Towards a Zero Trust Architecture

Solutions for Modern Application Environments

Shain Singh, Principal Security Architect, F5

Hi, nice to meet you. I'm Shain.

Shain Singh

Principal Security Architect @F5

- 25+ years in security, networks and IT
- Across telco/ISPs, education and government sectors
- Current Interests:
  - DevSecOps (Continuous security in operations)
  - 5G Security (IIoT, Smart Cities, Edge Networks)
  - API/Application Security
  - Government/Industry Standards and Compliance

Social

https://linkedin.com/in/shsingh

shsingh@ieee.org

https://twitter.com/shainsingh

https://github.com/shsingh

https://shain.io

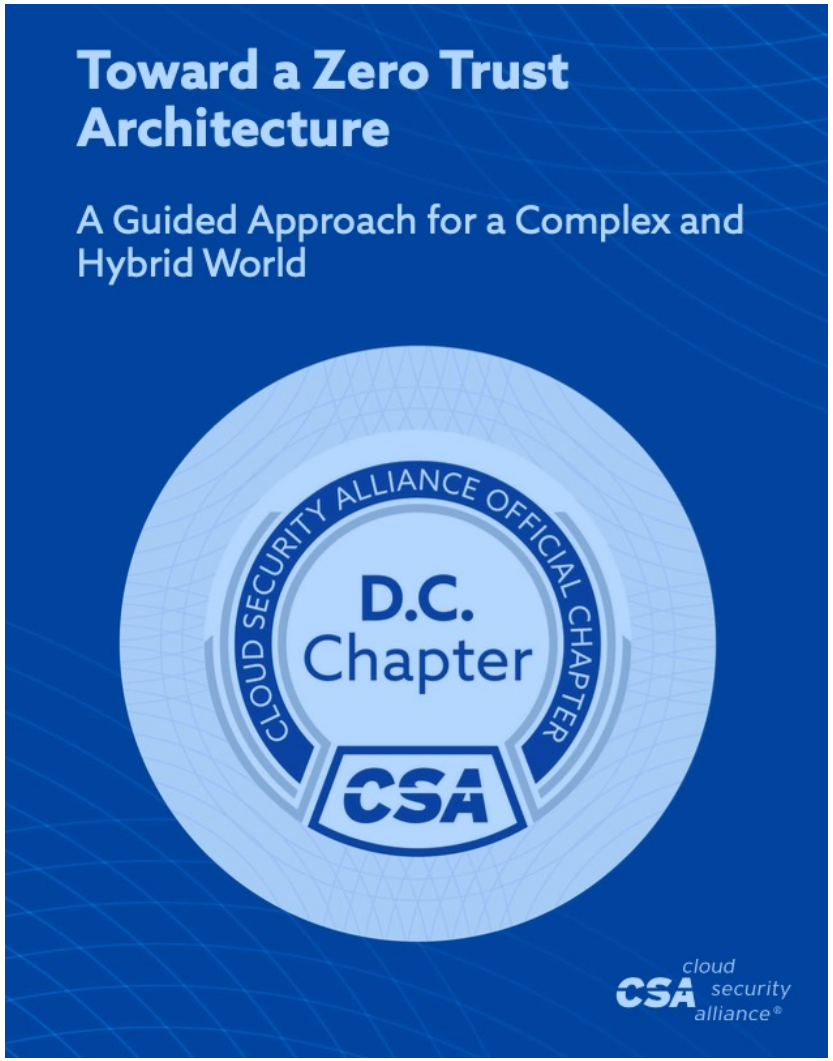
Professional Memberships

Agenda

- Defining the Scope
  - Guidelines
  - Maturity Model
- F5 Solutions for Modern Application Architectures
- Why Zero Trust is Important

Defining the Scope

Zero Trust Guidelines



https://cloudsecurityalliance.org/artifacts/towards-a-zero-trust-architecture/

Zero Trust Maturity Model

Pre-decisional Draft

June 2021

Version 1.0

Cybersecurity and Infrastructure Security Agency
Cybersecurity Division

https://www.cisa.gov/publication/zero-trust-maturity-model

Recommendations from CSA

The CISA ZTA capability maturity model (ZTA-CMM) assessment approach should be adopted, as prescribed in this paper.

Industry and government should continue to collaborate to provide organizations with ongoing guidance to evaluate ZT solutions that best fit their roadmap requirements.

As such, **leading organizations should continue to share their progress on solution evaluations through industry forums**. This will help in the identification of ZTA best practices that work in similar environments.

Lastly, it is recommended that **the vendor ecosystem should re-evaluate its capability to address the range of ZTA requirements, from policy automation to real technology capabilities that promote interoperability, control, and context**.

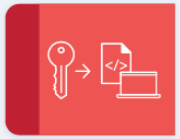
Zero Trust Tenets – NIST 800-207

Zero Trust Tenets from NIST

1 All data sources and computing services are “resources”

2 Communications are secured regardless of location

3 Access to individual resources is granted on a per-session basis



4 Access to resources is determined by dynamic policy and other behavioral and environmental attributes

5 Integrity and security posture of owned and associated assets is monitored and measured

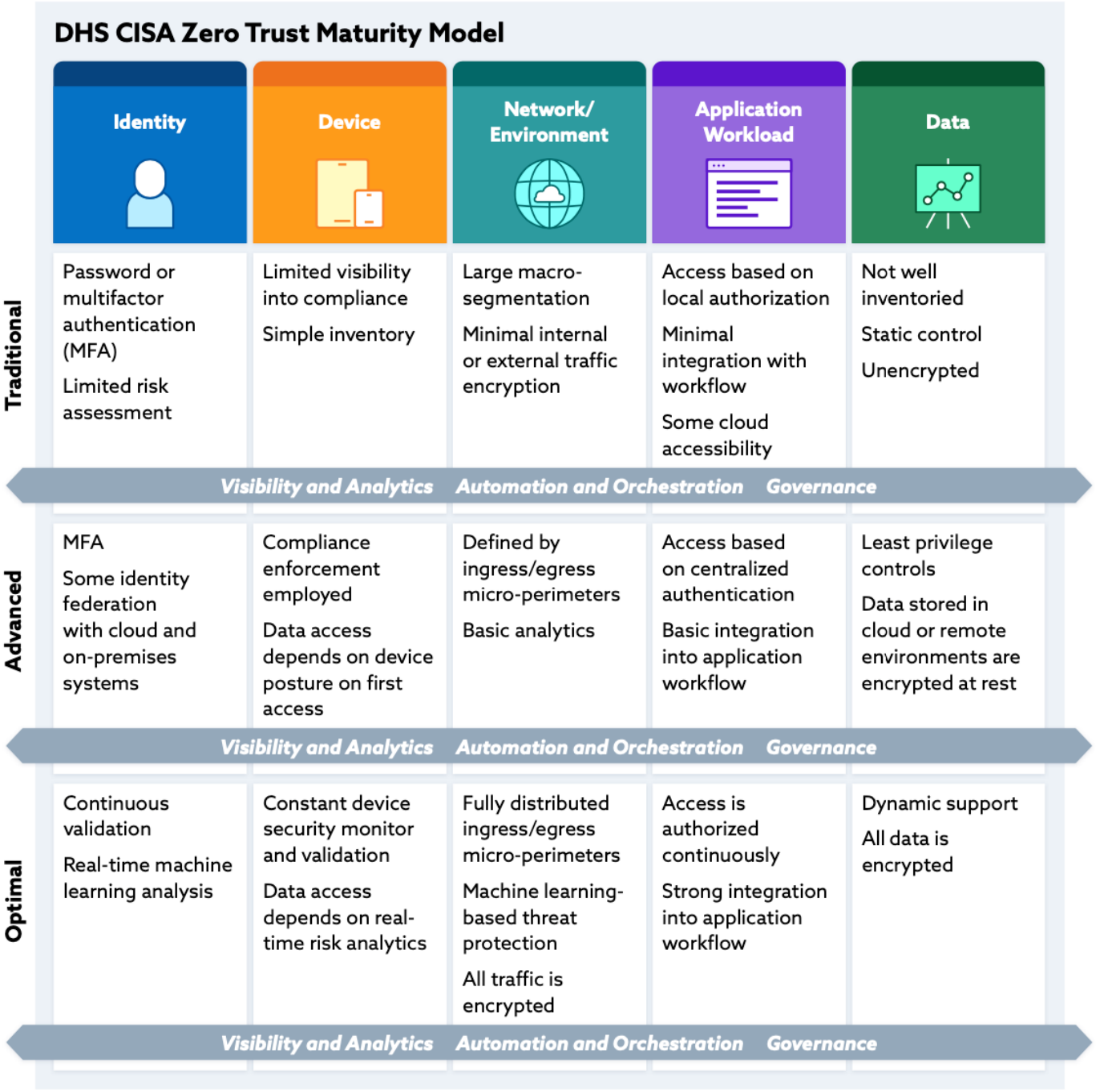
6 Dynamic resource authentication and authorization are strictly enforced before access is allowed

7 Information on current state of asset, network infrastructure, and communications is collected to improve security posture

Zero Trust Pillars

CISA ZTA-CMM

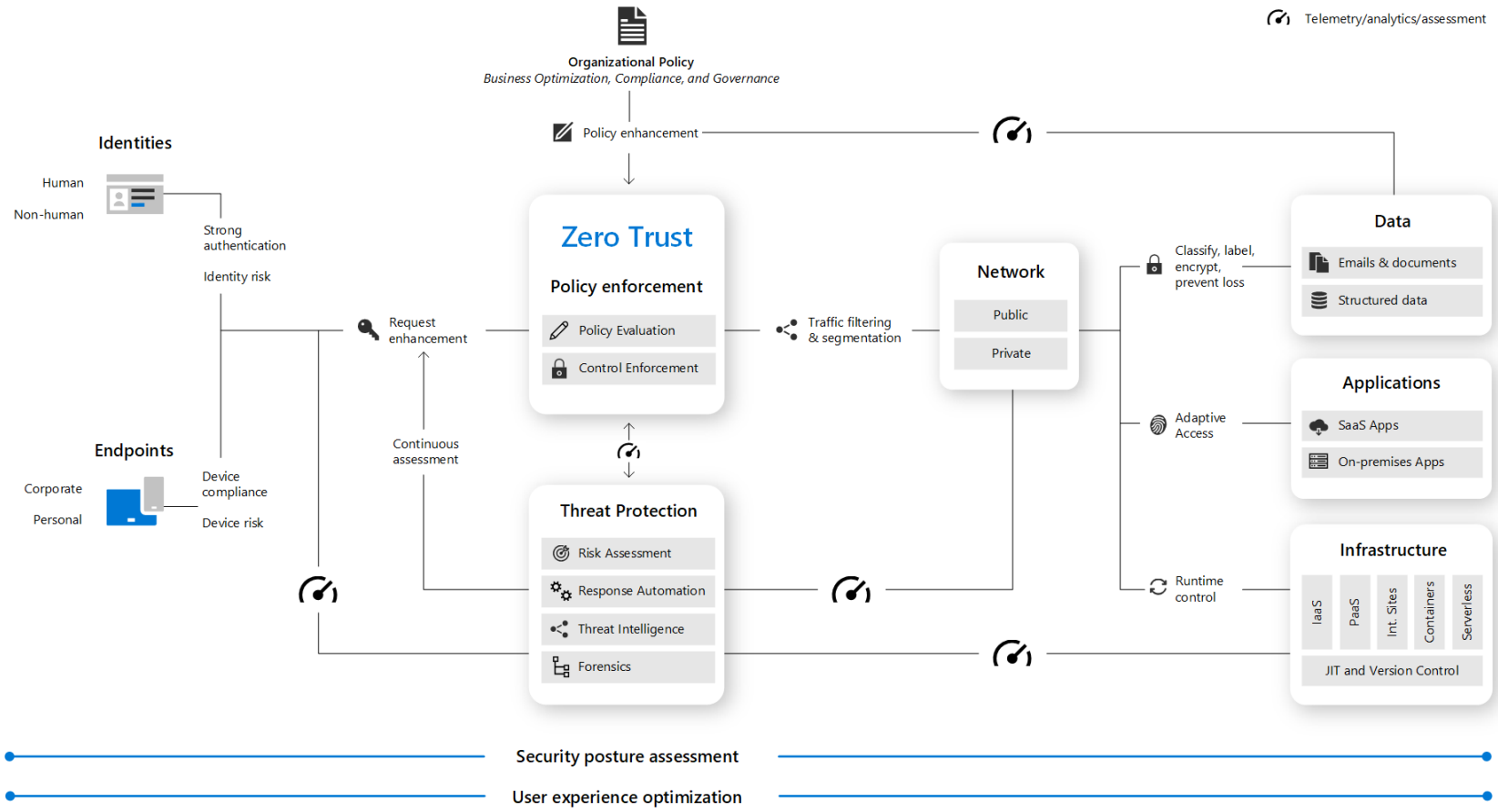
(Zero Trust Architecture Capability Maturity Model)



Solution Landscape for a Zero Trust Architecture

TECHNOLOGY COMPONENTS DEFINED BY CLOUD SECURITY ALLIANCE (CSA)

- **Software-Defined Perimeter**
- **Identity Aware Proxy**
- **Network Segmentation**
- **Service Mesh**
- **Edge Computing**
- **Policy as Code**



SOURCE: https://docs.microsoft.com/en-us/microsoft-365/security/microsoft-365-zero-trust?view=o365-worldwide

F5 Solutions for Zero Trust in Modern Application Environments

F5 Solutions for Modern Application Architectures

EXTENDING ZERO TRUST BEYOND THE SOFTWARE DEFINED PERIMETER

Service Mesh

- Network and Application Isolation (NGINX Service Mesh, Aspen Mesh)

Network Segmentation

- Hybrid Cloud and Edge Network Environments (F5 Distributed Cloud Services)

Security Posture Assessment

- Application Runtime Protection (F5 Application Infrastructure Protection – ThreatStack)

What Does A Service Mesh Actually Do?

• Proxy	⟸ *Data Plane*
• Orchestration	⟸ *Control Plane*
• Policy Management	⟸ *Management Plane*
• Policy Enforcement	⟸ *Data Plane*
• Monitoring	⟸ *Data + Control Planes*

Zero Trust Model ⟹

- *mTLS Enforcement and Access Control*
- *Service Identity for E/W and N/S traffic*
- *Pod and network isolation*
- *Ingress/Egress default deny*
- *Traffic governance*

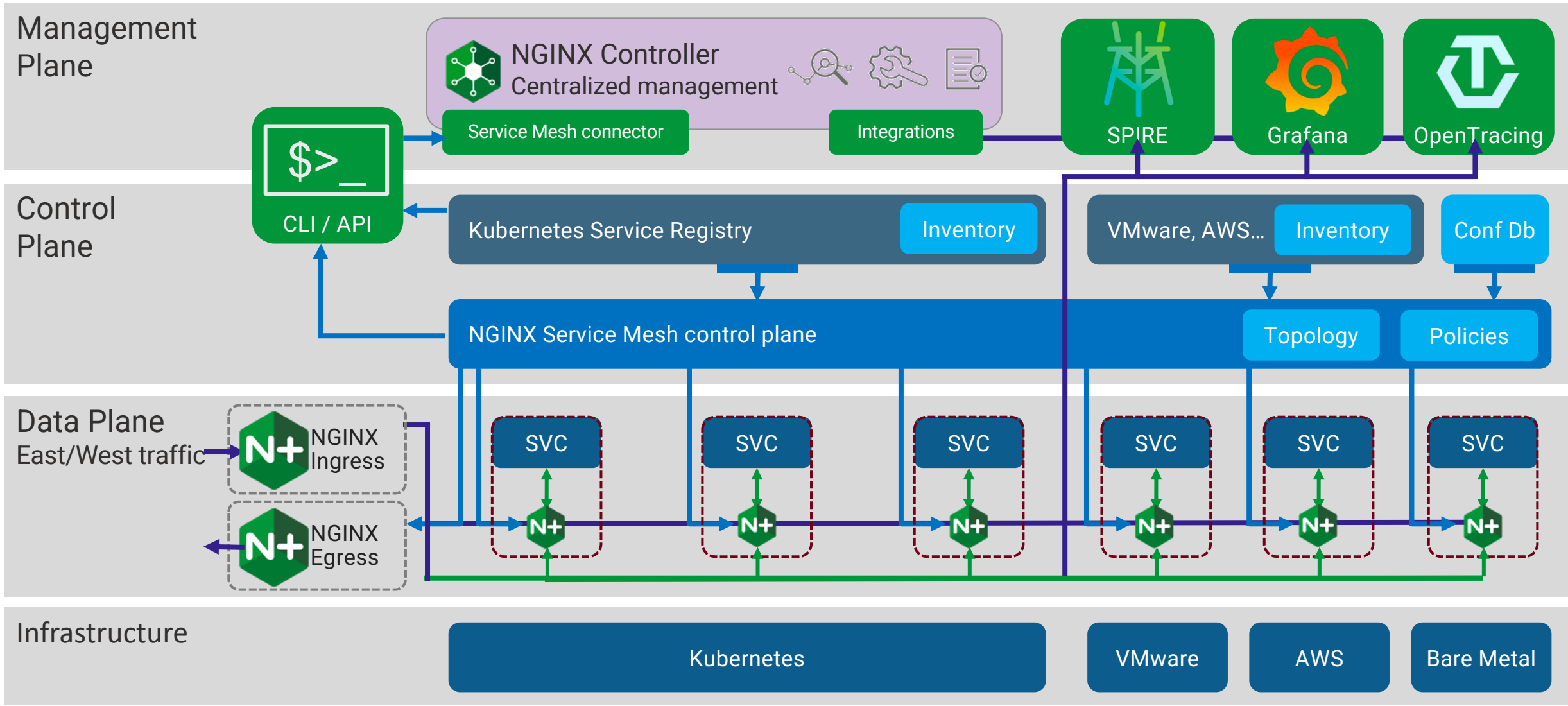
A Tale of Two Service Meshes

DIFFERENT OPTIONS FOR DIFFERENT USE CASES

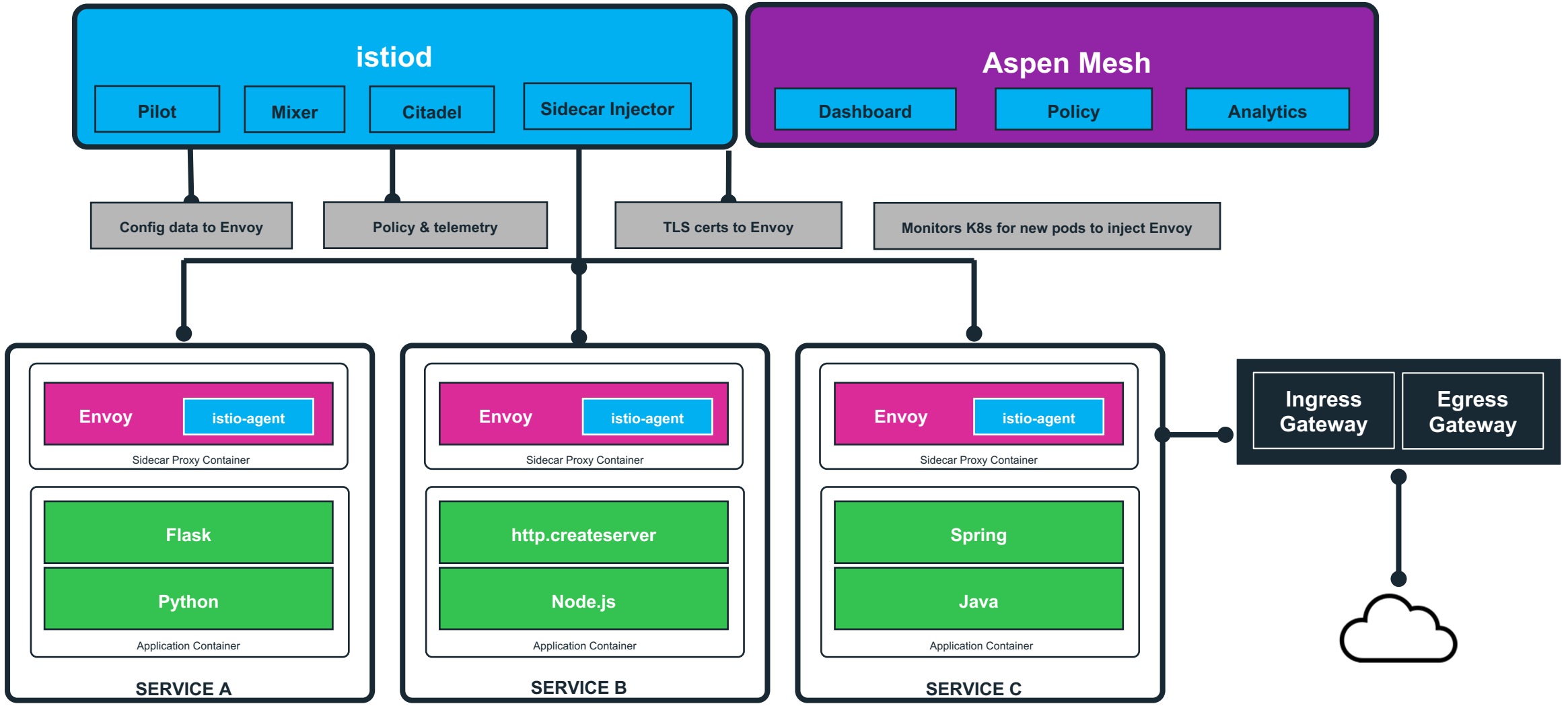
- **DEV**ops oriented
- Unified data plane for E/W and N/S control
- Integrates with Ingress Controller and WAF
- Light-weight resource footprint

- **NET**Ops oriented
- Istio-based
- Network-centric control of environment
- Service Provider specific use cases

NGINX Service Mesh Architecture



Aspen Mesh Architecture Overview



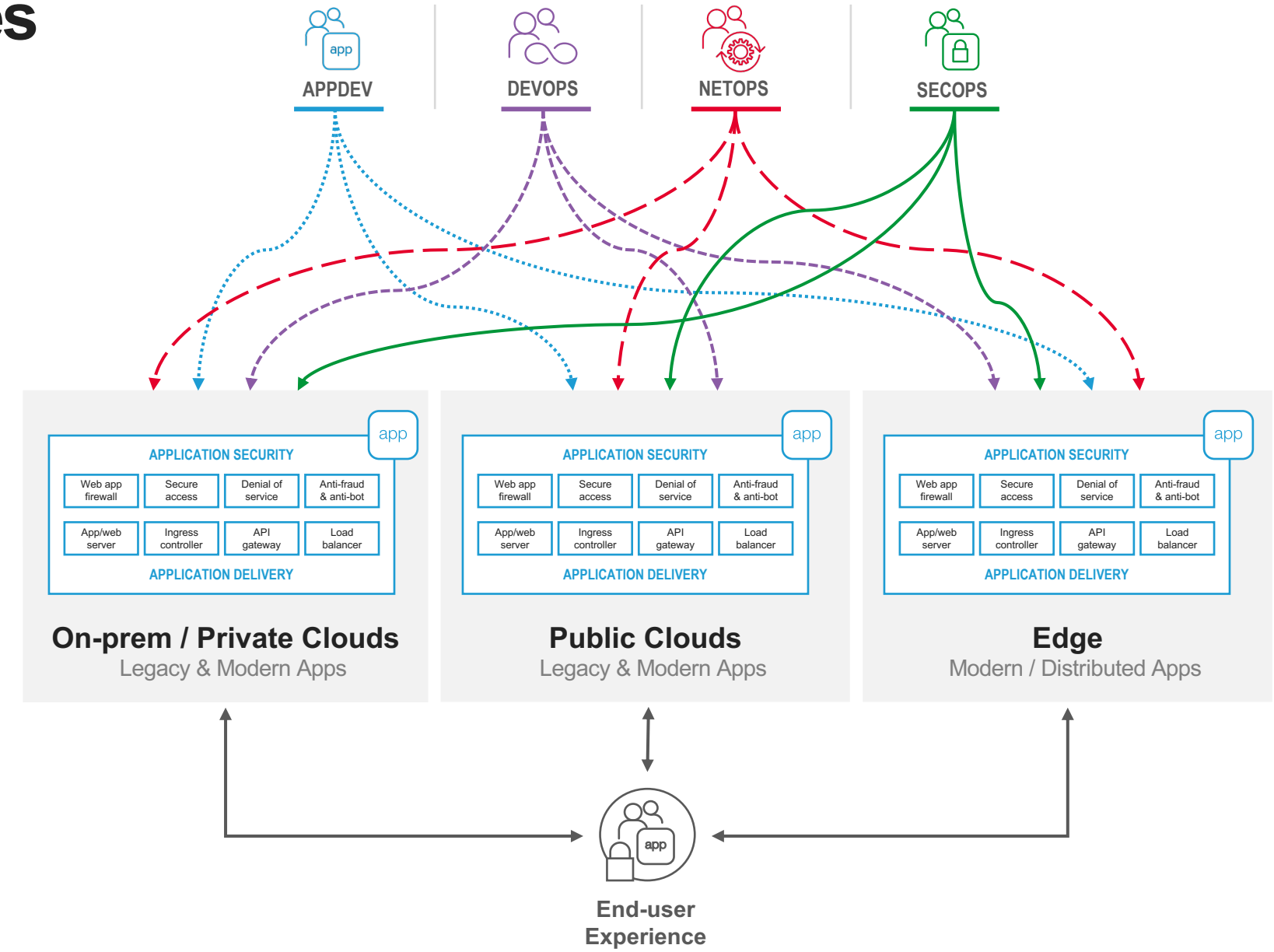
Technical challenges of delivering apps

#1 Complex coordination because of technology inconsistencies between teams and across environments

#2 Automation challenge ”stitching” multiple environments, layering net, security, and apps, at scale

#3 Security difficulties due to multiple different attack surfaces and sophistication of bad actors

#4 Limited observability of siloed telemetry trapped in disjointed systems & environments



Key Building Blocks in Modern Application Deployments

UNDERSTANDING THE CRITICAL COMPONENTS

Networking

- Router
- Firewall
- ADC
- DDoS Mitigation (Layer 3-4)
- API Gateway

App Security

- WAF
- API security
- DDoS Mitigation (Layer 7)
- Firewall
- Bot Defense

Distributed Networking and Security Services

App Development & Delivery

- K8s Compute Platform
- K8s Cluster Management
- Service Discovery
- Identity
- Secrets Management

Kubernetes Platform Services for Distributed Applications

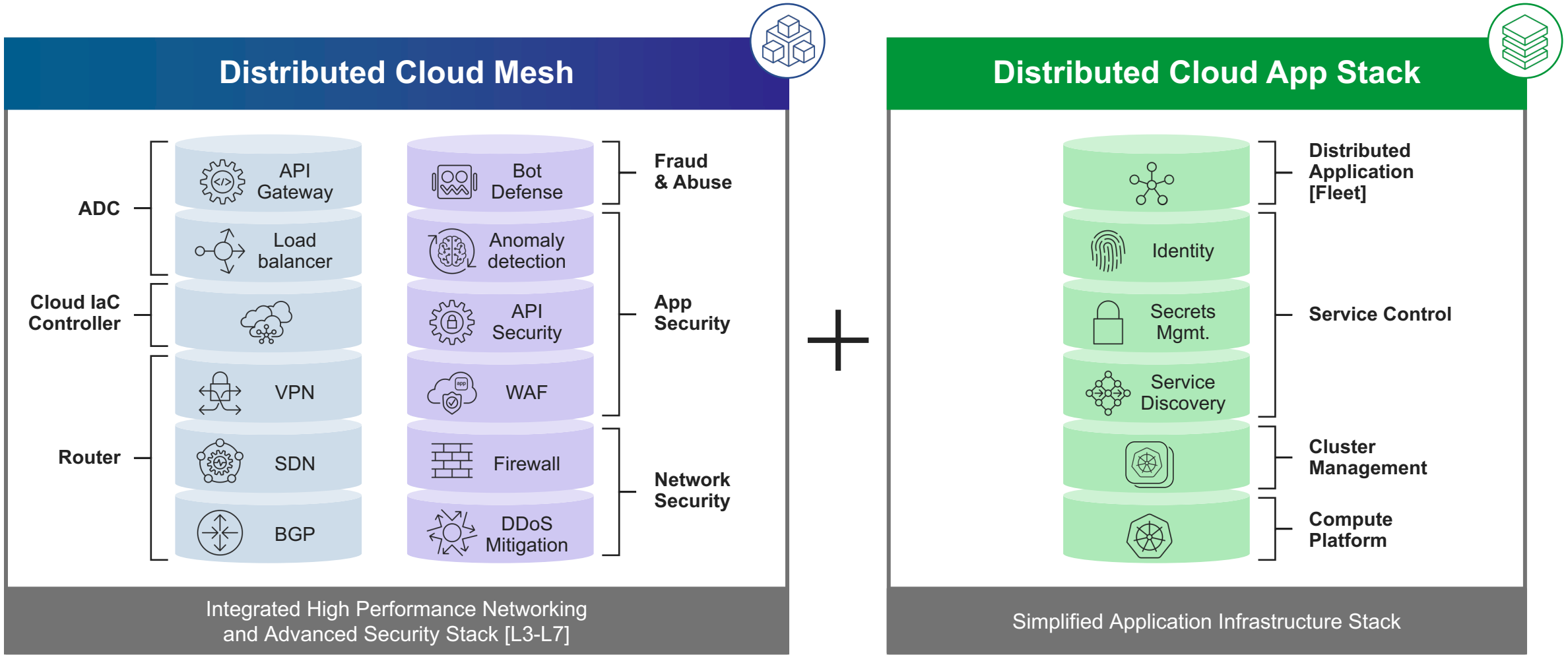
Distributed Cloud Console

SaaS-based centralized console managing application lifecycle and visibility

- Visibility and Analytics
- Centralized Operations
- Artificial Intelligence/ Advanced Insights

Leveraging a Distributed Node Architecture

FLEXIBLE DEPLOYMENT OPTIONS ACROSS CLOUD AND EDGE SITES



Modernization Increases the Threat Surface for Attack

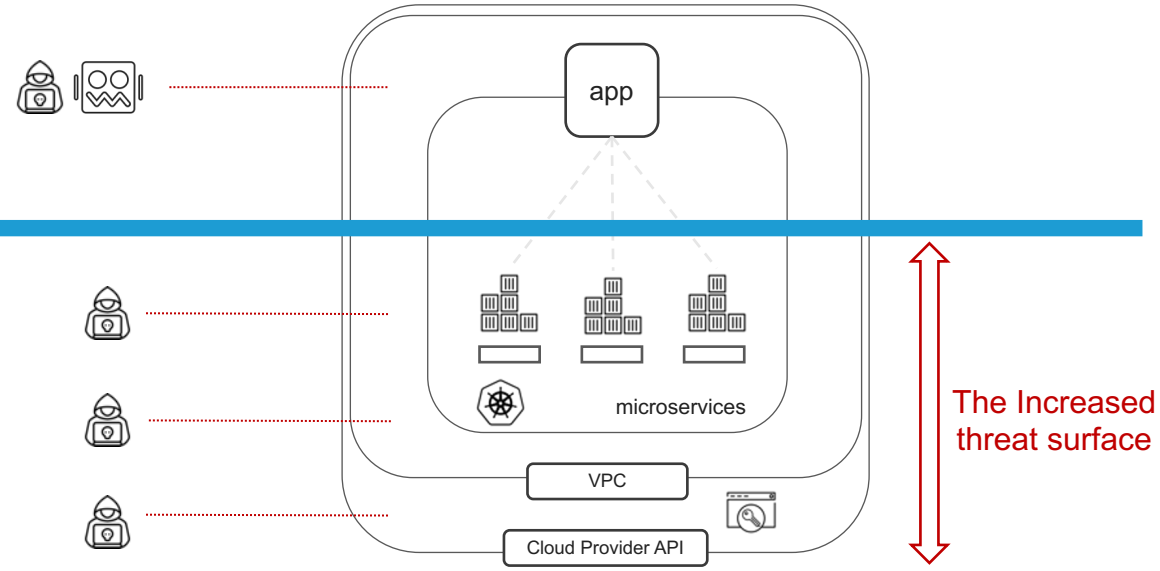
MODERN APPLICATIONS ARE COMPLEX, DISTRIBUTED, AND EPHEMERAL

1 The Application

Applications and APIs are susceptible to attacks that exploit vulnerabilities in code, software, or business logic.

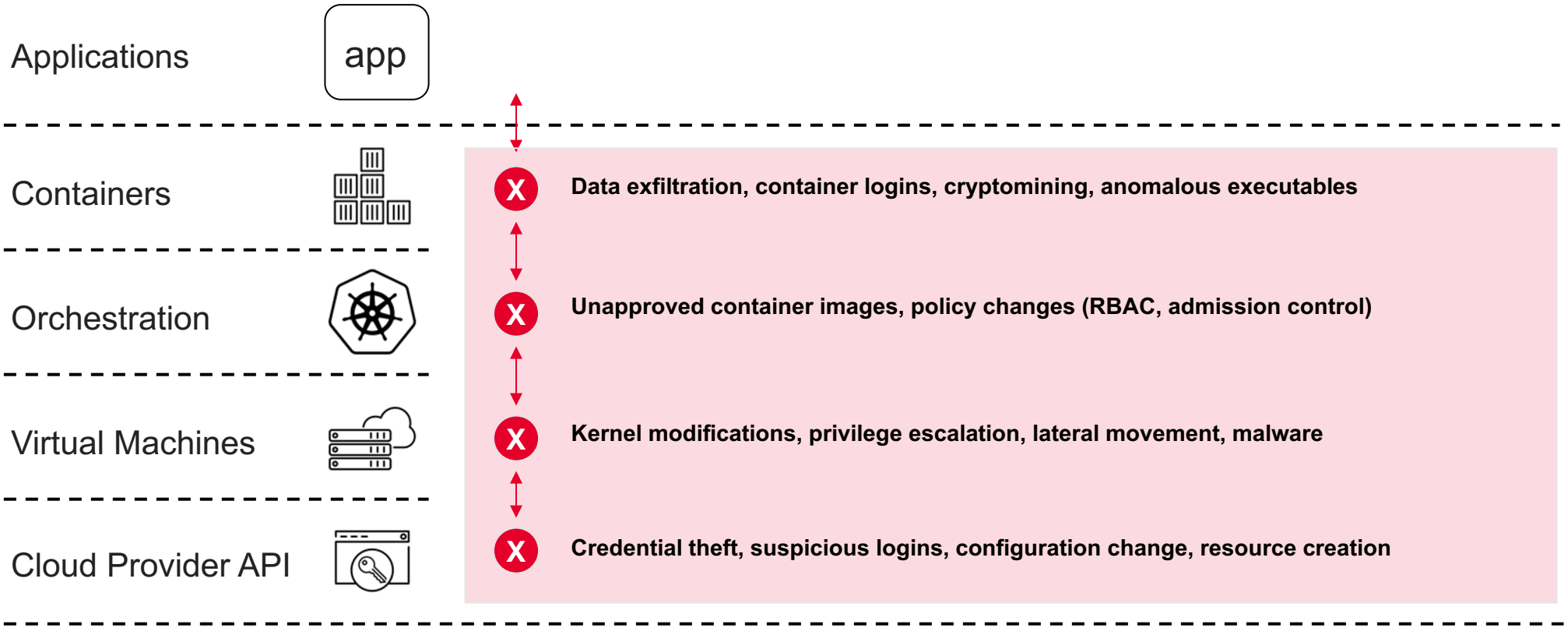
2 Cloud-native Infrastructure

Stolen keys, vulnerabilities, and misconfigurations in cloud-native infrastructure leave applications open to attack from internal or external threat actors.



Applications are only as secure as the workloads on which they run.

The Increased Threat Surface



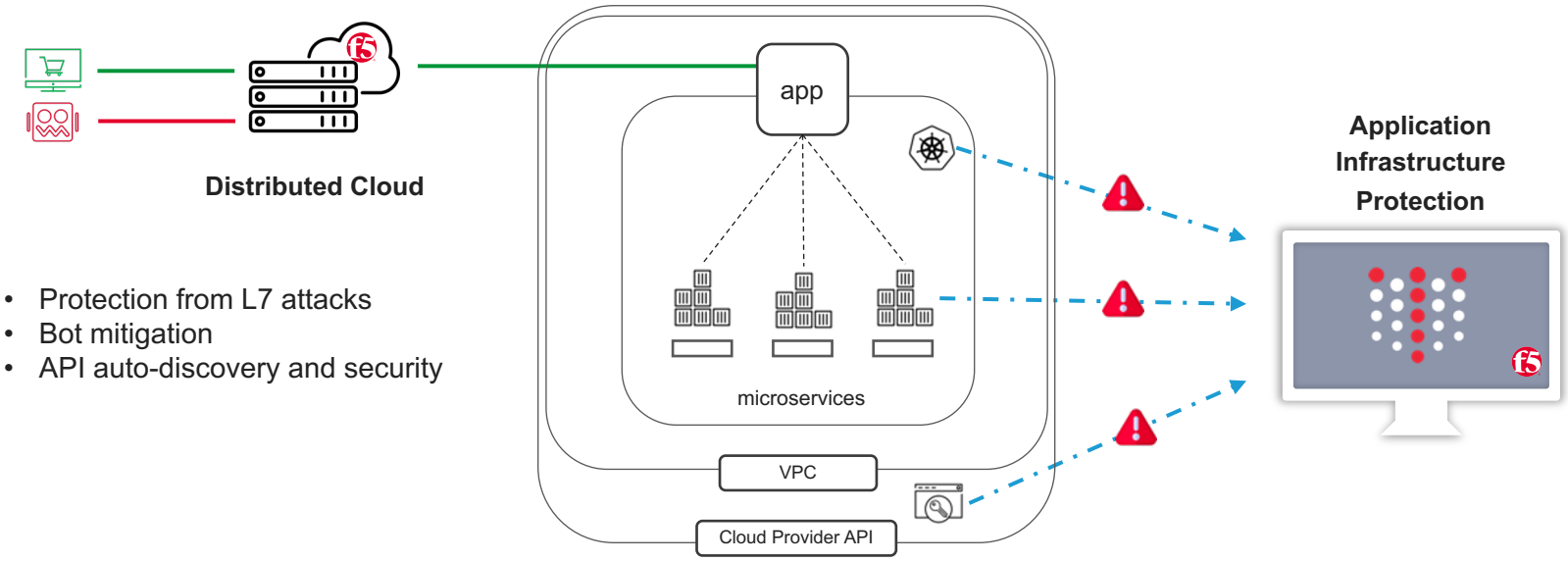
These are all behaviors that indicate compromise

Comprehensive Application Protection

DISTRIBUTED CLOUD SERVICES AND APPLICATION INFRASTRUCTURE PROTECTION DELIVERED AS A SAAS

Application and API Security

Application Infrastructure Protection



Distributed Cloud

- Protection from L7 attacks
- Bot mitigation
- API auto-discovery and security

Application Infrastructure Protection

- Intrusion detection for cloud-native workloads
- Real-time analysis of telemetry to detect threat and risk of exfiltration
- Monitor VMs, pods and Kubernetes
- 24x7/365 SOC

Observability and Security from Customer to Code

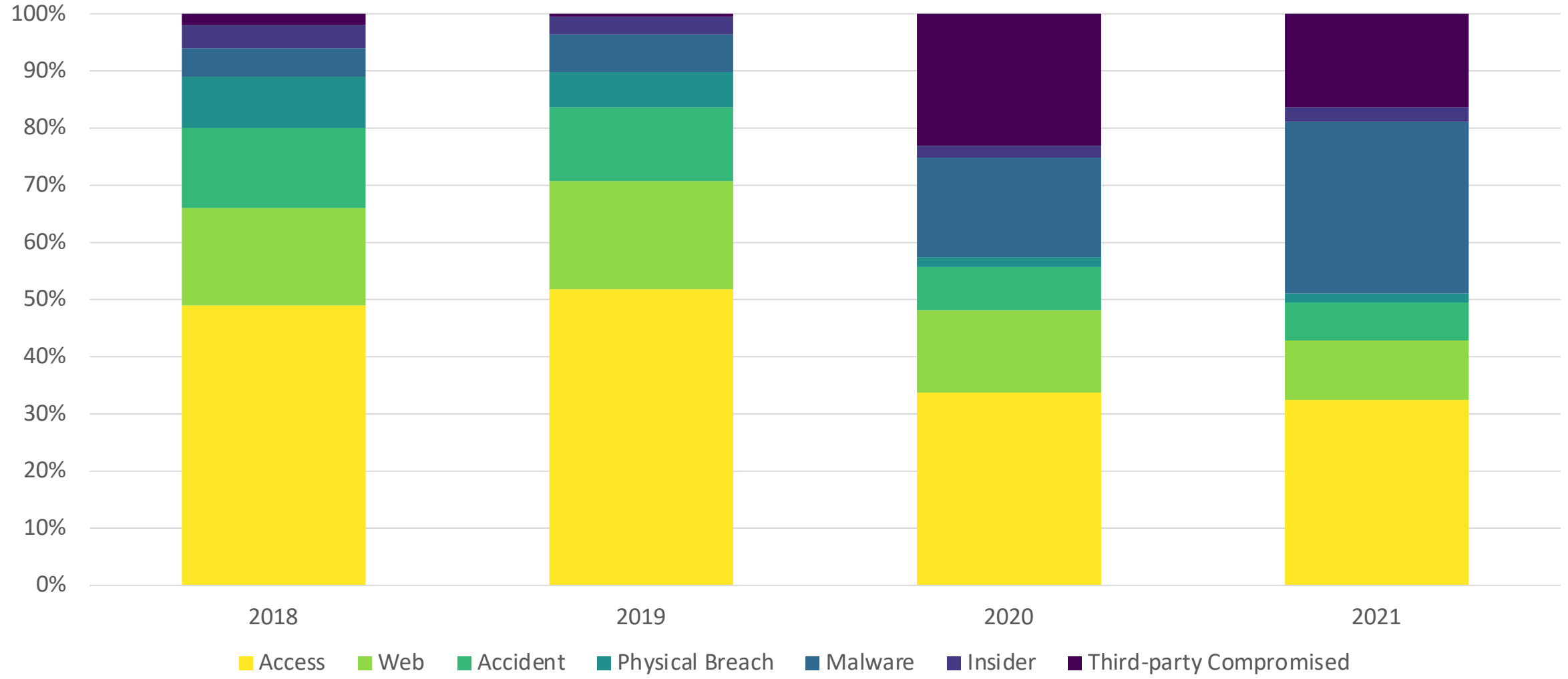
Why Zero Trust is Important

Application Protection Report

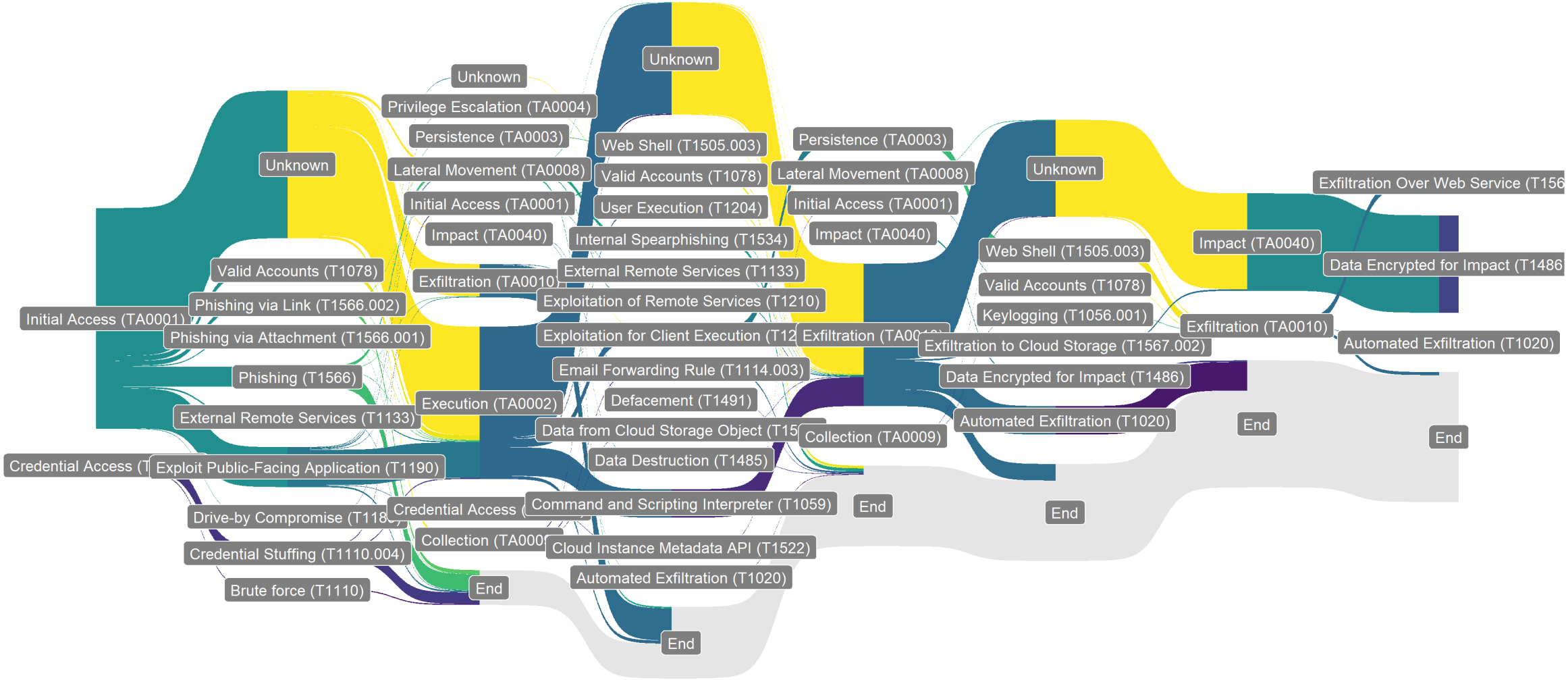
Using data to unite tactics and strategy in risk-based security

2018 - 2021 Data Breach Distribution

Historical view, Application Tiers Model



Data Breach Attack Chain Analysis



Recommended Mitigations

Arbitrary effectiveness coefficient = frequency x coverage

Mitigation	Arbitrary Effectiveness Coefficient
Data Backup	1.26
Network Segmentation	0.85
Restrict Web-Based Content	0.85
Application Isolation and Sandboxing	0.68
Exploit Protection	0.68
Privileged Account Management	0.68
Disable or Remove Feature or Program	0.61
Update Software	0.51
Network Intrusion Prevention	0.50
User Training	0.43
Filter Network Traffic	0.38
Antivirus/Antimalware	0.36
Vulnerability Scanning	0.34
Multifactor Authentication	0.29
Execution Prevention	0.24

Thanks for listening!