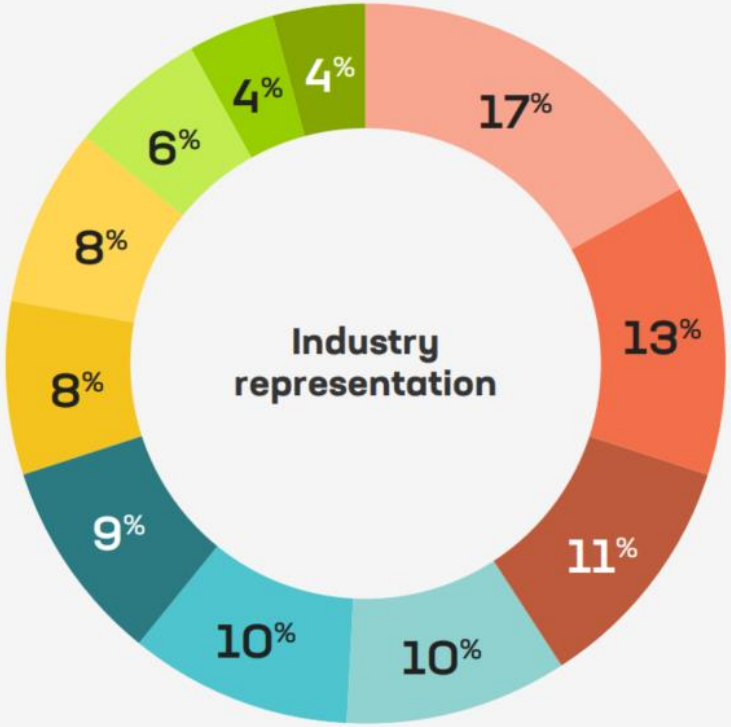
Alkalmazás védelem
a kockázatok elhárításának módjai és lehetőségei

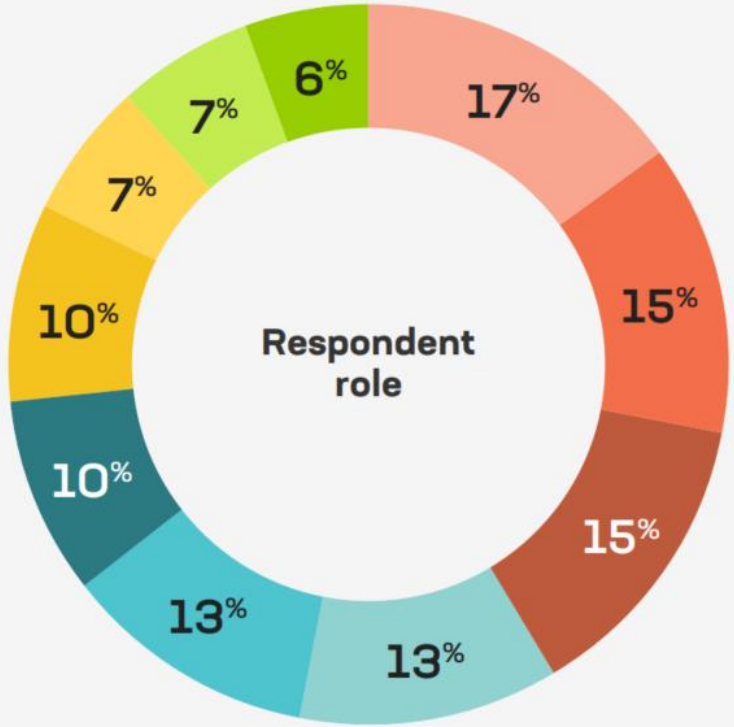
Gulyás Krisztián
F5 Solutions Architect & Team Lead
ALEF Distribution HU Kft.
krisztian.gulyas@alef.com
+36 30 985 7376

F5 Certified Trainer

2023 State of Application Strategy Report

More than 1,000 IT decisionmakers from around the globe

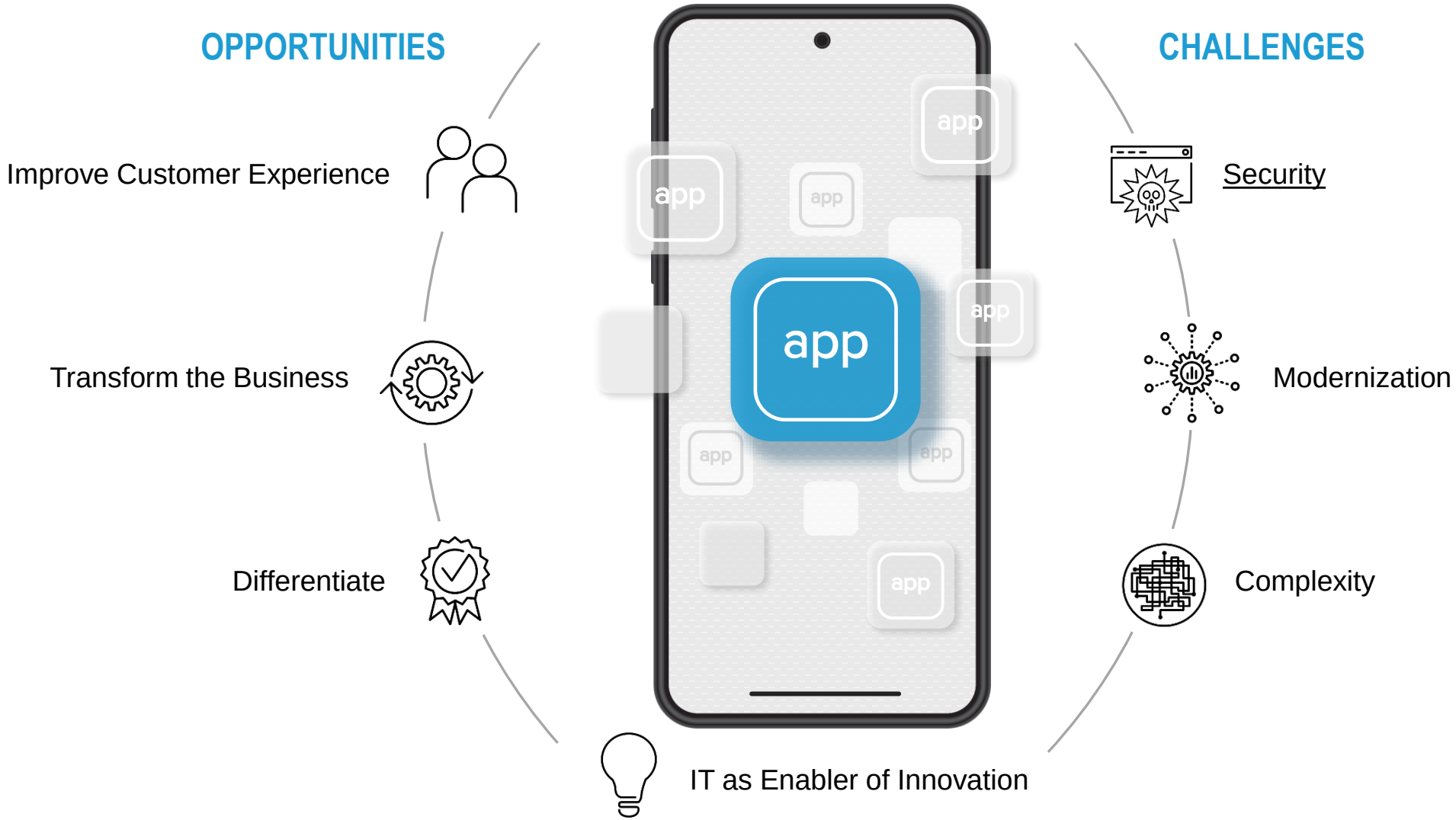




- Technology
- Financial services
- Manufacturing and resources
- Distribution and services, including retail, wholesale, transportation, and media
- Government/public sector
- Cloud service provider
- Telecommunications
- Education
- Other
- Healthcare
- Energy/utilities

- IT leader
- Network
- Data science
- Operations
- Other
- Security
- Business leader
- Business or tech app owner
- Cloud or enterprise architect
- Site reliability engineer (SRE), developer, DevOps, or DevOps manager

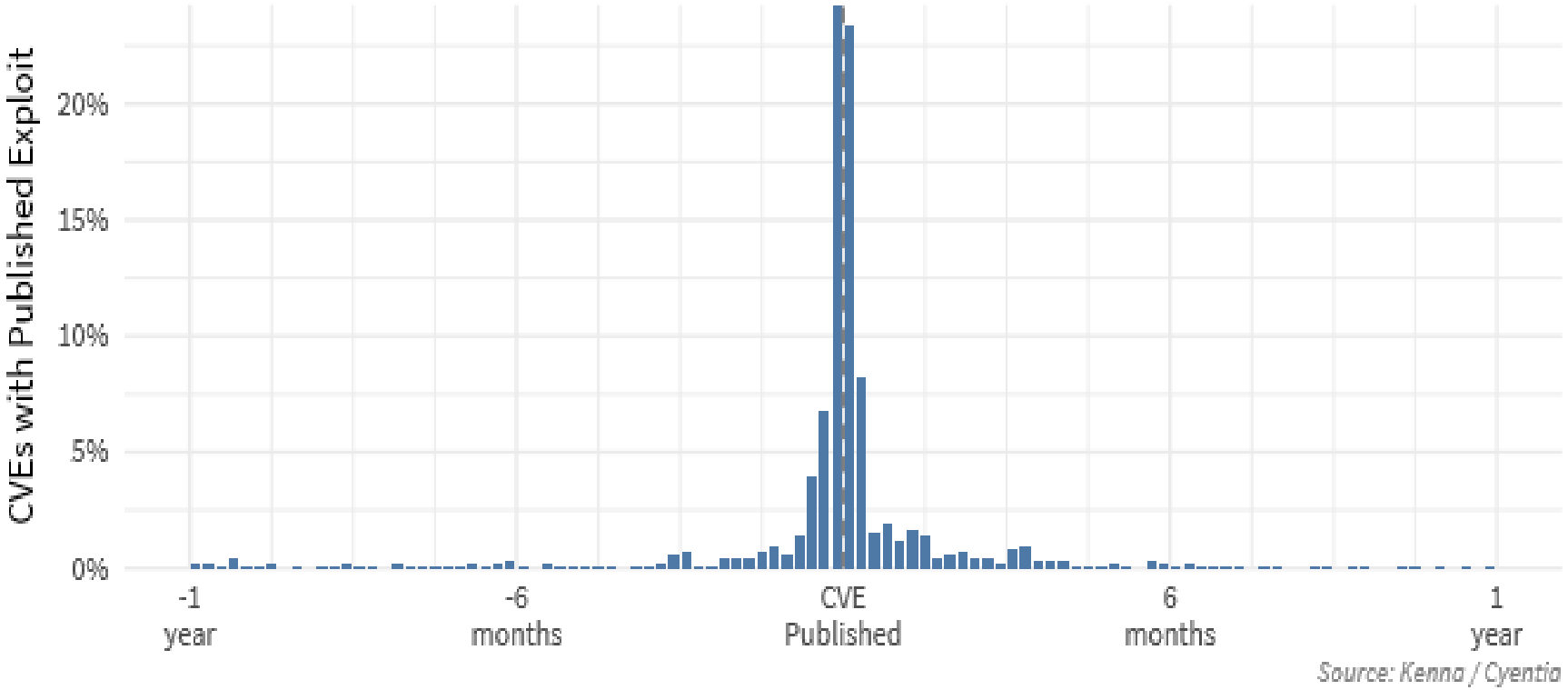
Driven by accelerated digital transformation, the explosive growth of applications presents incredible opportunities and challenges



Software vulnerabilities

SOFTWARE VULNERABILITIES IN APPLICATION STACKS (CVEs)

FREQUENTLY OCCURRING WEAKNESSES IN APPLICATION CODE (OWASP Top 10)

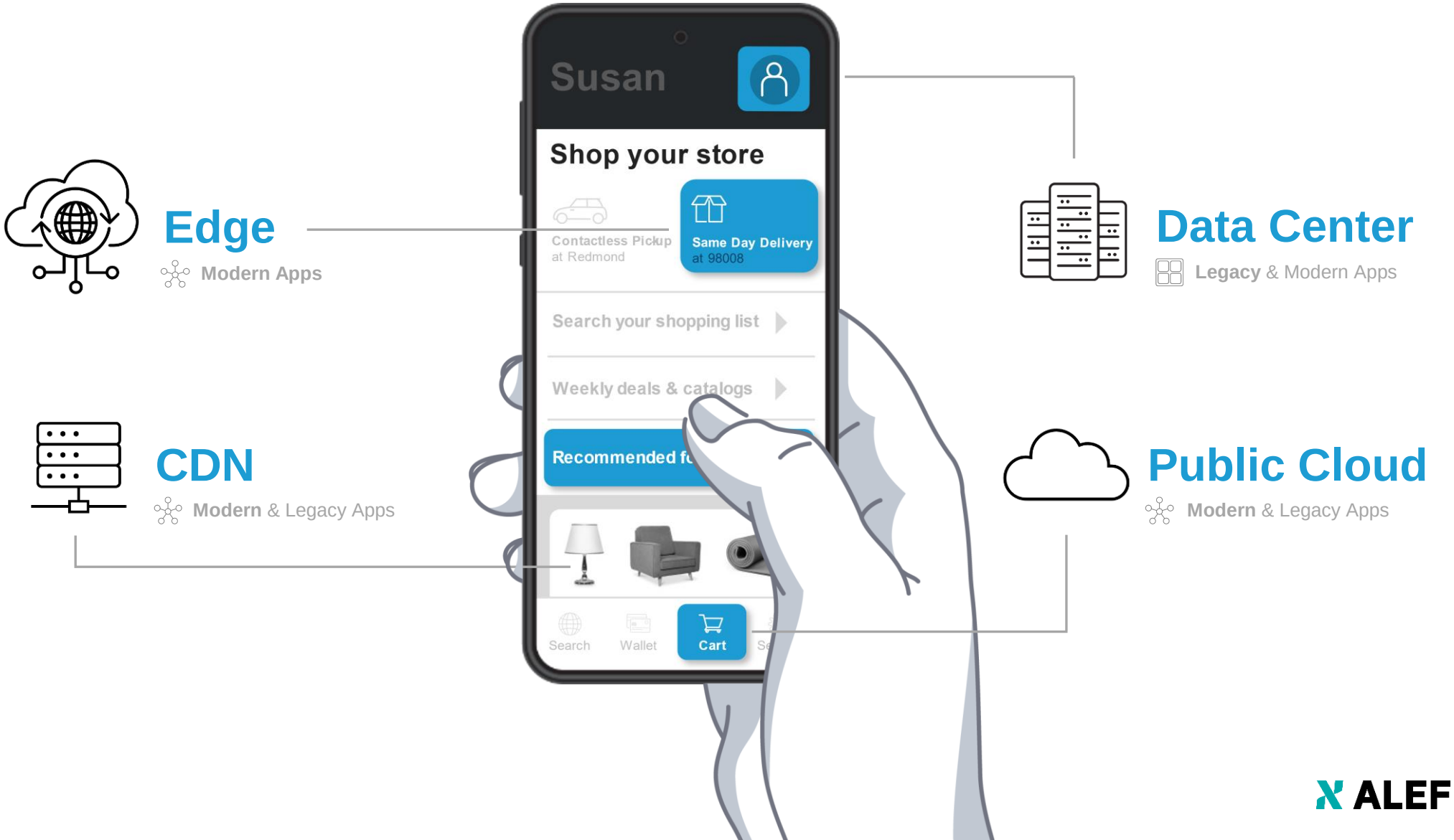


Exploit publication date relative to CVE publication date

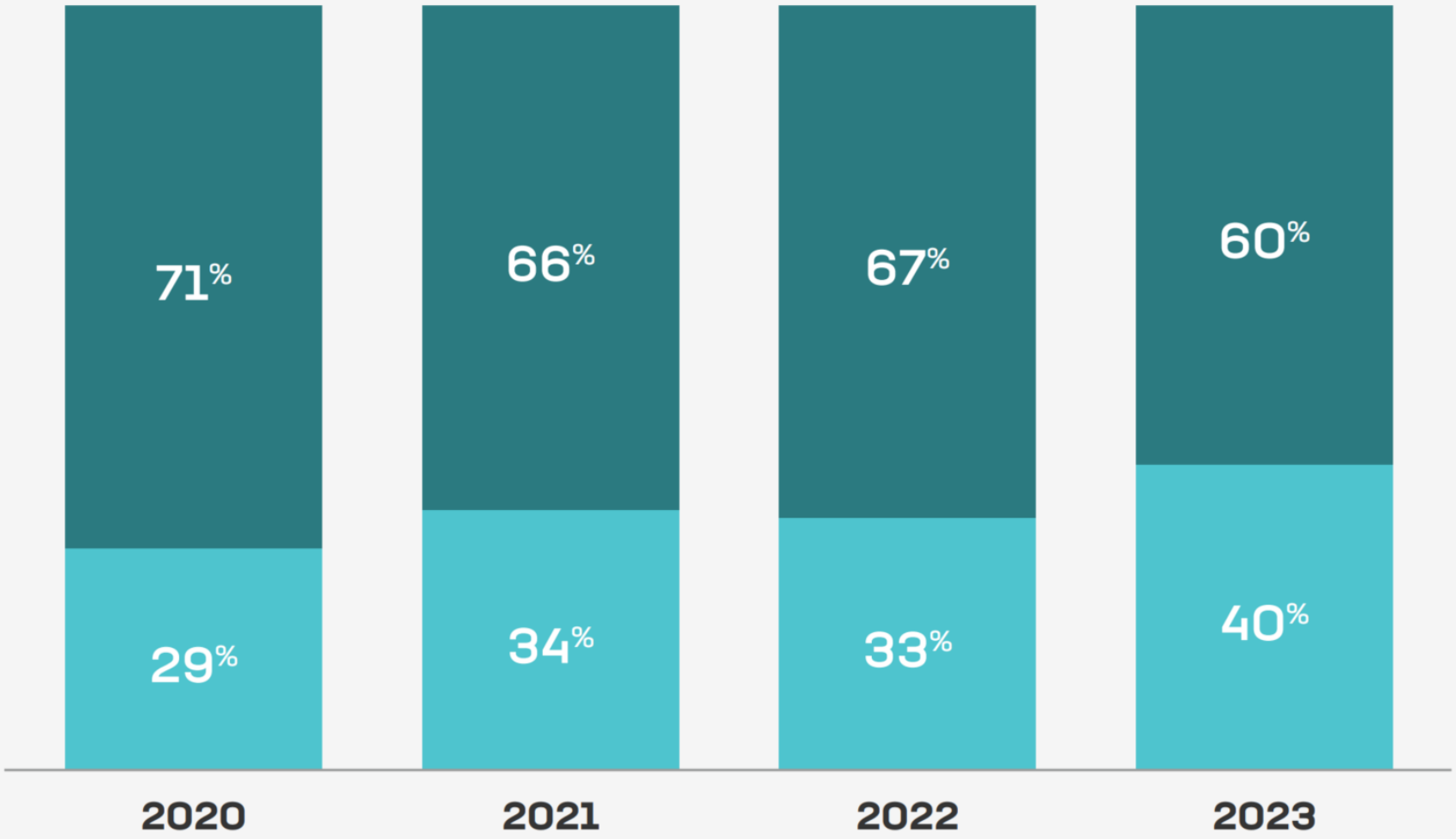
22%

of vulnerabilities can be weaponized with public exploit code

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



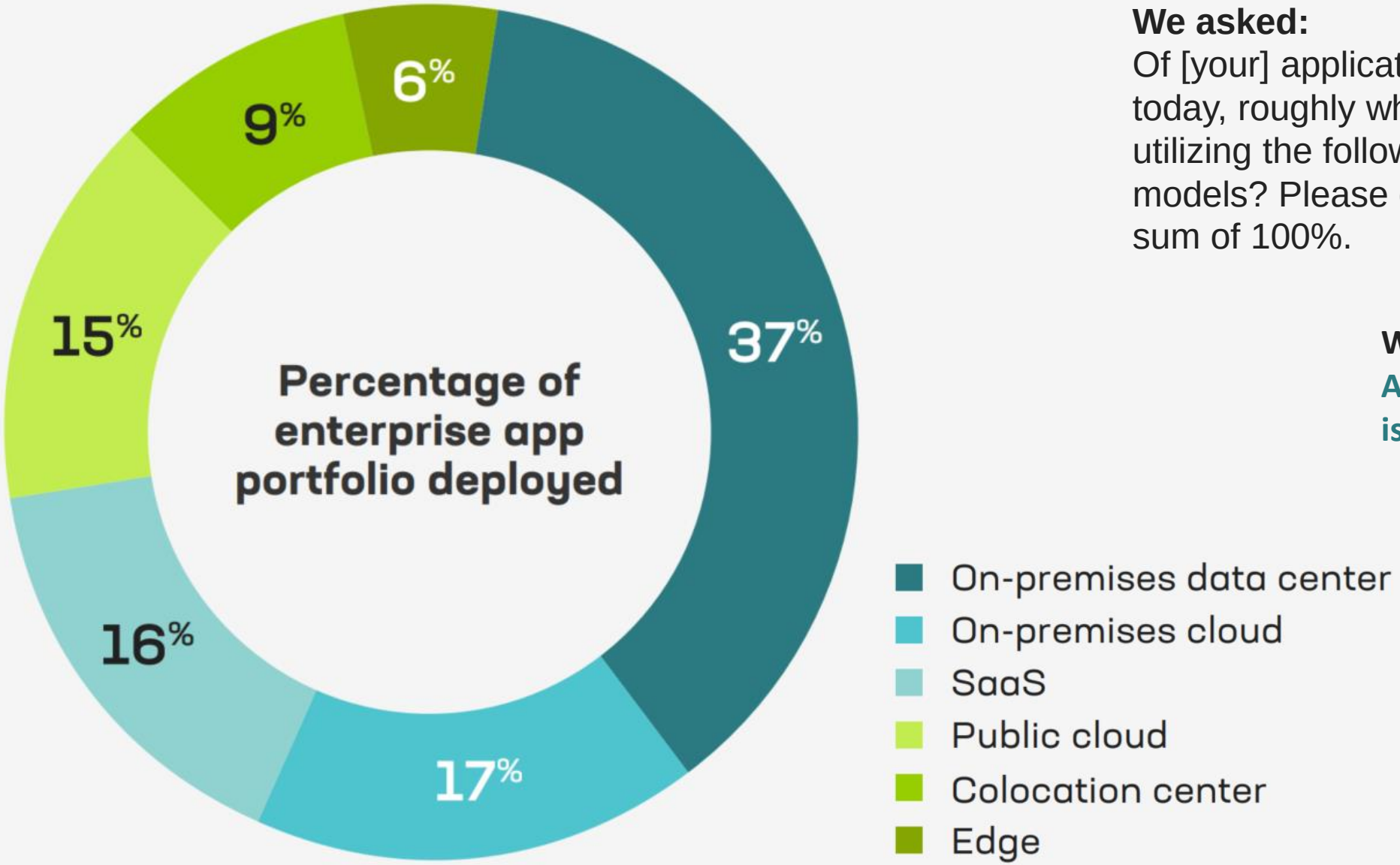
Modern App Architectures Continue Their Growth



We asked:
Of all your applications deployed today, roughly what percentage fit into the following categories? Please enter numbers for a sum of 100%.

We learned:
Modern app architectures are approaching half of the average portfolio.

Multi-Cloud Environments Will Endure

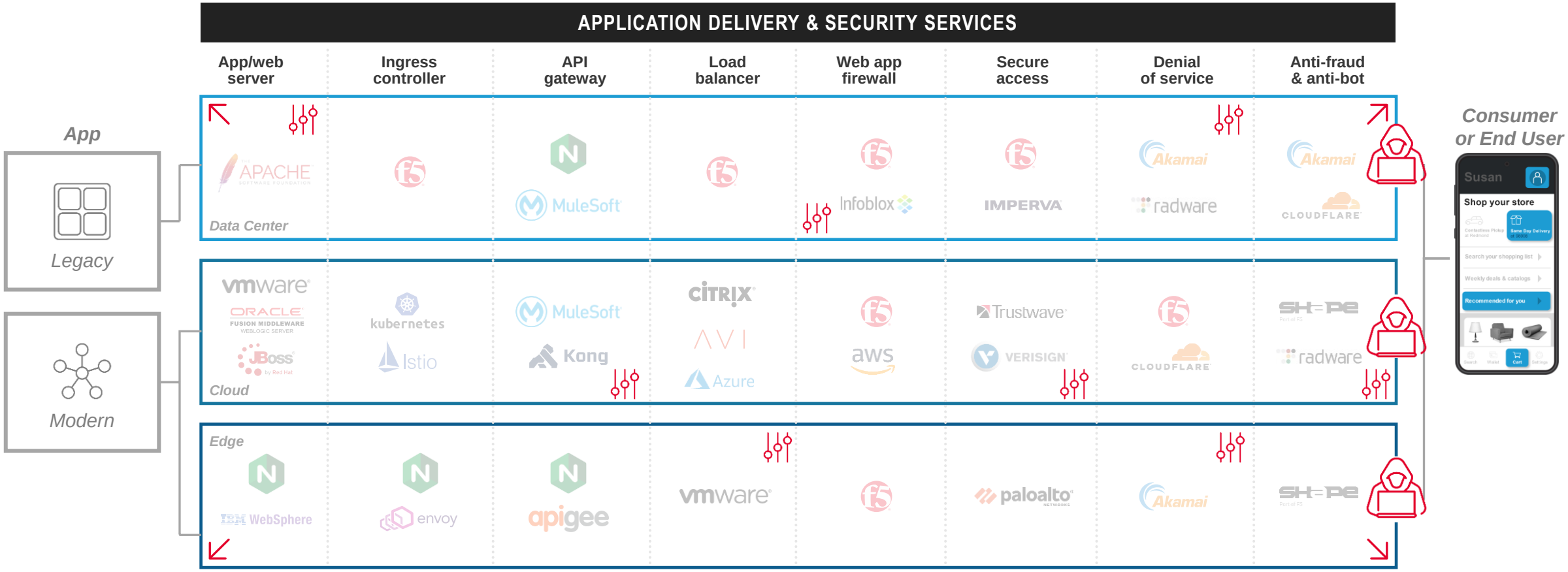


We asked:
Of [your] applications deployed today, roughly what percentage are utilizing the following deployment models? Please enter numbers for a sum of 100%.

We learned:
A diversity of app locations is the norm.

Behind these digital experiences, there is a complex, heterogenous, rigid system vulnerable to massive security breaches

Fragmented | Inconsistent | Difficult to scale | Trapped data | Vulnerable to attack

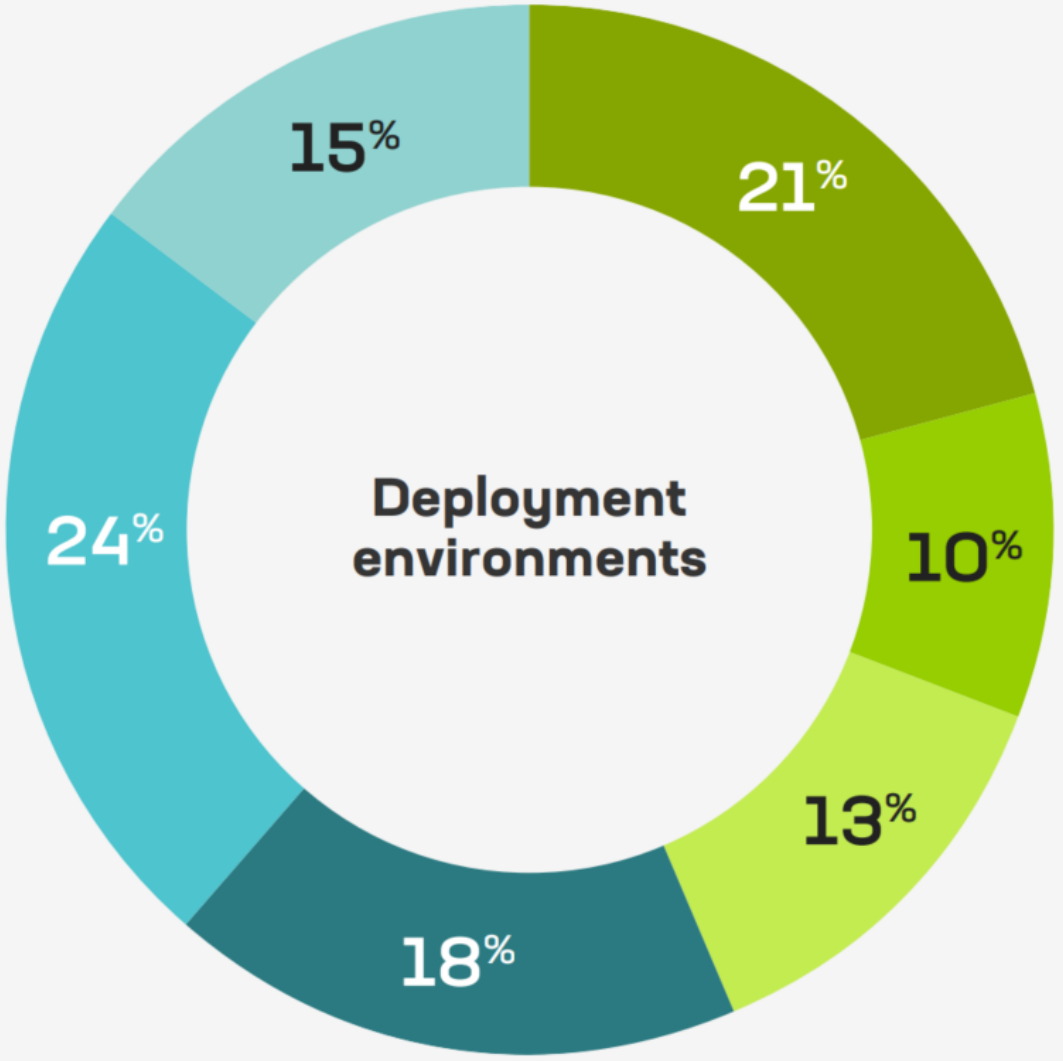


This graphic is illustrative and not meant to be an exhaustive list of all providers

Apps Are Widely Distributed

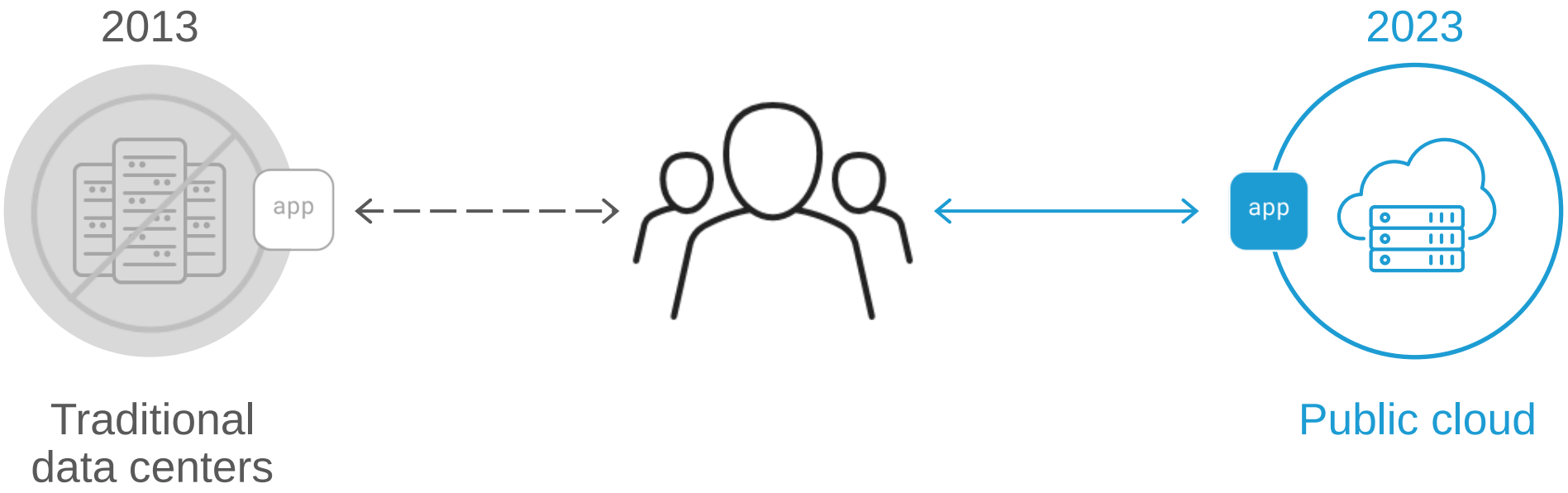
We asked:
What is the amount of the different environments that your organization is deploying applications in?

We learned:
Organizations have realized that there's simply no one environment that's best for them all.

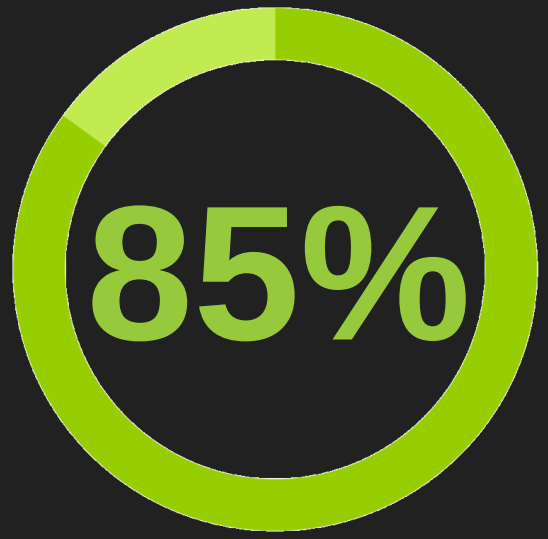


All Applications Moving to the Cloud?

Not very long ago, it was commonly assumed that in the "end state", all apps would be in the public cloud



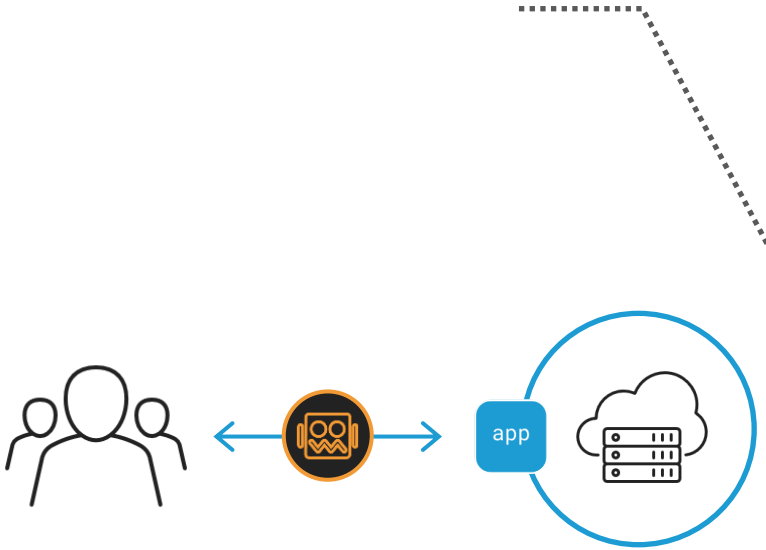
This is not what happened



IT Will Remain Hybrid Indefinitely

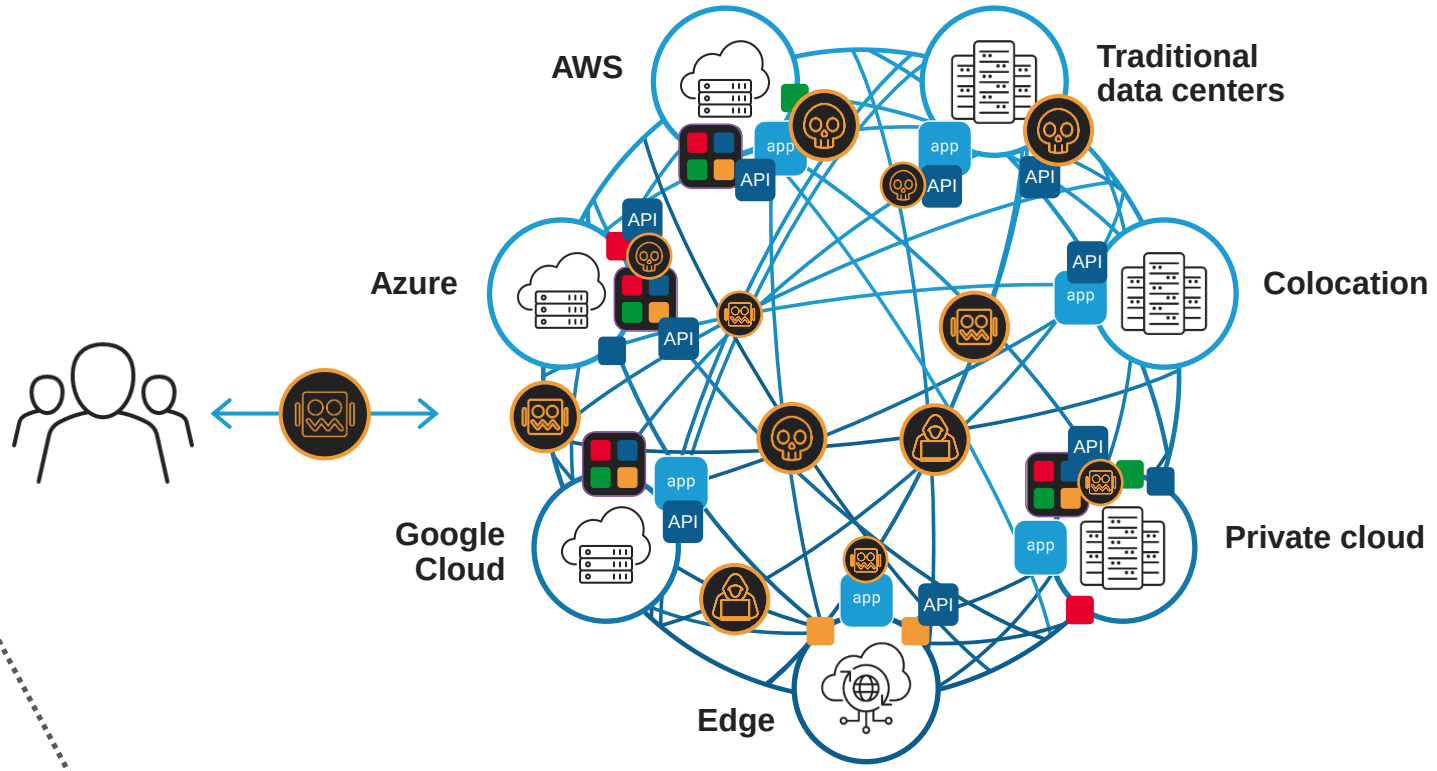
Of organizations operate multiple app architectures and locations

This is where we thought we would be...



app Traditional monolithic app

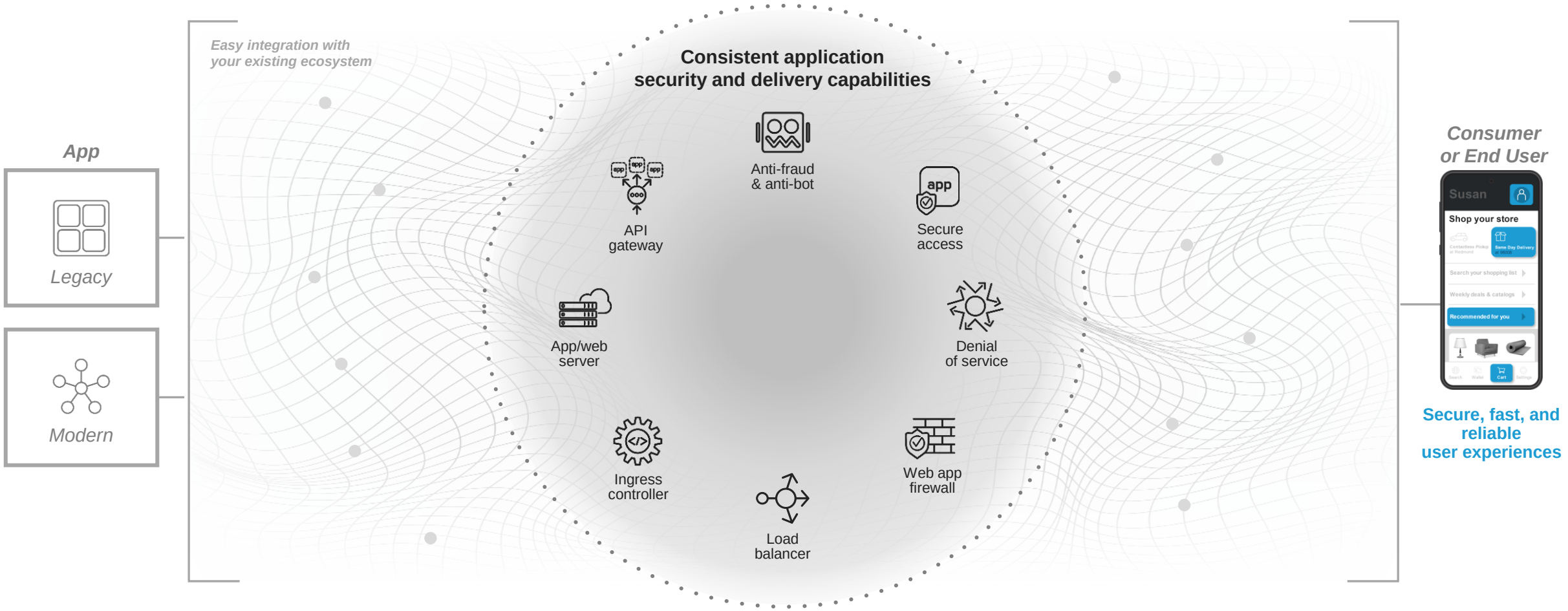
Modern cloud native app



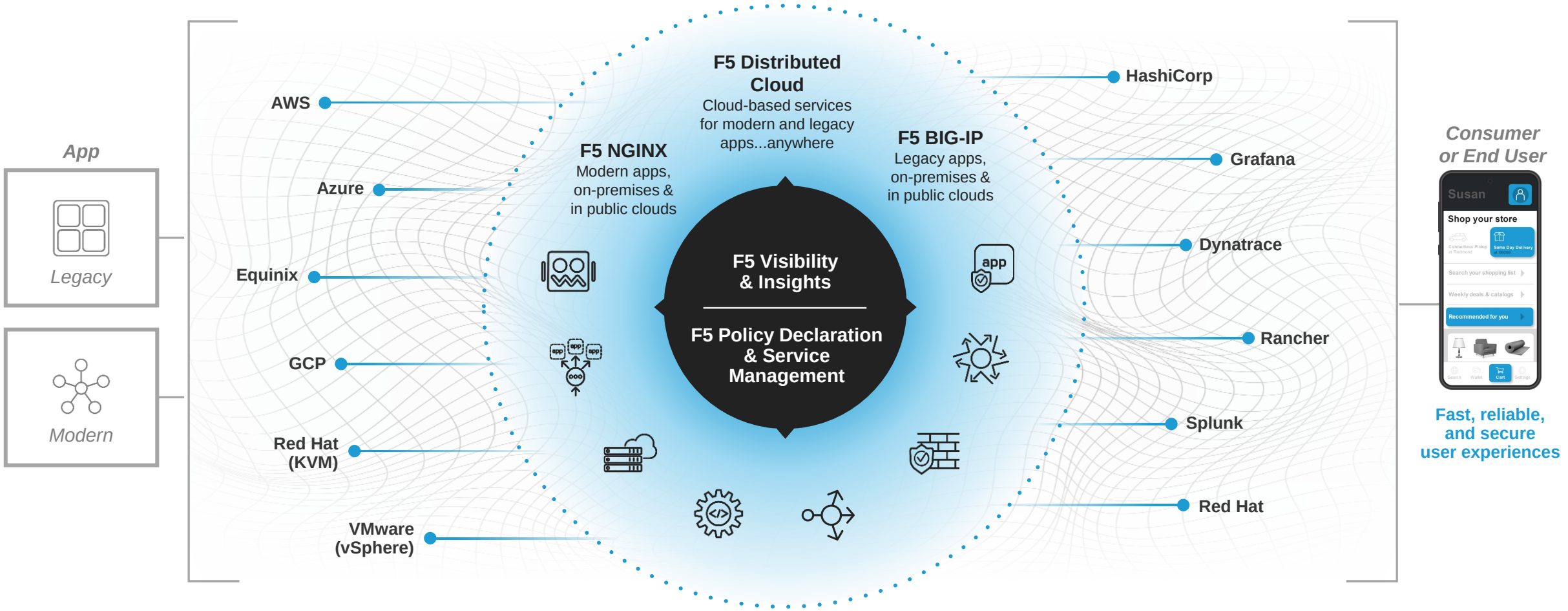
and this is where we have ended up

ALEF

A Distributed Cloud Architecture for app security and delivery increases an organization's ability to keep up with ever growing security needs, even as they modernize



F5's Architecture for app security and delivery provides a blueprint for enterprises to significantly heighten and maintain their security posture



This graphic is illustrative and not meant to be an exhaustive list of all providers

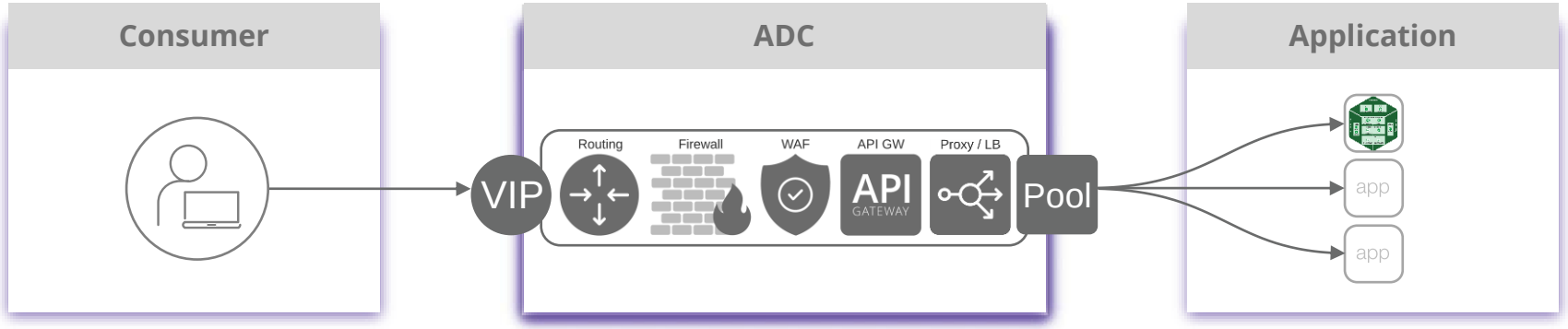
BIG-IP & NGINX – deployed close to the App…

DNS
- Business Continuity
- DNS Security / Services
- DNS Firewall
- GSLB

FW
- ACLs
- IPS
- IP Feed Lists
- IP Intelligence
- L4 BADoS – Dynamic Signatures

Acceleration
- TCP Optimisation
- Caching/Compression
- End User Experience
- HTTP/2, HTTP/3, QUIC

ADC
- Full Proxy
- TLS/SSL Offload / Visibility
- SLB
- Application Awareness
- Persistence
- Monitoring
- Deep Packet Modification
- Protocol Transformation



UAC
- Remote Access (SSL VPN, App Tunnel, VDI / Citrix, VMWare, MS RDP /, Portal Access)
- Pre-Authentication
- Multi-factor/SSO/Federation
- End Point Inspection
- API Security
- ADFS Proxy Replacement
- Cloud Federation
- SAML, OAuth, OpenID

WAF
- L7 Firewall
- Positive & Negative Security
- Advanced BOT Detection
- Brute Force Protection
- Form Encryption & Obfuscation
- Credential Stuffing
- Client Fingerprinting
- L7 BADoS Mitigation
- API Security
- PCI Compliance
- XML / JSON Firewall

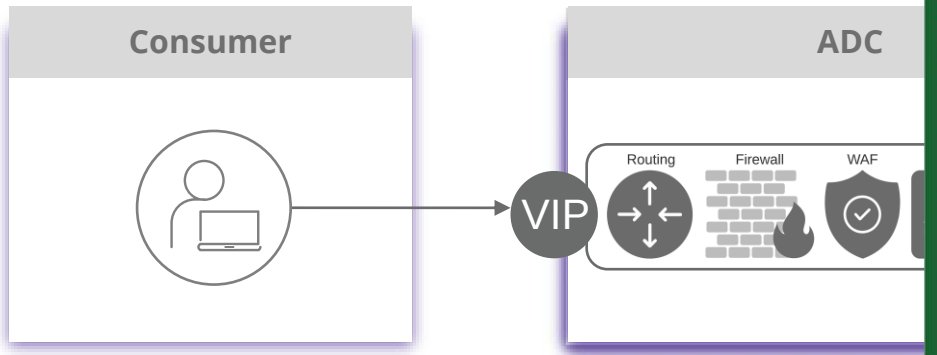
ALEF

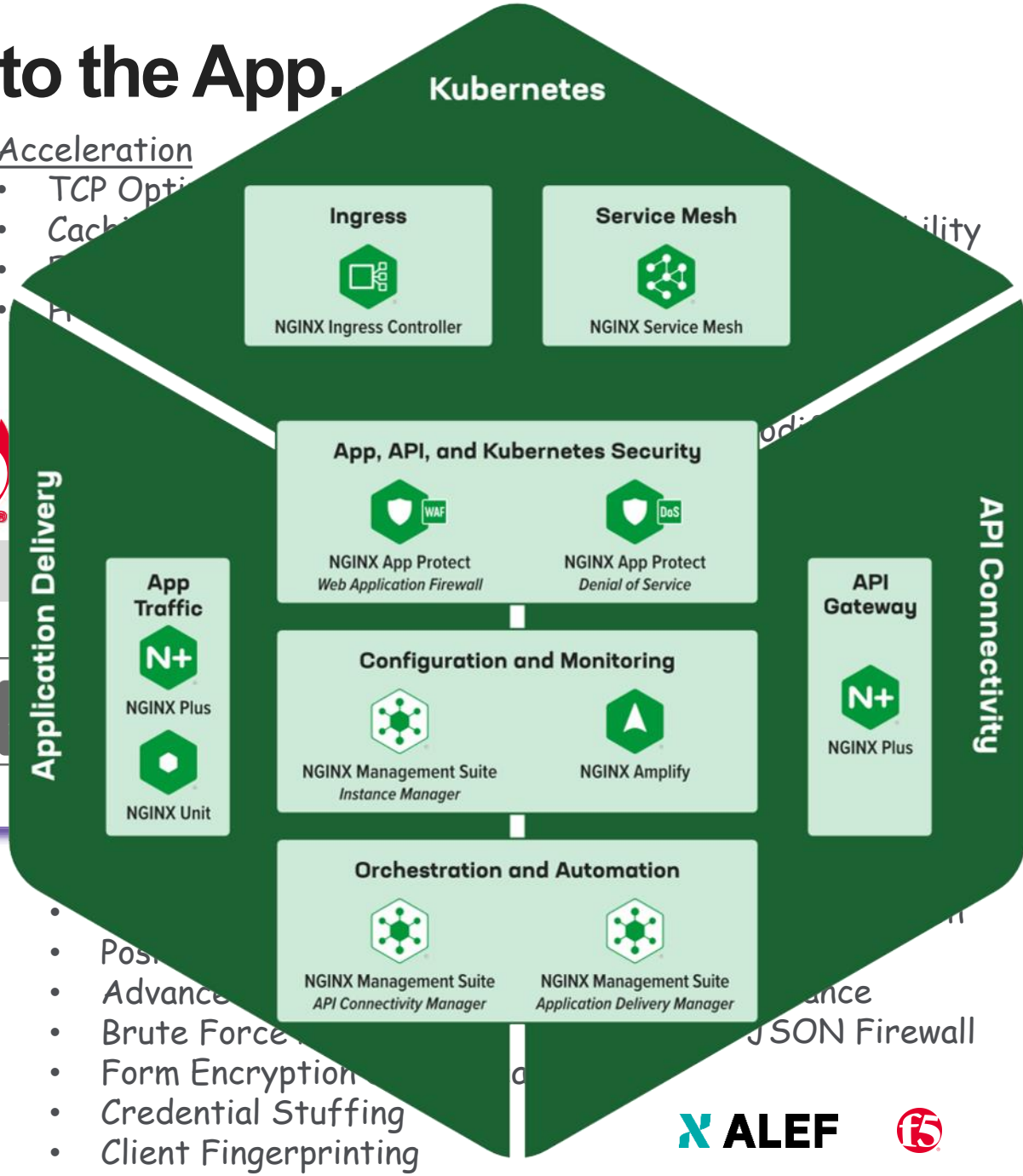
BIG-IP & NGINX – deployed close to the App.

DNS
- Business Continuity
- DNS Security / Services
- DNS Firewall
- GSLB

FW
- ACLs
- IPS
- IP Feed Lists
- IP Intelligence
- L4 BADoS – Dynamic Signatures

Acceleration
- TCP Opti
- Cach
-
-





UAC
- Remote Access (SSL VPN, App Tunnel, VDI / Citrix, VMWare, MS RDP /, Portal Access)
- Pre-Authentication
- Multi-factor/SSO/Federation
- End Point Inspection

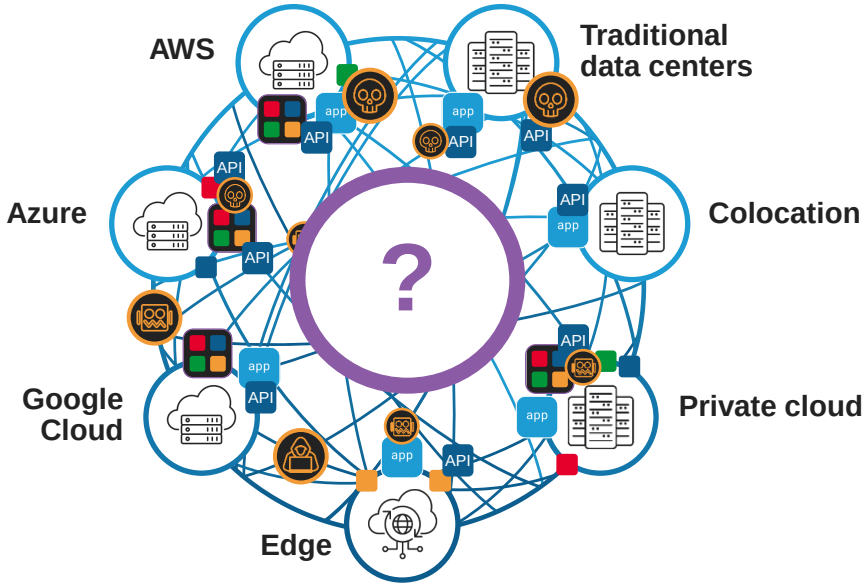
- API Security
- ADFS Proxy Replacement
- Cloud Federation
- SAML, OAuth, OpenID

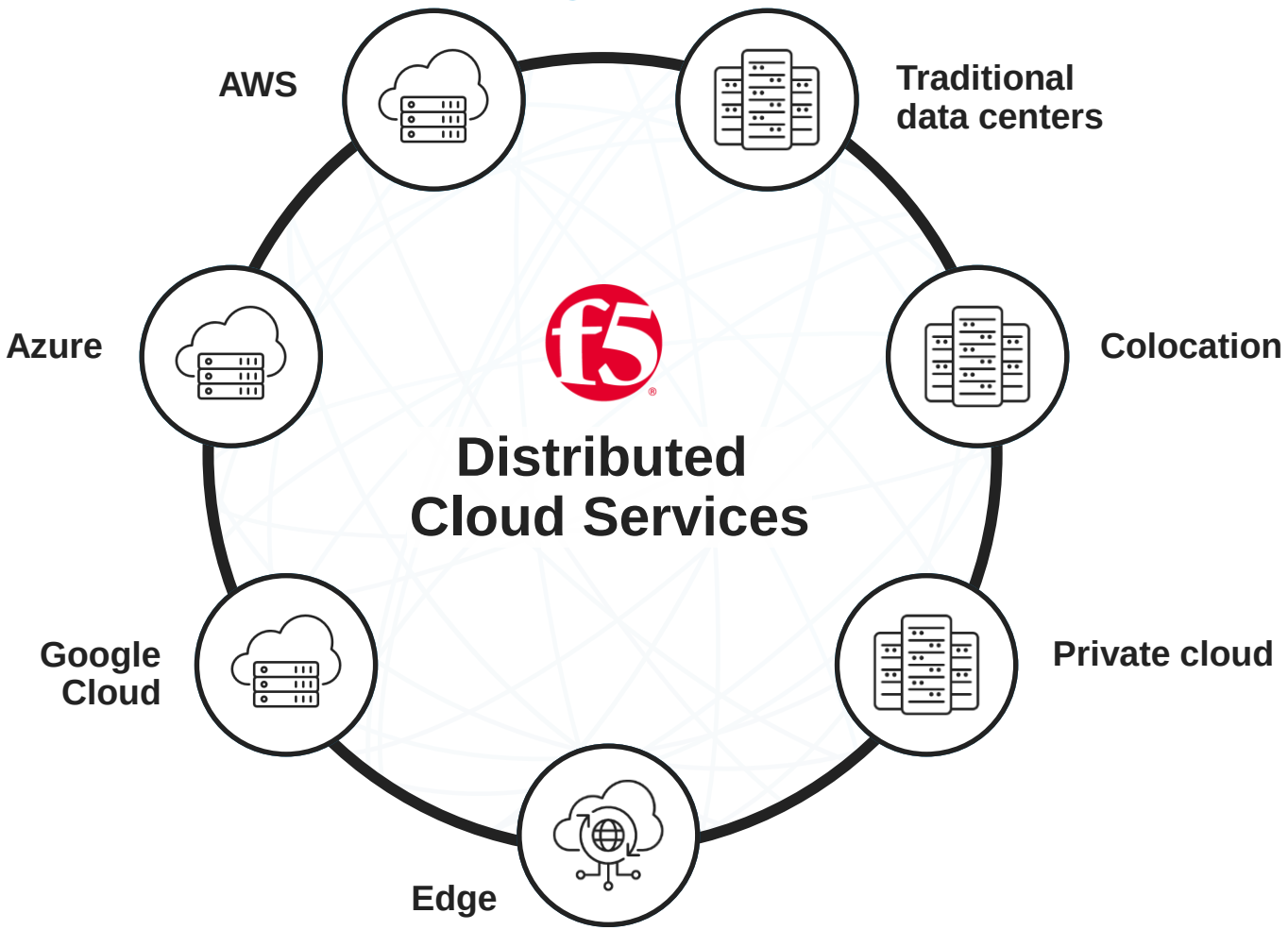
- Pos
- Advance
- Brute Force
- Form Encryption
- Credential Stuffing
- Client Fingerprinting

ility
ance
JSON Firewall

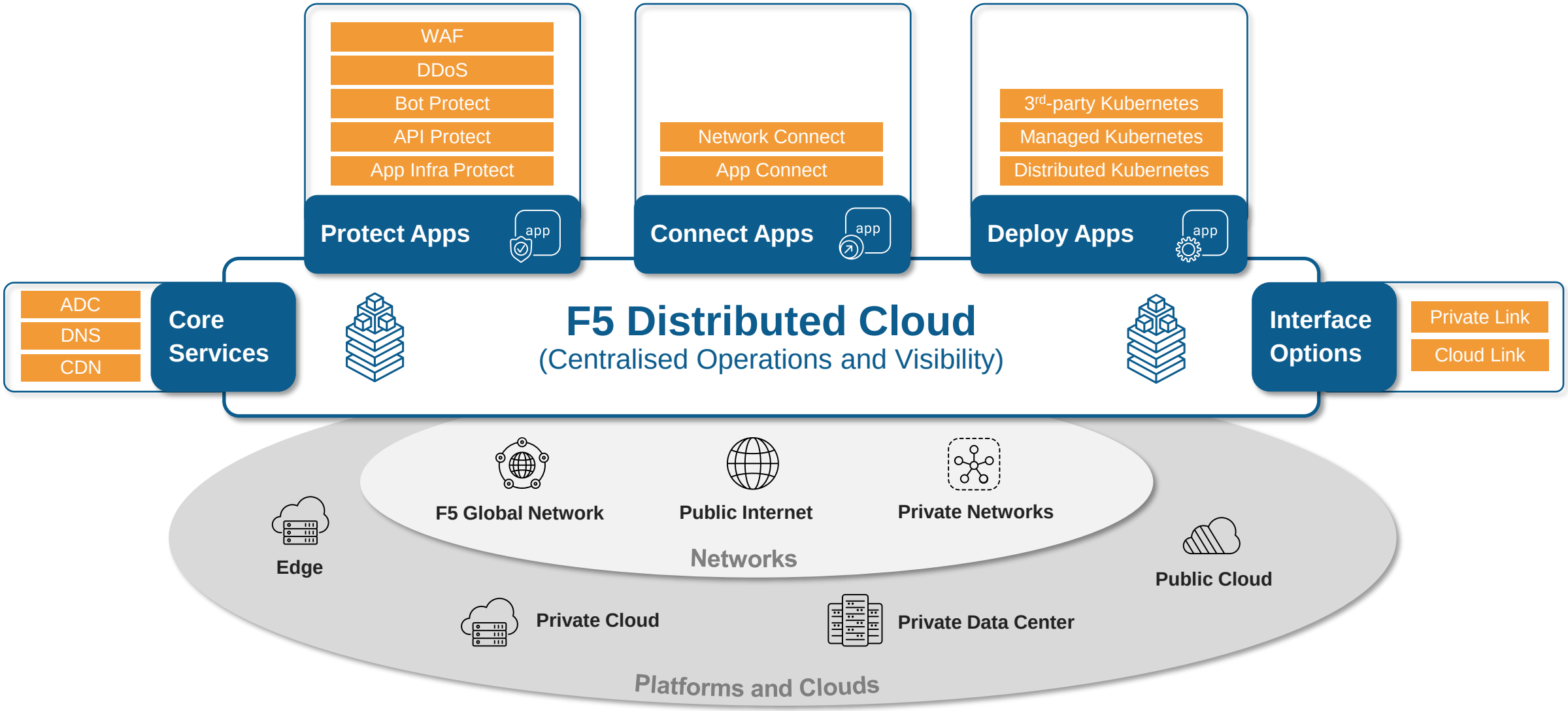
ALEF

Simplify Secure Connectivity across Public Cloud and Edge



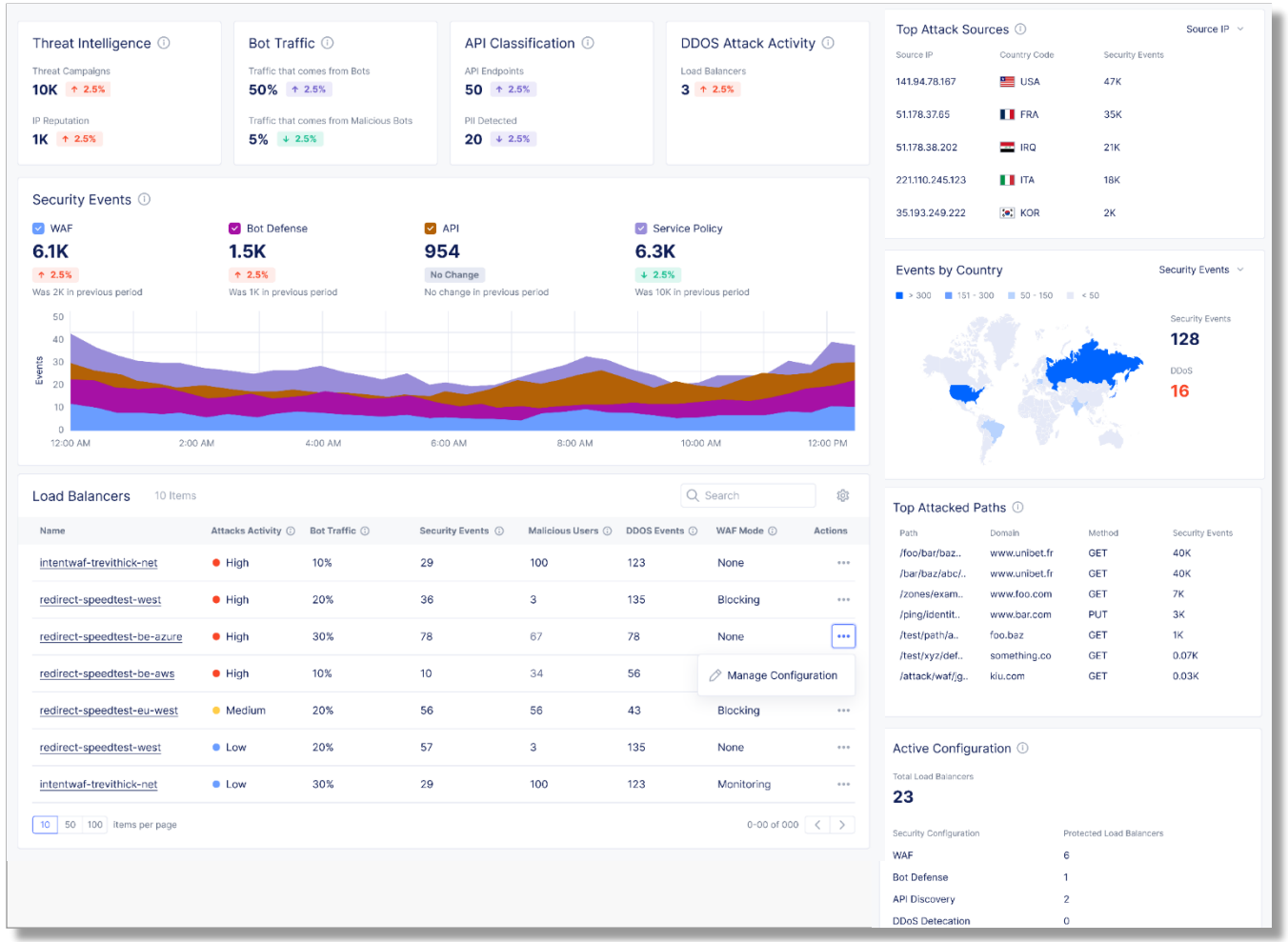


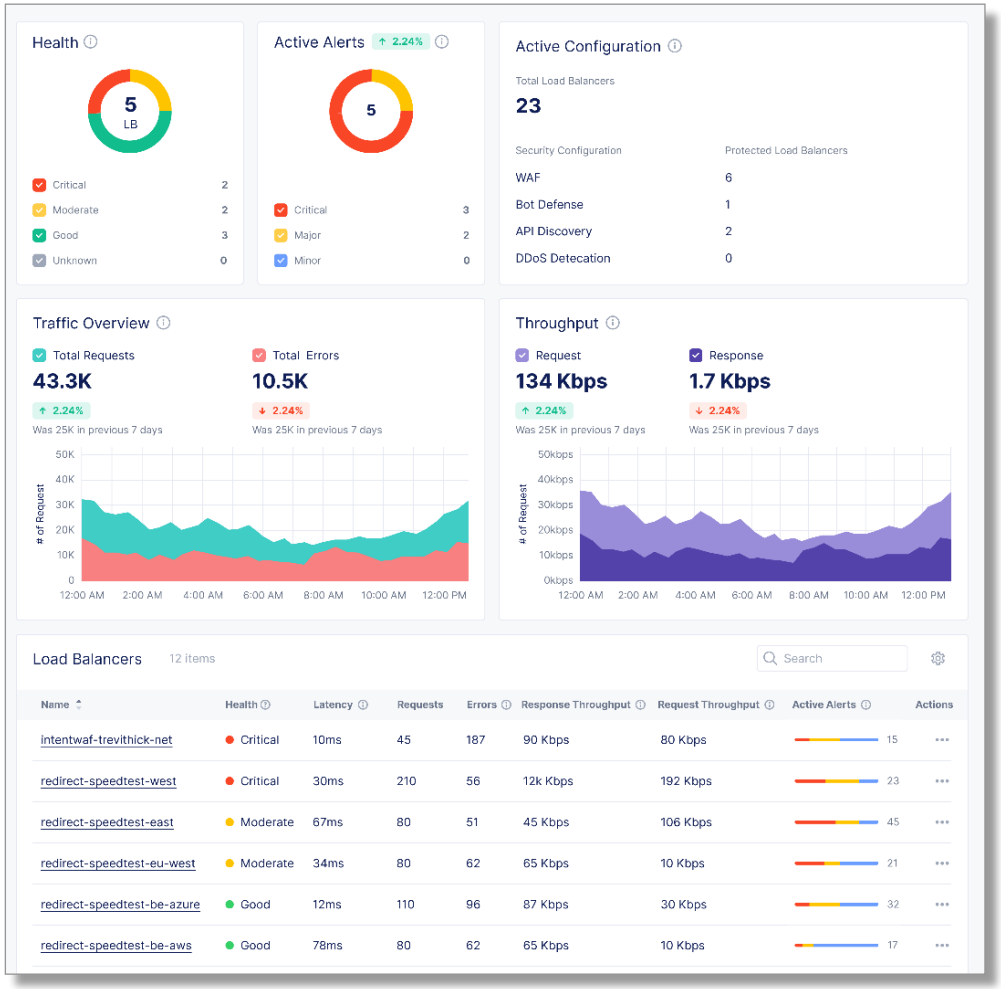
F5 Distributed Cloud – The Platform



Distributed Cloud – Multi-App Dashboards

Rich observability with 360-degree view of performance and security posture for all apps together





Security | **Performance**

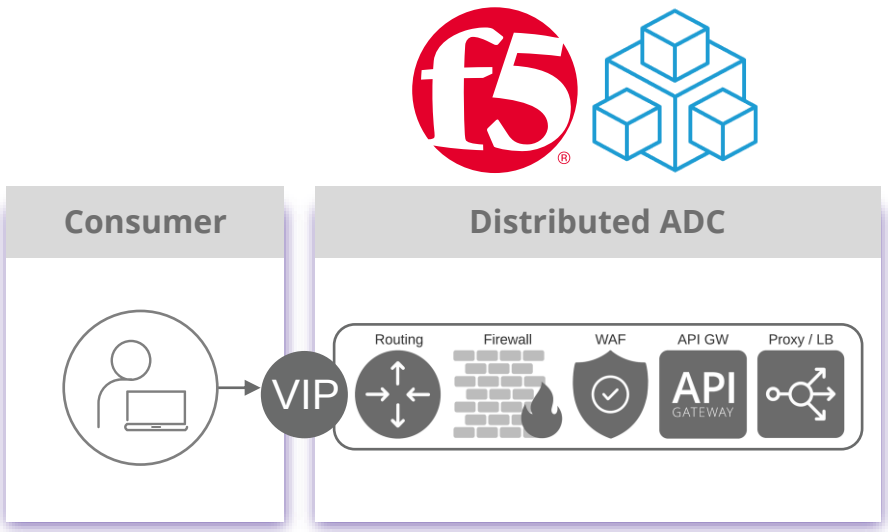
ALEF

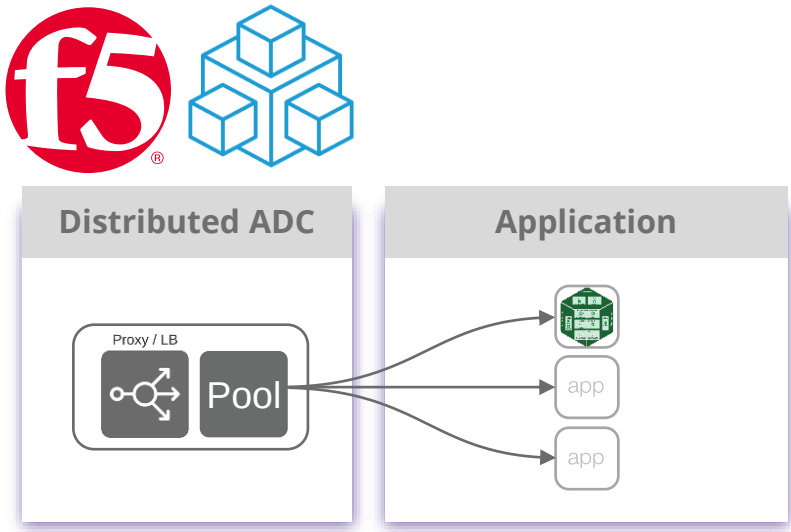
a force for platform & security

that shouts „GO GO GO”

more than „NO NO NO”.

Imagine if you could split your ADC in half…



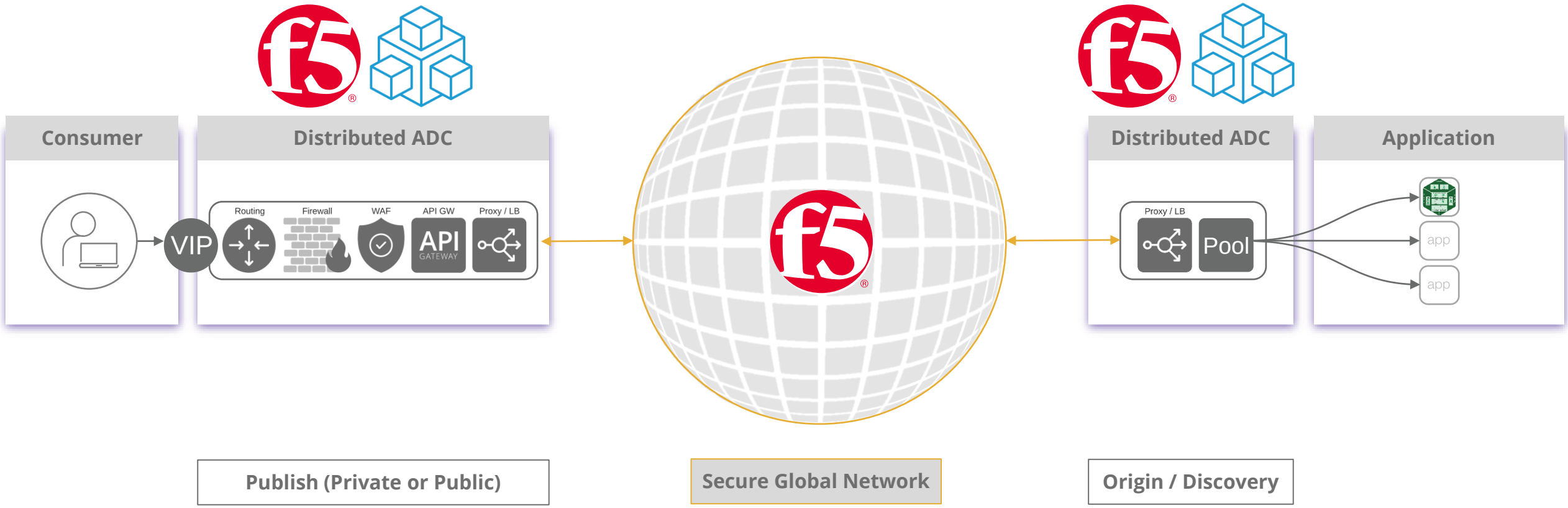


Publish (Private or Public)

Origin / Discovery

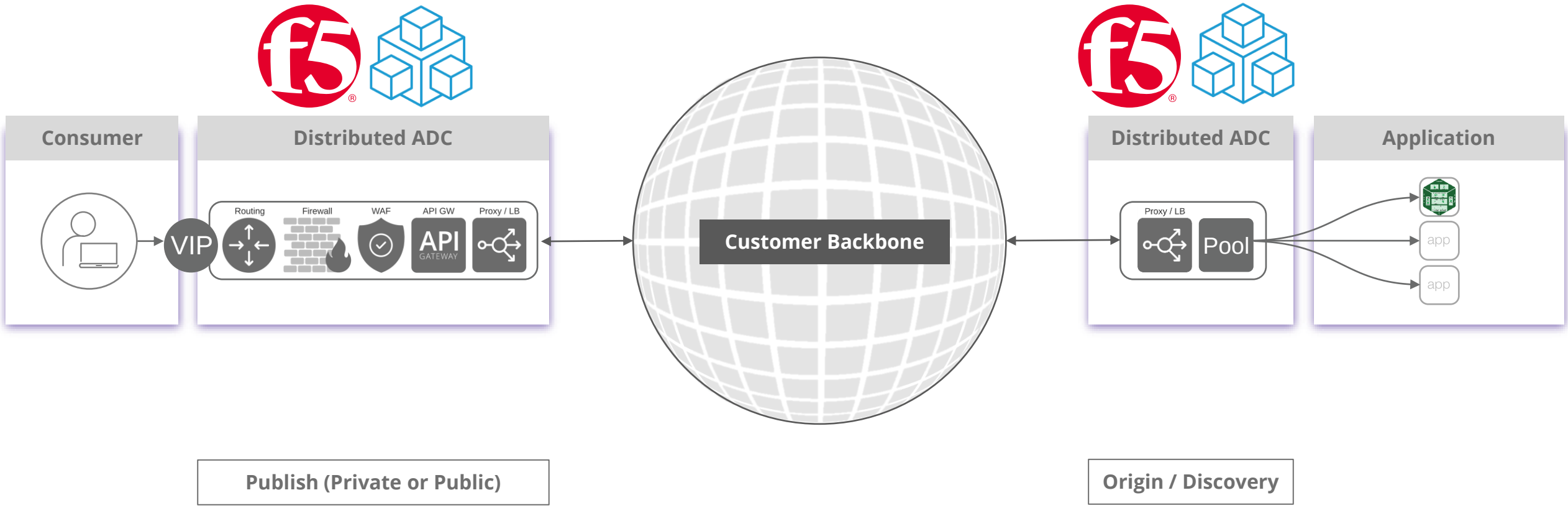
ALEF

and stretch it apart, across our Global Network…



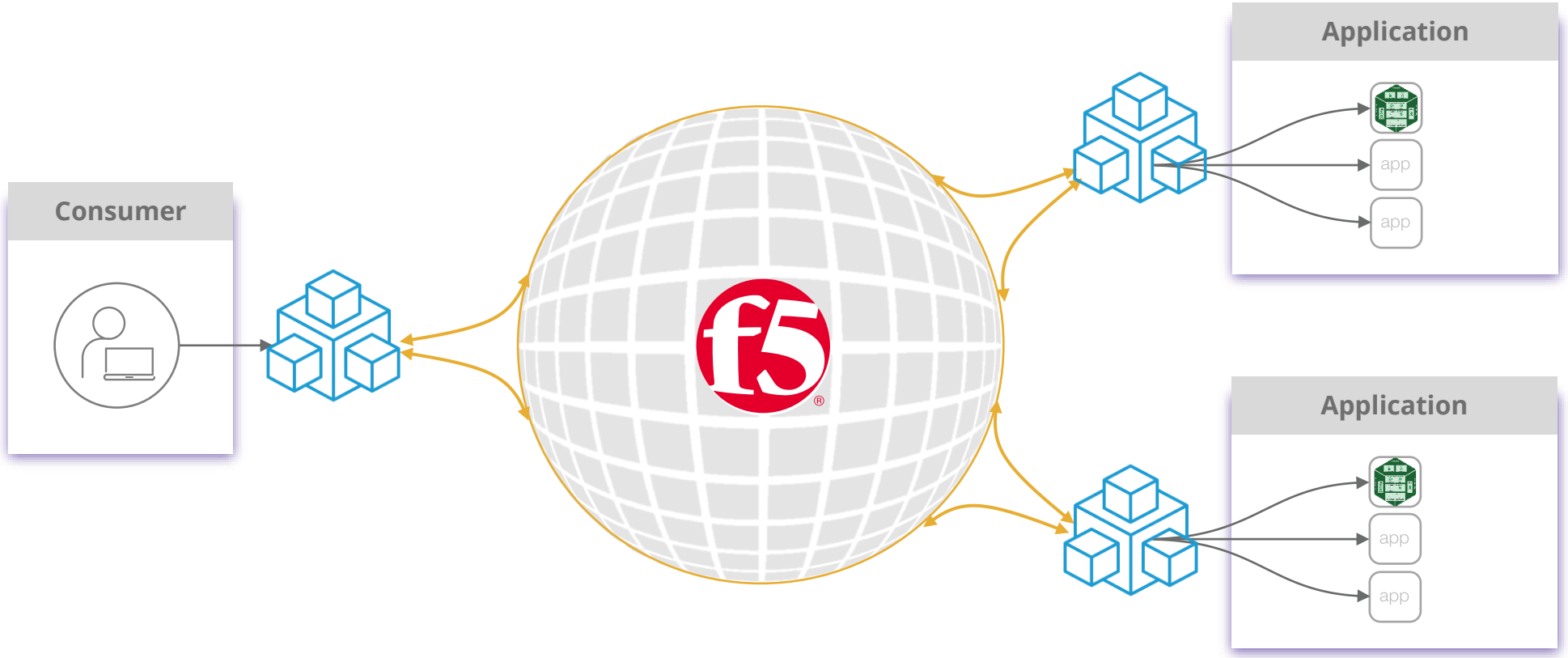
ALEF

...or across your own backbone…

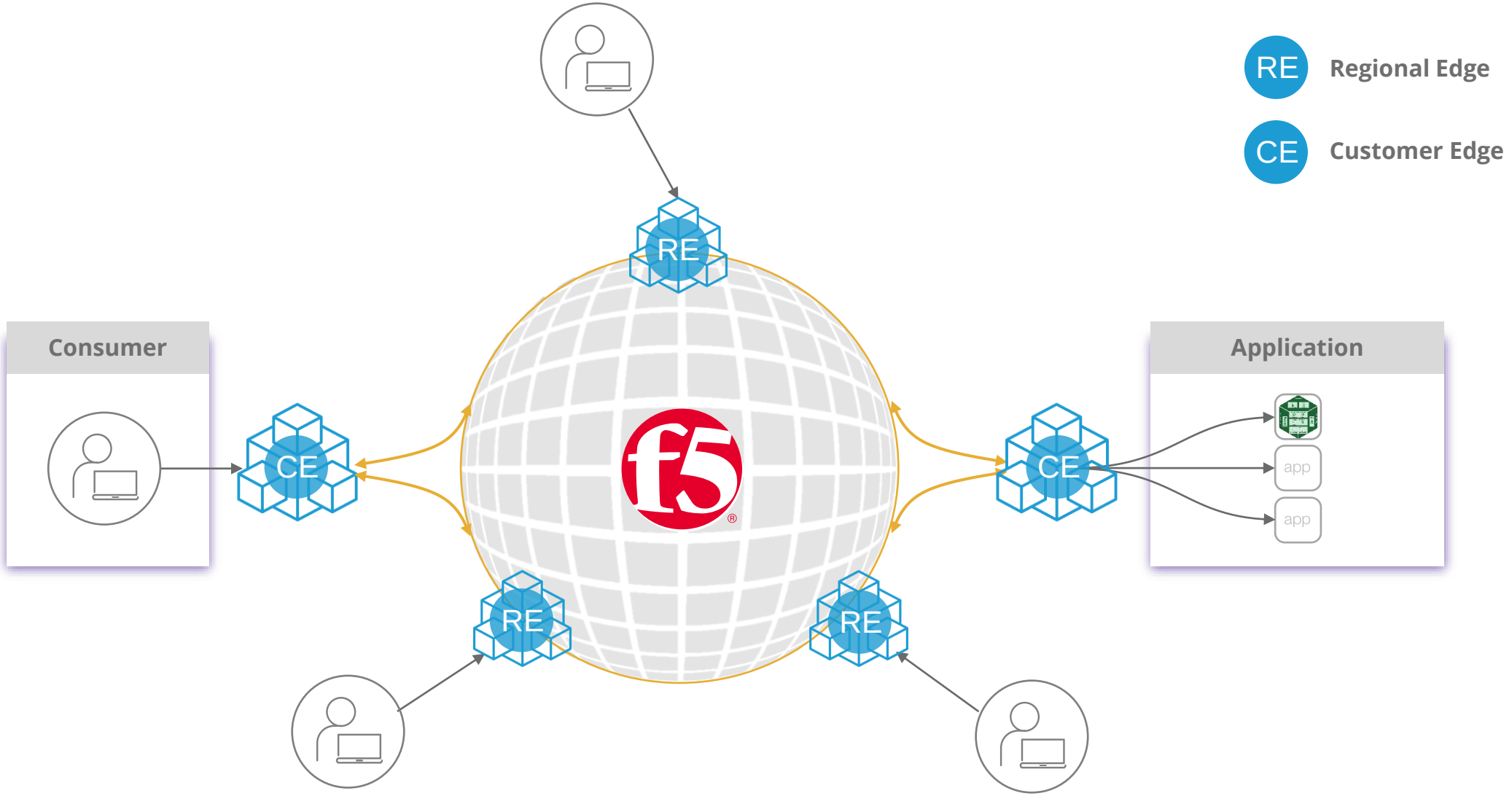


...we simply connect Locations…

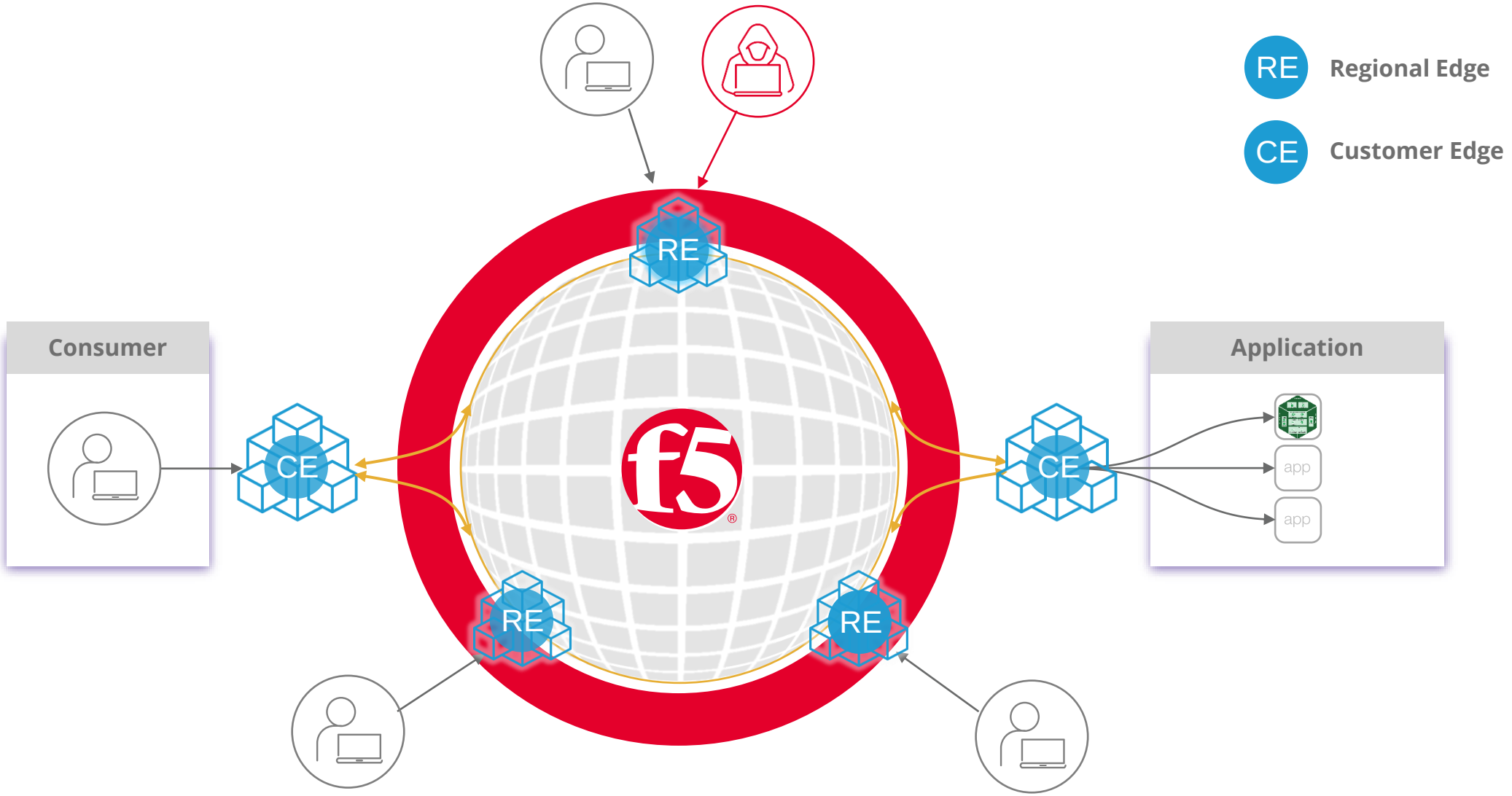
...we simply connect Locations…



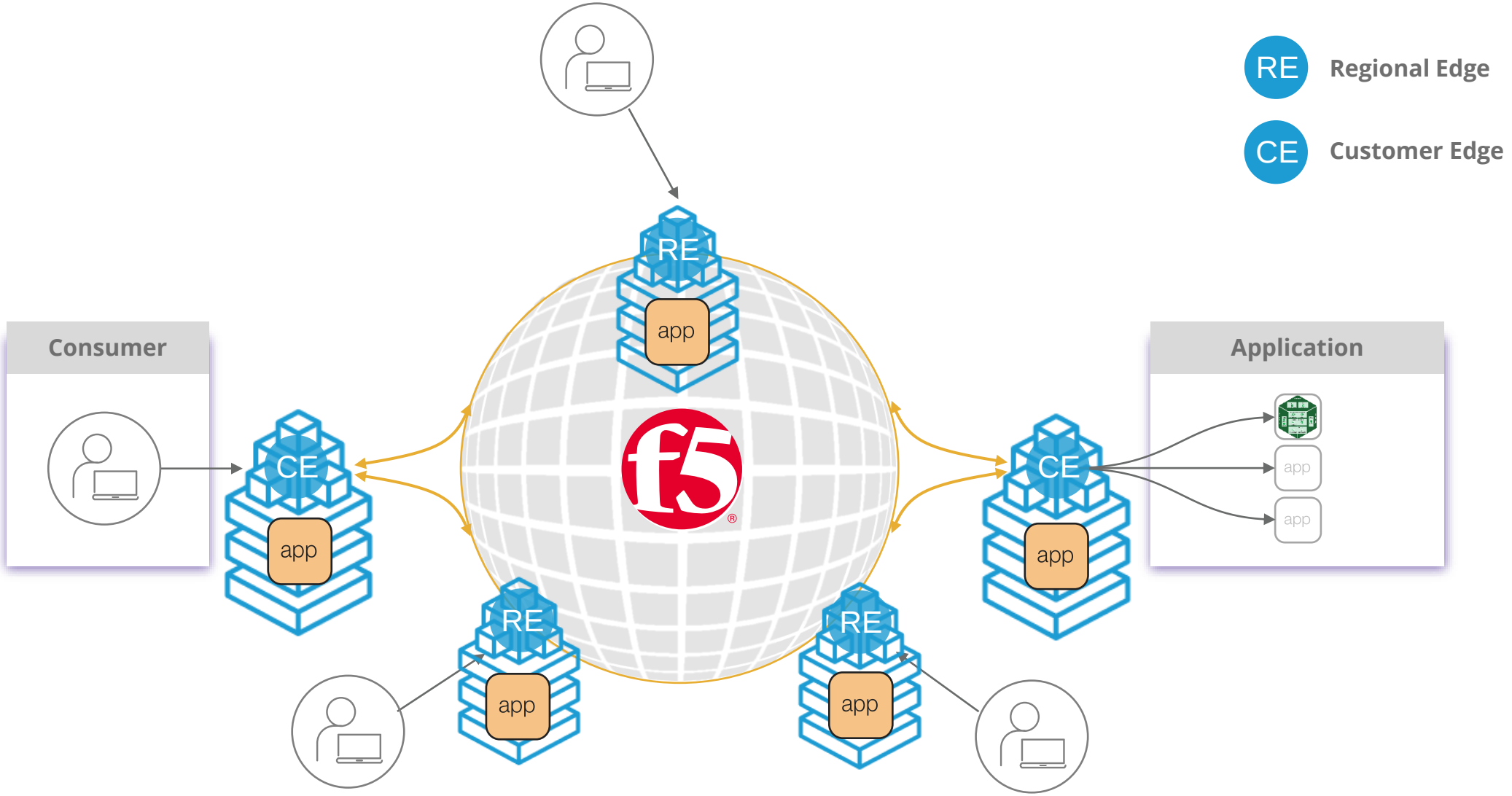
…and you can deploy your ADCs, onto our Infrastructure



…including the DDoS Protection of F5 Distributed Cloud



…and deploy pods into a distributed Virtual K8s



BIG-IP Advanced WAF

Flagship WAF offering, full set of application security capabilities including, credential protections, DevOps and security Automation, Threat Campaigns, layer 7 DoS protection and anti-bot protection.

KEY ABILITIES

- Advanced WAF security
- Layer 7 DoS mitigation
- Credential protection
- DevOps and Security Automation
- Integrated LTM for monitoring and improved performance
- API security
- Bot defenses

PORTFOLIO DIFFERENTIATION

- GraphQL support
- Declarative APIs for “shift left”
- Self-configured solution available as hardware and VE.
- Delivers the highest possible security value and the largest number of use cases
- Includes basic LTM capabilities
- Can be installed on-premises or as a virtual machine in public clouds (AWS, Azure, Google)

BIG-IP Advanced WAF | NGINX App Protect WAF | Silverline Managed WAF | F5 Distributed Cloud WAAP

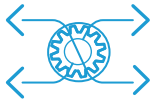
Security with BIG-IP Advanced WAF

Common WAF security

Layer 7 DoS mitigation

Credential protection

API security



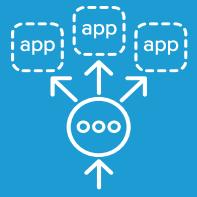
DevOps and Security Automation

Integrated LTM

Threat Campaigns

Leaked Credential Protection

Bot defenses



NGINX App Protect WAF

Dynamic Security module for the NGINX platform, designed for modern enterprise environments enabling security integration into DevOps deployment lifecycle.

KEY ABILITIES

- Light weight stand-alone security solution for cloud and microservices
- Modern application protection
- Low touch self-managed
- Can be easily scaled out automatically
- Simple integration into CI/CD tool chain

PORTFOLIO DIFFERENTIATION

- Self-managed, lightweight, for cloud and containers
- Native to Kubernetes Ingress controller
- Supports per pod / per service proxy in the Kubernetes clusters
- 10x in performance (RPS, MB)
- Superior security efficacy and efficiency
- Native to NGINX Ingress Controller
- Manage security as a code

BIG-IP Advanced WAF | **NGINX App Protect WAF** | Silverline Managed WAF | F5 Distributed Cloud WAAP

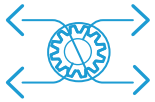
Security with NGINX App Protect WAF

Common WAF security

Layer 7 DoS mitigation

Credential protection

API security



DevOps and Security Automation

Integrated LTM

Threat Campaigns

Leaked Credential Protection

Bot defenses

Silverline Managed WAF

F5's premier cloud-delivered managed WAF. Turn-key customer solution that is fully managed and supported by the security experts in the F5 SOC. Threat Intelligence and security-based iRule support.

KEY ABILITIES

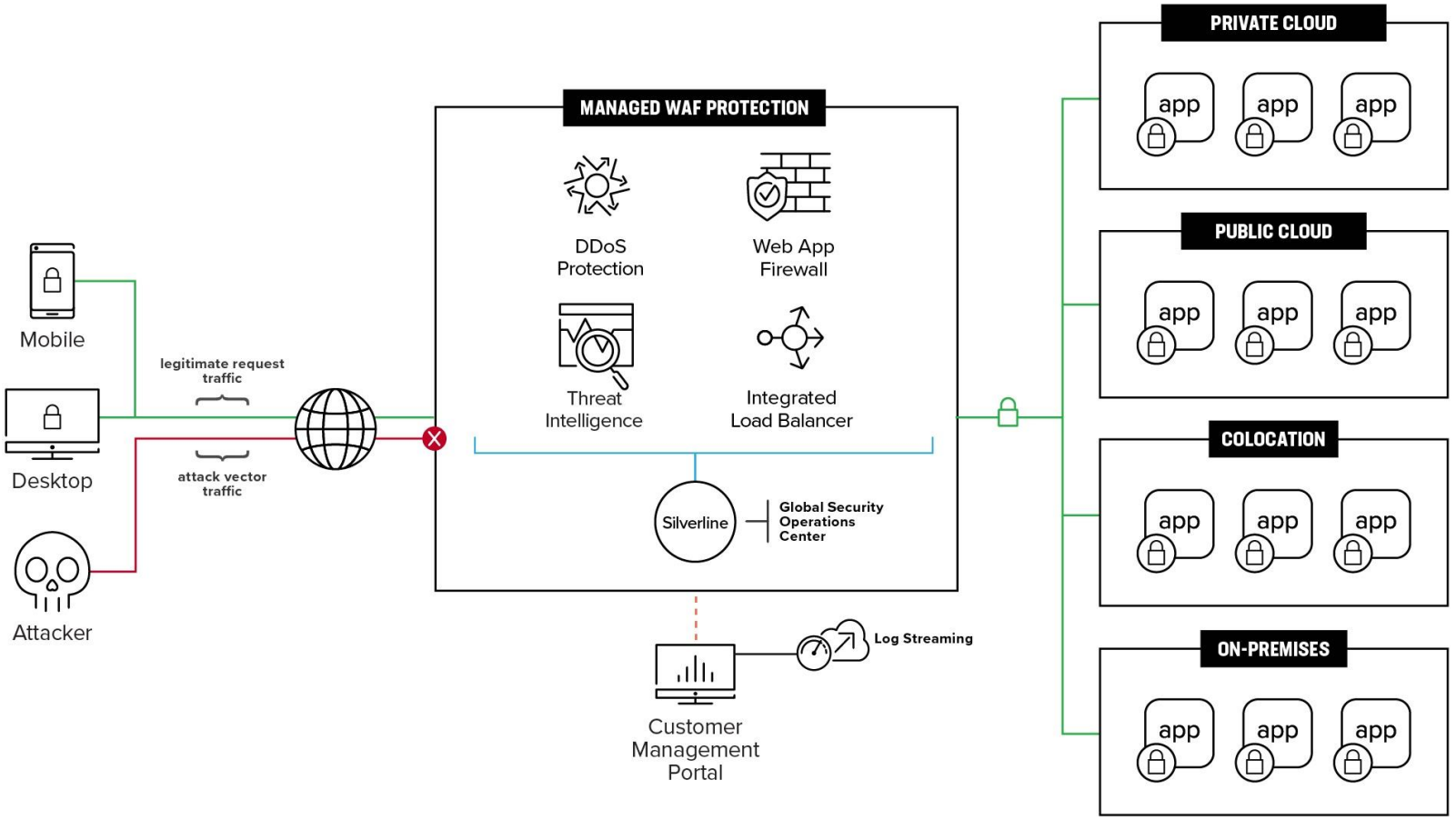
- L7 DoS protection
- App security and compliance
- Subscription pricing with SLAs
- Ability to import and export existing ASM policies
- Proactive bot defense

PORTFOLIO DIFFERENTIATION

- Built on BIG-IP Advanced WAF technology
- Cloud-delivered service/Multi-cloud
- Managed by F5 SOC augmenting current IT staff
- WAF experts at your service, 24x7
- Integrated portal for DDoS protect, WAF, anti-bot
- Gartner emphasis on Silverline as one of the few WAAP services offering a positive security model

BIG-IP Advanced WAF | NGINX App Protect WAF | **Silverline Managed WAF** | F5 Distributed Cloud WAAP

Security with Silverline Managed WAF



- Attack insights and intelligence
- Virtual Patching
- Operational and cost efficiencies
- WAF experts available 24x7

F5 Silverline Web App Firewall: Use Cases

L7 DDoS Protection

Stop bad actors consuming resources and impacting application performance. Mitigations that adapt to user interactions.

Limit Sensitive Data Exposure

Limit the inadvertent exposure of sensitive information to scanners about the make-up and functionality of your application infrastructure

Reduce Data Exfiltration

Prevent criminals extracting data and code from your web applications via SQL injection or other OWASP threats

Prevent Application Misuse

Secure your digital transformation by only allowing your applications to be used as intend to optimize brand reputation

Mitigate Business Logic Attacks

Maximize business uptime by removing fraud, IP theft, and functionality abuse such as parameter tampering

Vulnerability Management

Ensure your application estate is virtually patched against exploits and vulnerabilities detect by 3rd party DAST tools

F5 Distributed Cloud WAAP

Take the complexity out of securing application across any cloud using a "click-to-enable", fast, and scalable application protection service built on a cloud-native, software as a service (SaaS) platform.

KEY ABILITIES

- Portal and API driven self-service
- Deploy anywhere closer to the app
  - F5 Distributed Cloud Edge Global Network
  - All major public clouds
  - Extend the solution to customer edge locations
- Easy to deploy and maintain
- Signature and behavioral (AI/ML) powered WAF protection
- Advanced Bot Defense with Shape
- API security with automated discovery and policy management
- Layer 3-7 DDoS mitigation

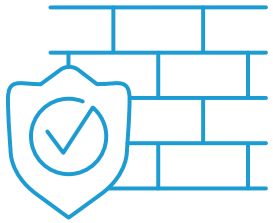
PORTFOLIO DIFFERENTIATION

- Best of breed Web application and API protection (WAAP) as-a-service offering
- SaaS based solutions that is easy to deploy and maintain
- End-to-end observability and policy management of app networking and security
- Purpose built for multi-cloud deployments and microservices
- Increases agility and collaboration across teams and reduces operation complexity and costs
- Lower TCO through false positive suppression via AI/ML
- Plans for Individual, Teams and Enterprises

BIG-IP Advanced WAF | NGINX App Protect WAF | Silverline Managed WAF | **F5 Distributed Cloud WAAP**

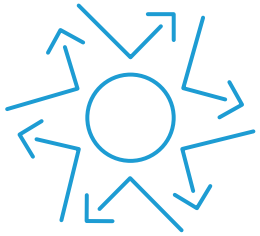
F5 Distributed Cloud WAAP

Take the complexity out of securing application across any cloud using a “click-to-enable”, fast, and scalable application protection service built on a cloud-native, software as a service (SaaS) platform.



Web Application Firewall

Core technology from F5 Advanced WAF
AI technology from F5
AI technology from Volterra
Threat Campaigns from F5 Labs



DDoS Protection

Layer 3/4 volumetric protection
Layer 7 DDoS protection
Global network
Anycast support

Advanced Bot Protection

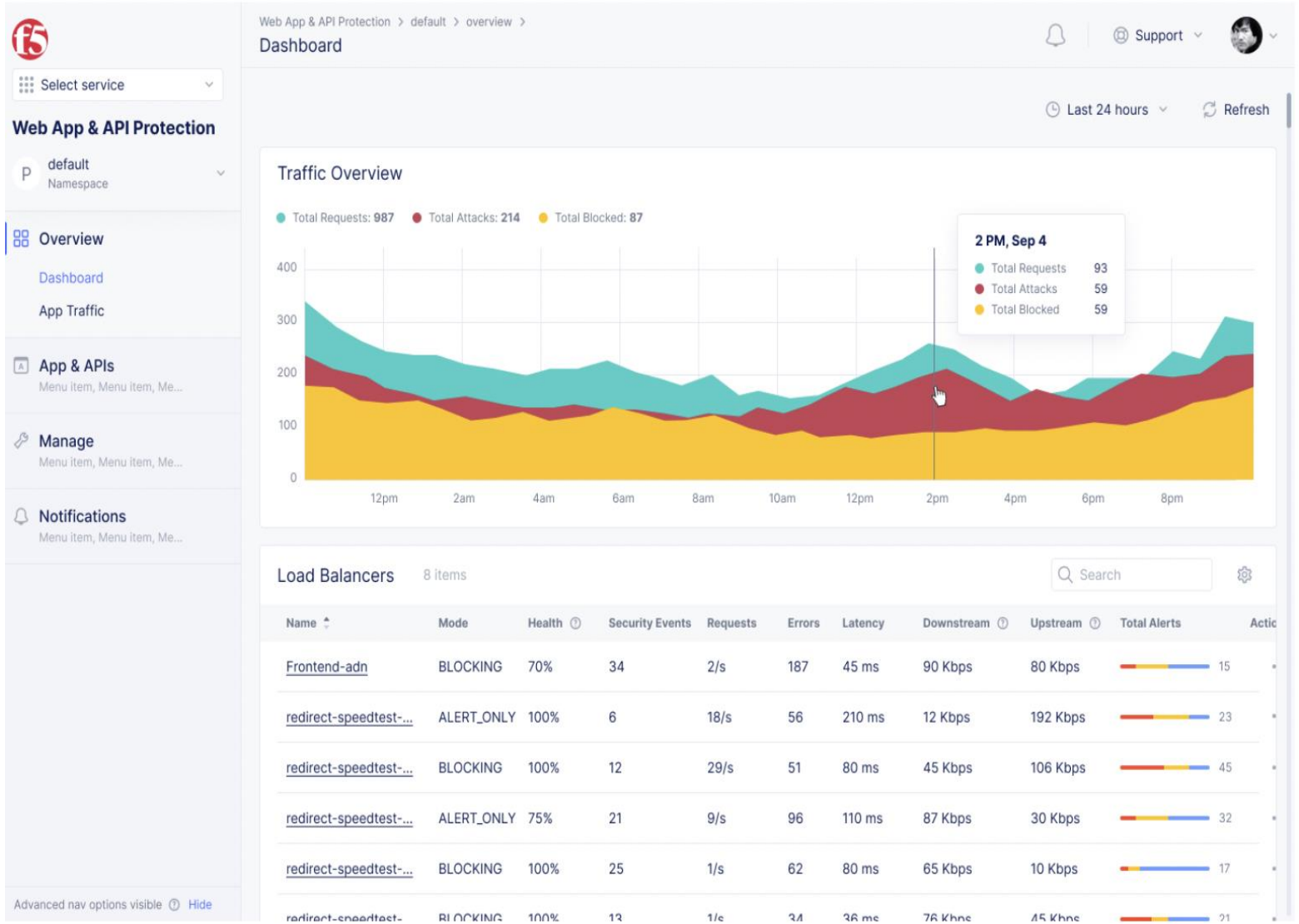
Class-leading bot protection from Shape

Consistent UX with other Shape bot offerings

API Protection

Automatically discovers APIs
Automatically allow good APIs
Identifies malicious users
Rich reporting framework

Security with F5 Distributed Cloud WAAP



- SaaS
- WAAP Protection
- Bot Defense
- Risk and address compliance

F5 WAF Solutions

	Self-Managed (User Deployed)	Self-Managed (Software-as-a-service)	Fully Managed w SOC (on-demand analyst response)
Proactive Defense Real-time security analysis and monitoring including custom policy management			
Specialized Controls Advanced fraud and highly specialized techniques targeted at specific organization(s)	F5 Distributed Cloud Bot Defense	F5 Distributed Cloud WAAP	Silverline Shape Defense + WAF
Tailored Controls Targeted attacks and advanced threat actors (includes fundamentals)	BIG-IP Advanced WAF NGINX App Protect WAF		
Fundamental Controls Software vulnerabilities and common attack vectors (e.g., long-tail apps)		F5 Distributed Cloud Bot Defense	
	Traditional Apps / Modern Apps		

Integrates core of Adv WAF into Volterra delivering it in a SaaS consumption model

F5 Application Protection

Secures against the broadest array of threats