	MDM Browser Control

Security posture is difficult to life-cycle and audit

- Current solutions chain siloed controls that don't share context

Security operations don't scale

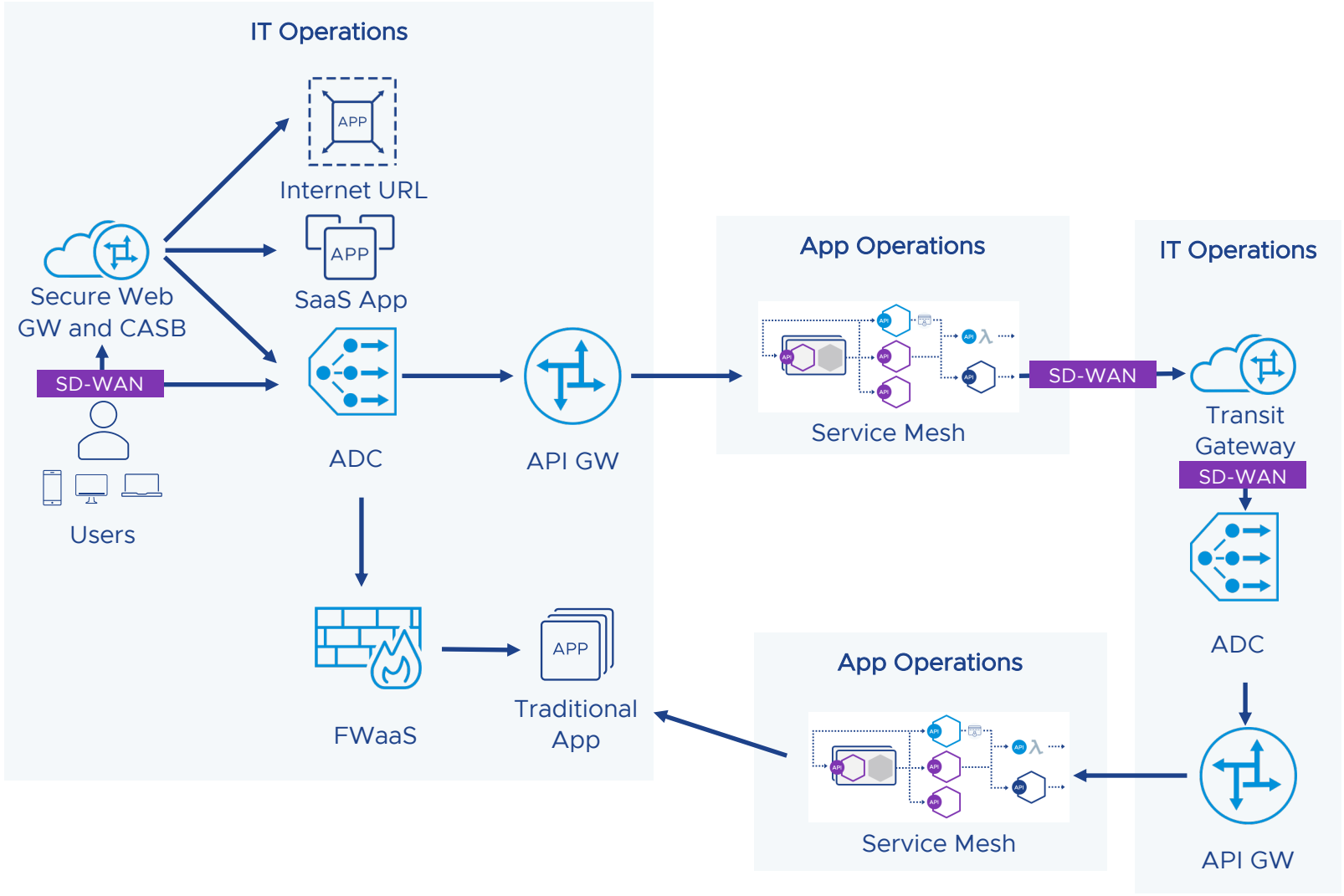
- Risk is binary: allow or block
- Risk is static: participants' behavior changes over time aren't captured
- Vast amount of time optimizing one-time access decisions
- Each control: +OPEX +CAPEX

Security ROI is difficult to calculate

- Model based on how much is blocked. But blocking is disruptive for IT and LOBs

Traditional connectivity approach is still network-centric

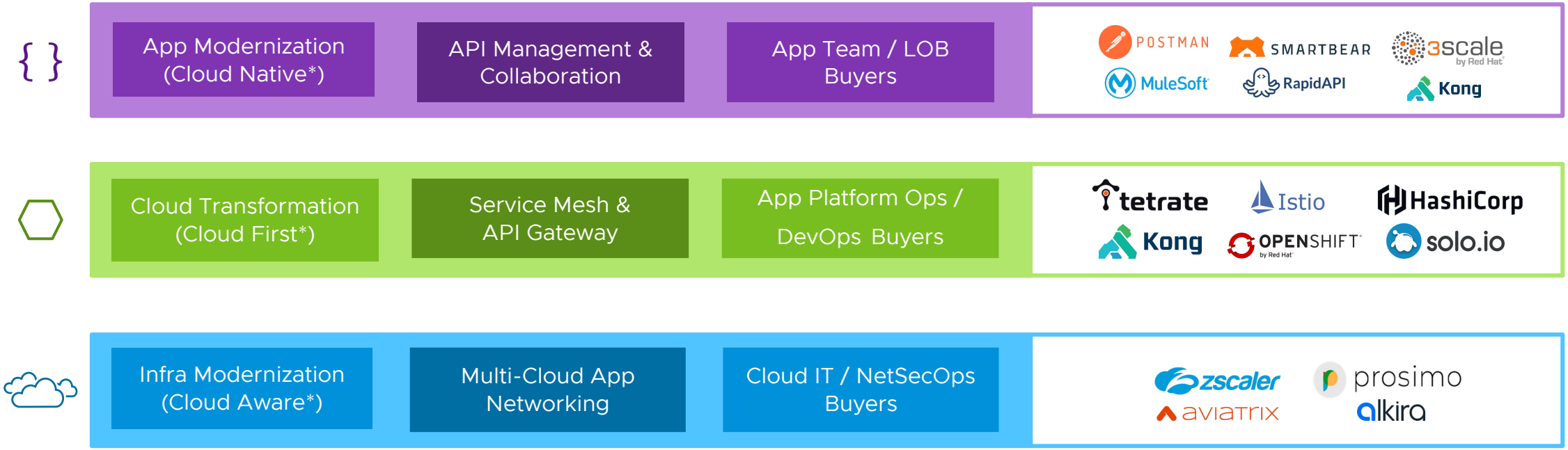
Siloed data planes, PAP and PEP



Multi-Cloud application connectivity and security

A very fragmented space

Patchwork of commercial and open-source technologies creates **operational complexity** for teams

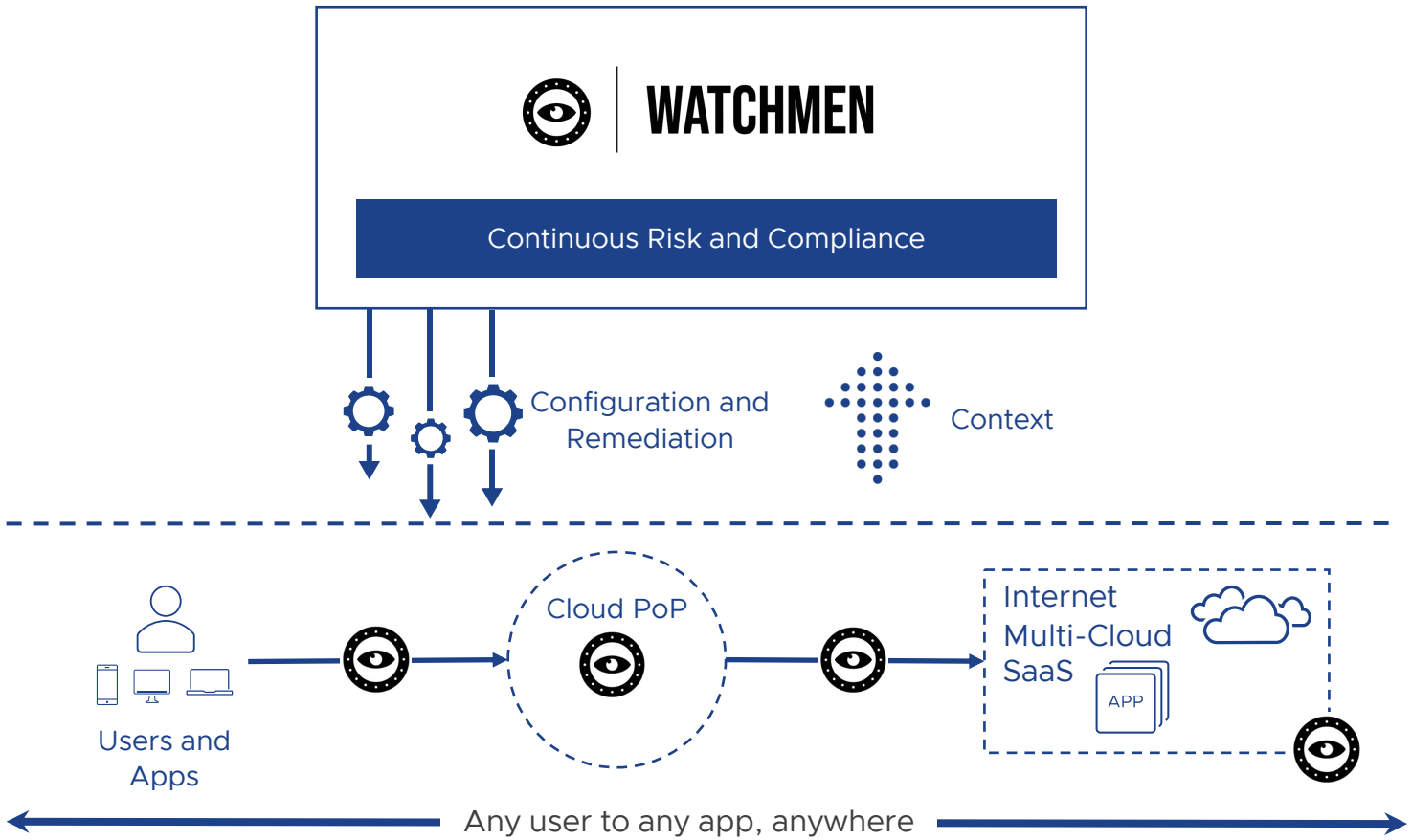


No Single Vendor is Addressing the End-to-End Transaction and Runtime Context

* https://www.bcg.com/publications/2022/developers-influence-in-enterprise-tech-sales

Continuous risk and compliance management

Proposal of a Zero Trust Architecture



Consolidated data plane

- Service-level connectivity across datacenter, multi-cloud, and edge
- Portable and pluggable security controls

Automated security operations

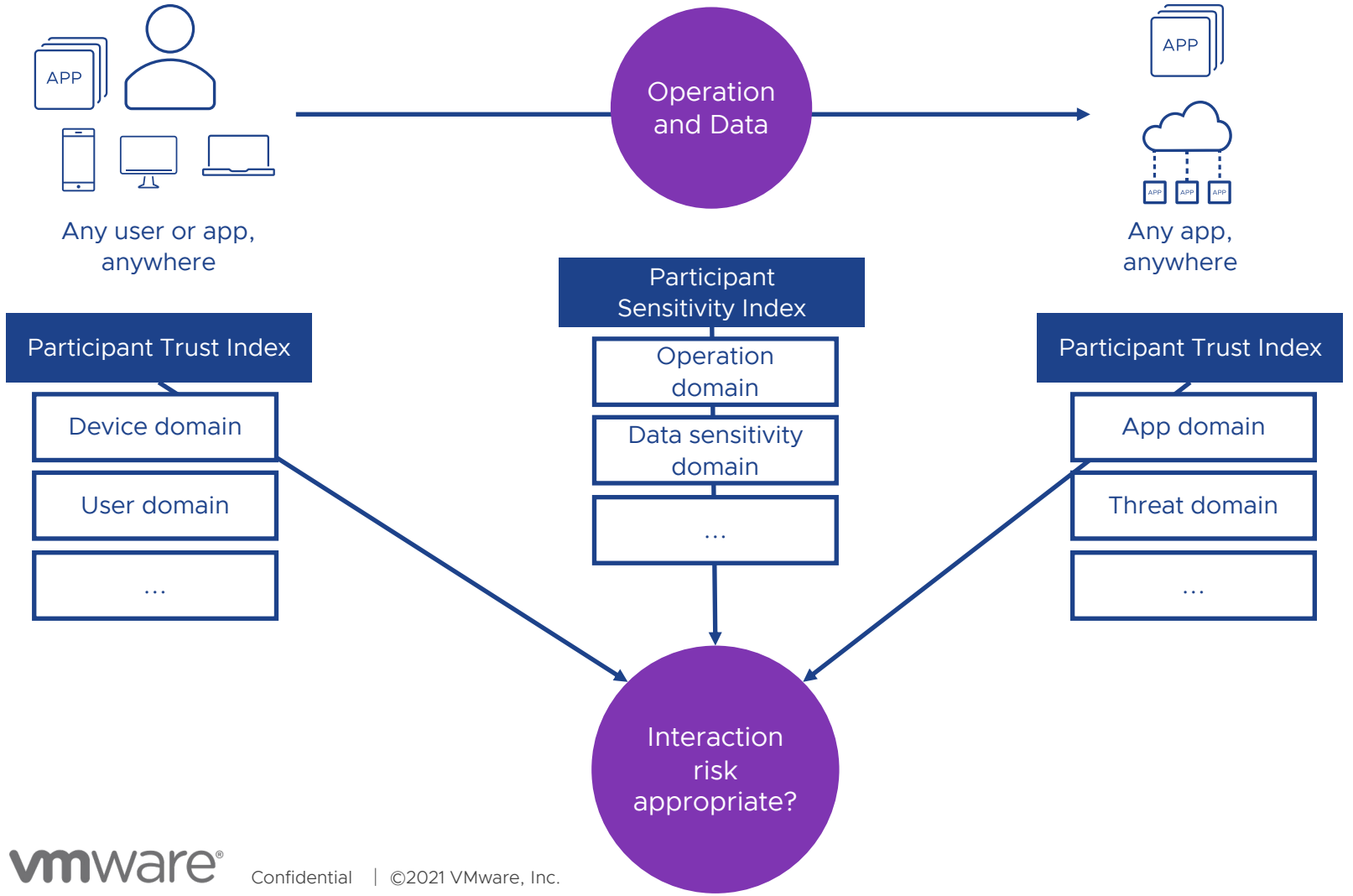
- Simplified multi-cloud connectivity and security operations
- Increased service agility and stability (fewer human errors)

Continuous risk and compliance

- Continuous, end to end risk and compliance assessment
- Diverse set of adaptative risk mitigation actions

Project Watchmen

Continuous trust and risk assessment: how to make a yes continue to be a yes?



Change in security mindset

- Bad will inevitably happen past the one-time access control gate
- Shift goal from "perfect" block/allow to continuous risk assessments and rapid remediation
- Context-aware micro-decisions, constantly evaluating ever-changing participants' trust

Should A talk to B?

- What is the trust levels of A and B?
- What is the requested behavior?
- What is the data sensitivity?
- What is the acceptable level of risk?

Policy Model and Example

Demo time!

Demo time!

Thank you!

sergioh@vmware.com

sergio.pozo@gmail.com