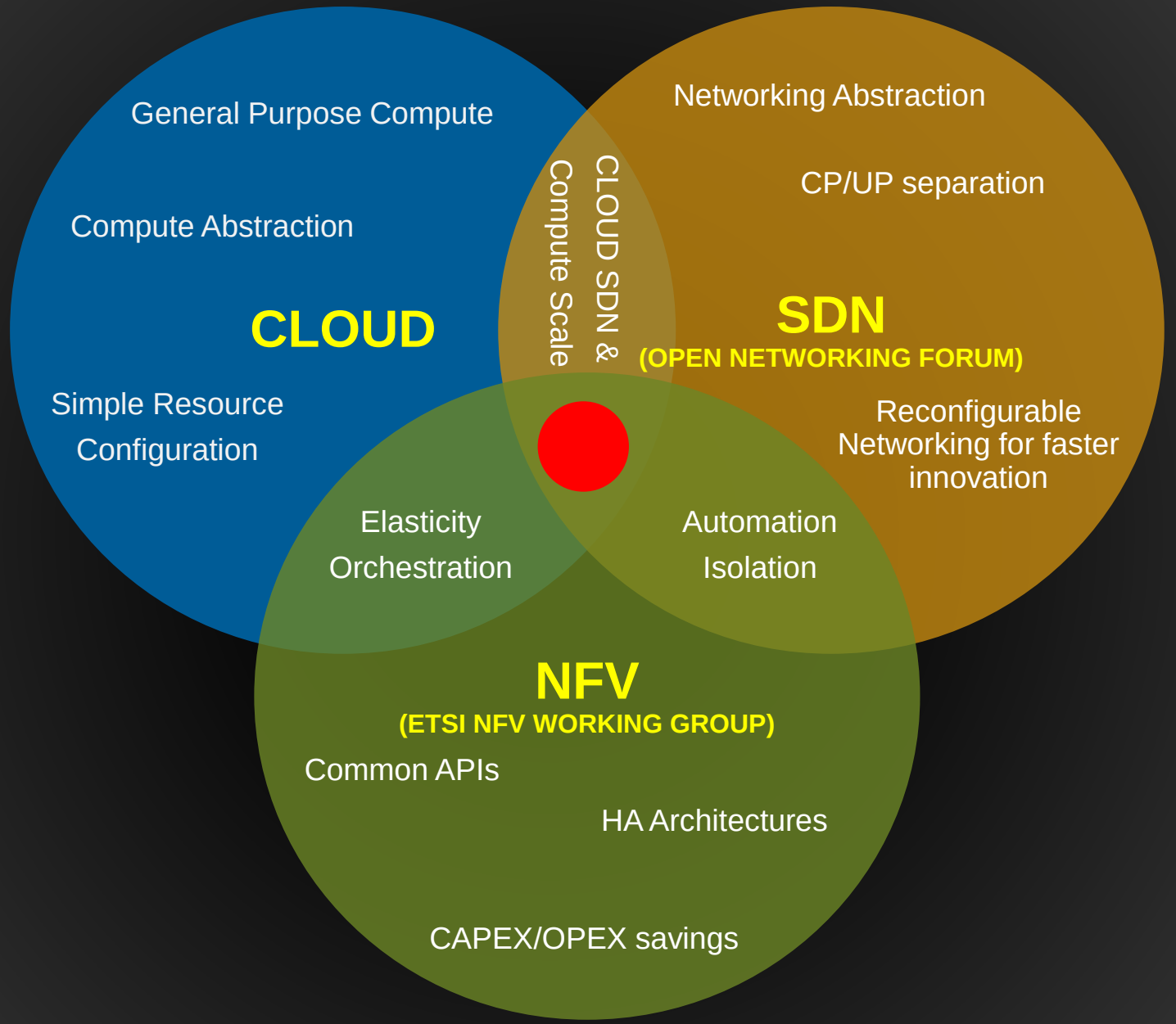
Transition to the Cloud

Protect your Identity,
Protect your Application,
Secure Your Data

Martin Oravec
F5 System Engineer
m.oravec@f5.com +421 908 747633


NFV
Orchestration
Private
Cloud
VNF
Hybrid
Public
SaaS
IaaS
PaaS
SDN



Cloud deployment models

Public Cloud

- Available to anyone
- Shared infrastructure
- Lower costs

Virtual Private Cloud

- Pool of shared computing resources
- Logically isolated through separation of IP subnets / virtual communications

Hybrid Cloud

- Combination of either in-house or private cloud with public cloud
- Allows secure sensitive data and efficiencies of non-sensitive data

Private Cloud

- Secure environments
- Only customer has access
- Physically isolated

Types of Cloud Computing Services

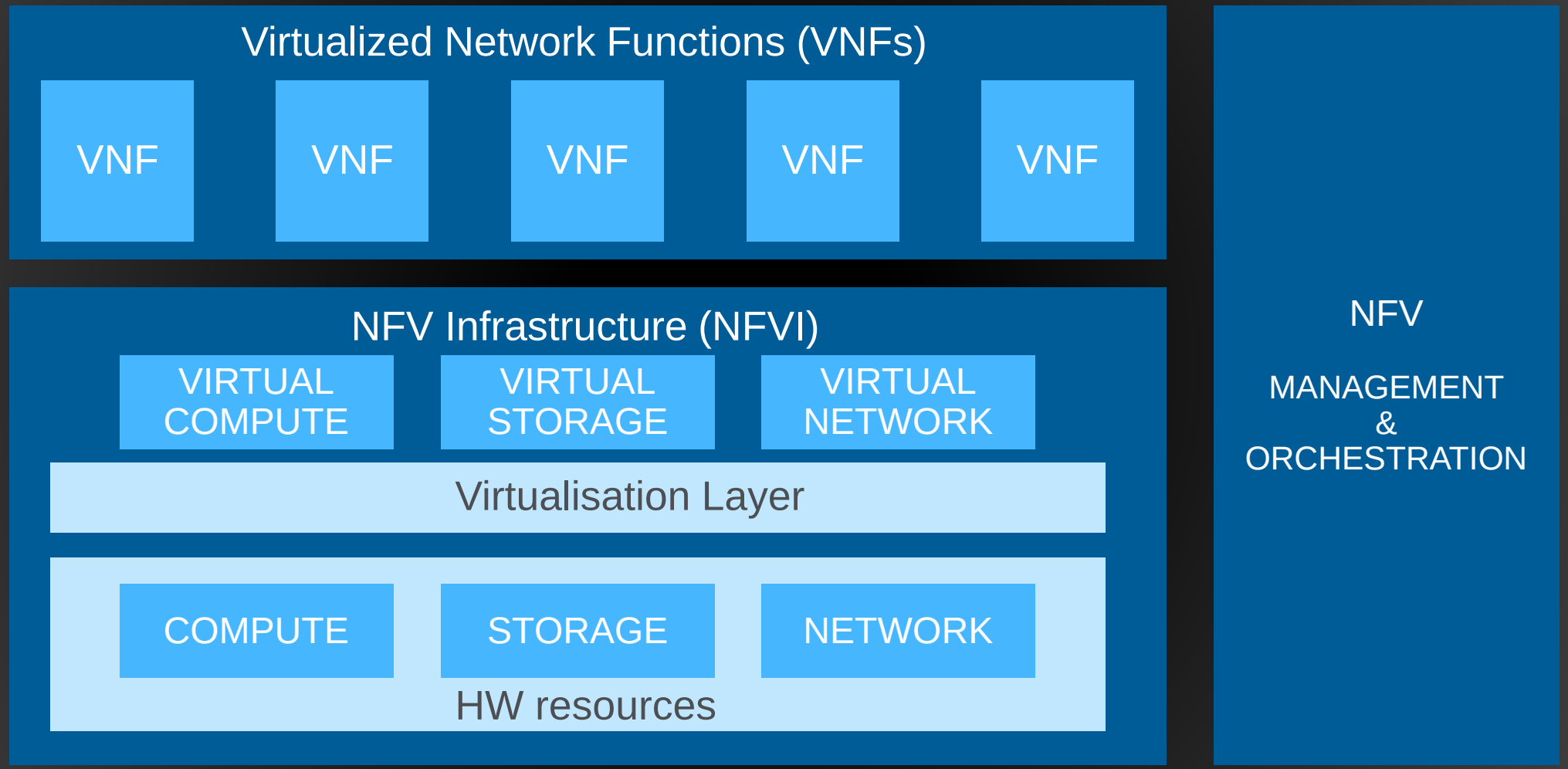
Cloud Layer	Service Models		
	IaaS	PaaS	SaaS
Data			
Interfaces (APIs, GUIs)			
Applications			
Solution Stack (Programming languages)			
Operating Systems (OS)			
Virtual Machines			
Virtual network infrastructure			
Hypervisors			
Processing and Memory			
Data Storage (hard drives, removable disks, backups, etc.)			
Network (interfaces and devices, communications infrastructure)			
Physical facilities / data centers			

Infrastructure as a Service (IaaS)

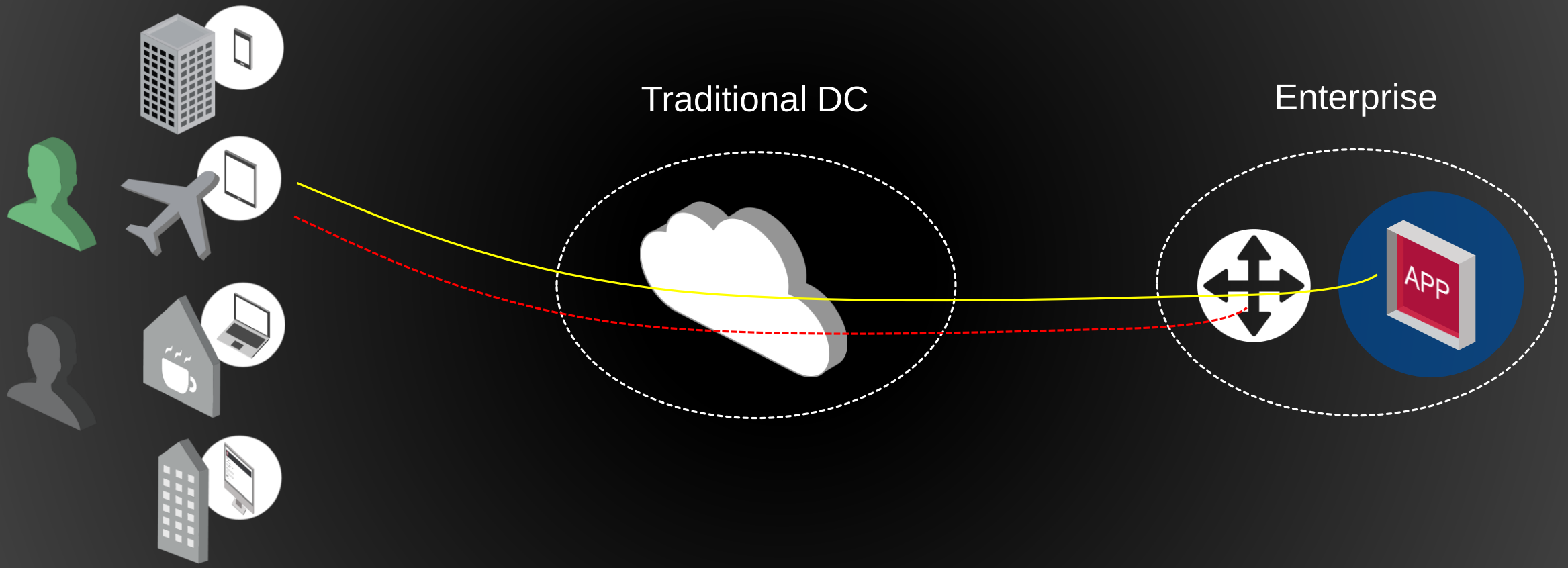
Platform as a Service (PaaS)

Software as a Service (SaaS)

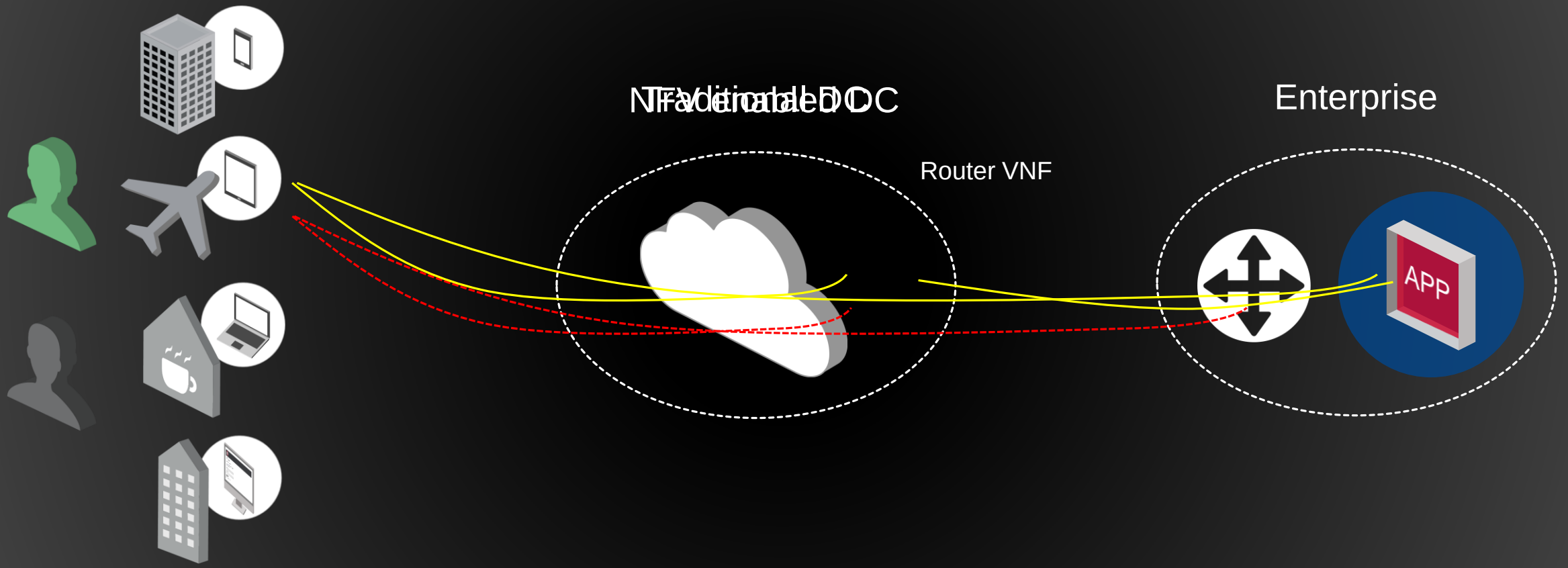
NFV vs VNF



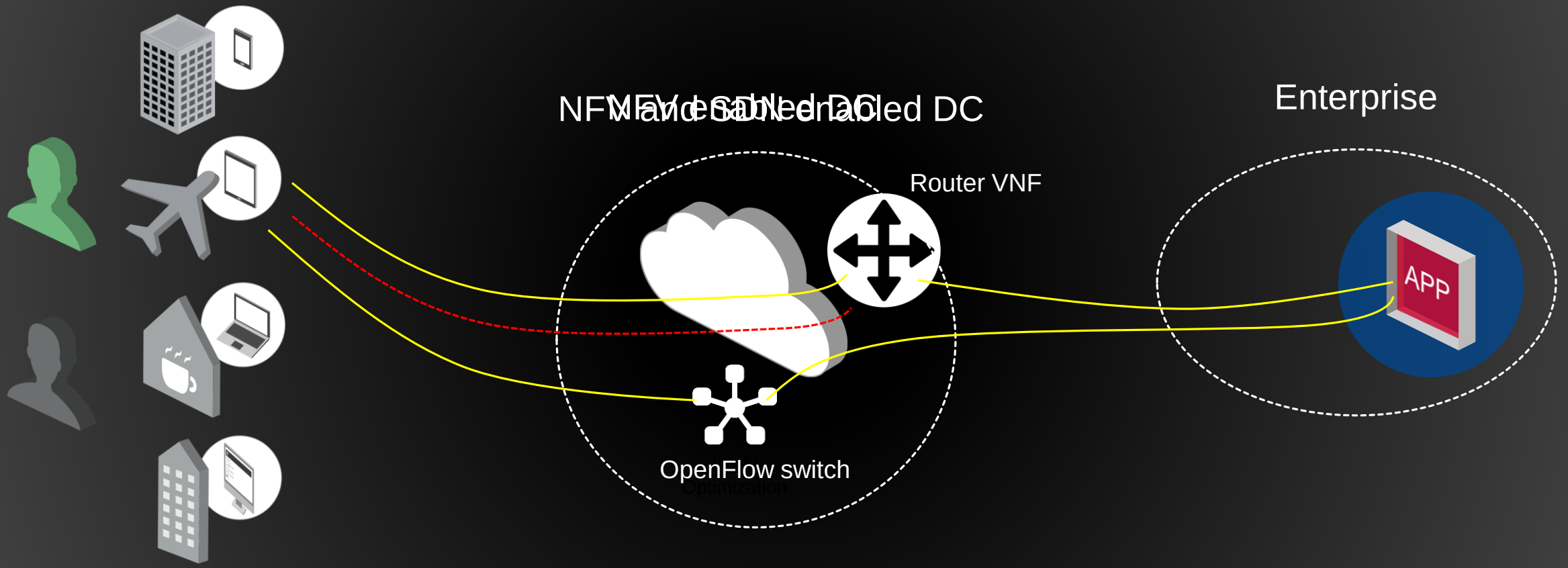
SDN and NFV - working together ?



SDN and NFV - Managed Router using NFV



SDN and NFV - Managed Router using NFV + SDN



Transition to the Cloud

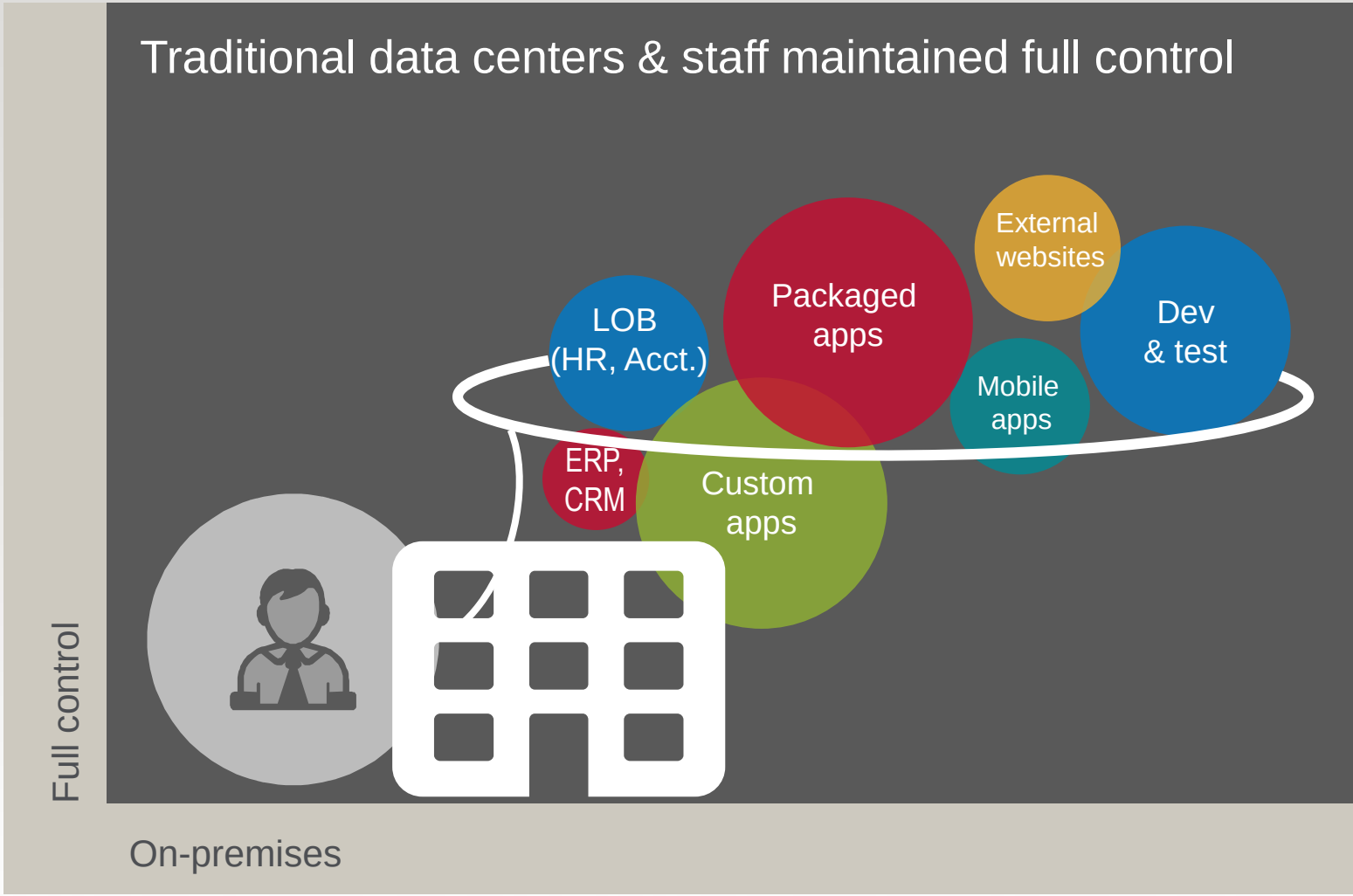
Security perimeter change

Traditional DC strategy

Applications centrally managed under one infrastructure

Data center boundaries providing protection

IT staff ensures availability, performance, and security

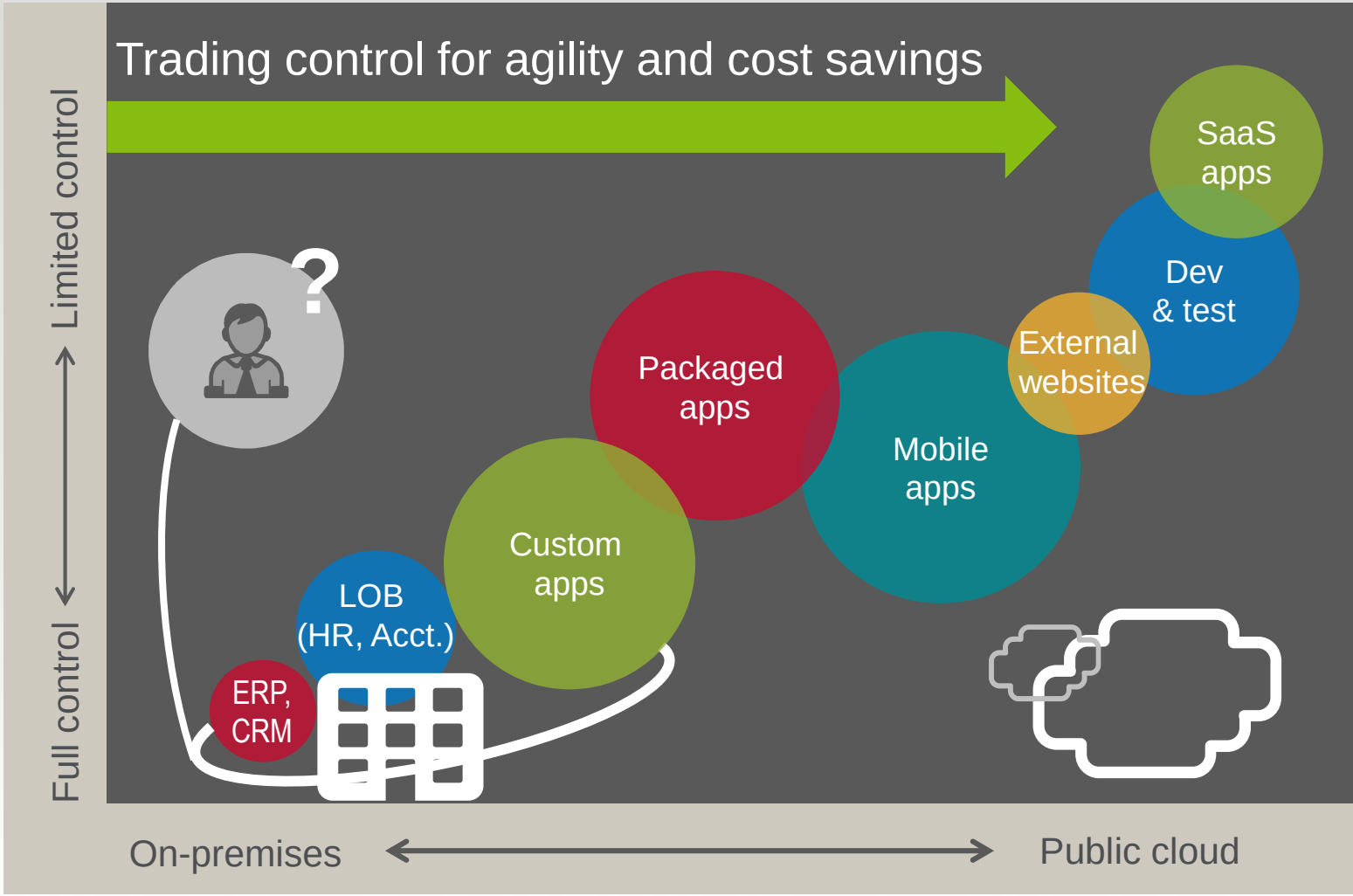


The DC evolution

72% of orgs expect to put **more than half of workloads in the cloud by 2017**[1]

CIOs trading control for **agility and cost savings**

Traditional data center **perimeters are dissolving**



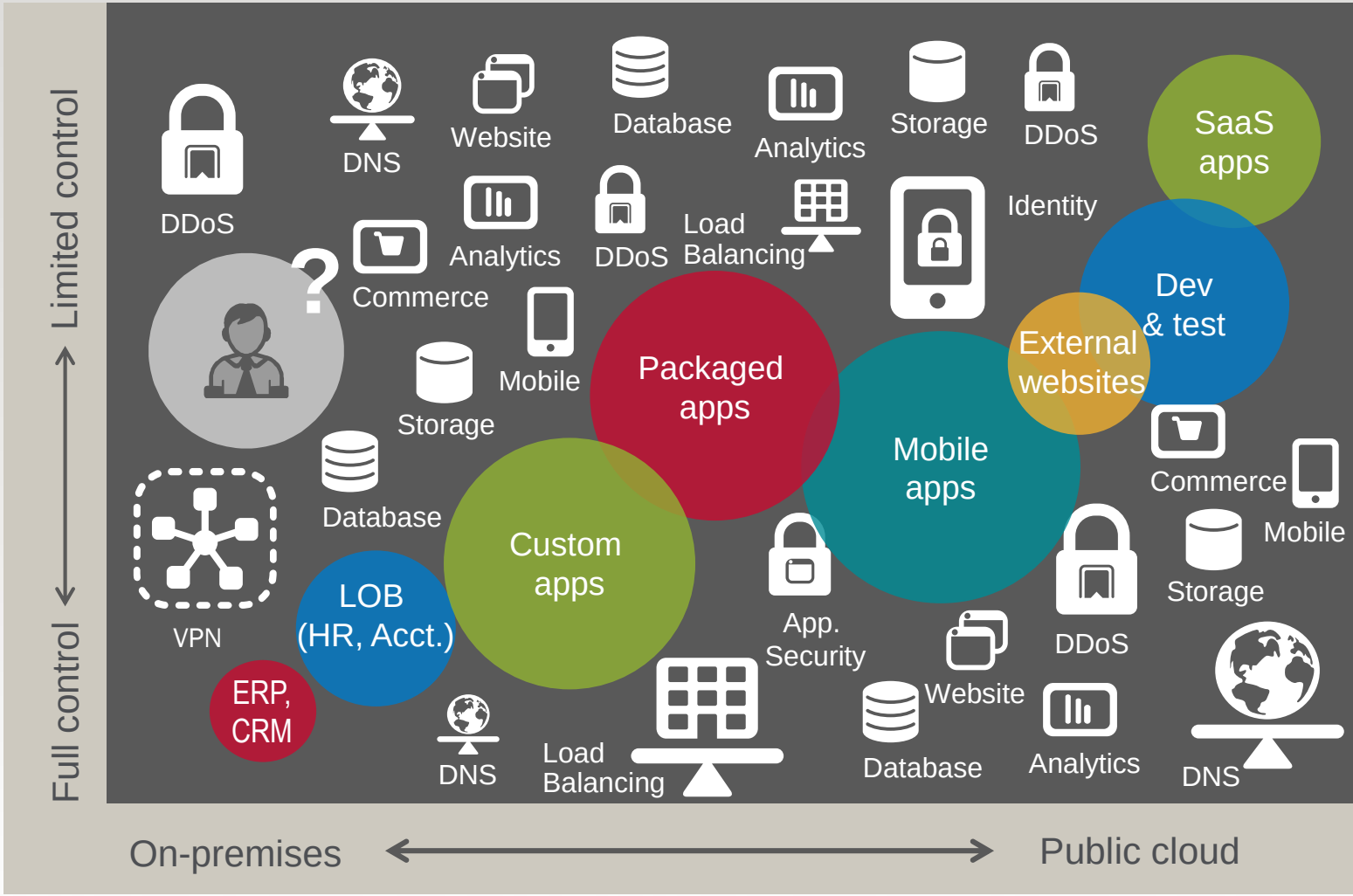
Sources: [1]Research report for Verizon

A new world of complexity and risk emerging

Cloud vendors deliver a services-centric model via disparate building blocks (i.e. data, app tier, DNS…)

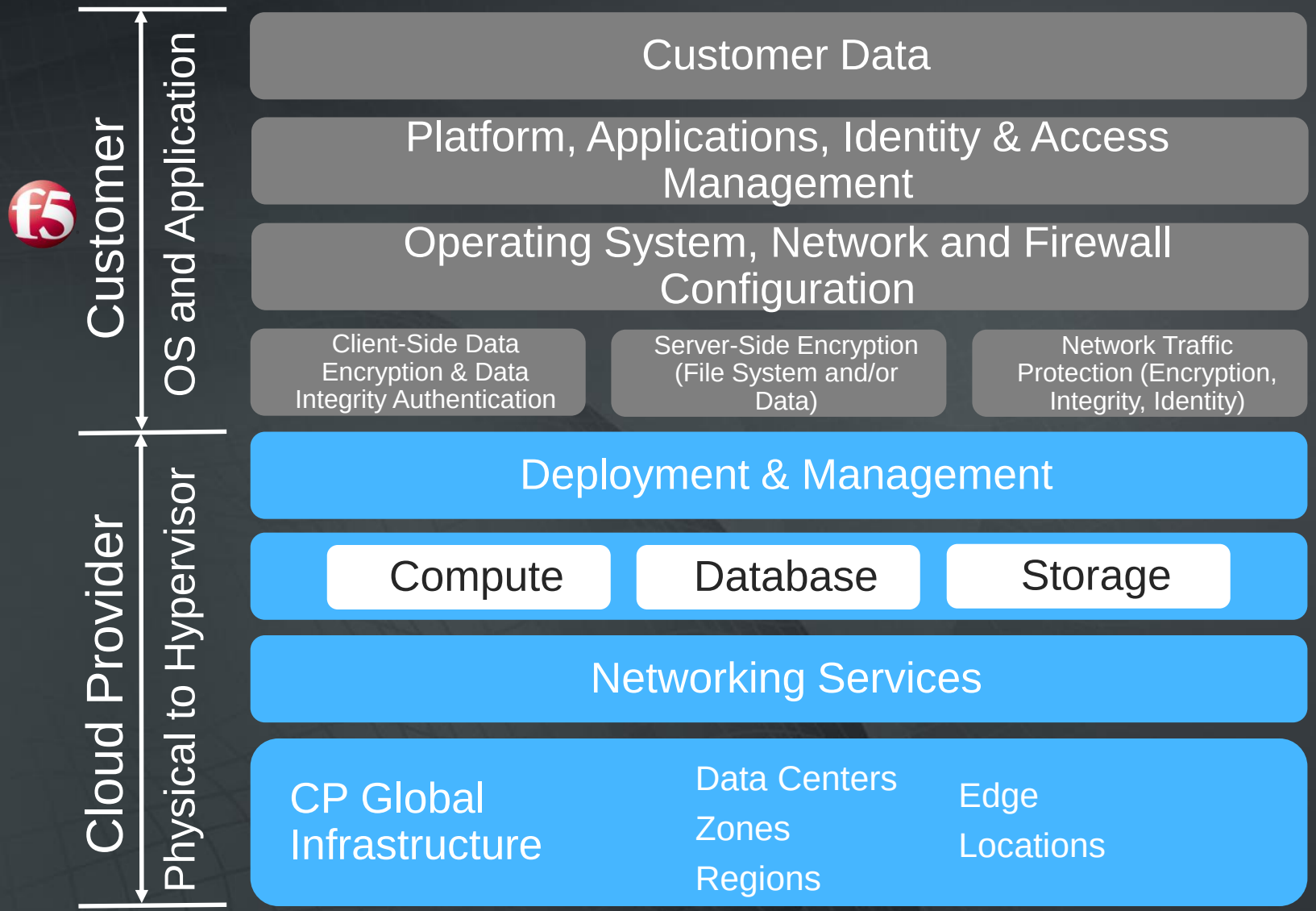
Availability and security limited to infrastructure and the individual services; not the apps

90% of organizations are **concerned about public cloud security**[1]



Sources: [1]Cloud Security Spotlight Report

Public Cloud - Shared Responsibility Security Model



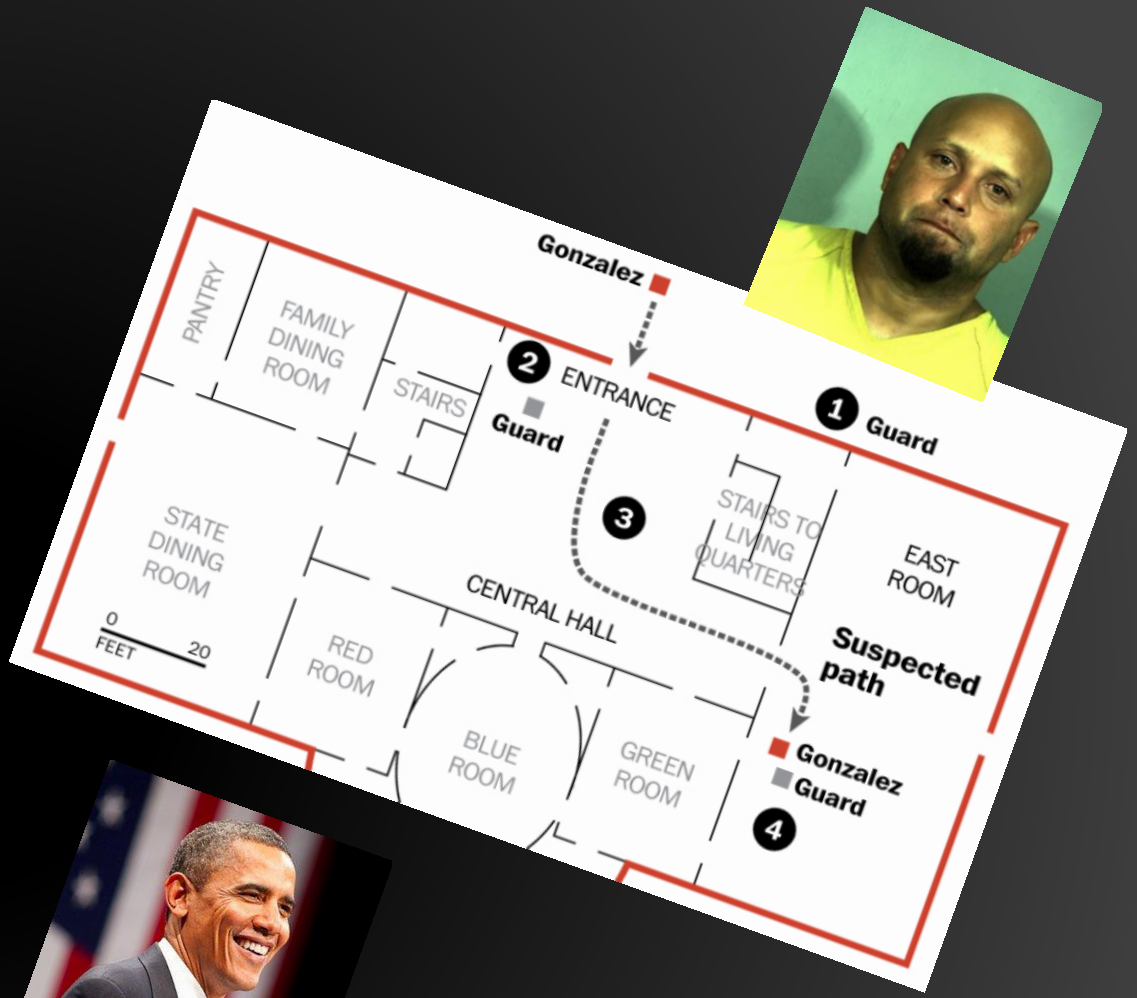
Customer's responsibility

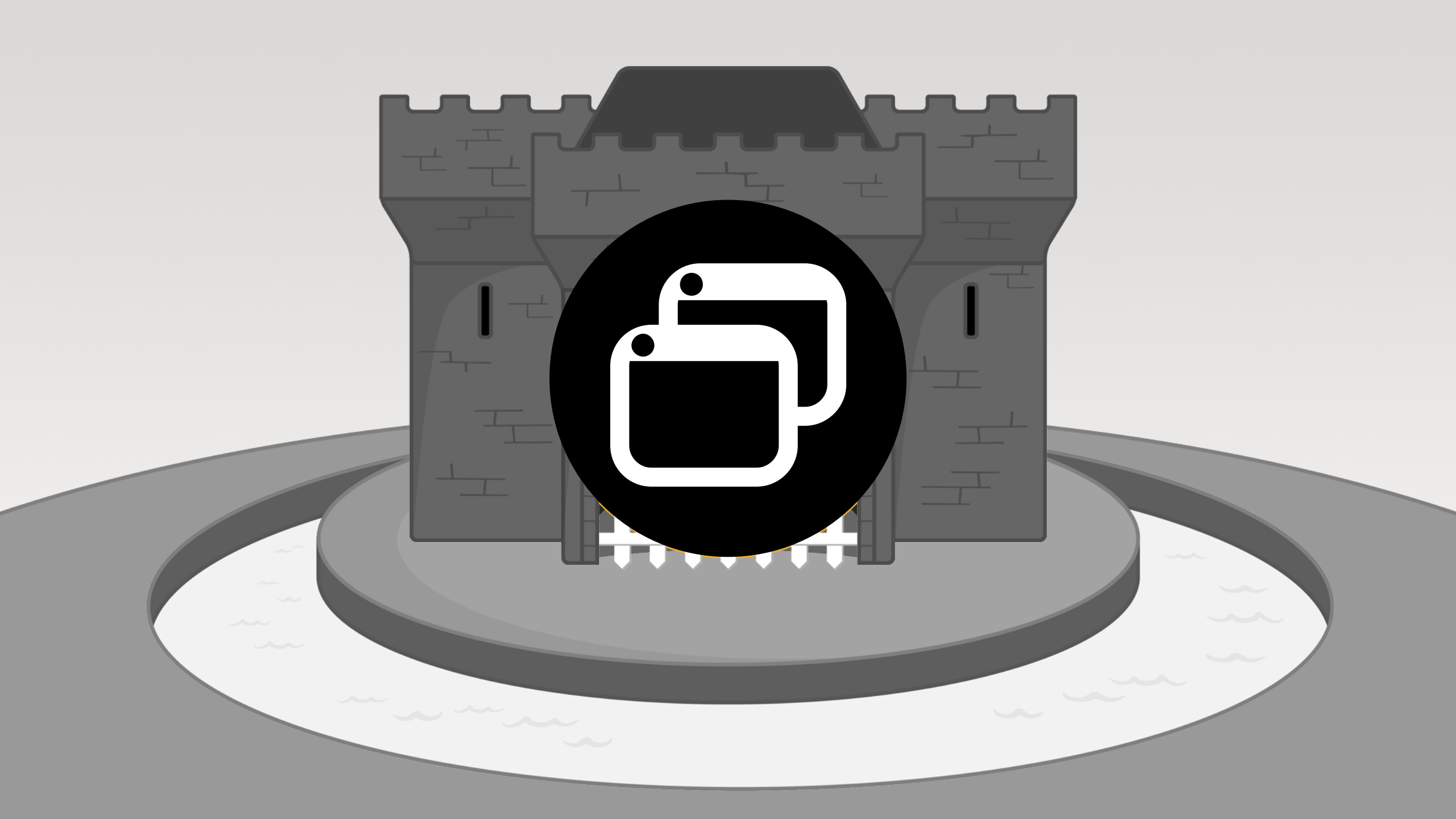
- Protecting the confidentiality, integrity, and availability of their data in the cloud
- OS and application-level security

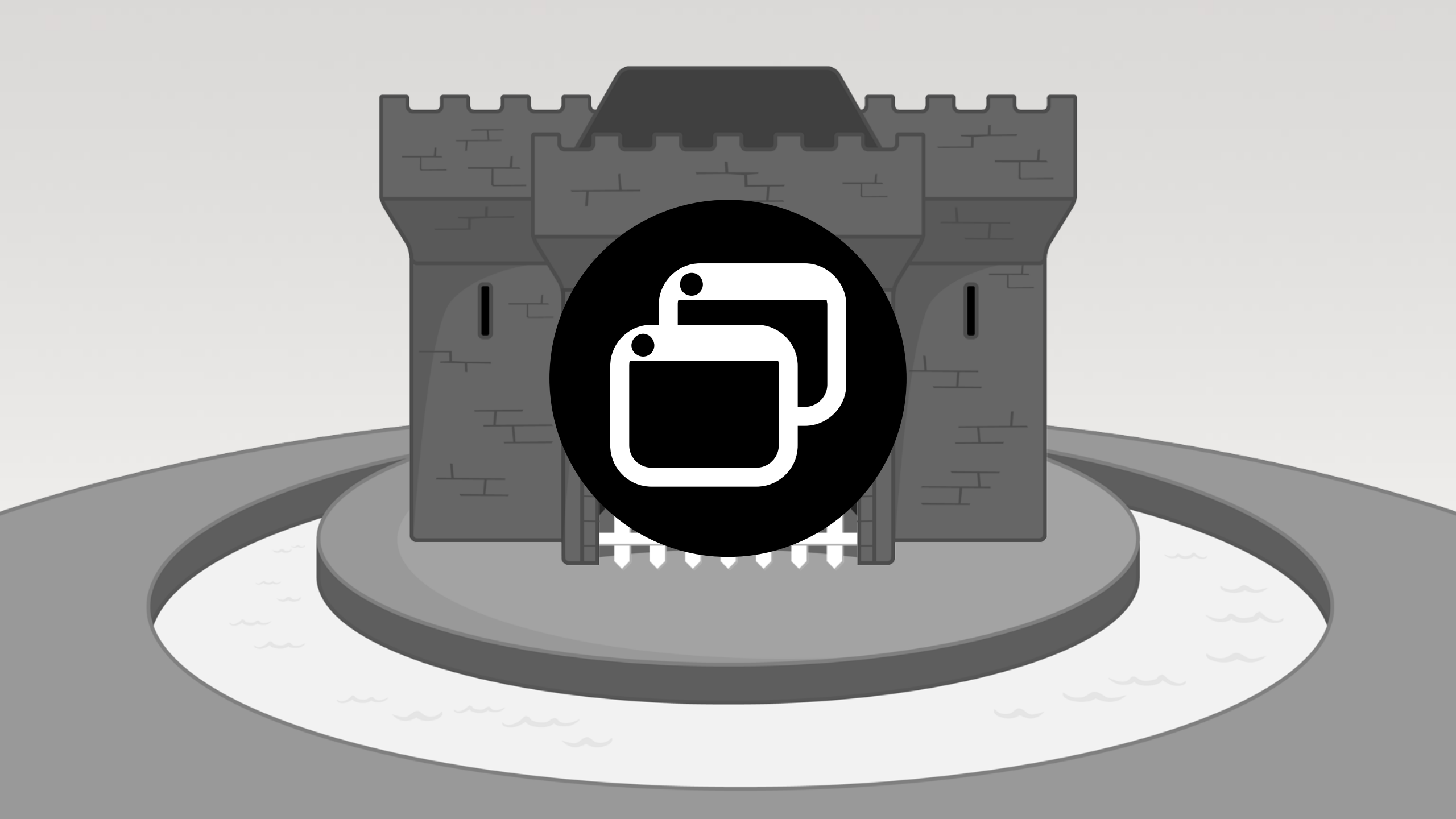
Cloud Provider responsibility

- Providing a global secure infrastructure and services


You can’t secure what you don’t know


Gonzalez
PANTRY
FAMILY DINING ROOM
STAIRS
2 ENTRANCE
Guard
1 Guard
3
STAIRS TO LIVING QUARTERS
EAST ROOM
STATE DINING ROOM
CENTRAL HALL
0 FEET 20
RED ROOM
BLUE ROOM
GREEN ROOM
Suspected path
Gonzalez
Guard
4





Control through context

Client Information + Traffic Content + Application Health

1. Client context in security

Device

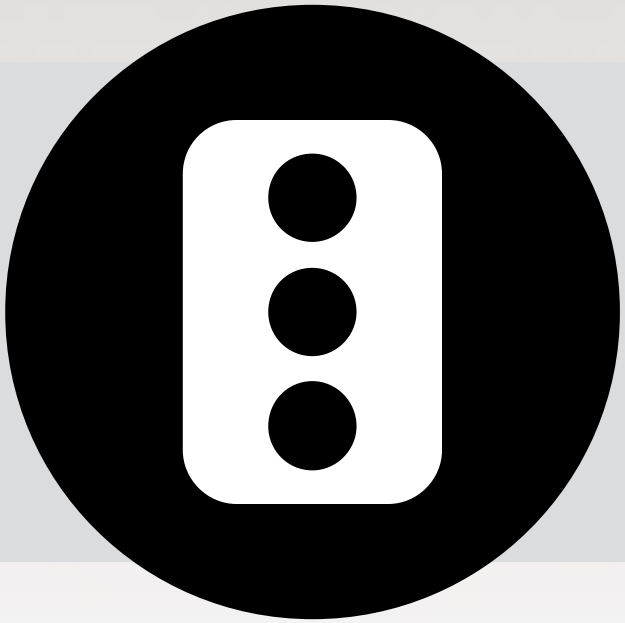
Operating system

Browser

Geolocation

IP intelligence

2. Traffic context in security



Unauthorized access

SYN flood

XSS

SQL injection

Fraud

3. Application context in security

App health

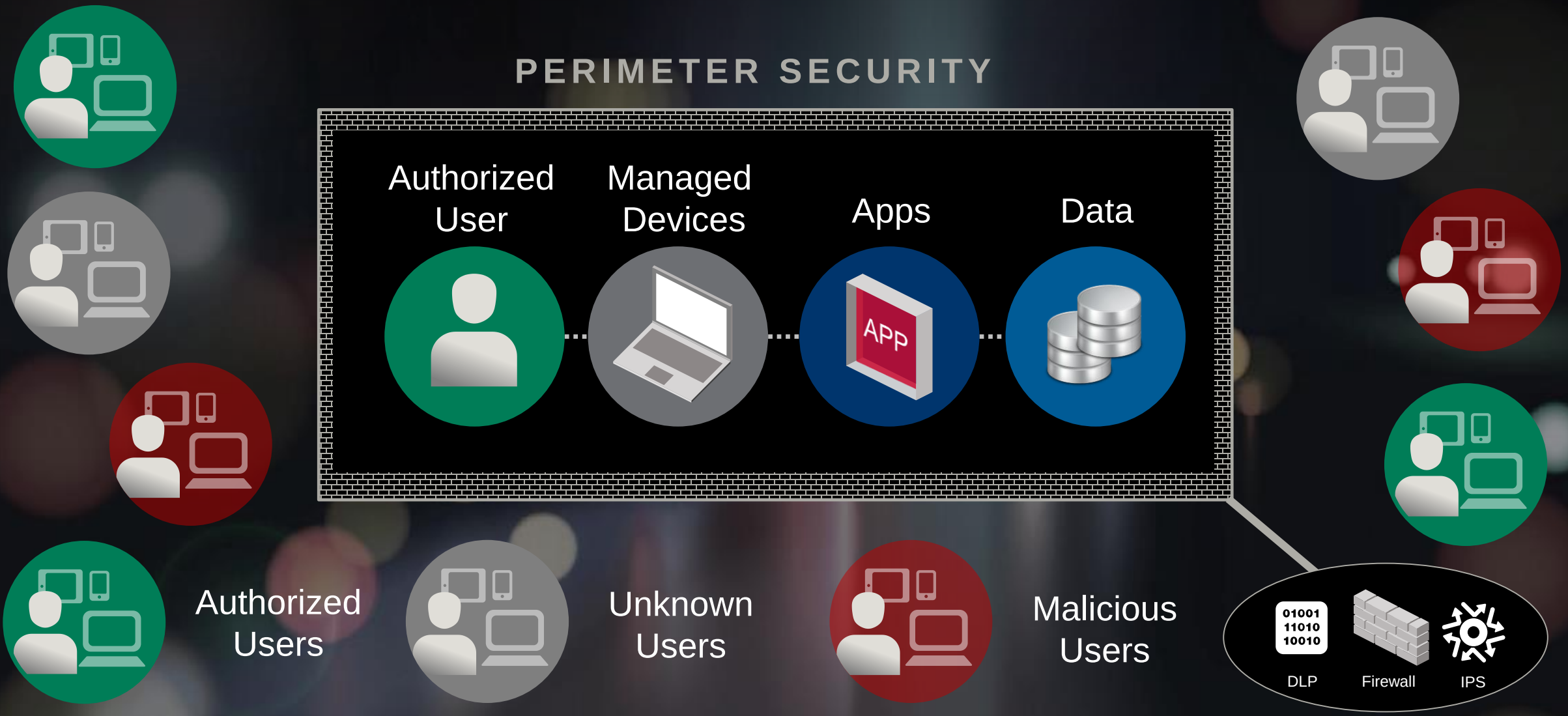
Server status

Software type/version

App vulnerability

Resource capacity

Traditionally, data was secure inside the perimeter



The Perimeter has dissolved…

Untrusted Users

PERIMETER SECURITY

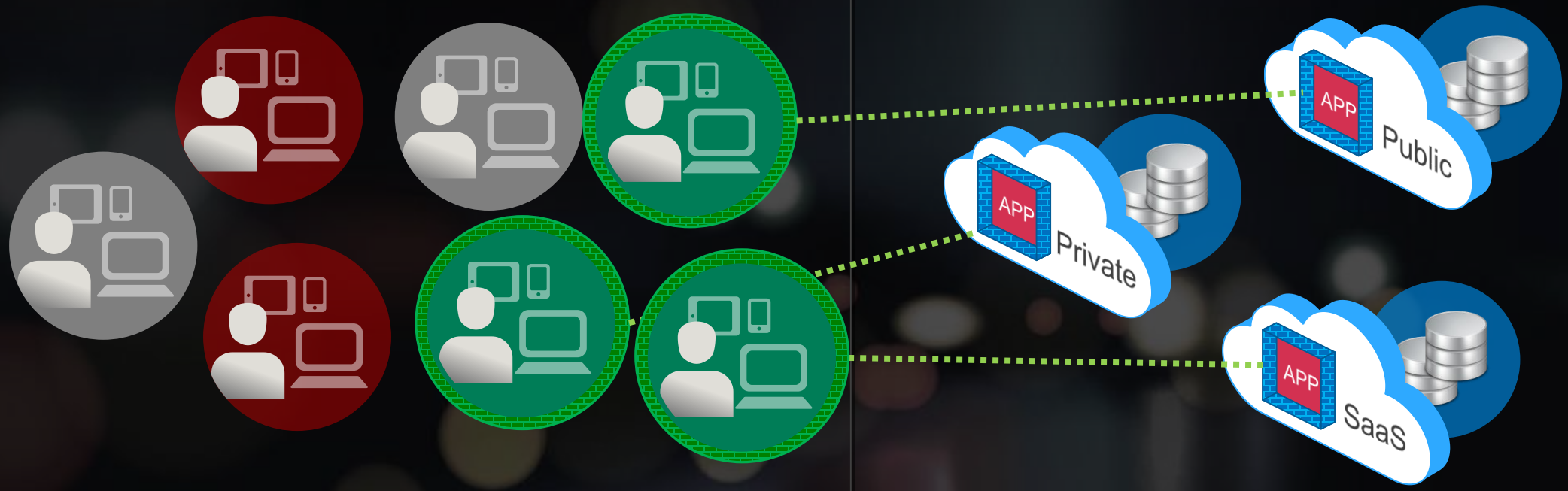
ZERO TRUST

…and Zero Trust is the new mantra

F5s Access, Identity, and App Protection Solutions

F5 IDENTITY & ACCESS MANAGEMENT

F5 APPLICATION PROTECTION



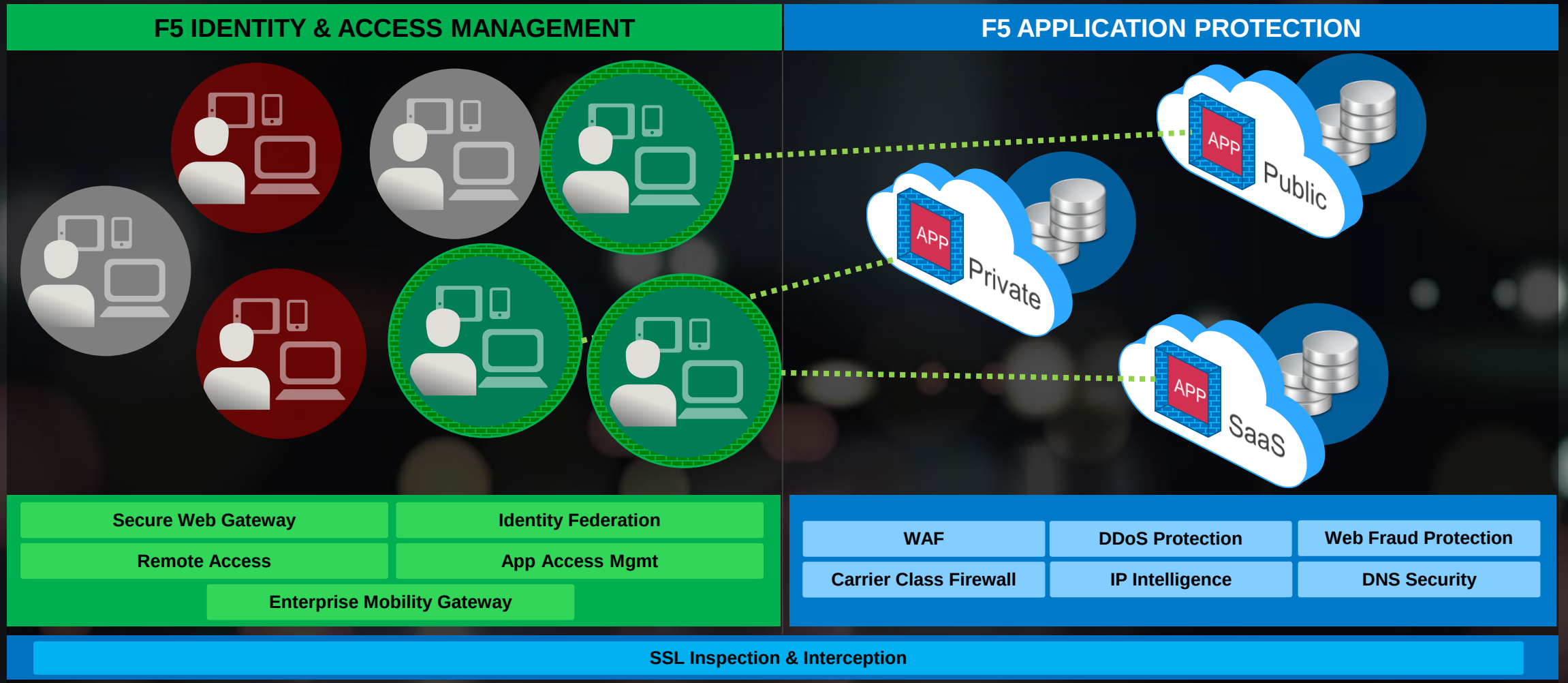
PROTECT ACCESS & IDENTITY

Enable secure access for any user on any device

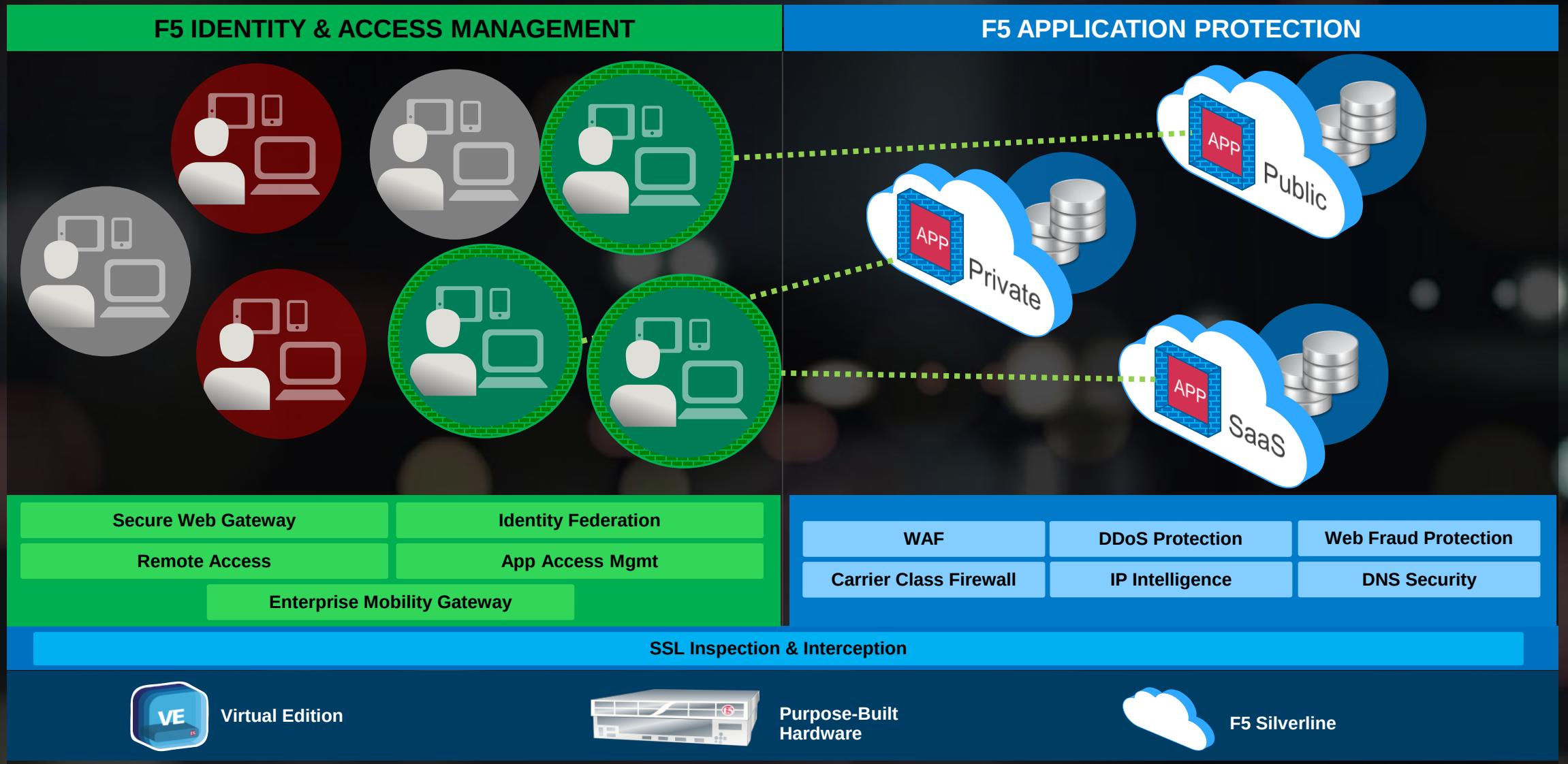
PROTECT APPLICATIONS

Safeguard your apps, regardless of where they live

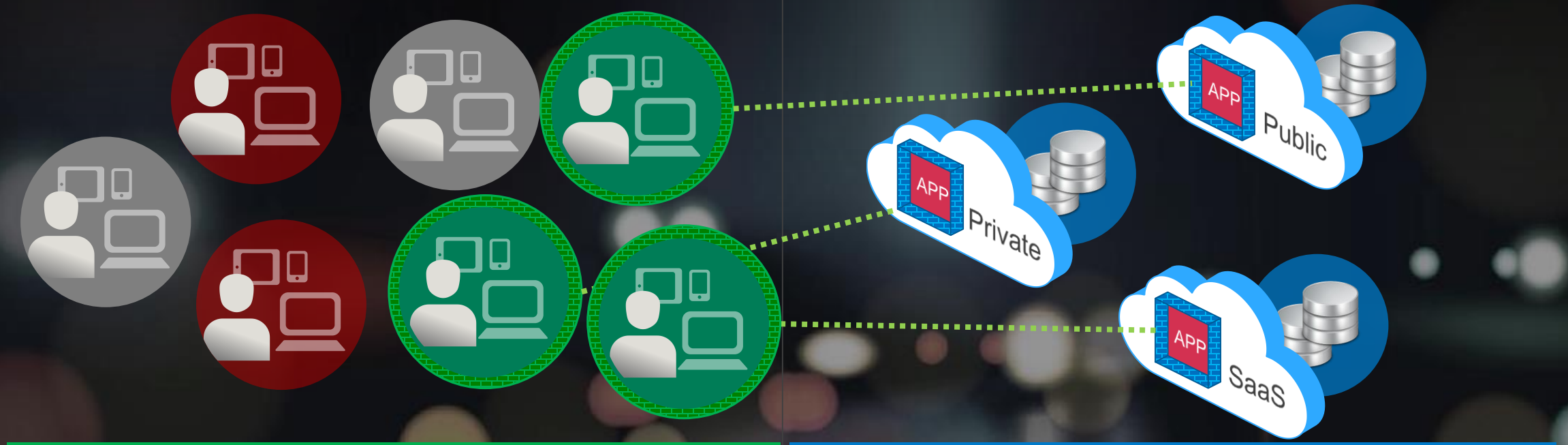
F5s Access, Identity, and App Protection Solutions



F5s Access, Identity, and App Protection Solutions



…integrate with existing controls to enhance security



Secure Web Gateway	Identity Federation
Remote Access	App Access Mgmt
Enterprise Mobility Gateway	

WAF	DDoS Protection	Web Fraud Protection
Carrier Class Firewall	IP Intelligence	DNS Security

SSL Inspection & Interception

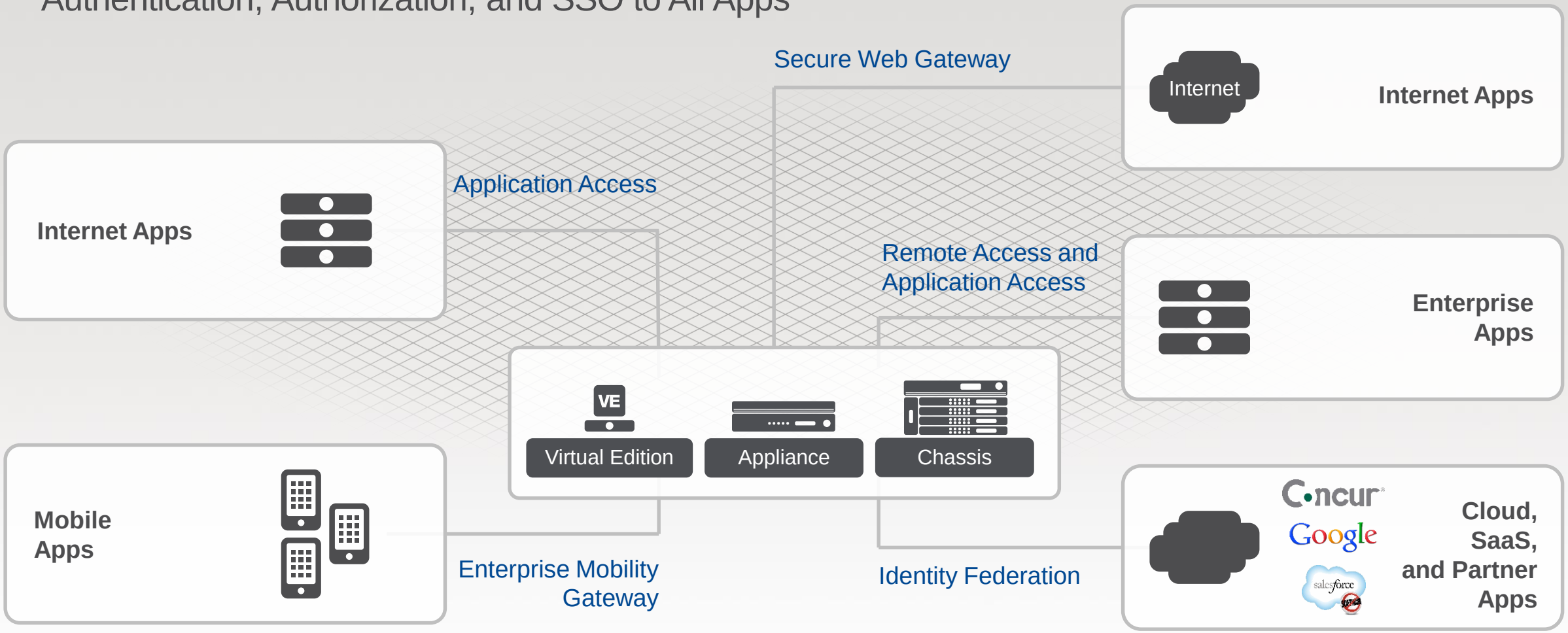
PARTNER ECOSYSTEM

NGFW	IDS	Data Loss Prevention	APT Scanning
Vulnerability Scanning	Packet / Forensics	HSM	IPS

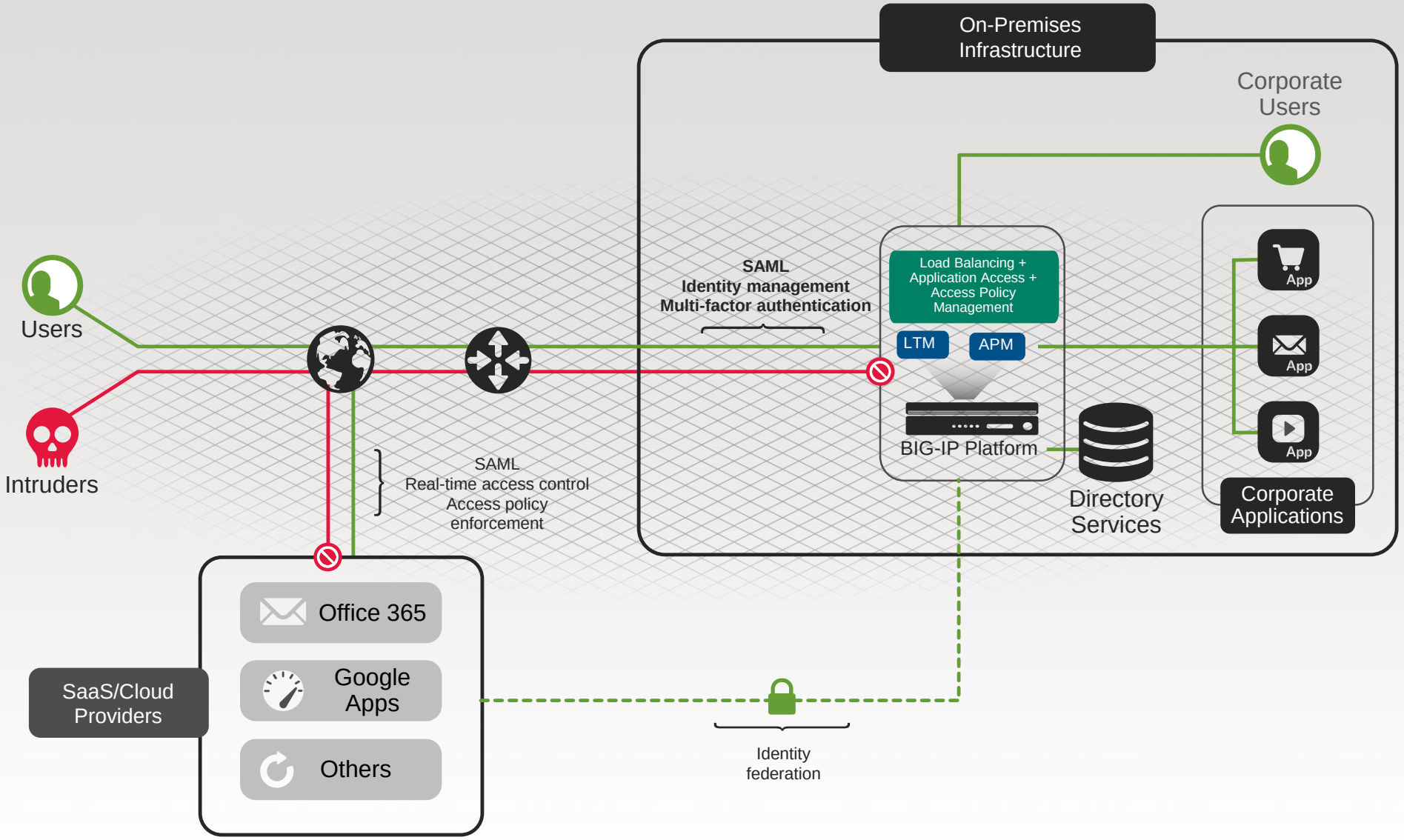
Identity and Access Management (IAM) Solution

Securing access to applications from anywhere

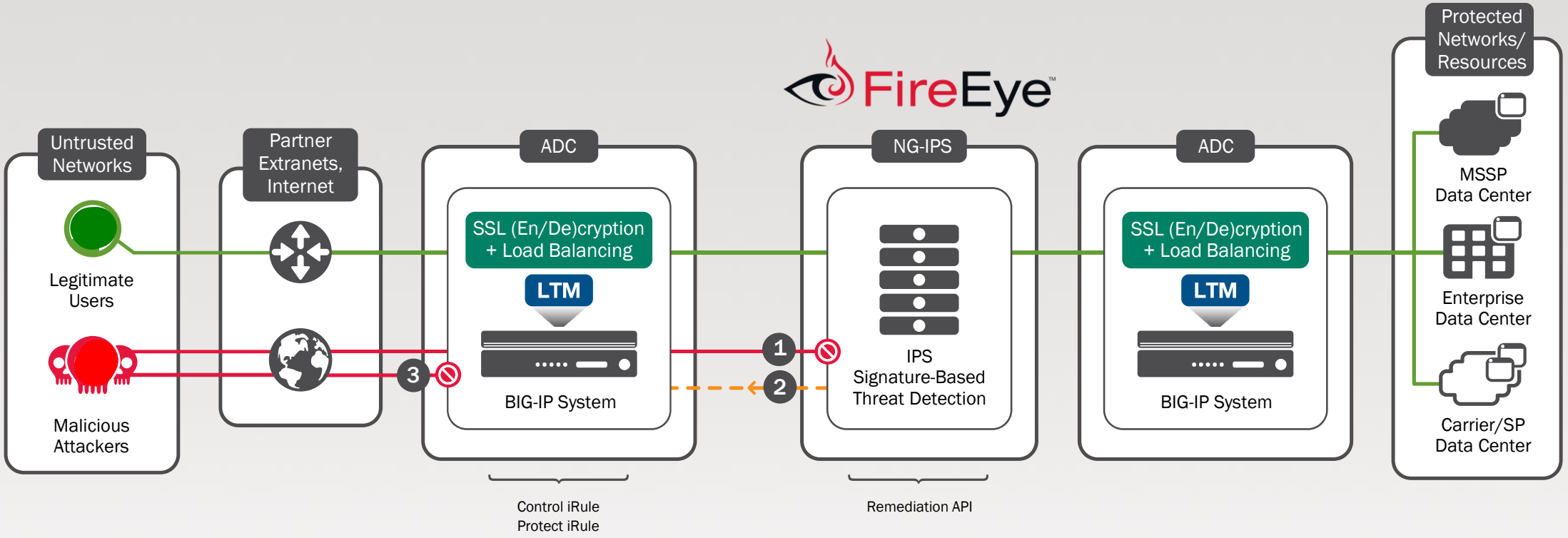
Authentication, Authorization, and SSO to All Apps



Powerful, secure SaaS/Cloud Federation Access



Next Generation IPS Reference Architecture



Next-Generation IPS-Integrated ADC Infrastructure

1. Malicious attacker is identified and blocked by NG-IPS
2. NG-IPS sends blacklisted IP information from remediation API to ADC
3. ADC begins blocking malicious attacker

LTM BIG-IP Local Traffic Manager

Simplified Business Models

GOOD | BETTER | BEST

Application Protection Solution

Protecting your applications regardless of where they live

Bringing deep application fluency and price performance to firewall security

ICSA labs CERTIFIED IPSEC

ICSA labs CERTIFIED SSL VPN

ICSA labs CERTIFIED FIREWALL - CORPORATE

ICSA labs CERTIFIED WEB APPLICATION FIREWALL

Common Criteria
EAL2+
EAL4+ (in process)

NSS LABS
DC FW (in process)
WAF (in process)
DDoS (pending)

F5's Approach to Application Security

Protecting your Applications and Information – Wherever they reside

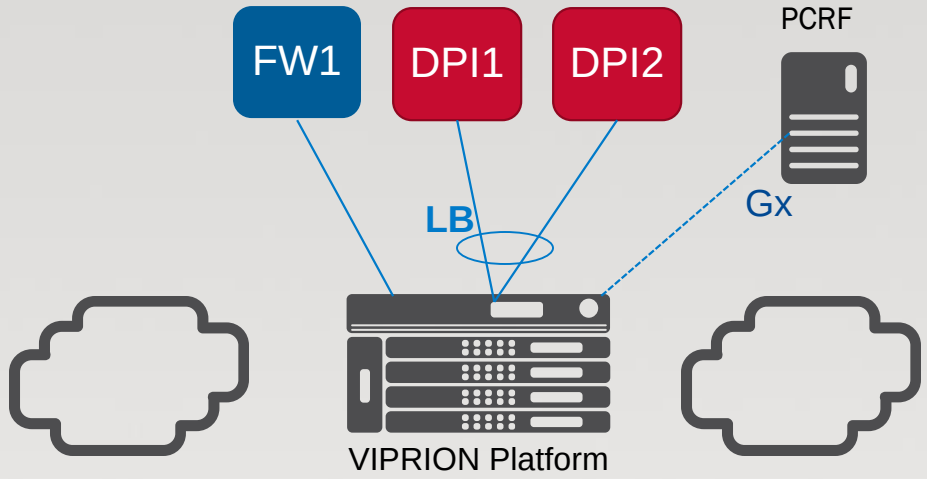
IDENTITY AND ACCESS MANAGEMENT (IAM) | **APPLICATION PROTECTION**

Service Provider NFV

Service Chaining

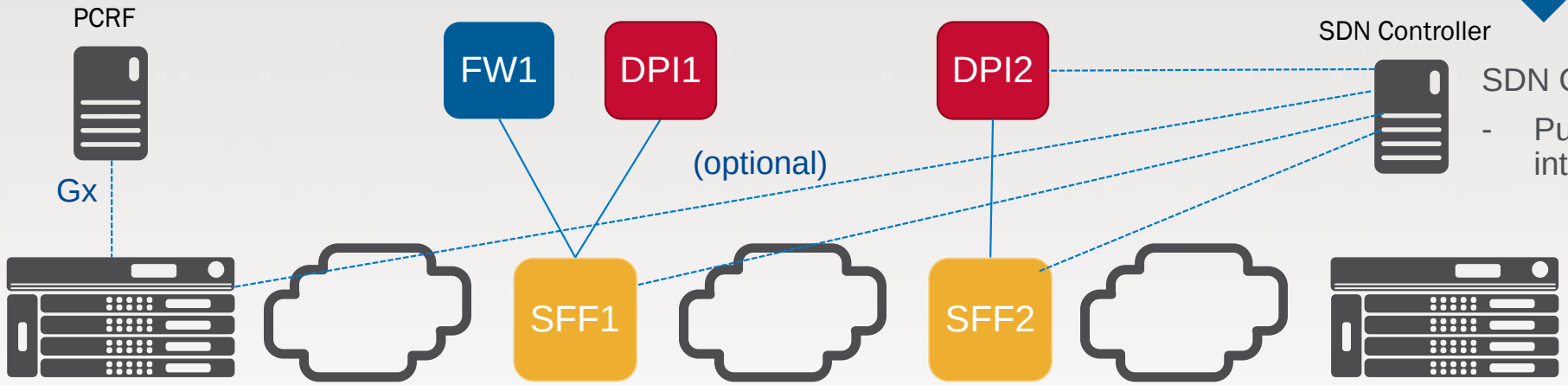
Service Providers - Service Chaining

Traditional Model



Evolution Path

- Keep PCRF to control per-subscriber service chaining
- Keep BIGIP for contextual classification of traffic (including Radius attributes)
- Migrate from proxy-based forwarding in BIGIP to SDN based forwarding using NSH



SDN Controller

- Pushes NSH forwarding rules into all NSH-aware nodes

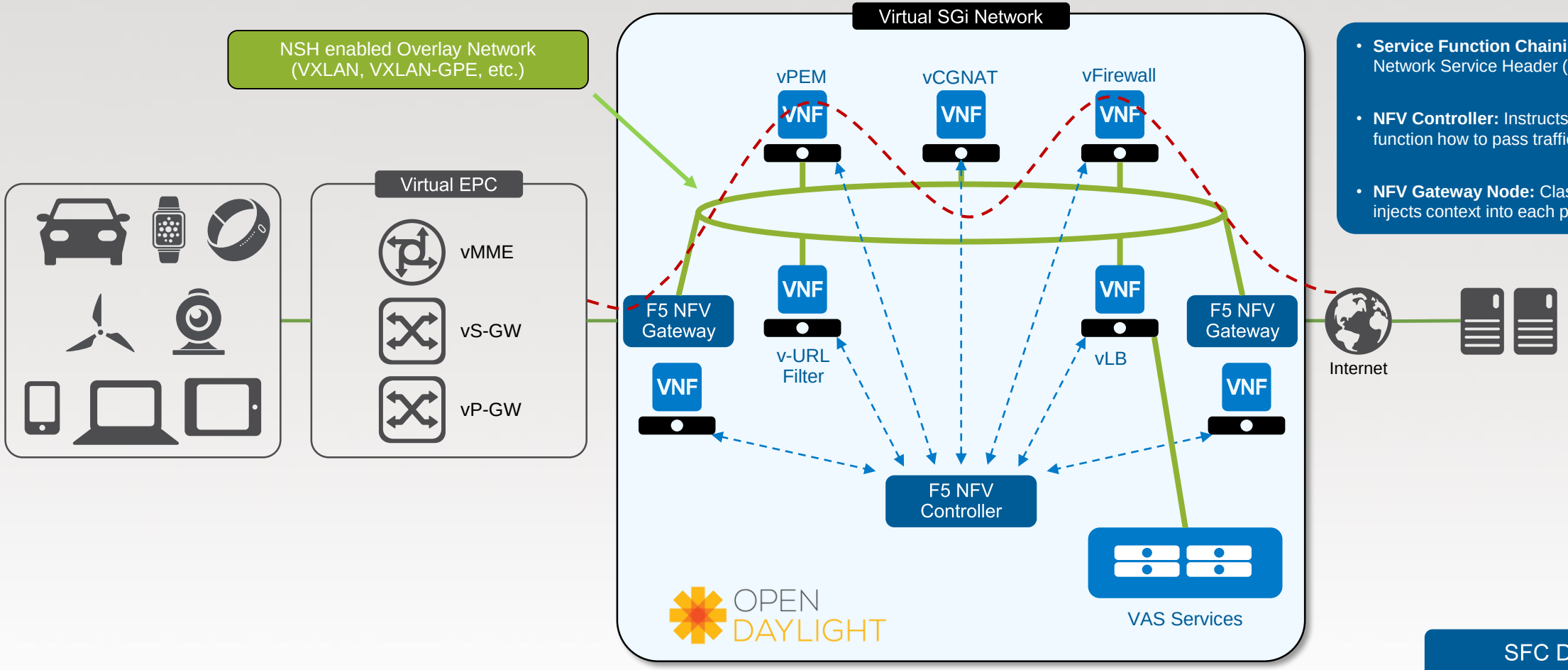
F5 as ingress ‘Service Classifier’

- Adds NSH header based on policy assigned by PCRF
- Forwards packets based on forwarding rules pushed by SDN controller (or using static routes)

F5 as egress ‘Gateway’

- Removes NSH header and forwards to internet
- Based on auto-lasthop feature return traffic will get the right NSH and traffic gets forwarded to appropriate nexthop

Service Function Chaining of F5 VNFs Using Network Service Header (NSH)



- **Service Function Chaining:** Using Network Service Header (NSH)
- **NFV Controller:** Instructs each service function how to pass traffic
- **NFV Gateway Node:** Classifies and injects context into each packet

SFC DEMO

Martin Oravec

m.oravec@f5.com

+421 908 747 633