Application Security in depth

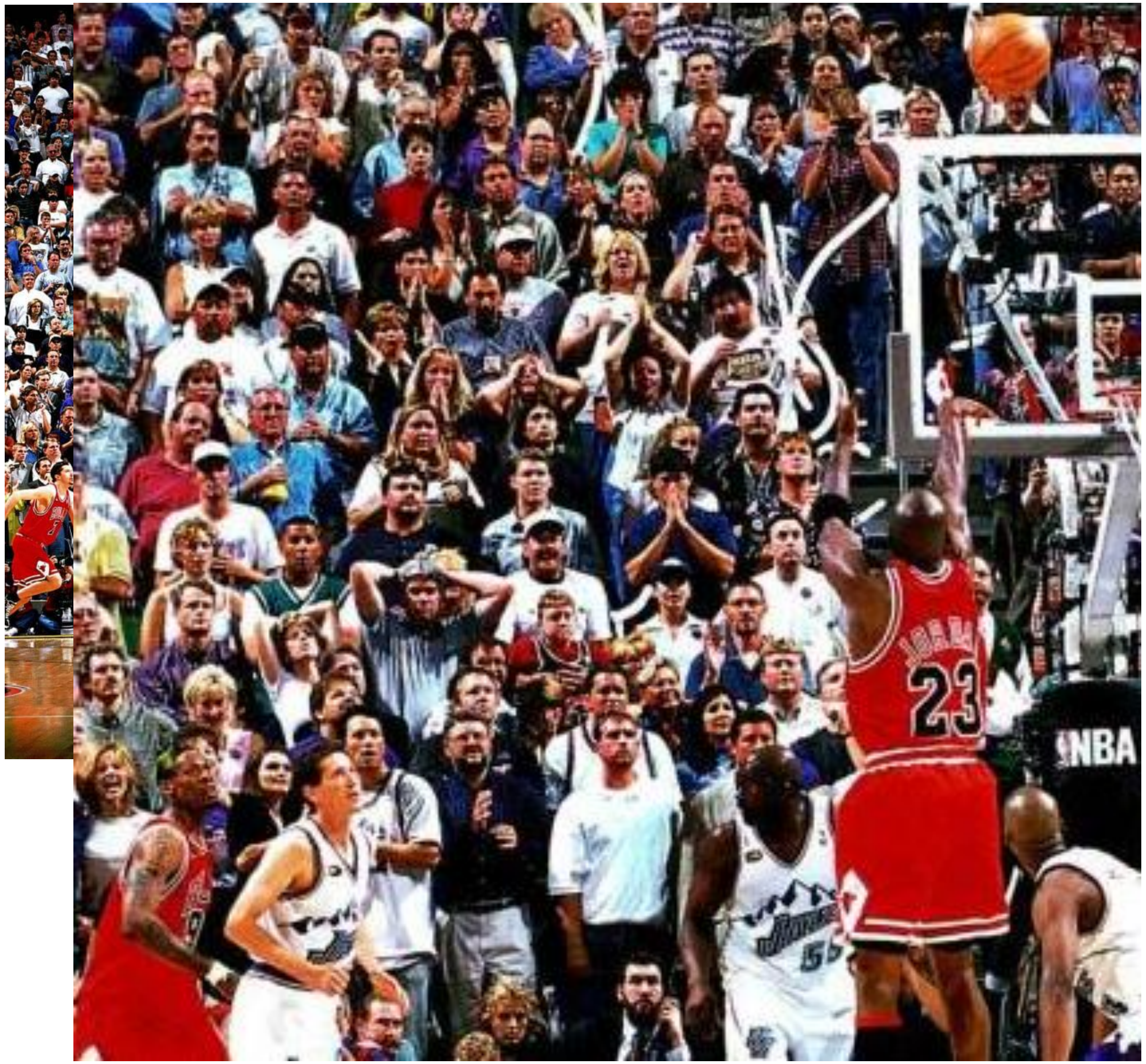
Dimi Doukas/Arrow ECS Finland 25.10.2023

1998 vs 2023

Michael Jordan

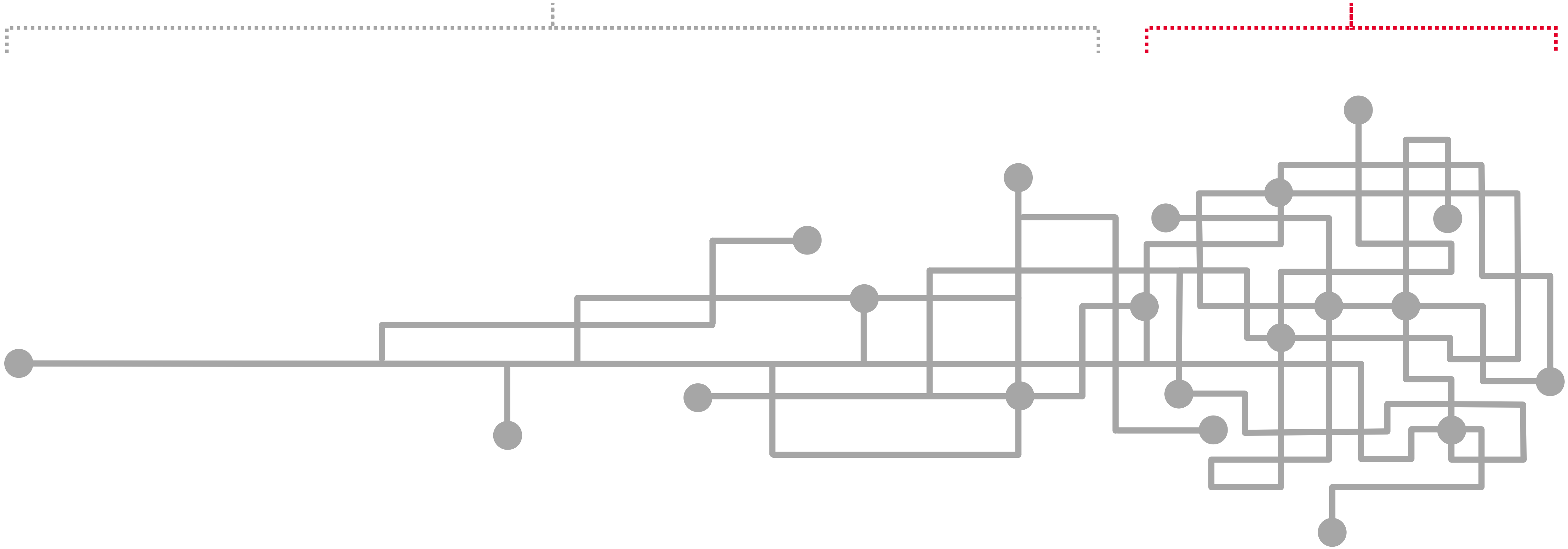
Lebron James

1998 vs 2023

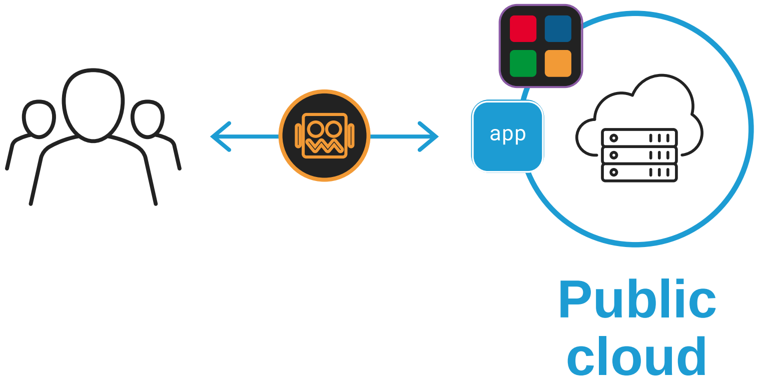


IT complexity has built up over time

until it has become an **existential threat** to business success

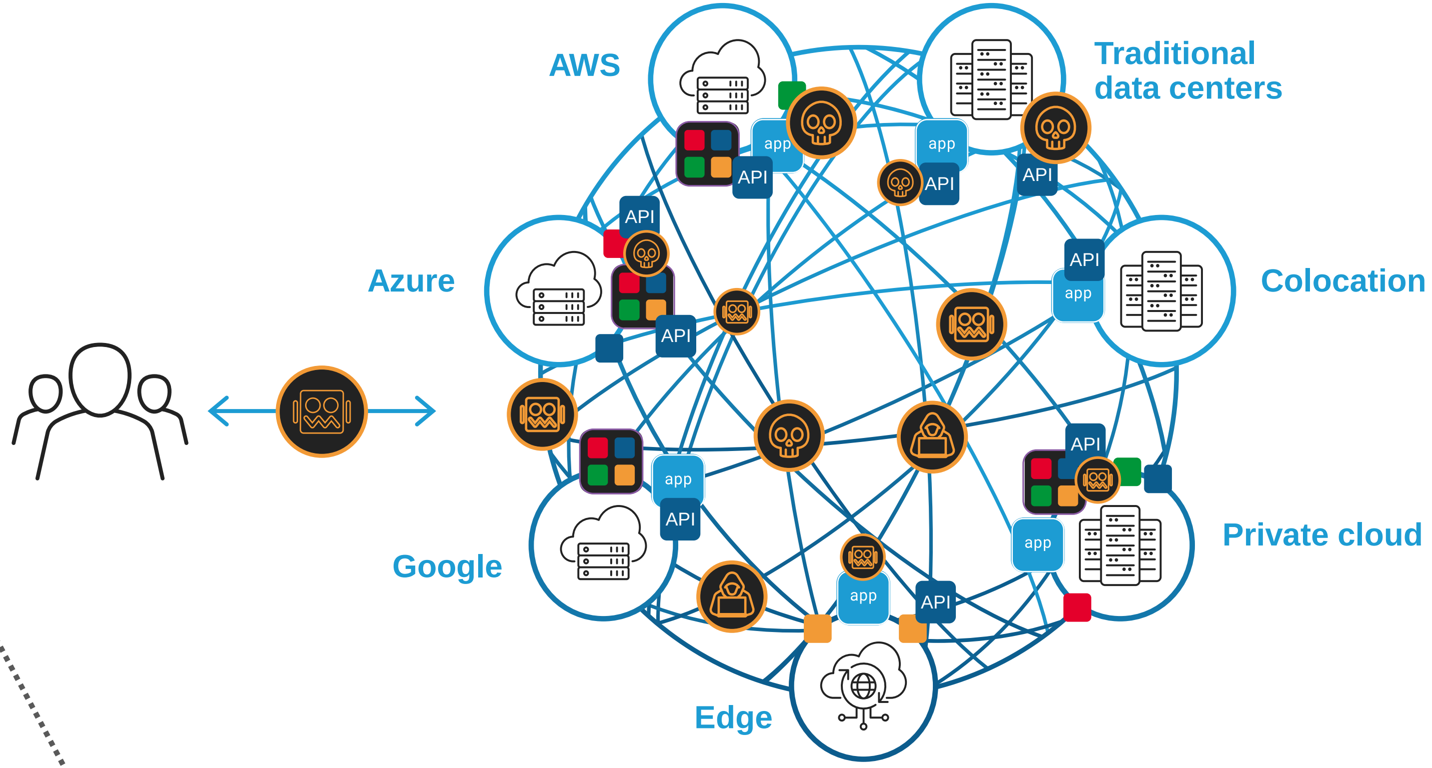


This is where we thought we would be...



app Traditional monolithic app

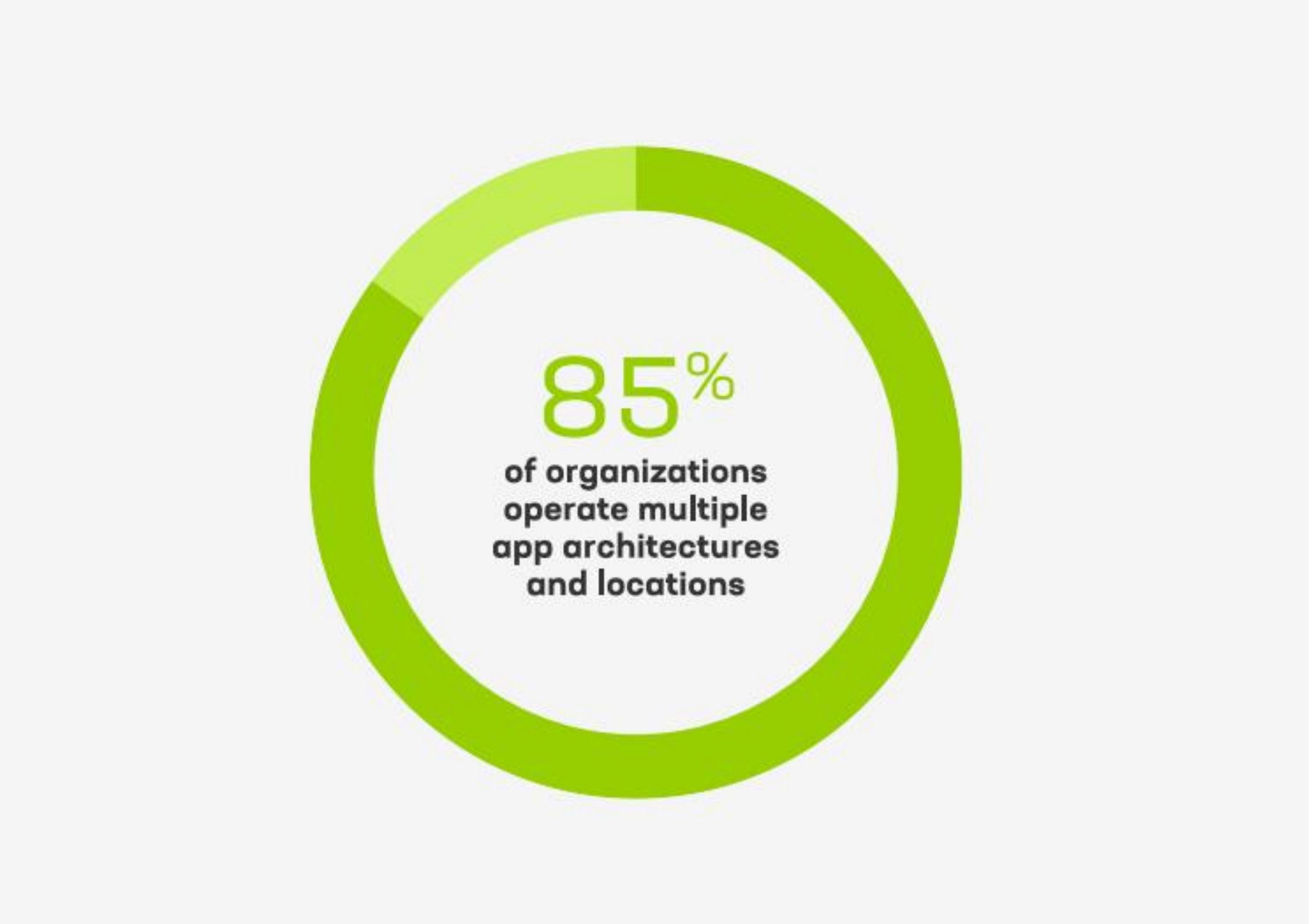
🟥🟦🟩🟧 Modern cloud native app



and this is where we have ended up

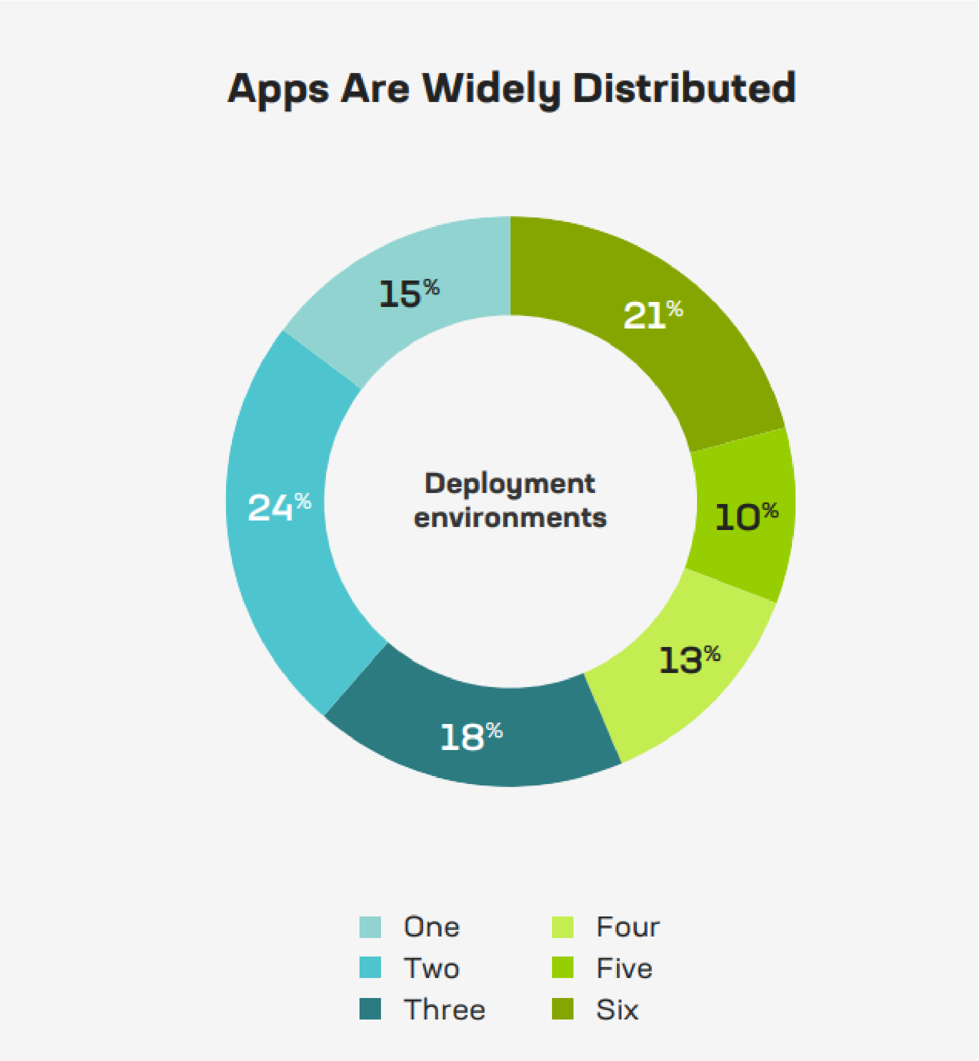
F5 – state of the application strategy report 2023

More than one app architecture and location



F5 – state of the application strategy report 2023

Hybrid is here to stay

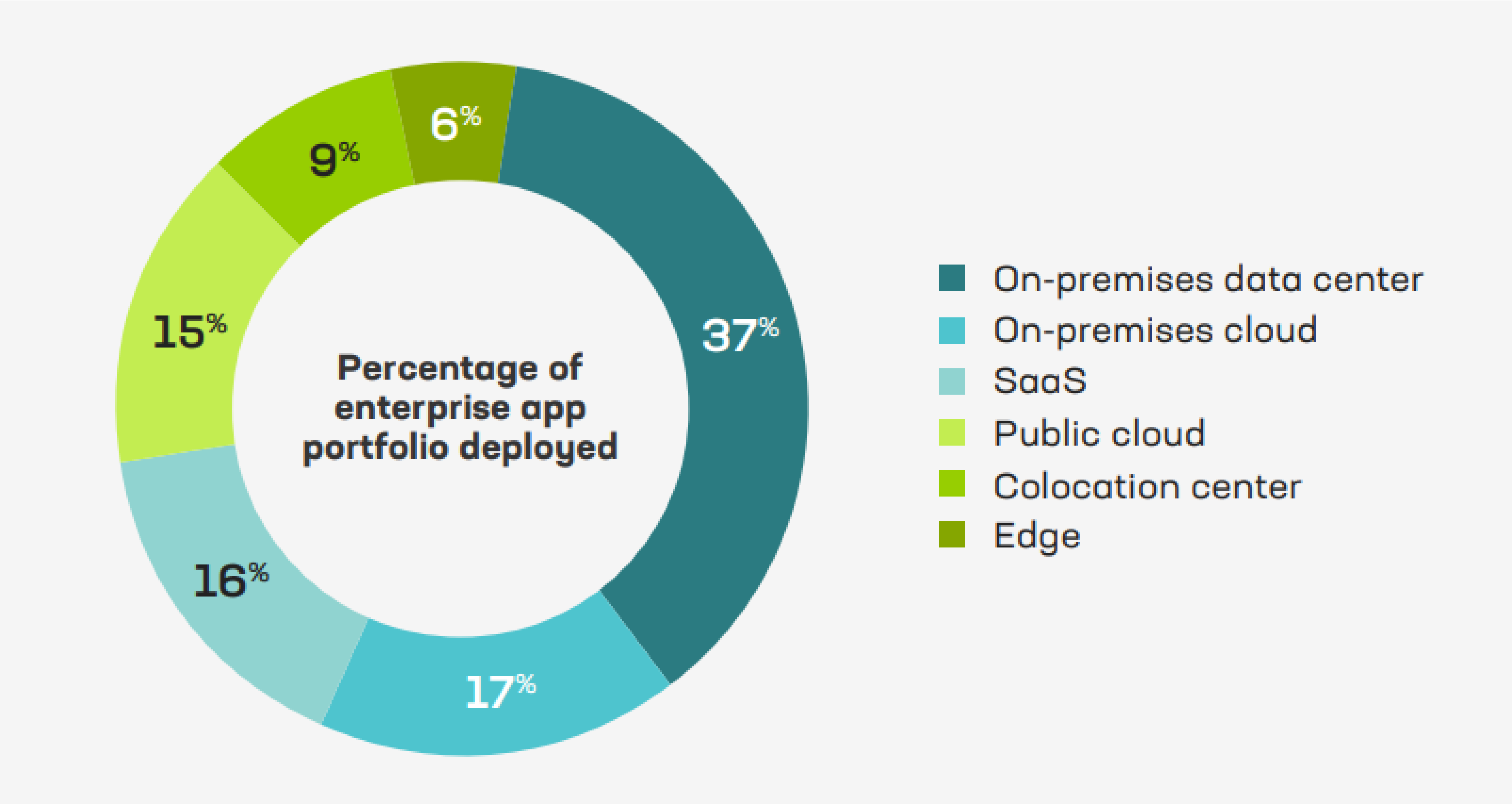


Today, just under half of all respondents (48%) say they currently have any apps deployed in the cloud, and on average organizations deploy only **15% of their app portfolio in the cloud.** The considerations limiting public cloud deployments probably include concerns about data control, security, or cost at scale.

Public clouds remain an option for many organizations, particularly for backup and business resilience purposes, but public clouds are not always the first choice for hosting applications.

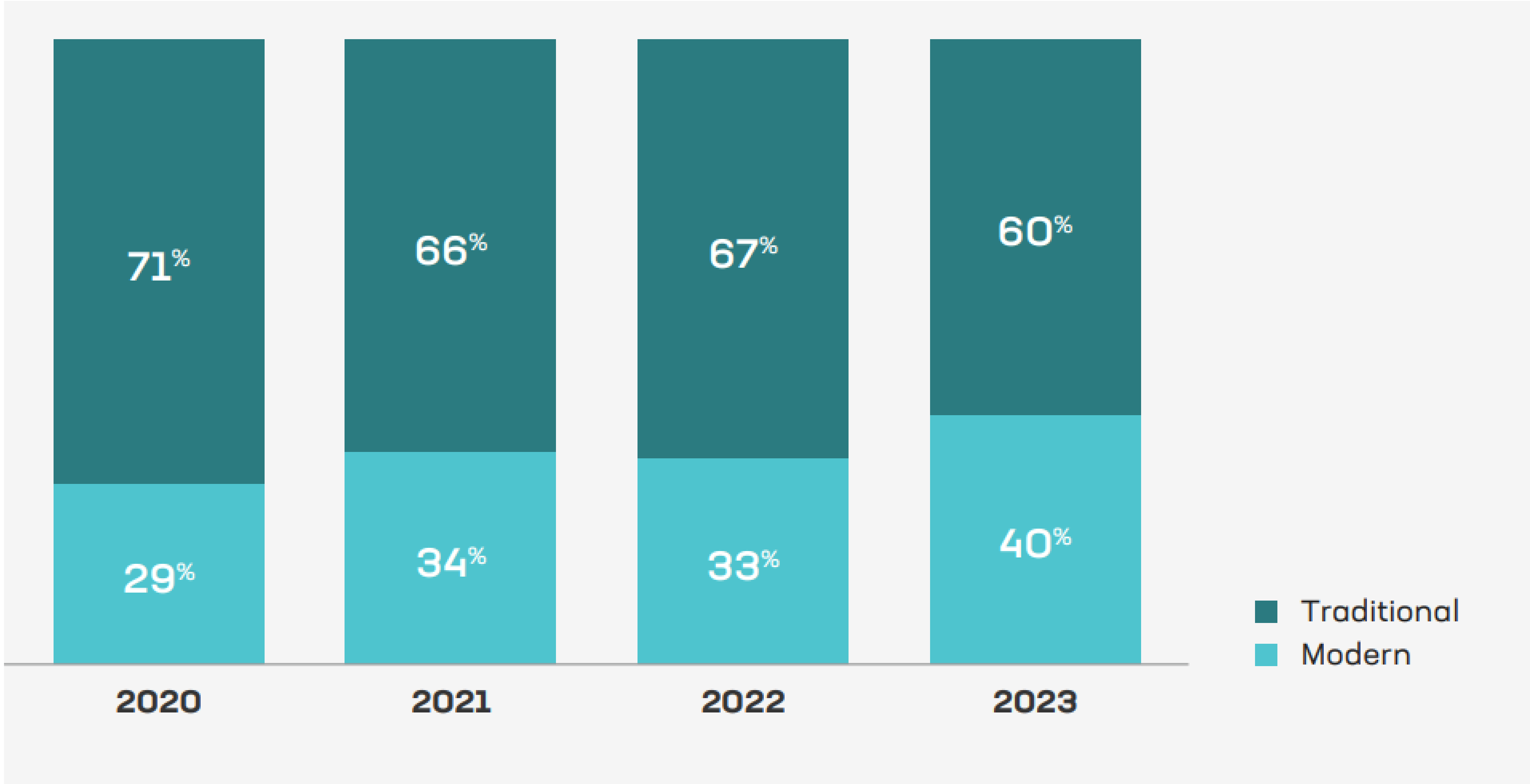
F5 – state of the application strategy report 2023

Multi-Cloud Environments Will Endure



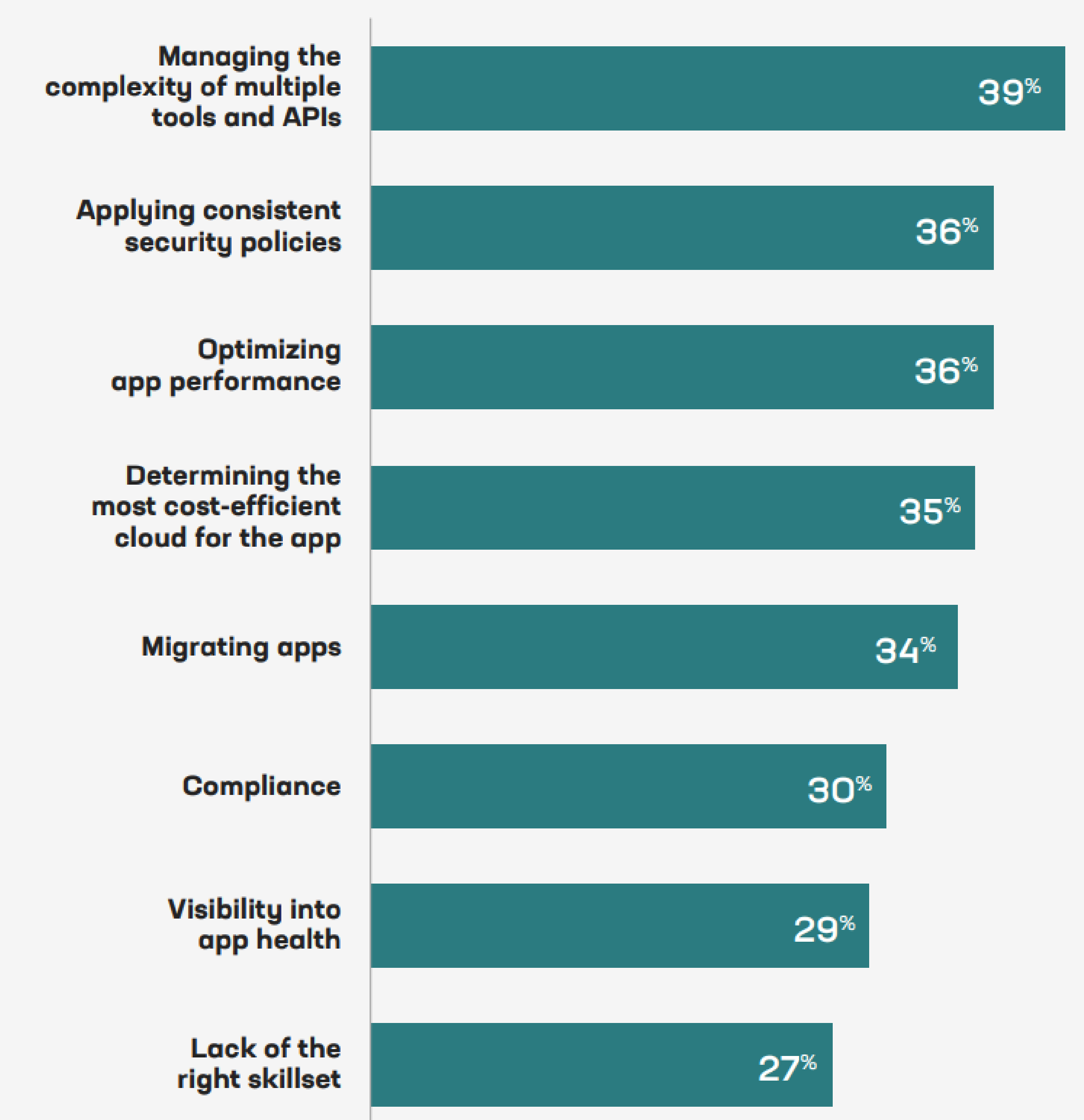
F5 – state of the application strategy report 2023

Modern App Architectures Continue Their Growth



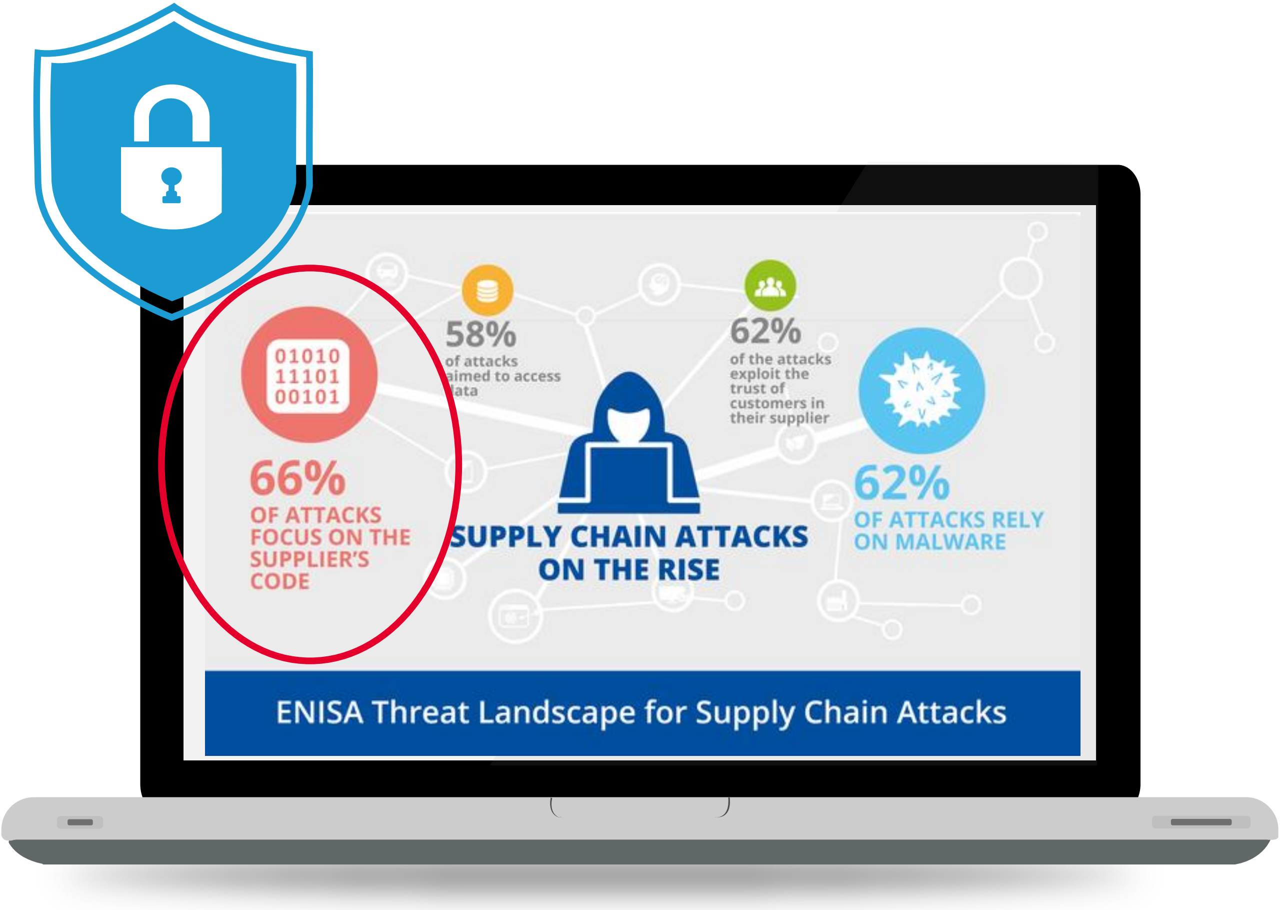
F5 – state of the application strategy report 2023

Complexity Tops Many Multi-Cloud Challenges



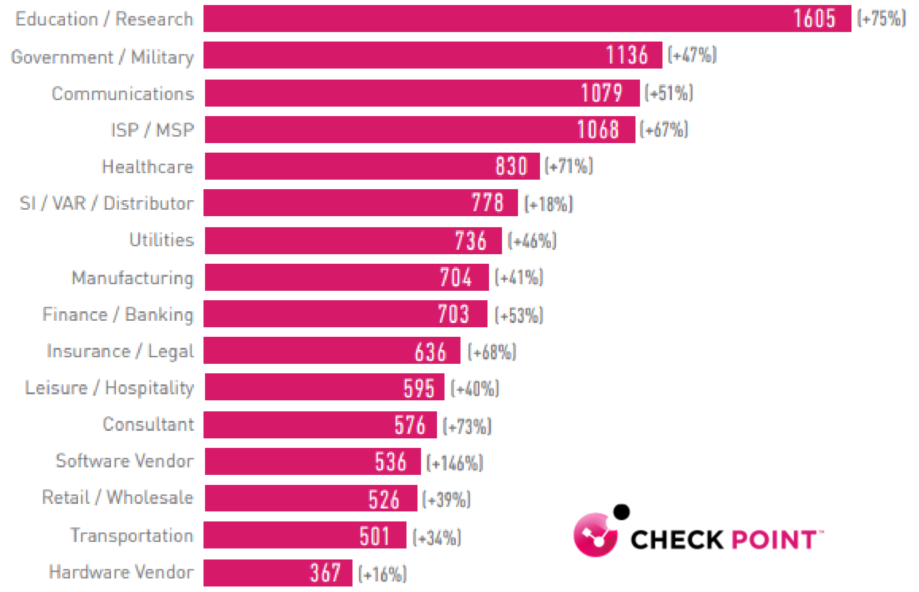
Why is securing applications so difficult?

Supply Chain Attacks



01010
11101
00101
66%
OF ATTACKS FOCUS ON THE SUPPLIER'S CODE
58%
of attacks aimed to access data
62%
of the attacks exploit the trust of customers in their supplier
SUPPLY CHAIN ATTACKS ON THE RISE
62%
OF ATTACKS RELY ON MALWARE
ENISA Threat Landscape for Supply Chain Attacks

Average weekly attacks per organization by Industry 2021, compared to 2020

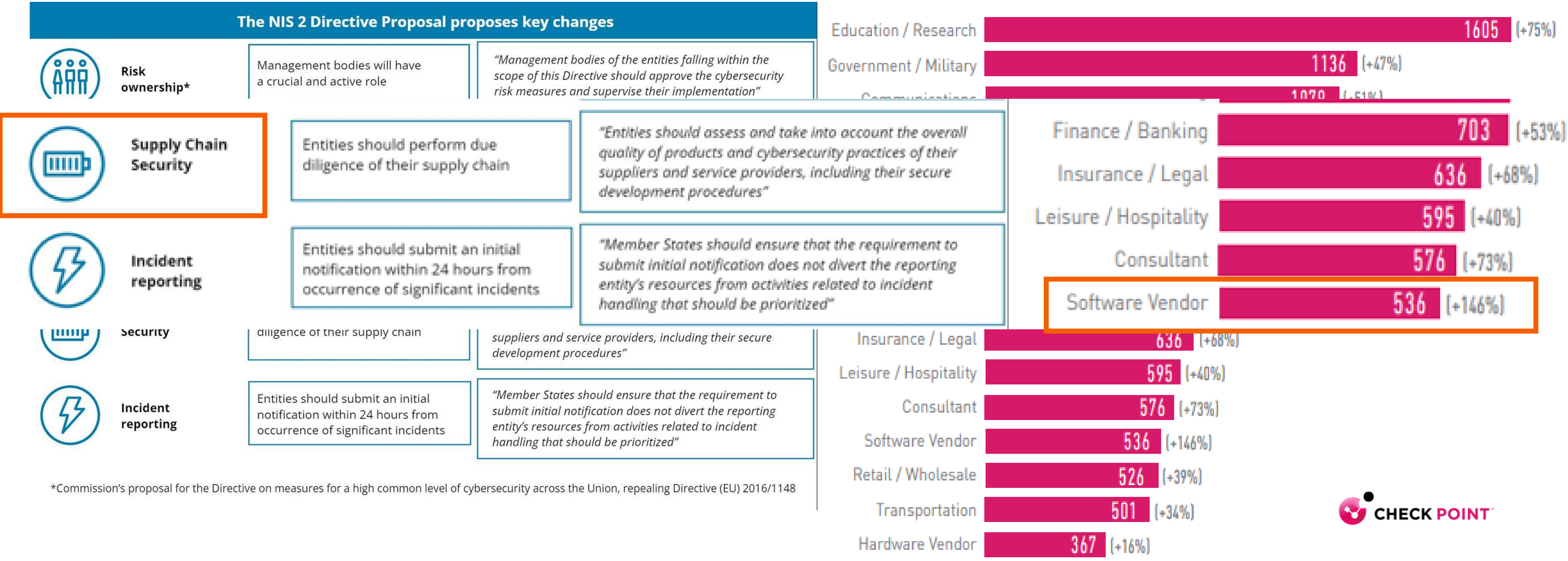


During 2021, global cyber attacks against corporate networks has increased by **50%**, in comparison to 2020.

Software Vendor category shows the largest year-on-year growth, with an increase of **146%**.

The rise in attacks against software vendors goes hand-in-hand with the ever-growing trend of software **supply chain attacks** observed during 2021.

NIS2 and Supply Chain Risk



The NIS 2 Directive Proposal proposes key changes

Risk ownership*	Management bodies will have a crucial and active role	*"Management bodies of the entities falling within the scope of this Directive should approve the cybersecurity risk measures and supervise their implementation"*
Supply Chain Security	Entities should perform due diligence of their supply chain	*"Entities should assess and take into account the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures"*
Incident reporting	Entities should submit an initial notification within 24 hours from occurrence of significant incidents	*"Member States should ensure that the requirement to submit initial notification does not divert the reporting entity's resources from activities related to incident handling that should be prioritized"*

*Commission's proposal for the Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148

Supply Chain Security
Entities should perform due diligence of their supply chain
"Entities should assess and take into account the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures"
Incident reporting
Entities should submit an initial notification within 24 hours from occurrence of significant incidents
"Member States should ensure that the requirement to submit initial notification does not divert the reporting entity's resources from activities related to incident handling that should be prioritized"

Average weekly attacks per organization by Industry 2021, compared to 2020

Education / Research 1605 (+75%)
Government / Military 1136 (+47%)
Communications 1070 (+51%)
Finance / Banking 703 (+53%)
Insurance / Legal 636 (+68%)
Leisure / Hospitality 595 (+40%)
Consultant 576 (+73%)
Software Vendor 536 (+146%)
Insurance / Legal 636 (+68%)
Leisure / Hospitality 595 (+40%)
Consultant 576 (+73%)
Software Vendor 536 (+146%)
Retail / Wholesale 526 (+39%)
Transportation 501 (+34%)
Hardware Vendor 367 (+16%)
CHECK POINT

Supply Chain Attack

A supply chain attack is a type of cyber attack that targets organizations by focusing on weaker links in an organization's supply chain

Individuals, organizations, resources, activities and technology involved in the creation and sale of a product

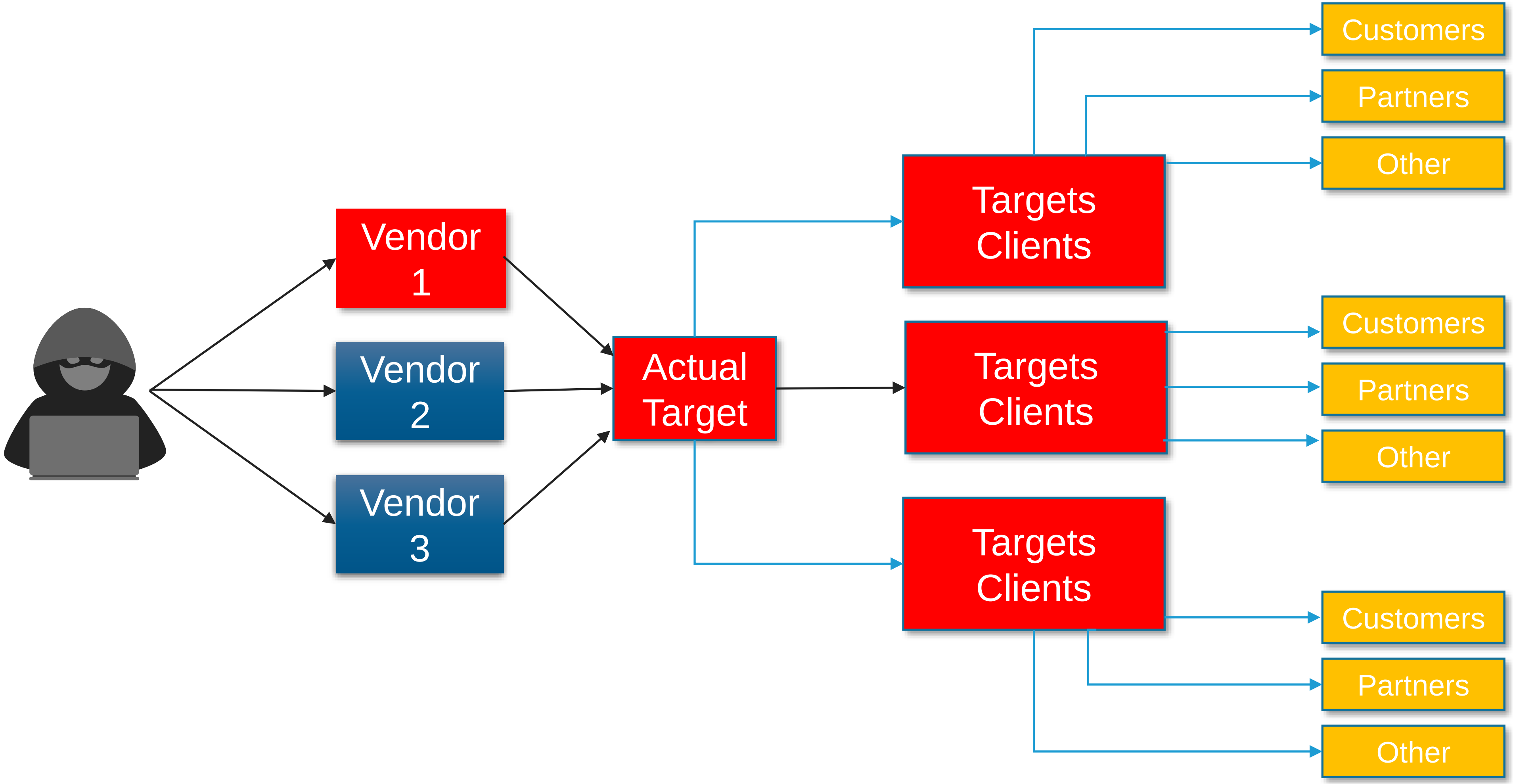
Cybercriminals will use supply chain attacks to tamper with the manufacturing processes

Hardware or software

Malware or any other malicious binary or code could be installed in any stage of the supply chain.

Considered to be number one threat now and in the future

Anatomy of Supply Chain Attack



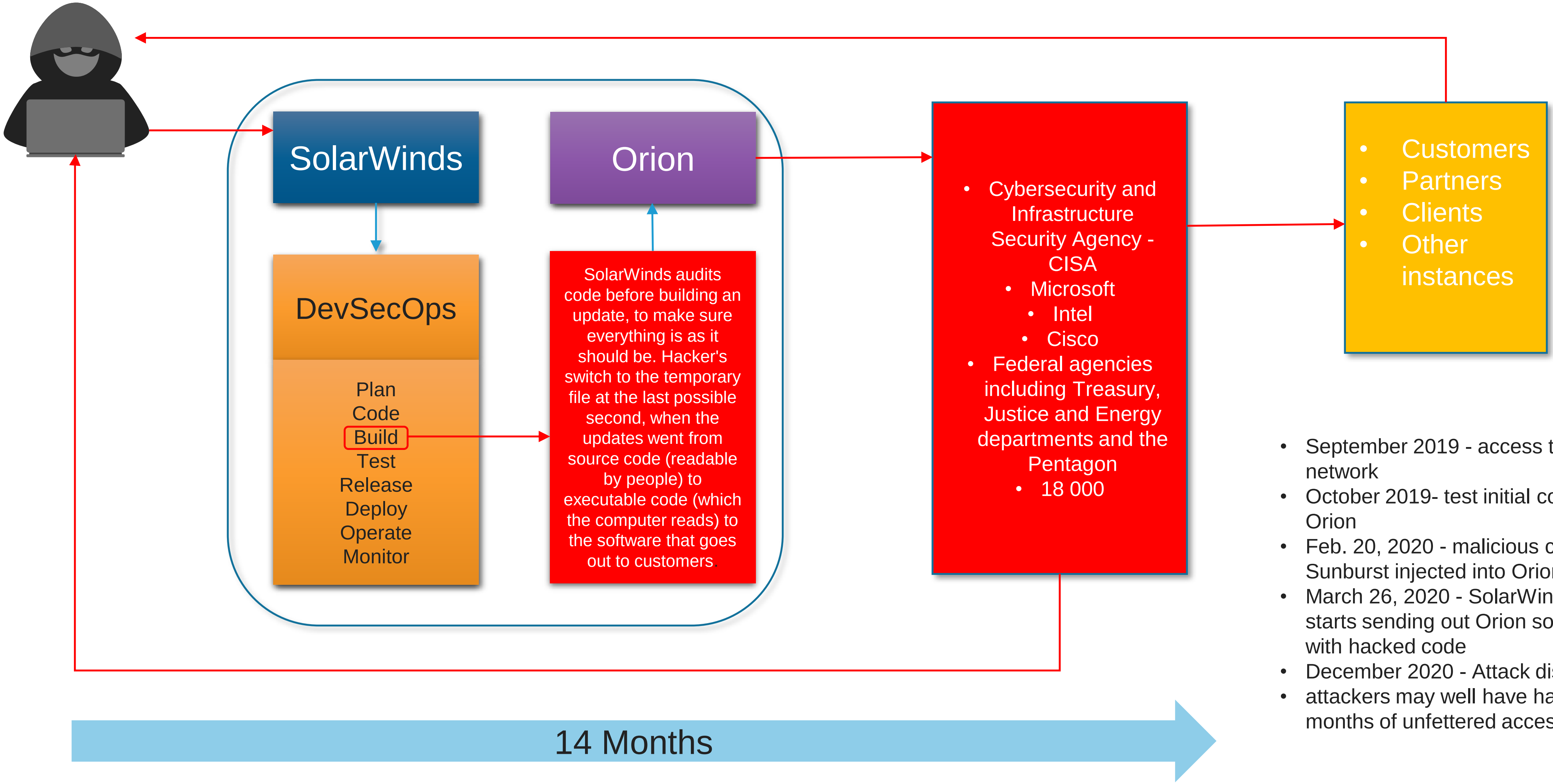
KILL CHAIN

Reconnaissance → Weaponization → Delivery → Exploitation →Installation → Command & Control → Actions on Objective

"This was the craziest f***ing thing I'd ever seen.“

Adam Meyers - vice president for threat intelligence at CrowdStrike

https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack



SolarWinds

Orion

DevSecOps

Plan
Code
Build
Test
Release
Deploy
Operate
Monitor

SolarWinds audits code before building an update, to make sure everything is as it should be. Hacker's switch to the temporary file at the last possible second, when the updates went from source code (readable by people) to executable code (which the computer reads) to the software that goes out to customers.

- Cybersecurity and Infrastructure Security Agency - CISA
- Microsoft
- Intel
- Cisco
- Federal agencies including Treasury, Justice and Energy departments and the Pentagon
- 18 000

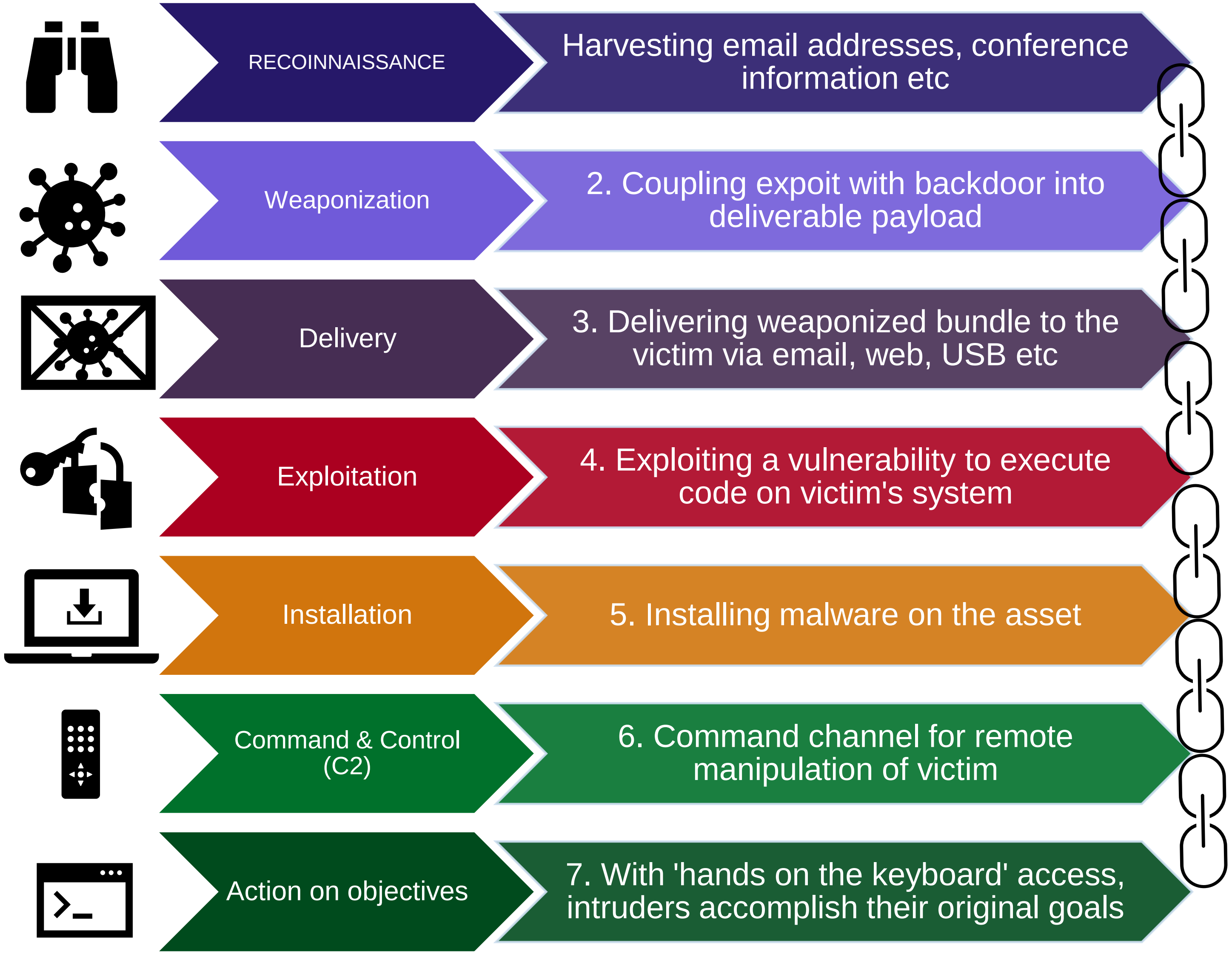
- Customers
- Partners
- Clients
- Other instances

14 Months

- September 2019 - access to SolarWinds network
- October 2019- test initial code injection into Orion
- Feb. 20, 2020 - malicious code known as Sunburst injected into Orion
- March 26, 2020 - SolarWinds unknowingly starts sending out Orion software updates with hacked code
- December 2020 - Attack discovered
- attackers may well have had 14 or more months of unfettered access

Cyber Kill Chain framework (dev by Lockheed Martin)

Identifies what the adveraries must complete to achieve their objective



RECOINNAISSANCE

Harvesting email addresses, conference information etc

Weaponization

2. Coupling expoit with backdoor into deliverable payload

Delivery

3. Delivering weaponized bundle to the victim via email, web, USB etc

Exploitation

4. Exploiting a vulnerability to execute code on victim's system

Installation

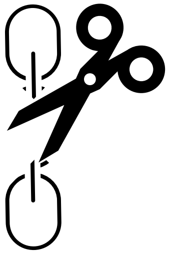
5. Installing malware on the asset

Command & Control (C2)

6. Command channel for remote manipulation of victim

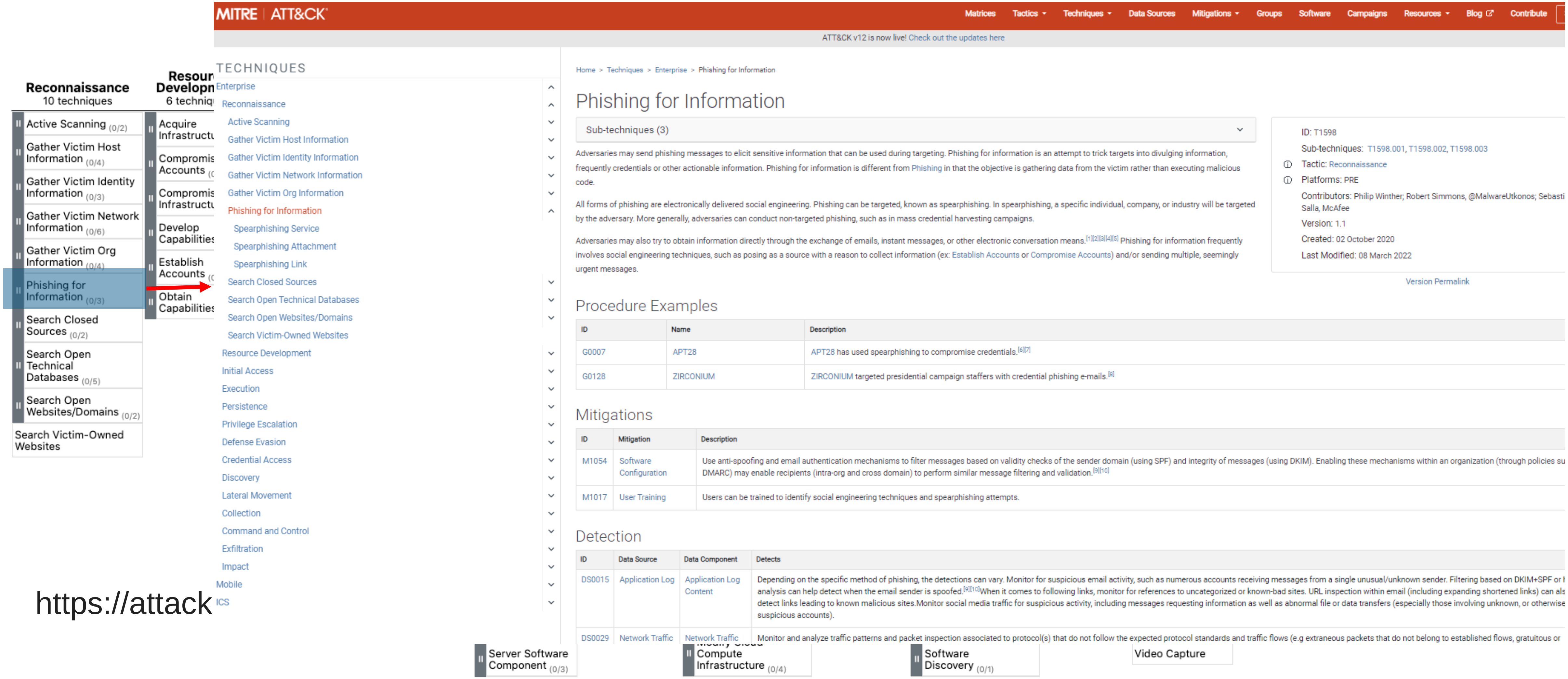
Action on objectives

7. With 'hands on the keyboard' access, intruders accomplish their original goals



Breaking any of the chains will stop the kill chain

MITRE ATT&CK Matrix – Cyber Kill Chain Framework



Reconnaissance
10 techniques

- Active Scanning (0/2)
- Gather Victim Host Information (0/4)
- Gather Victim Identity Information (0/3)
- Gather Victim Network Information (0/6)
- Gather Victim Org Information (0/4)
- Phishing for Information (0/3)
- Search Closed Sources (0/2)
- Search Open Technical Databases (0/5)
- Search Open Websites/Domains (0/2)
- Search Victim-Owned Websites

Resour Developn
6 techniq

- Acquire Infrastructu
- Compromis Accounts (
- Compromis Infrastructu
- Develop Capabilities
- Establish Accounts (
- Obtain Capabilities

Server Software Component (0/3)

Compute Infrastructure (0/4)

Software Discovery (0/1)

Video Capture

Phishing for Information

Sub-techniques (3)

Adversaries may send phishing messages to elicit sensitive information that can be used during targeting. Phishing for information is an attempt to trick targets into divulging information, frequently credentials or other actionable information. Phishing for information is different from Phishing in that the objective is gathering data from the victim rather than executing malicious code.

All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass credential harvesting campaigns.

Adversaries may also try to obtain information directly through the exchange of emails, instant messages, or other electronic conversation means.[1][2][3][4][5] Phishing for information frequently involves social engineering techniques, such as posing as a source with a reason to collect information (ex: Establish Accounts or Compromise Accounts) and/or sending multiple, seemingly urgent messages.

ID: T1598

Sub-techniques: T1598.001, T1598.002, T1598.003

Tactic: Reconnaissance

Platforms: PRE

Contributors: Philip Winther; Robert Simmons, @MalwareUtkonos; Sebasti Salla, McAfee

Version: 1.1

Created: 02 October 2020

Last Modified: 08 March 2022

Version Permalink

Procedure Examples

ID	Name	Description
G0007	APT28	APT28 has used spearphishing to compromise credentials.[6][7]
G0128	ZIRCONIUM	ZIRCONIUM targeted presidential campaign staffers with credential phishing e-mails.[8]

Mitigations

ID	Mitigation	Description
M1054	Software Configuration	Use anti-spoofing and email authentication mechanisms to filter messages based on validity checks of the sender domain (using SPF) and integrity of messages (using DKIM). Enabling these mechanisms within an organization (through policies su DMARC) may enable recipients (intra-org and cross domain) to perform similar message filtering and validation.[9][10]
M1017	User Training	Users can be trained to identify social engineering techniques and spearphishing attempts.

Detection

ID	Data Source	Data Component	Detects
DS0015	Application Log	Application Log Content	Depending on the specific method of phishing, the detections can vary. Monitor for suspicious email activity, such as numerous accounts receiving messages from a single unusual/unknown sender. Filtering based on DKIM+SPF or analysis can help detect when the email sender is spoofed.[9][10]When it comes to following links, monitor for references to uncategorized or known-bad sites. URL inspection within email (including expanding shortened links) can als detect links leading to known malicious sites.Monitor social media traffic for suspicious activity, including messages requesting information as well as abnormal file or data transfers (especially those involving unknown, or otherwise suspicious accounts).
DS0029	Network Traffic	Network Traffic	Monitor and analyze traffic patterns and packet inspection associated to protocol(s) that do not follow the expected protocol standards and traffic flows (e.g extraneous packets that do not belong to established flows, gratuitous or

https://attack

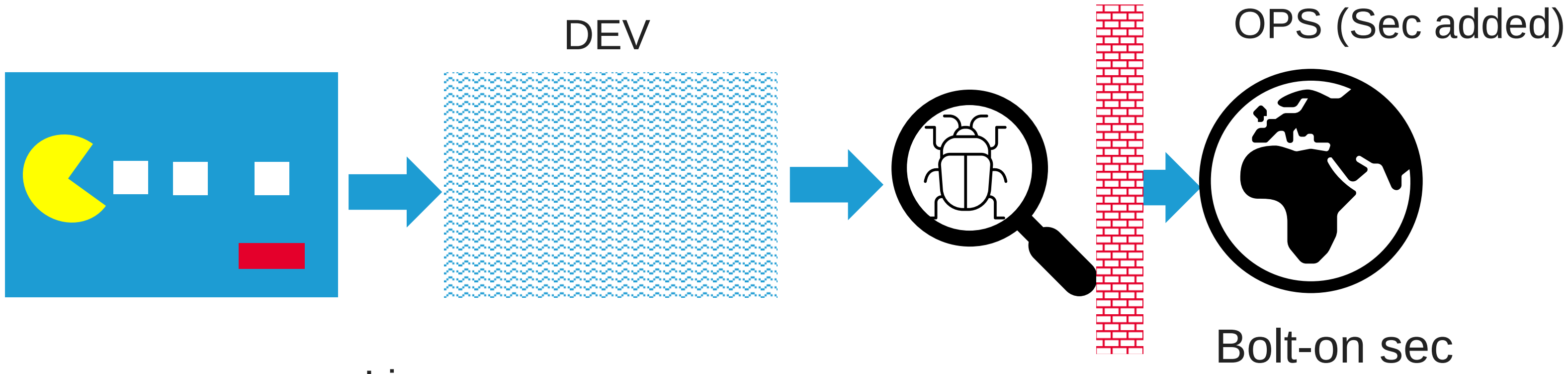
Securing applications and services

Tough Questions for Defenders

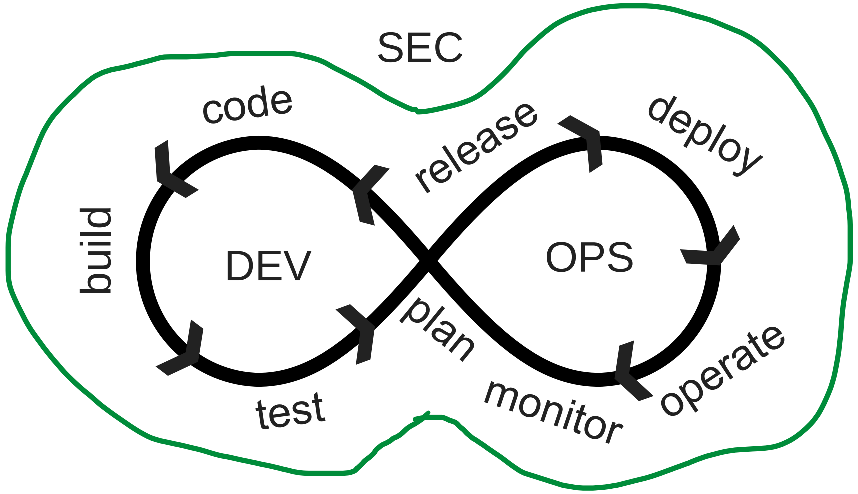
- How effective are my defenses?
- Do I have a chance at detecting APT29?
- Is the data I'm collecting useful?
- Do I have overlapping tool coverage?
- Will this new product help my organization's defenses?

Application Security – Software Development lifecycle

- All sofware have errors -> some of those become vulnerabilityes -> ‘all software have vulnerabilities’
- Cost of fixing vulnerability is exponentially more expensive the later we find it



- Linear
- Siloed
- Slow
- in flexible
- over the wall



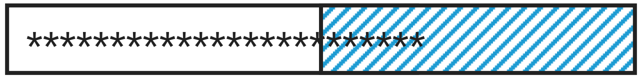
- cyclical
- rapid
- intergated
- agile

SHIFT (SECURITY) LEFT → DEVSECOPS

Application Security – Secure Coding

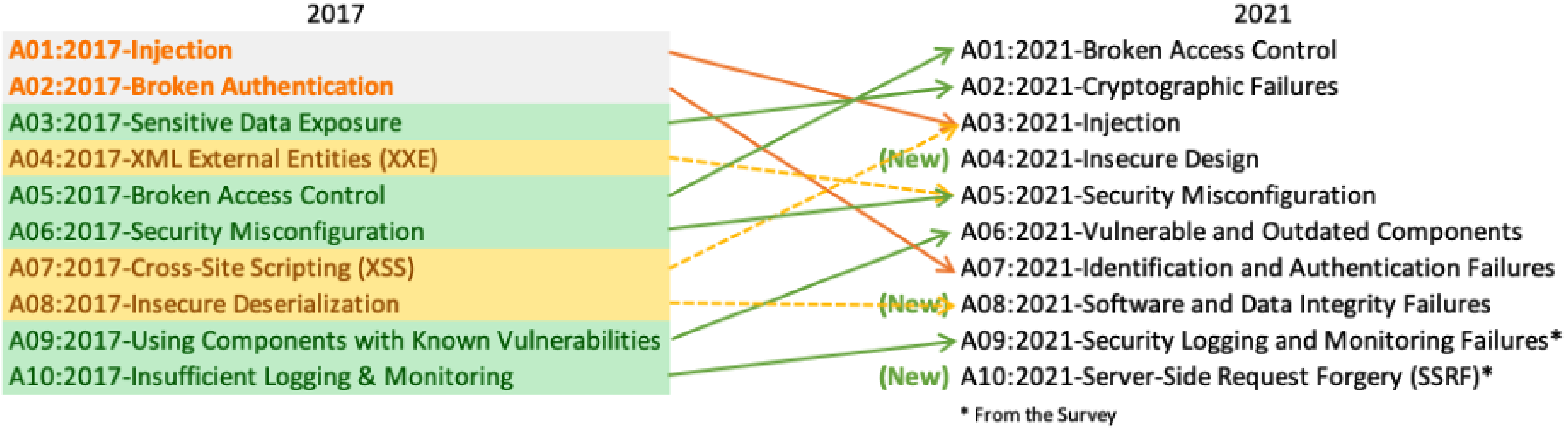
- Coding practices / Check list – OWASP.ORG
- Tursted libraries/sources (LOG4J routine)
- Standard architectures
- Mistakes to Avoid – OWASP TOP10
- Software Bill of Materials
  - Components
  - Libraries
  - Dependencies
  - Versions
  - Origins
  - Vulnaribilities

INPUT VALIDATION



Buffer overflow

Error handling



2017

A01:2017-Injection
A02:2017-Broken Authentication
A03:2017-Sensitive Data Exposure
A04:2017-XML External Entities (XXE)
A05:2017-Broken Access Control
A06:2017-Security Misconfiguration
A07:2017-Cross-Site Scripting (XSS)
A08:2017-Insecure Deserialization
A09:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring

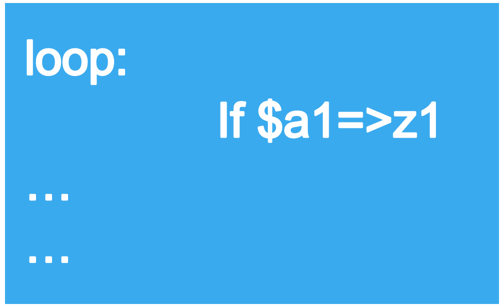
2021

A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
(New) A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
(New) A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures*
(New) A10:2021-Server-Side Request Forgery (SSRF)*

* From the Survey

Application Security – Vulnerability Testing

- SAST (Static Application Security Testing)
  - ‘White box’
  - Source code
  - Finds vulnerabilities earlier



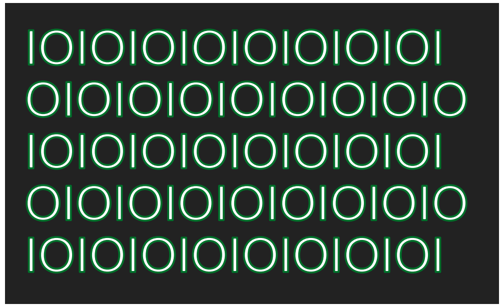
```
loop:
            If $a1=>z1
…
…
```

DAST (Dynamic Application Security Testing)

- ‘Black box’

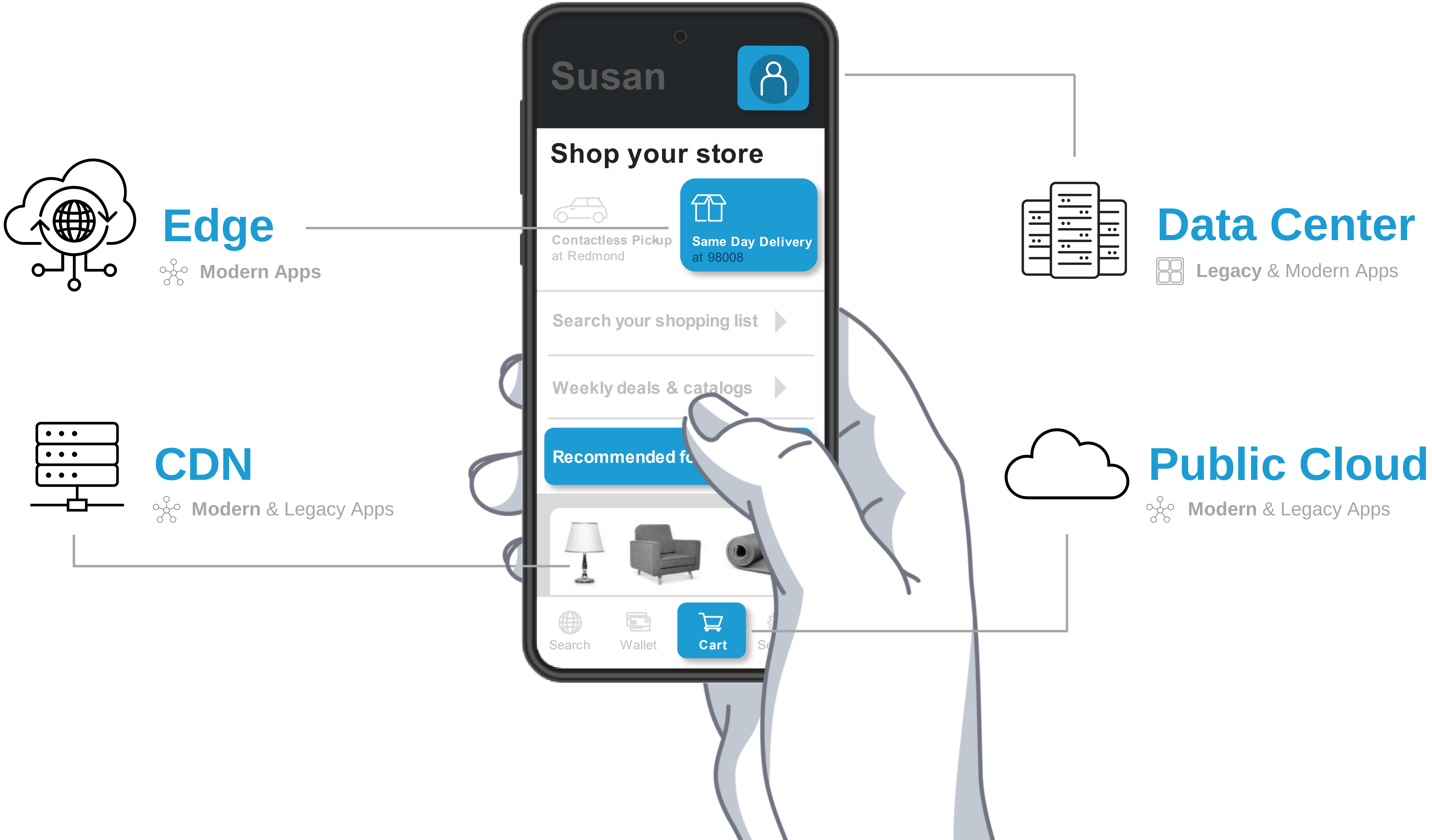
- Running applications

- Finds vulnerabilities later



```
IOIOIOIOIOIOIOIOI
OIOIOIOIOIOIOIOIO
IOIOIOIOIOIOIOIOI
OIOIOIOIOIOIOIOIO
IOIOIOIOIOIOIOIOI
```

Digital experiences are comprised of legacy and modern apps, with multiple app sources spanning on-prem to edge



Edge

Modern Apps

CDN

Modern & Legacy Apps

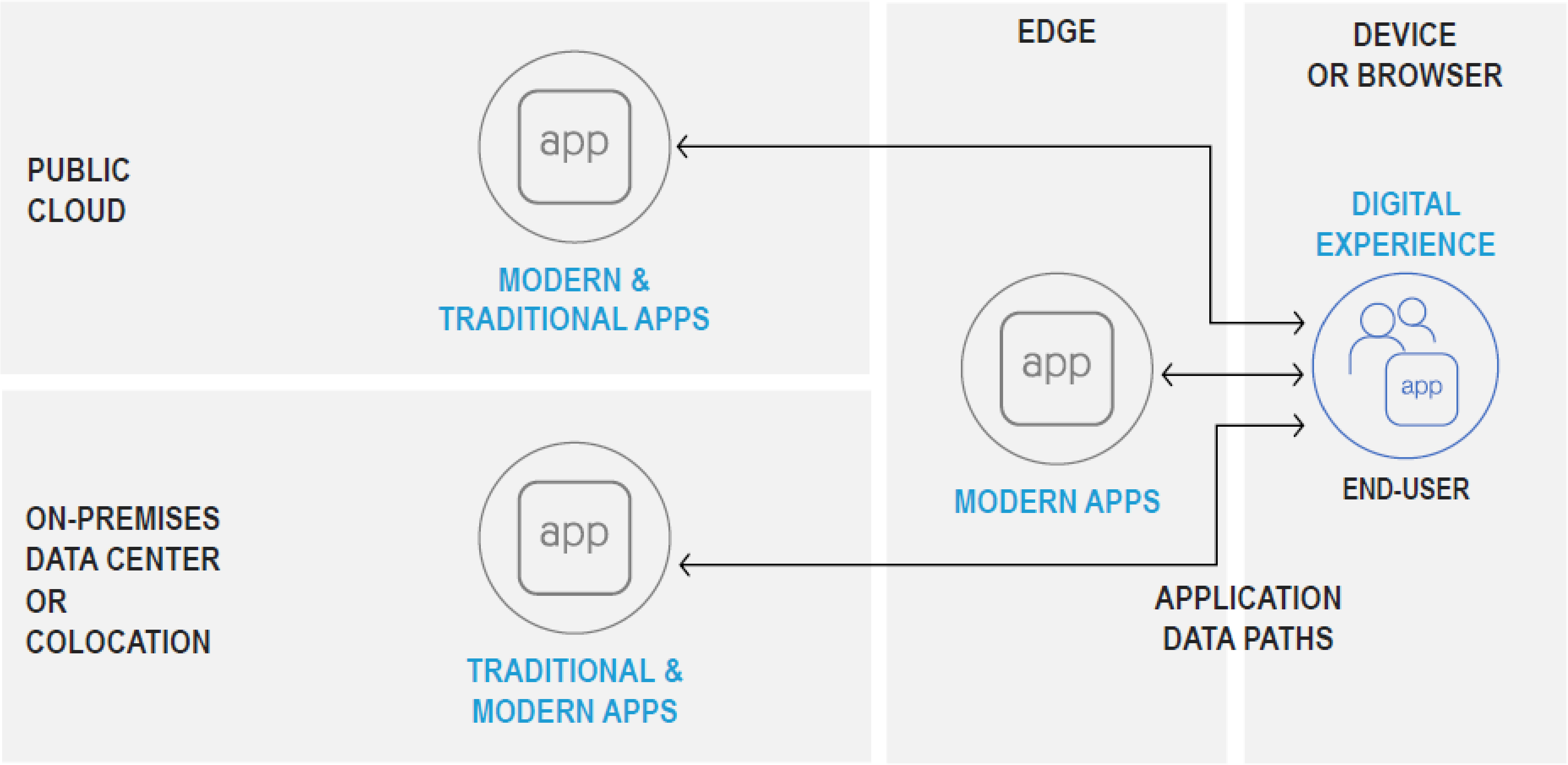
Data Center

Legacy & Modern Apps

Public Cloud

Modern & Legacy Apps

Most digital experiences are a blend of traditional and modern applications



Explosive app growth brings big opportunities & challenges

OPPORTUNITIES

Improve customer experience

Transform the business

Differentiate

CHALLENGES

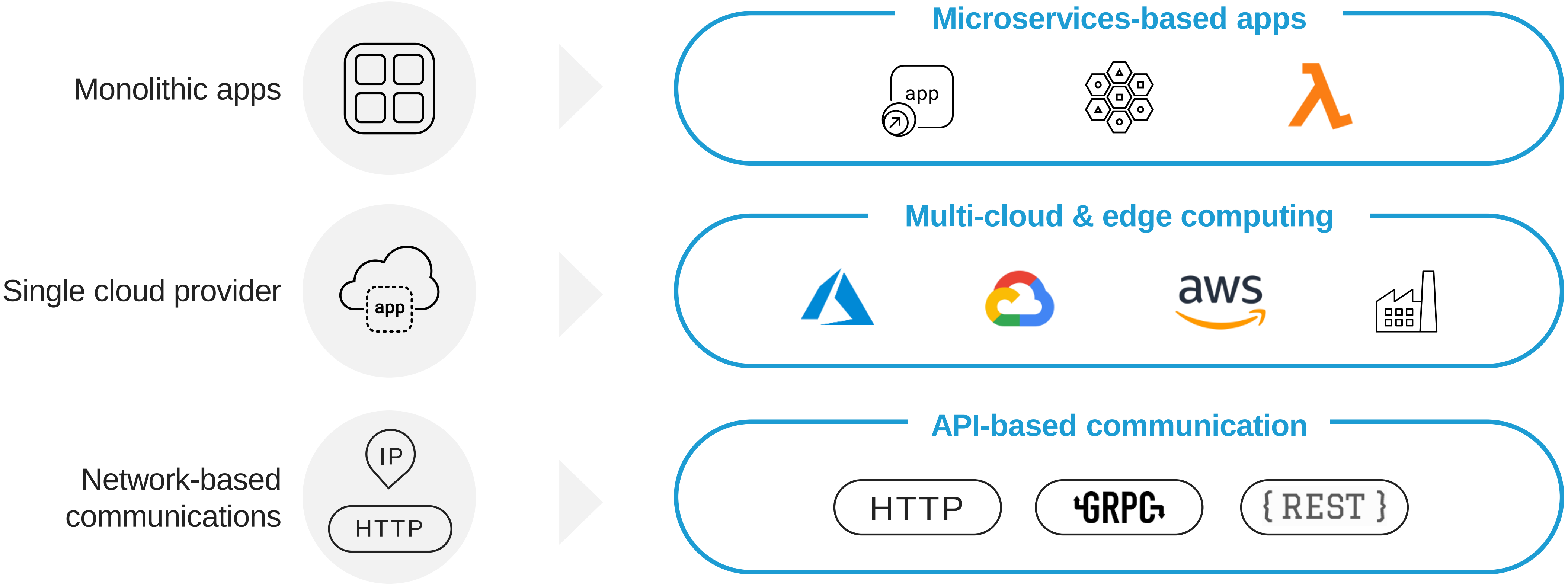
Security

Modernization

Complexity

IT as enabler of innovation

Combined with a shift in how apps are designed & deployed



Monolithic apps → Microservices-based apps

Single cloud provider → Multi-cloud & edge computing

Network-based communications → API-based communication

…thus securing apps & APIs has never been harder

Growing exposure

Log4j

Dynamic OWASP Top 10

Critical CVE growth

Ephemeral apps

Growing attack surface

Microservices

Containers

APIs

Distributed clusters

…thus securing apps & APIs has never been harder

Sprawl of tools, too small team

App firewall

API security

Identity

Bot mitigation

DDoS protection

Cloud security

Regulatory compliance

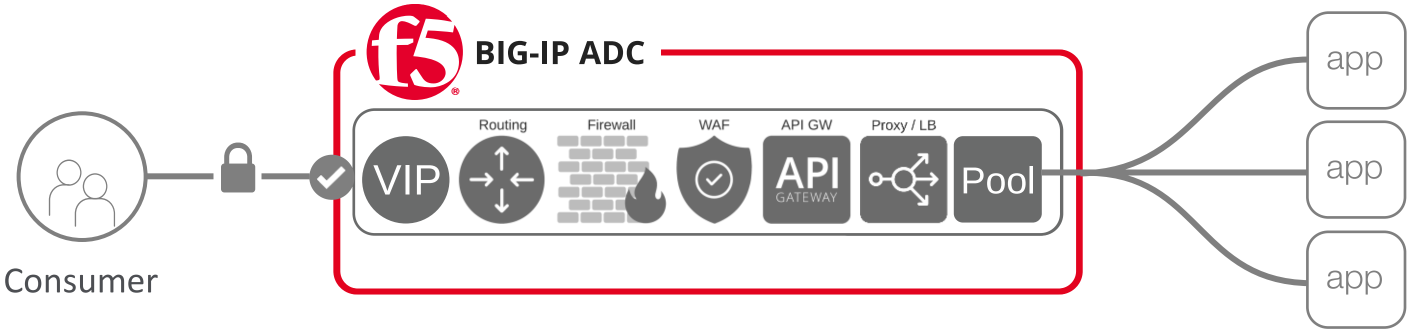
Data privacy

Cyber-insurance

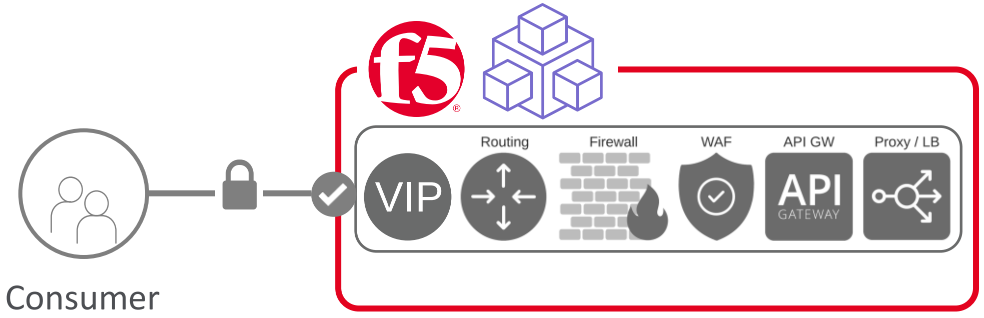
Domestic & global compliance

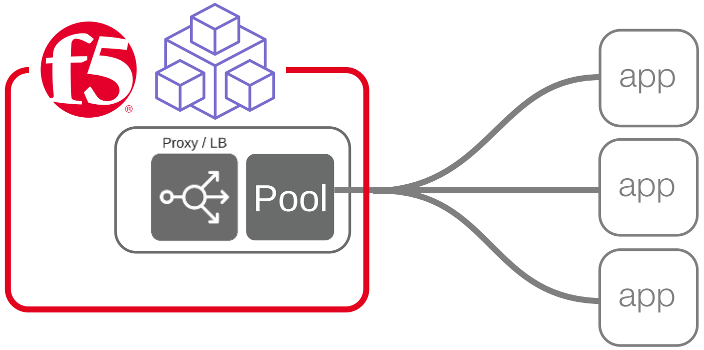
How to publish and protect applications in a multi-cloud environment?

Today, ADCs are deployed close to the App…

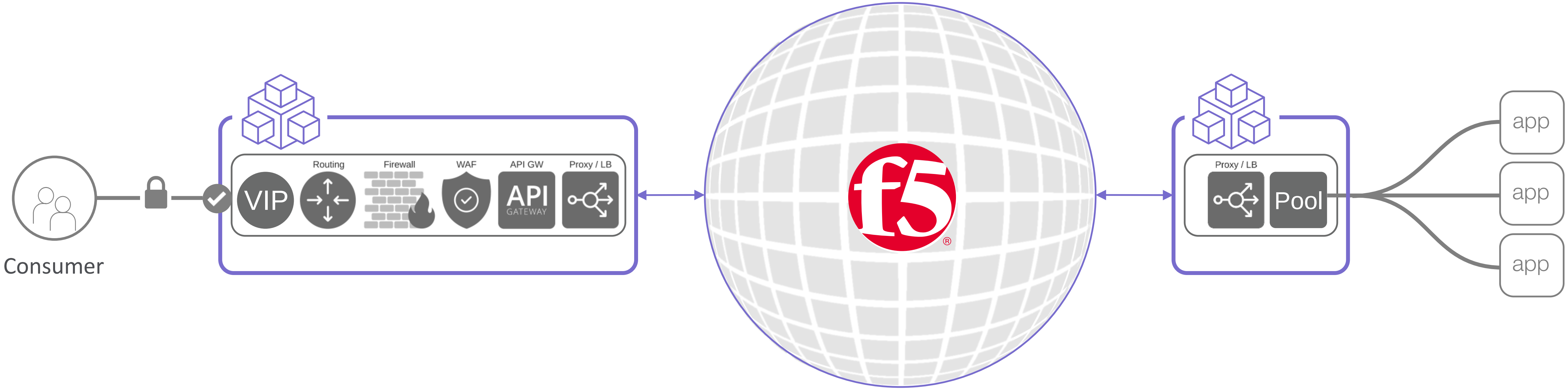


Imagine if you could split your ADC in half…





…and stretch it apart, across our global network

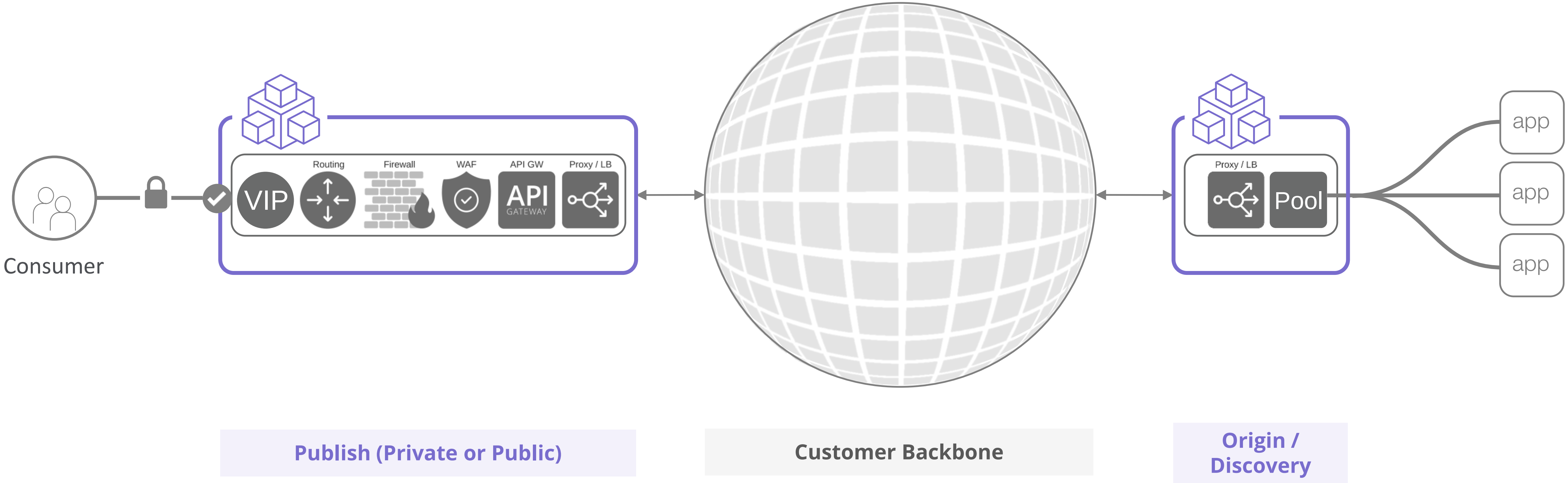


Publish (Private or Public)

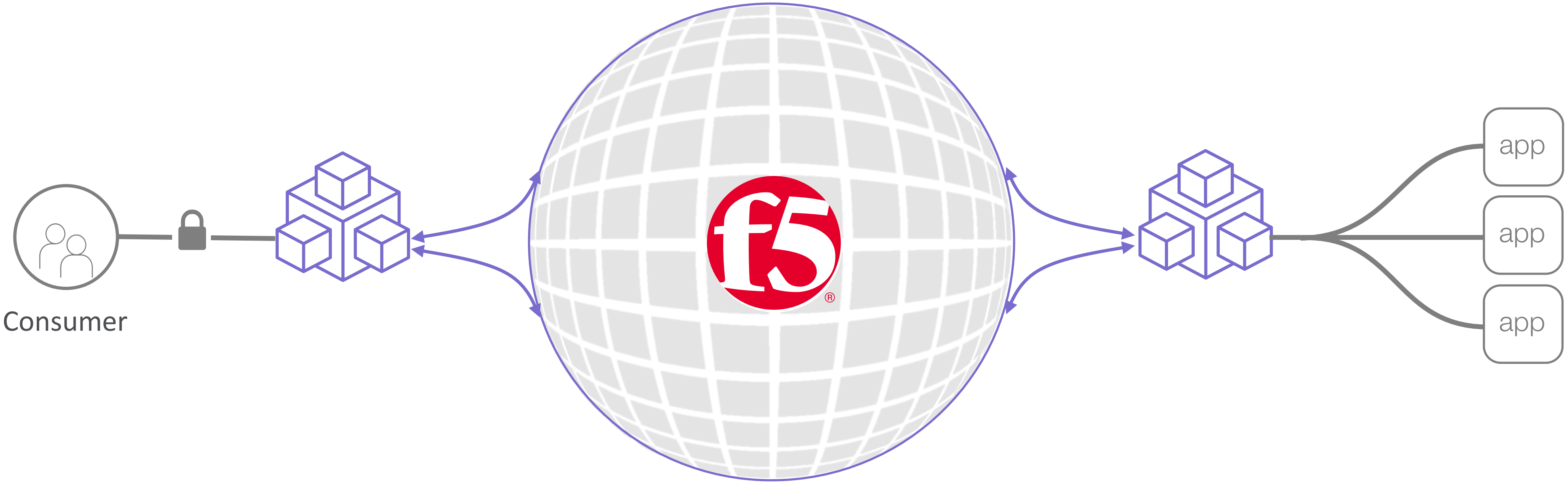
Secure Global Network

Origin / Discovery

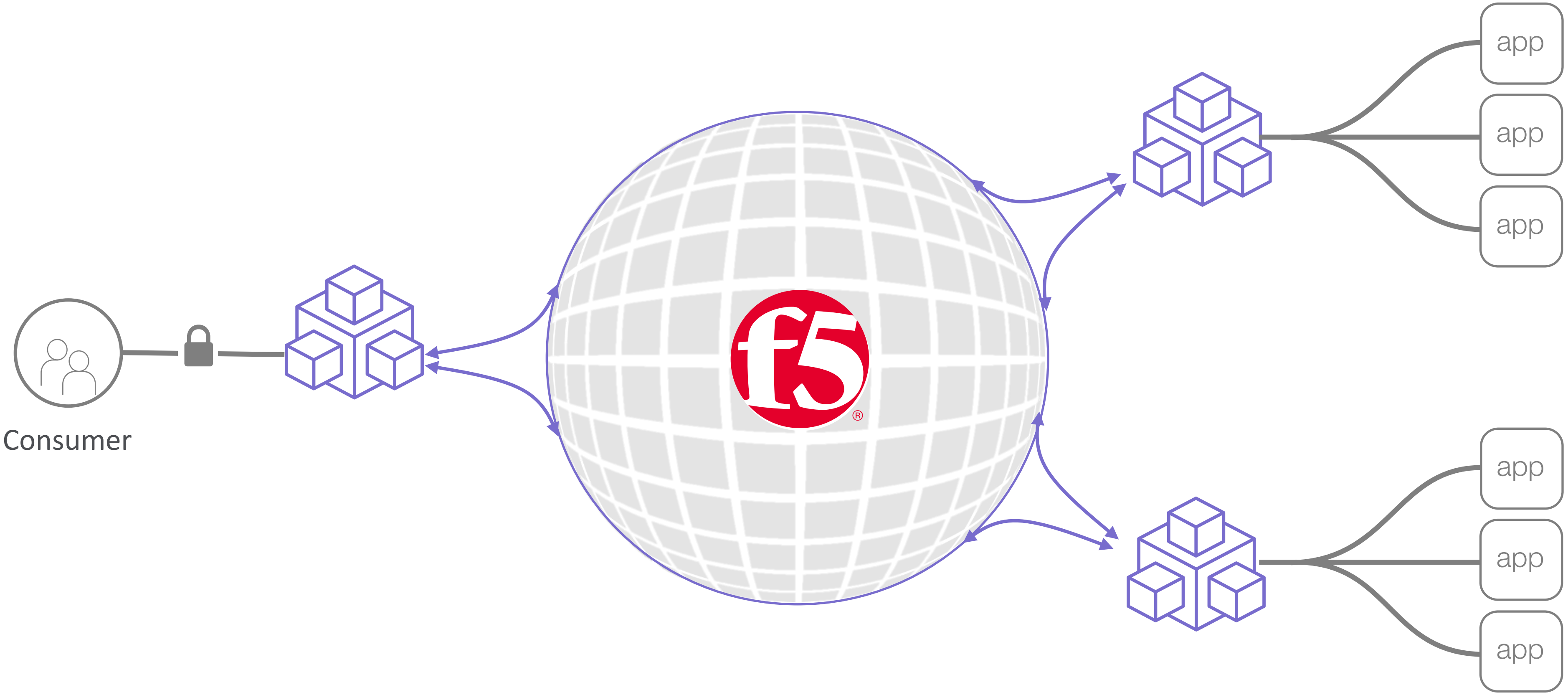
…or across your private backbone



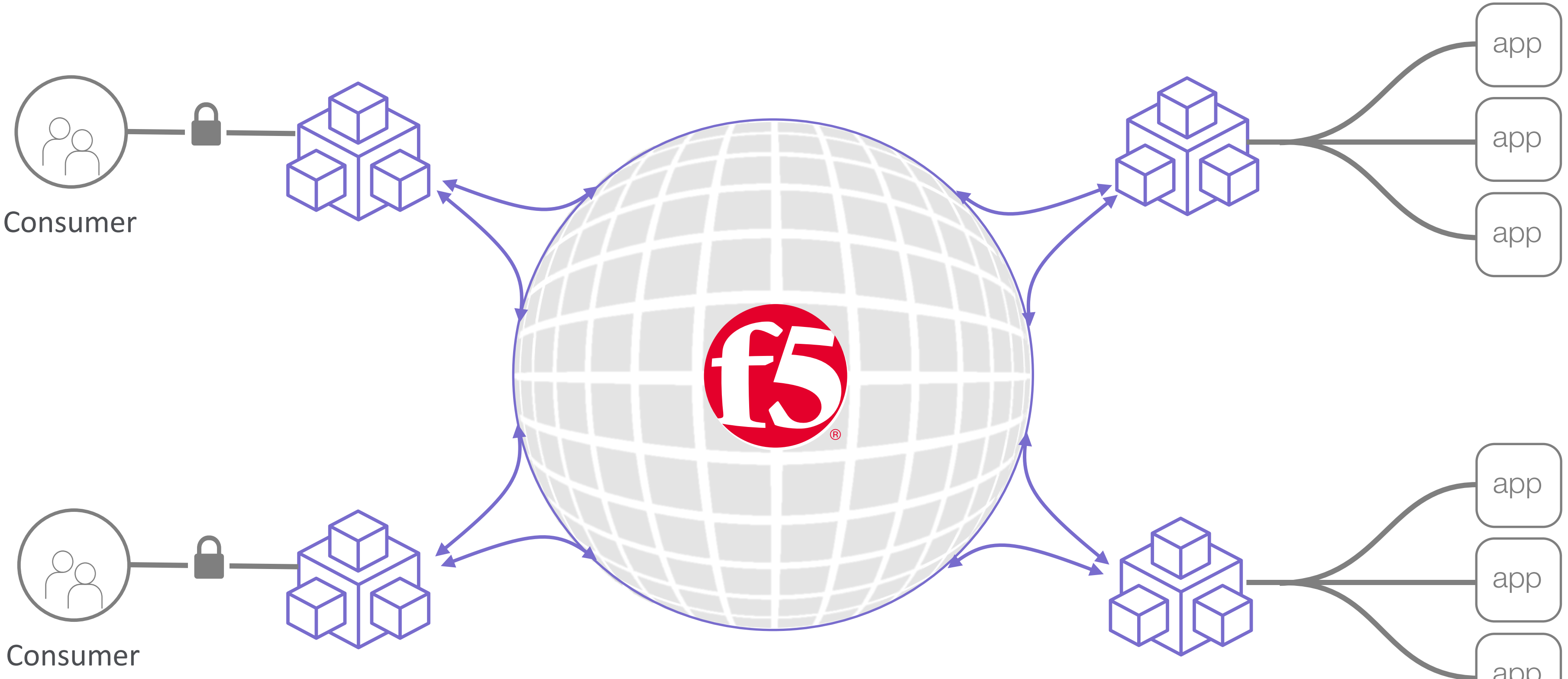
…we simply connect locations…



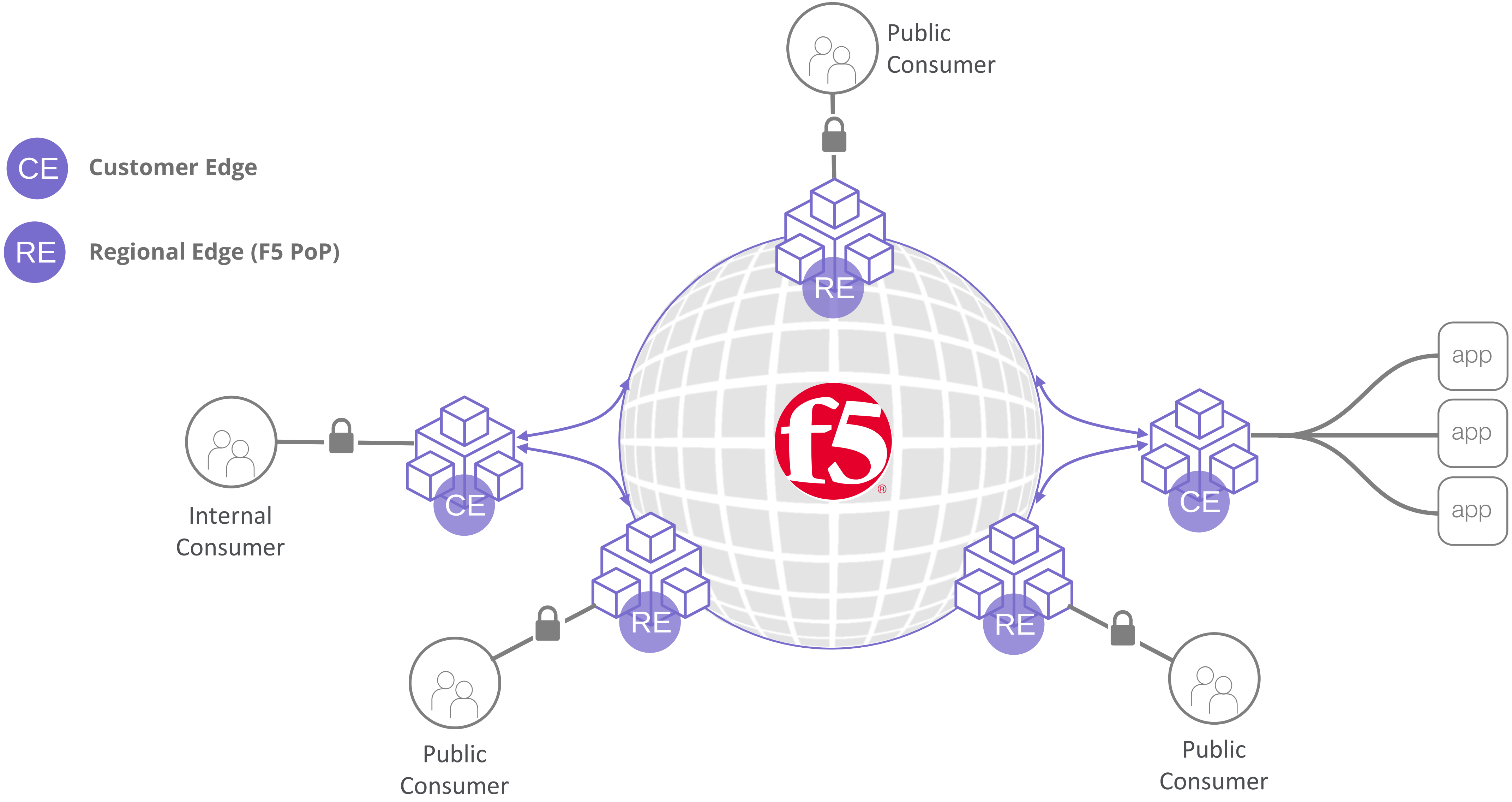
…we simply connect locations…



…we simply connect locations…



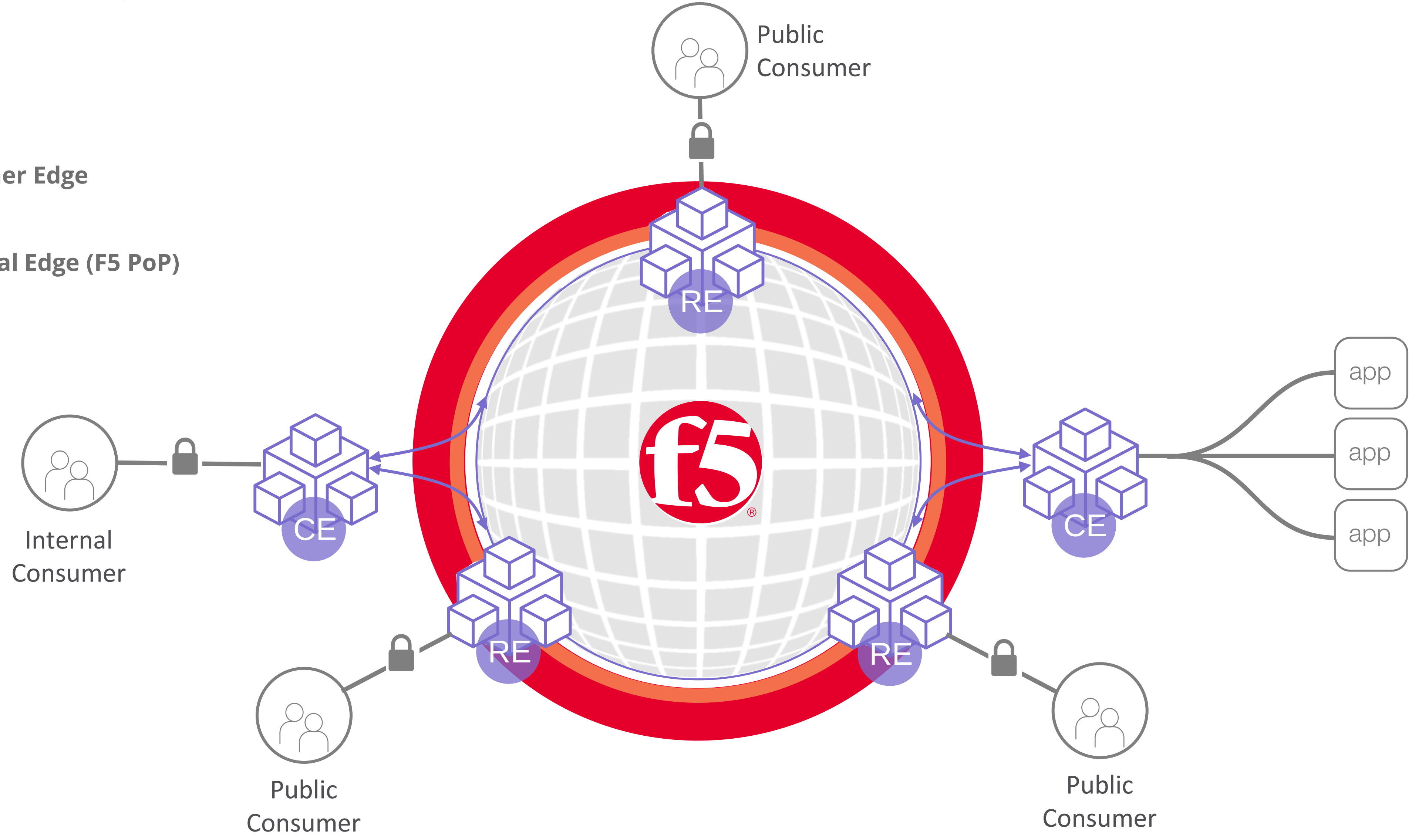
…and you can deploy LBs into our PoPs…



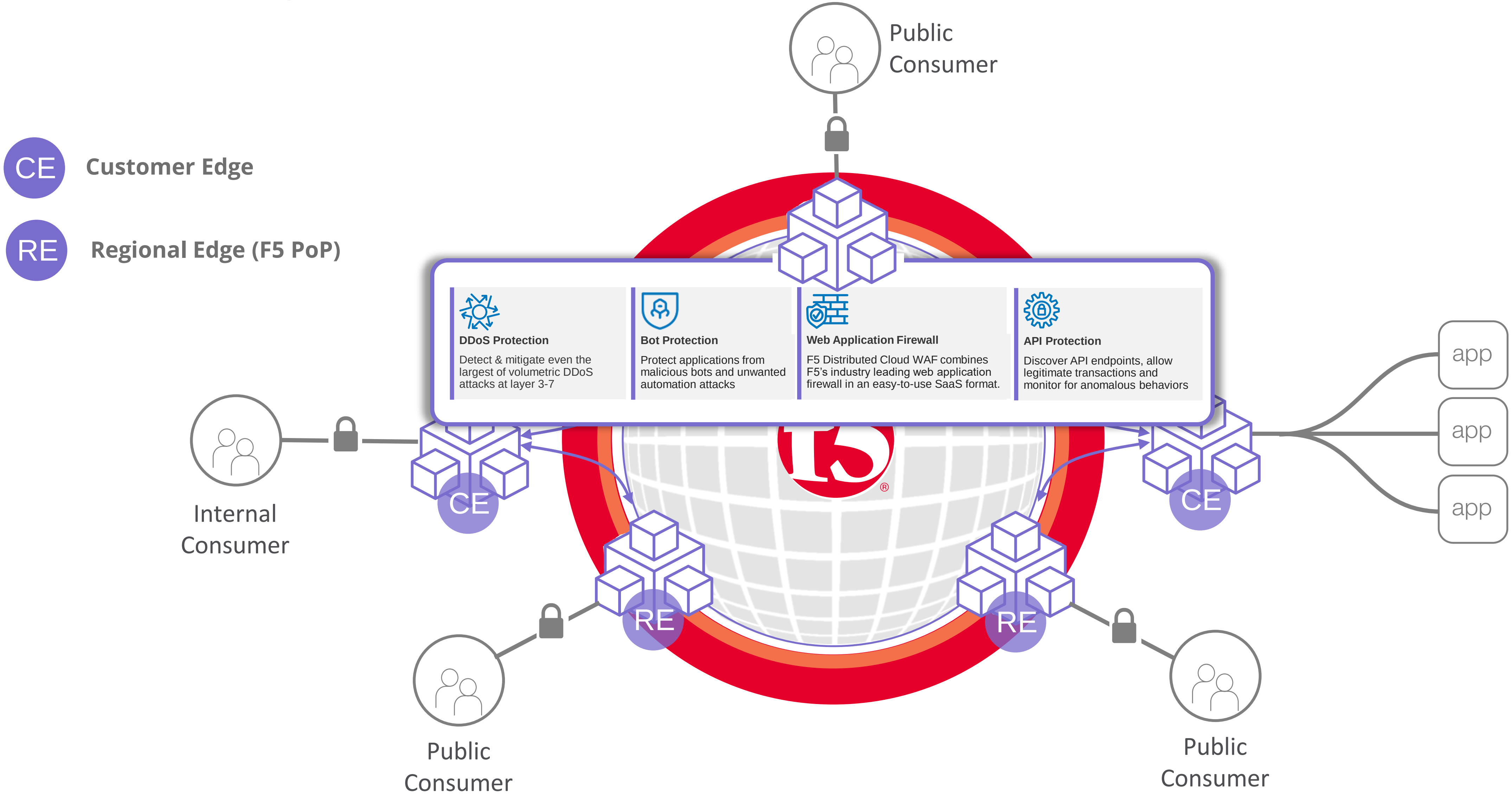
…including WAAP Protection (DDoS, Bot, API, WAF)

CE Customer Edge

RE Regional Edge (F5 PoP)



…including WAAP Protection (DDoS, Bot, API, WAF)



CE Customer Edge

RE Regional Edge (F5 PoP)

DDoS Protection

Detect & mitigate even the largest of volumetric DDoS attacks at layer 3-7

Bot Protection

Protect applications from malicious bots and unwanted automation attacks

Web Application Firewall

F5 Distributed Cloud WAF combines F5's industry leading web application firewall in an easy-to-use SaaS format.

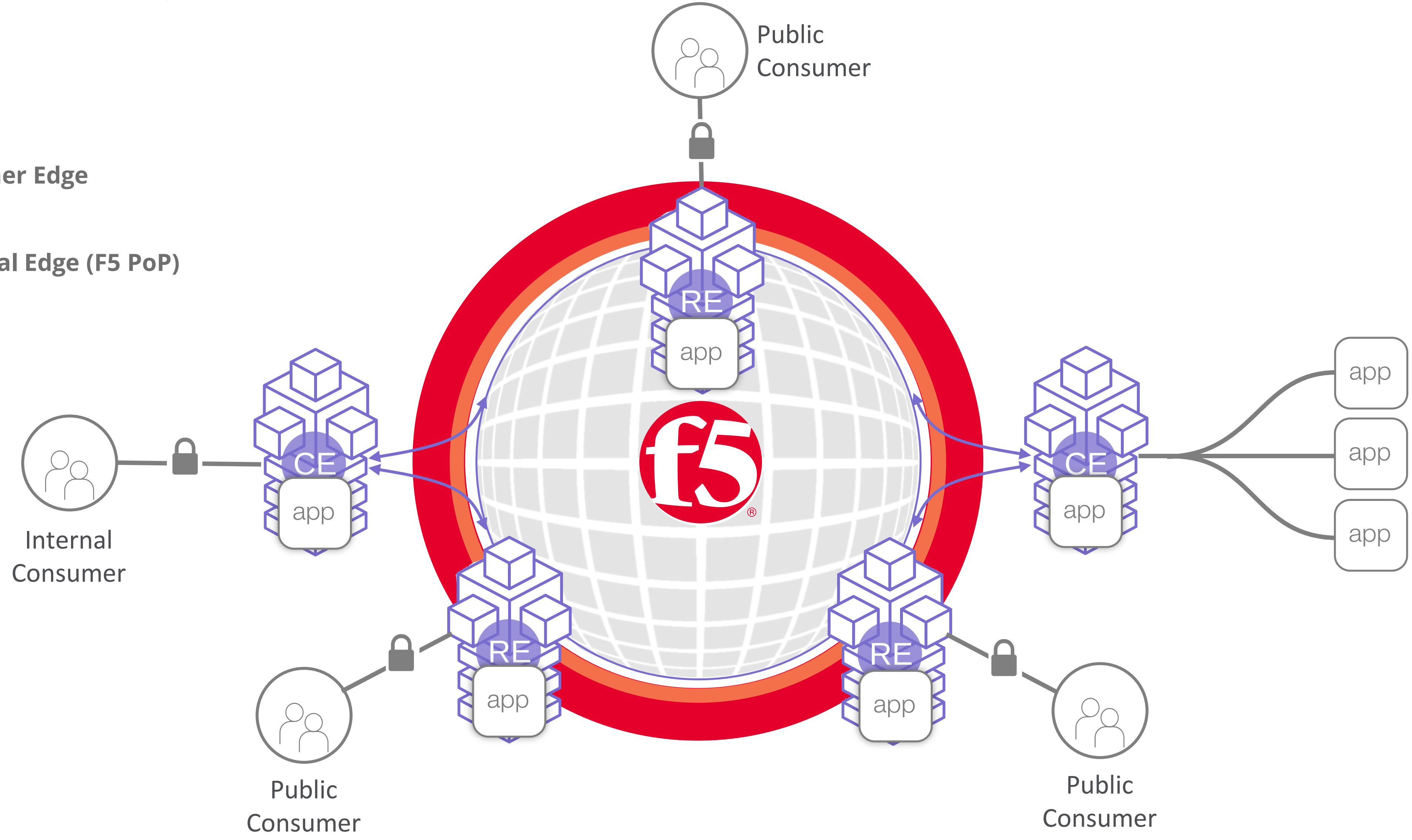
API Protection

Discover API endpoints, allow legitimate transactions and monitor for anomalous behaviors

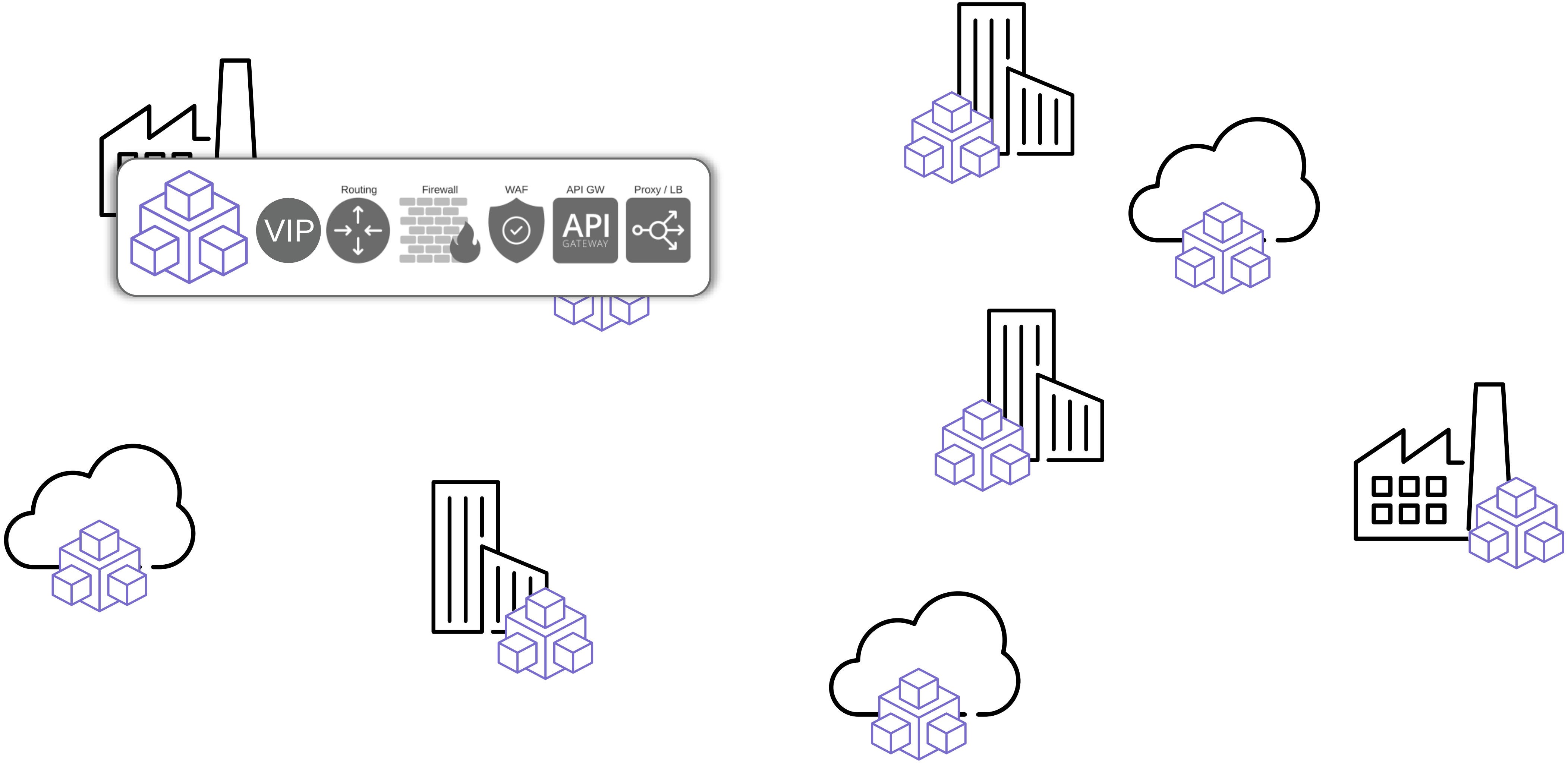
…and deploy pods into a distributed, virtual k8s

CE Customer Edge

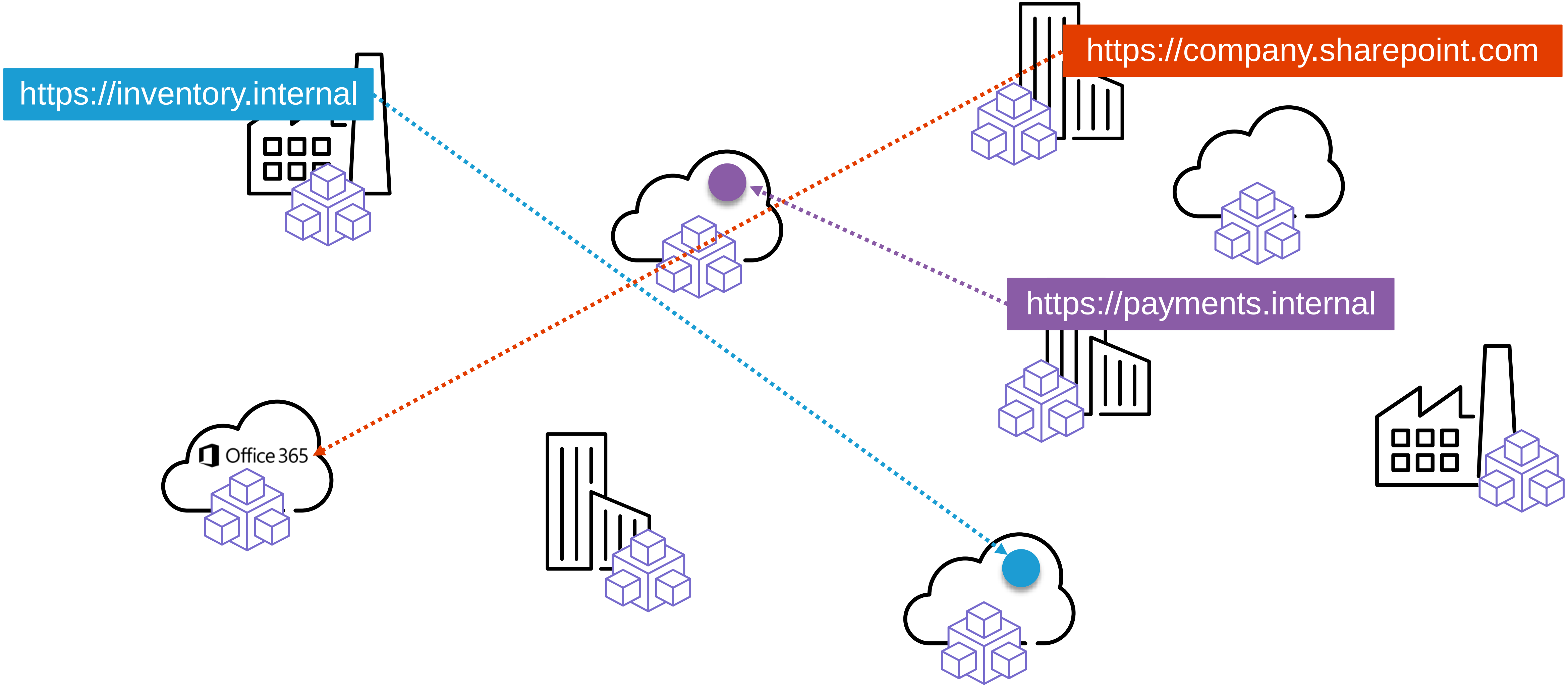
RE Regional Edge (F5 PoP)



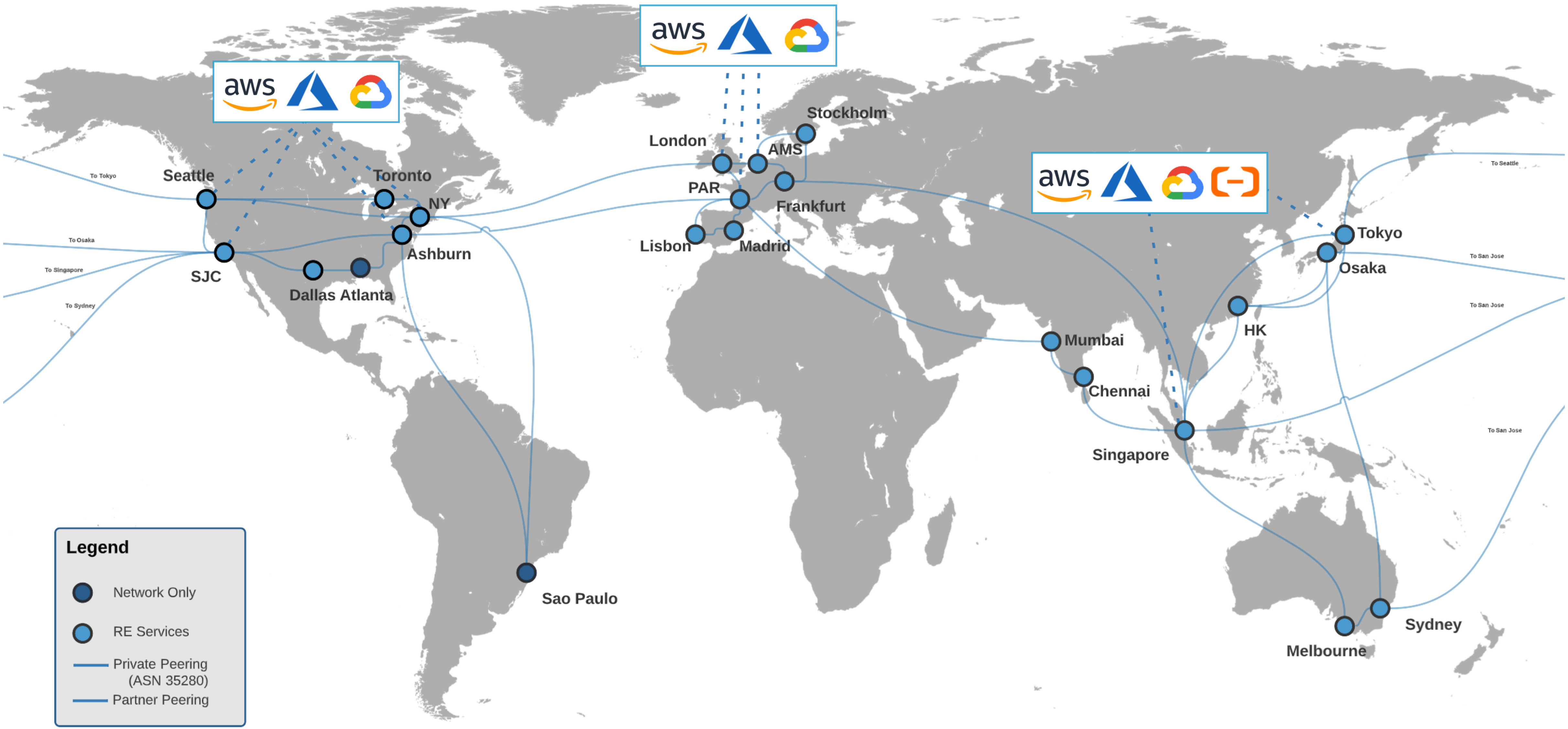
…connect any site Discover and Publish by Name



…connect any site Discover and Publish by Name


https://inventory.internal
https://company.sharepoint.com
https://payments.internal
Office 365

Our global Application Delivery Network (ADN)



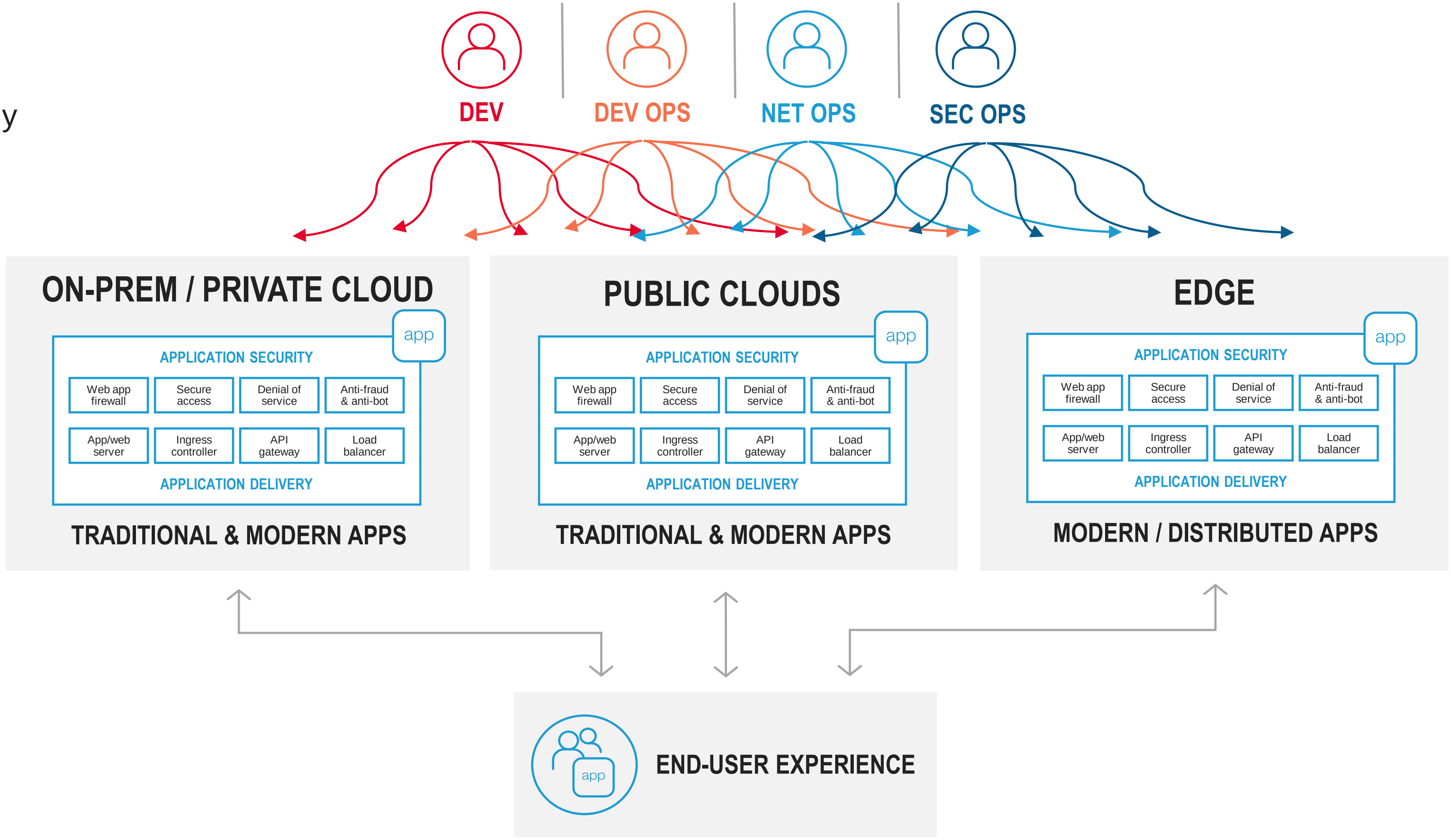
An Example Of That Complexity

#1 **Operational debt** due to technology inconsistencies across environments

#2 **Automation challenge** ”stitching” and scaling multiple environments, lack of consistency and visibility

#3 **Security landscape** due to increased attack surface and sophistication of bad actors

#4 **Limited observability** due telemetry trapped in silos of disjointed systems & environments



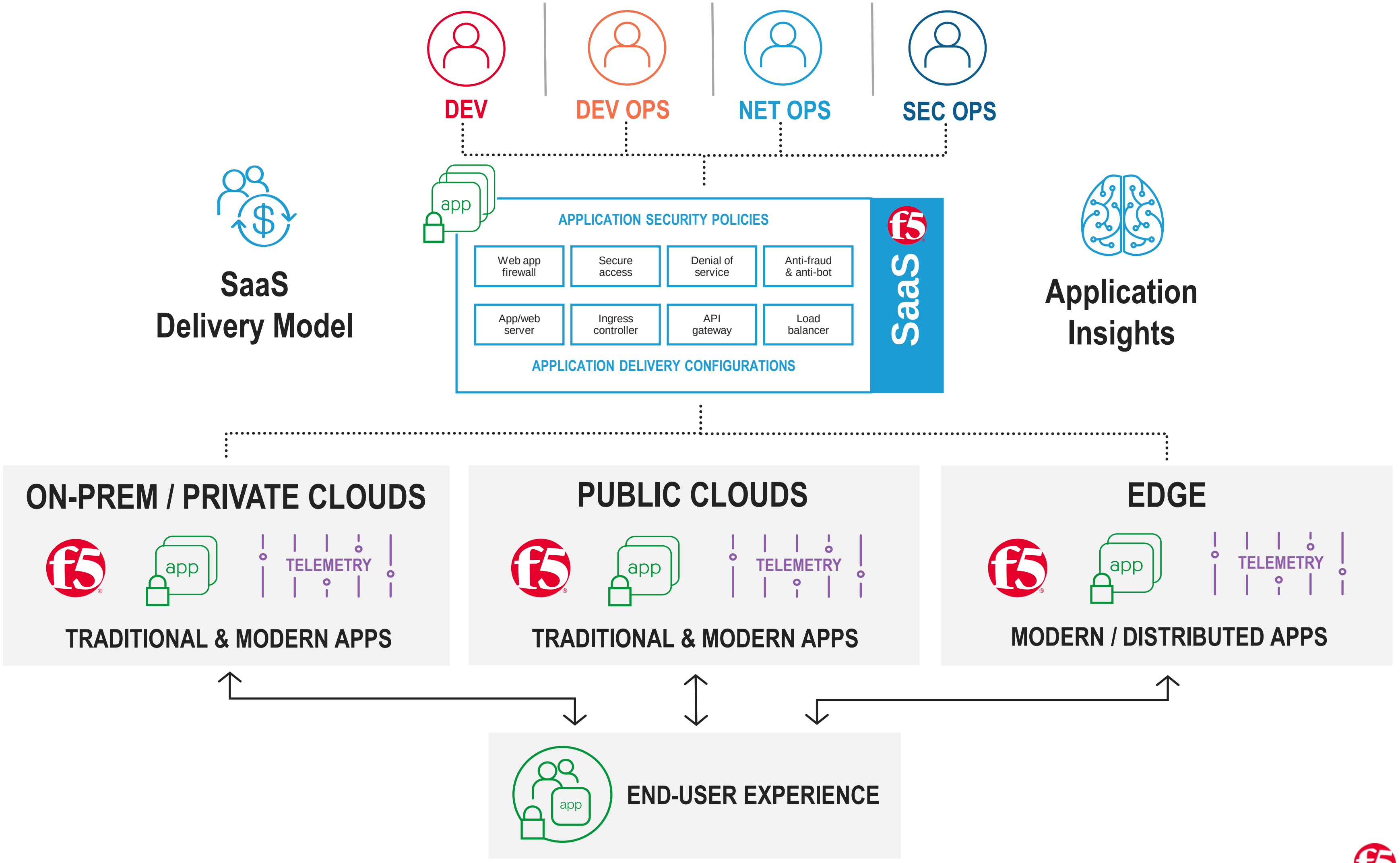
Reducing Complexity with F5's SaaS Platform - XC

SaaS Platform Delivers Business Outcomes:

#1 Reduce Operational Complexity with consistency across all environments

#2 Enhance End User Performance with Edge

#3 Improve Time to Service & Value by easing automation



DEV | DEV OPS | NET OPS | SEC OPS

SaaS Delivery Model

APPLICATION SECURITY POLICIES

Web app firewall	Secure access	Denial of service	Anti-fraud & anti-bot
App/web server	Ingress controller	API gateway	Load balancer

APPLICATION DELIVERY CONFIGURATIONS

SaaS

Application Insights

ON-PREM / PRIVATE CLOUDS — app — TELEMETRY — TRADITIONAL & MODERN APPS

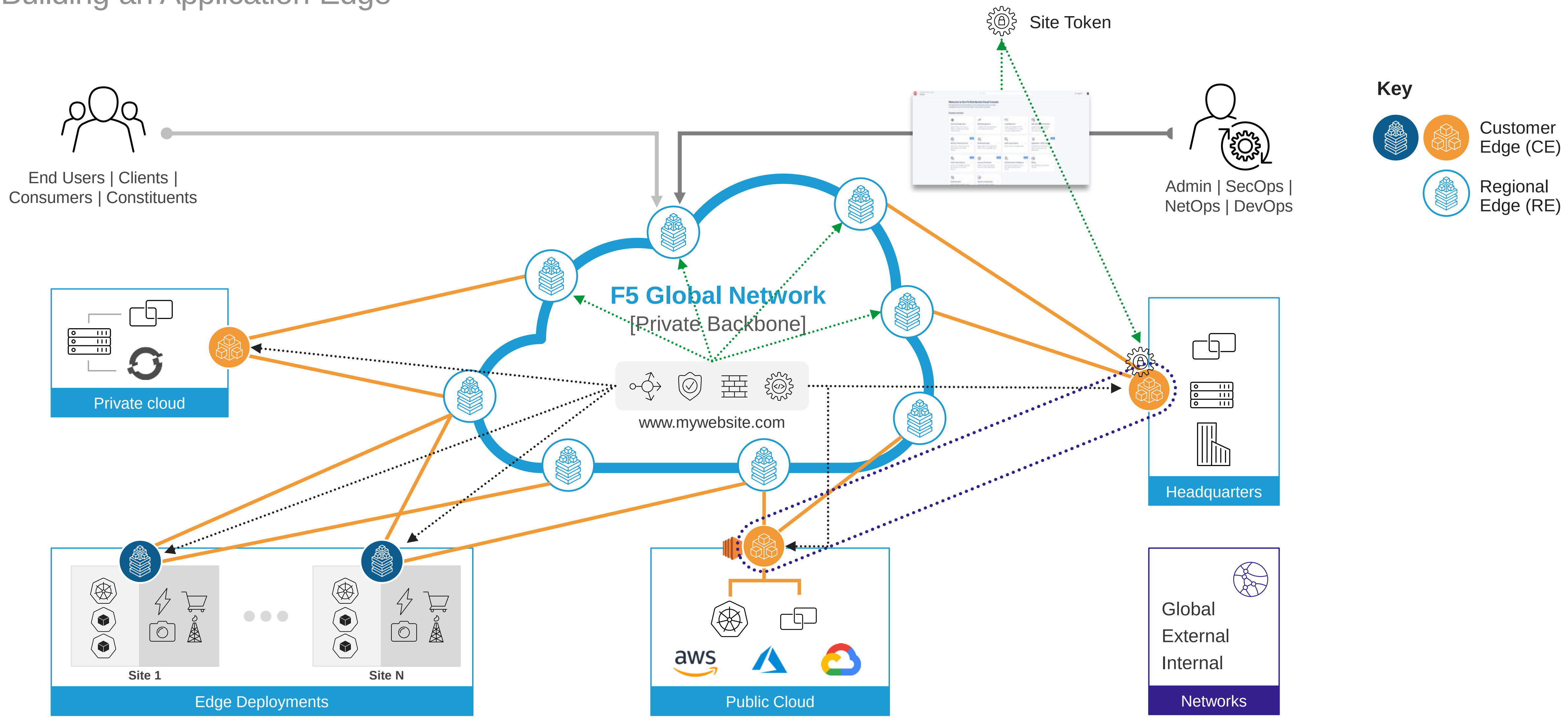
PUBLIC CLOUDS — app — TELEMETRY — TRADITIONAL & MODERN APPS

EDGE — app — TELEMETRY — MODERN / DISTRIBUTED APPS

END-USER EXPERIENCE

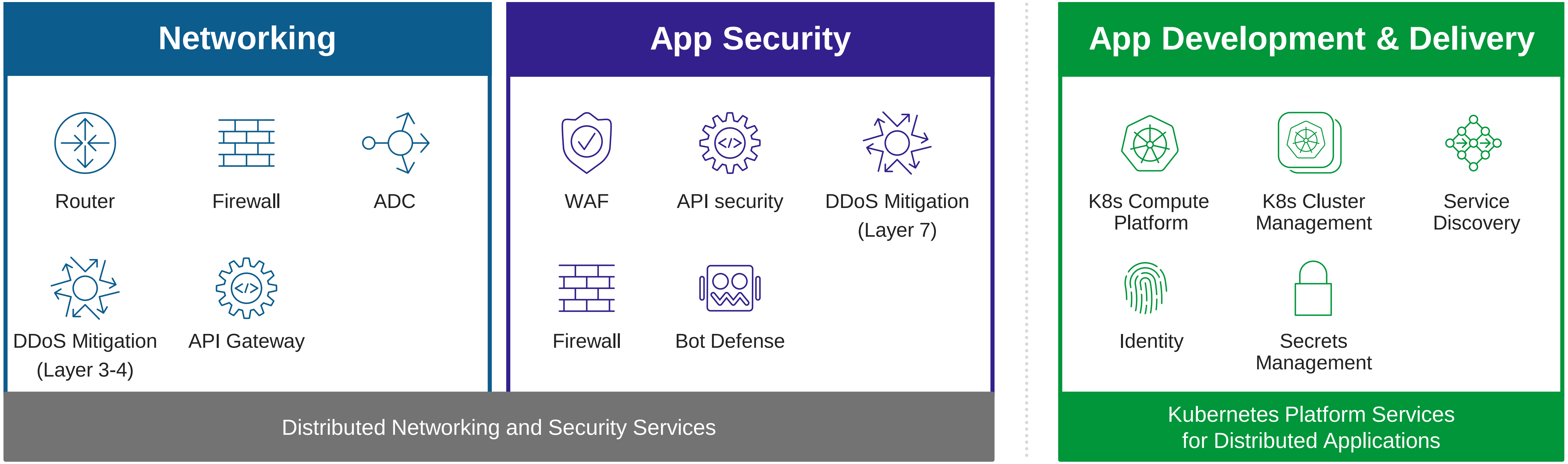
Linking everything together

Building an Application Edge



Key Building Blocks

- 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

F5 Distributed Cloud: Multi-cloud networking for applications

Deliver measurable improvements to your app delivery process

12x*

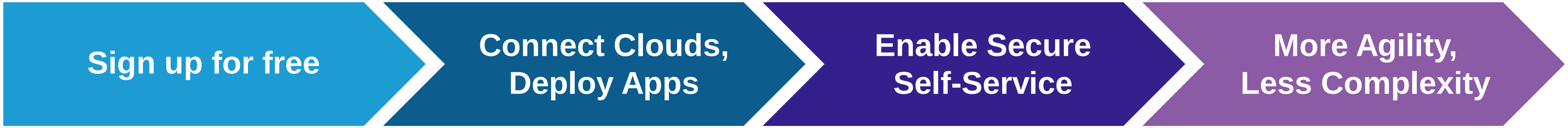
Reduction in Time to Service

70%*

Reduction in TCO (Deploy & Ops)

100%

Operational Delight



Sign up for free

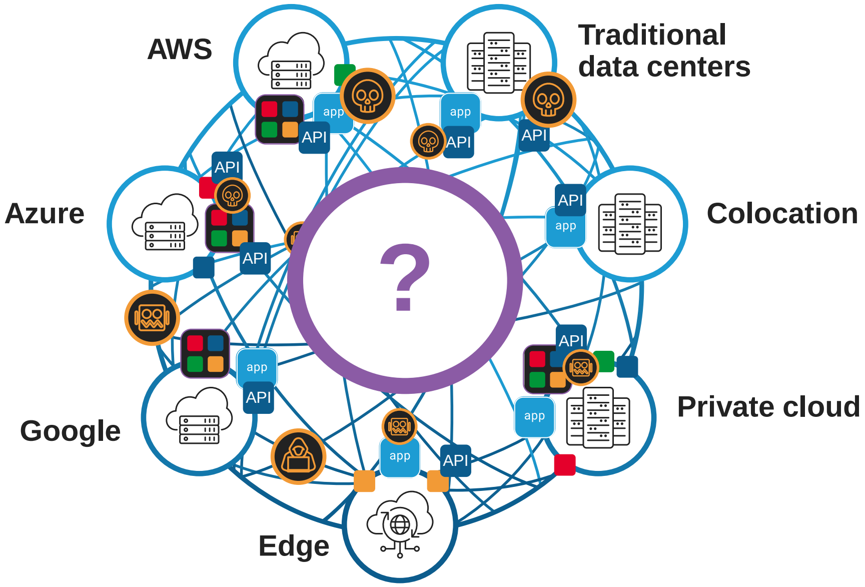
Connect Clouds, Deploy Apps

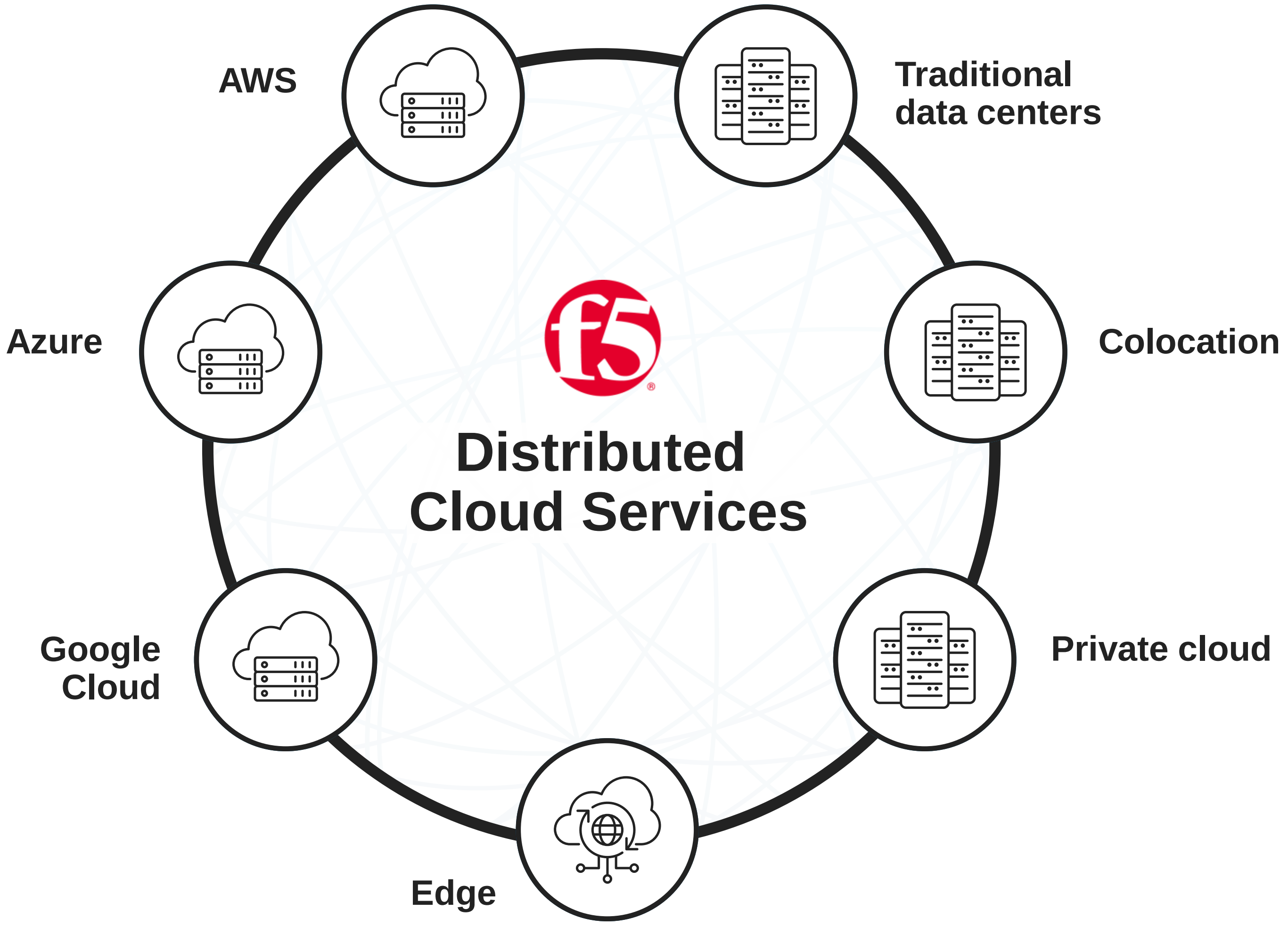
Enable Secure Self-Service

More Agility, Less Complexity

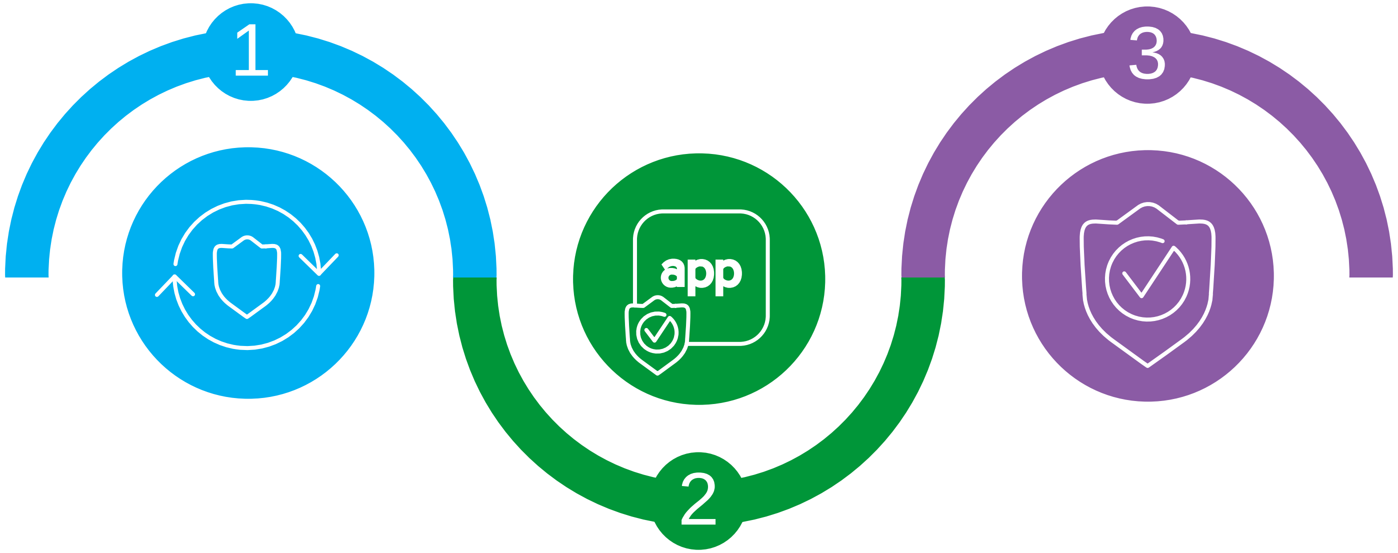
** Improvements in Time to Service and TCO based on customer-provided estimates*

Simplify secure connectivity across public cloud and edge





F5 secures apps & APIs everywhere



Make security enforcement more consistent & less complex across all apps

Maximize protection + reduce risk for modern apps & APIs at modern pace

Detect and mitigate threats more rapidly through AI, data & connected intelligence

THANK YOU

Five Years Out