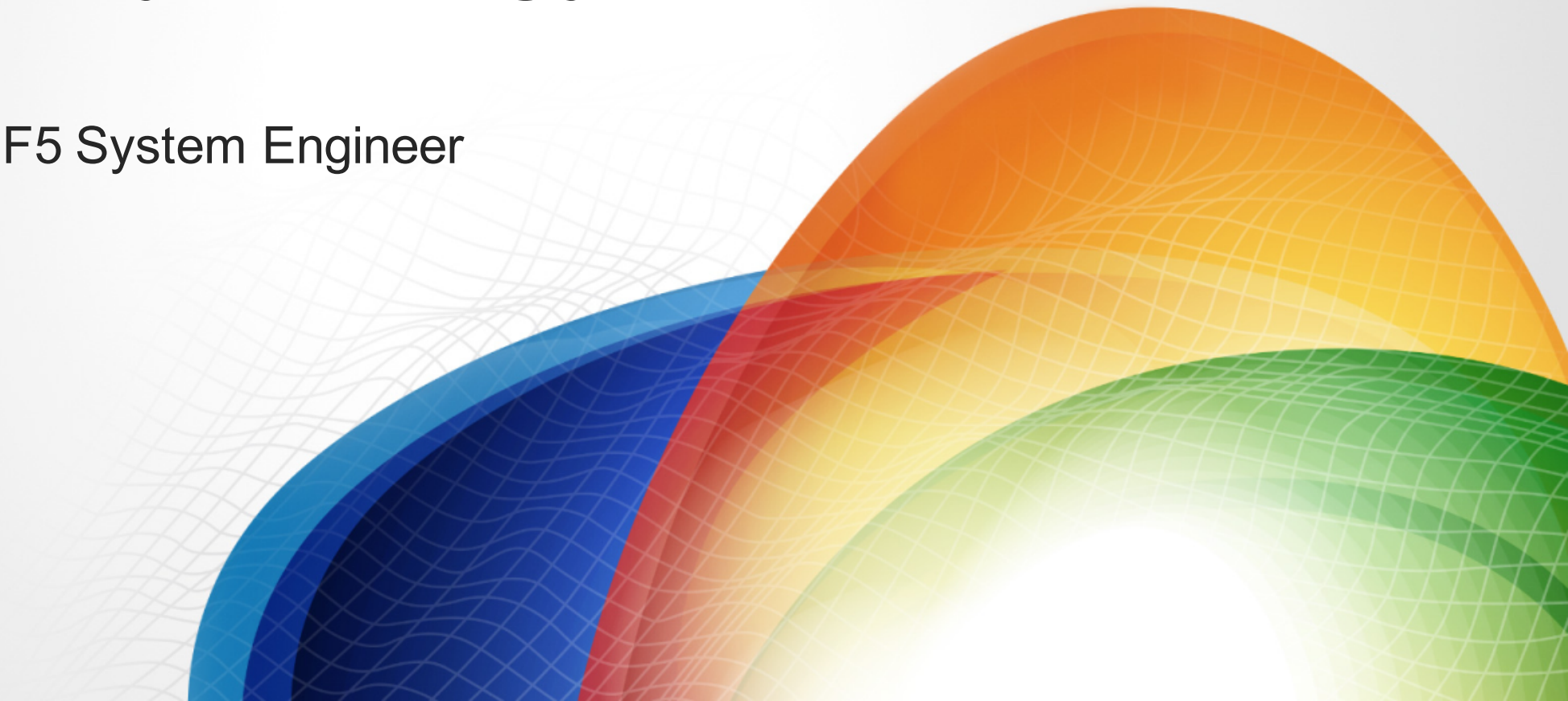




F5 Security Strategy

Luboš Klokner, F5 System Engineer

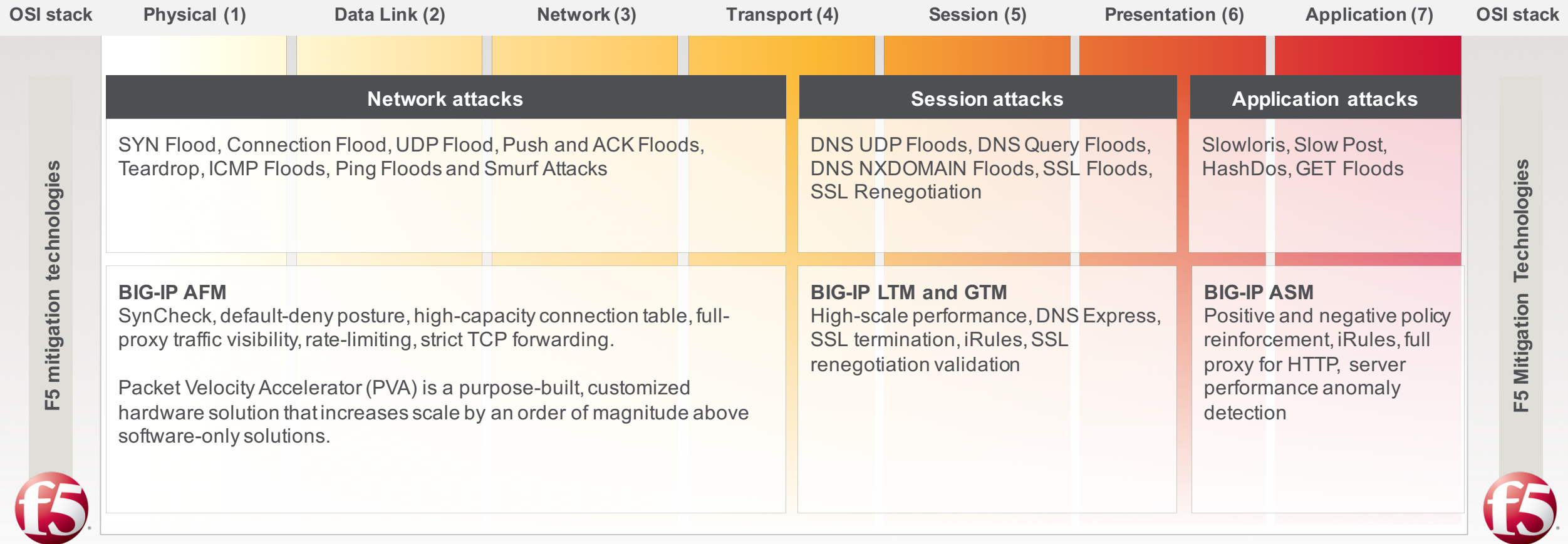
23.11.15



OSI and F5 modules

DoS

Increasing difficulty of attack detection



F5 mitigation technologies

F5 Mitigation Technologies



- Protect against DDoS at all layers – 38 vectors covered
- Withstand the largest attacks
- Gain visibility and detection of SSL encrypted attacks

DNS

- Business Continuity
- GSLB
- DNS Security

Users

Customers

Attackers

Client

- Encryption
- Phishing
- Malware
- Automated Transactions

FW

- ICSA Certified
- ACL's
- IP Intelligence
- IP Lists
- DoS Protections
- Default Deny
- Full Proxy
- SSL Offload / Visibility

Acceleration

- TCP Optimisation
- Caching/Compression
- End User Experience
- HTTP/2

ADC

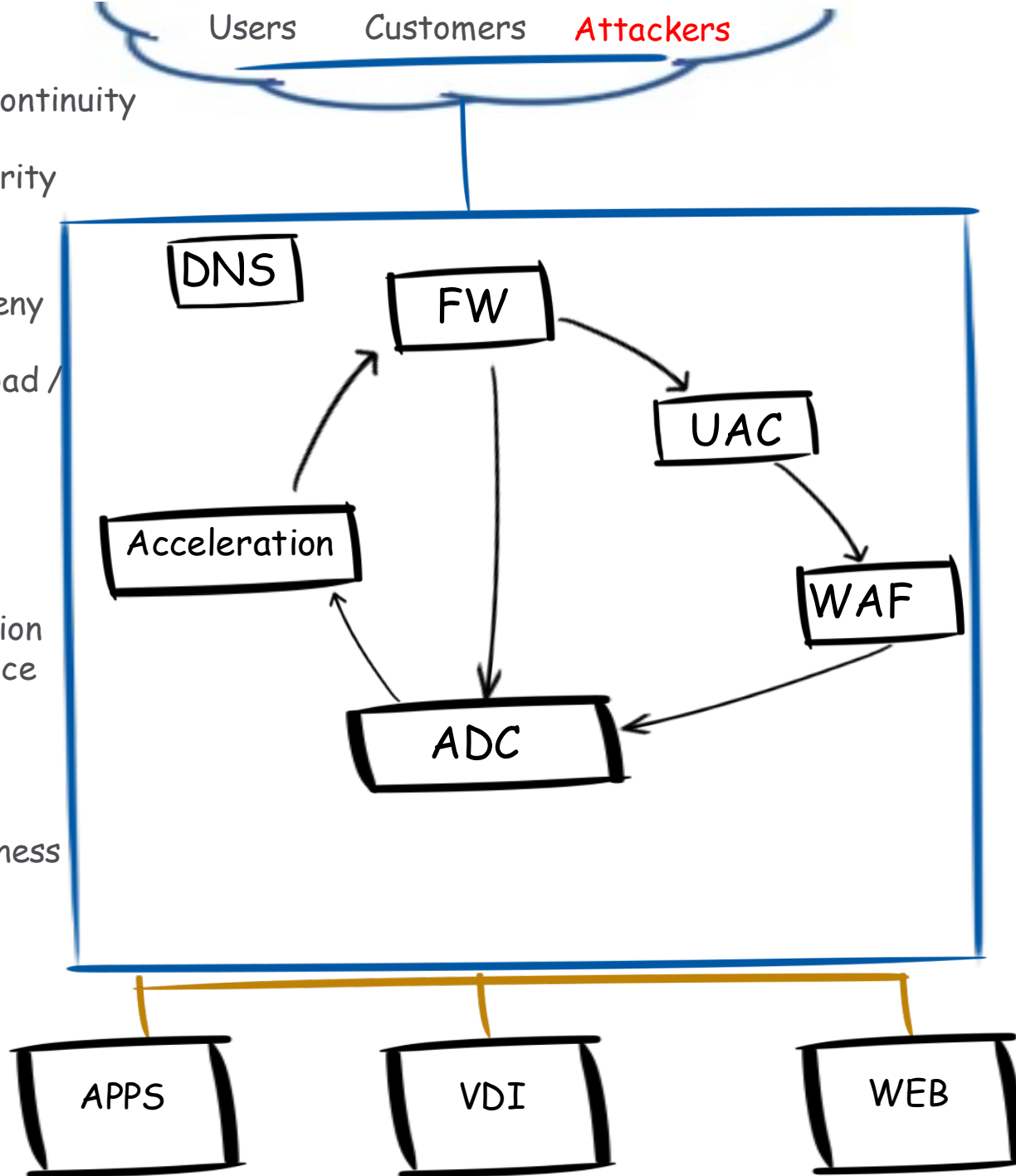
- SLB
- Application Awareness
- Persistence

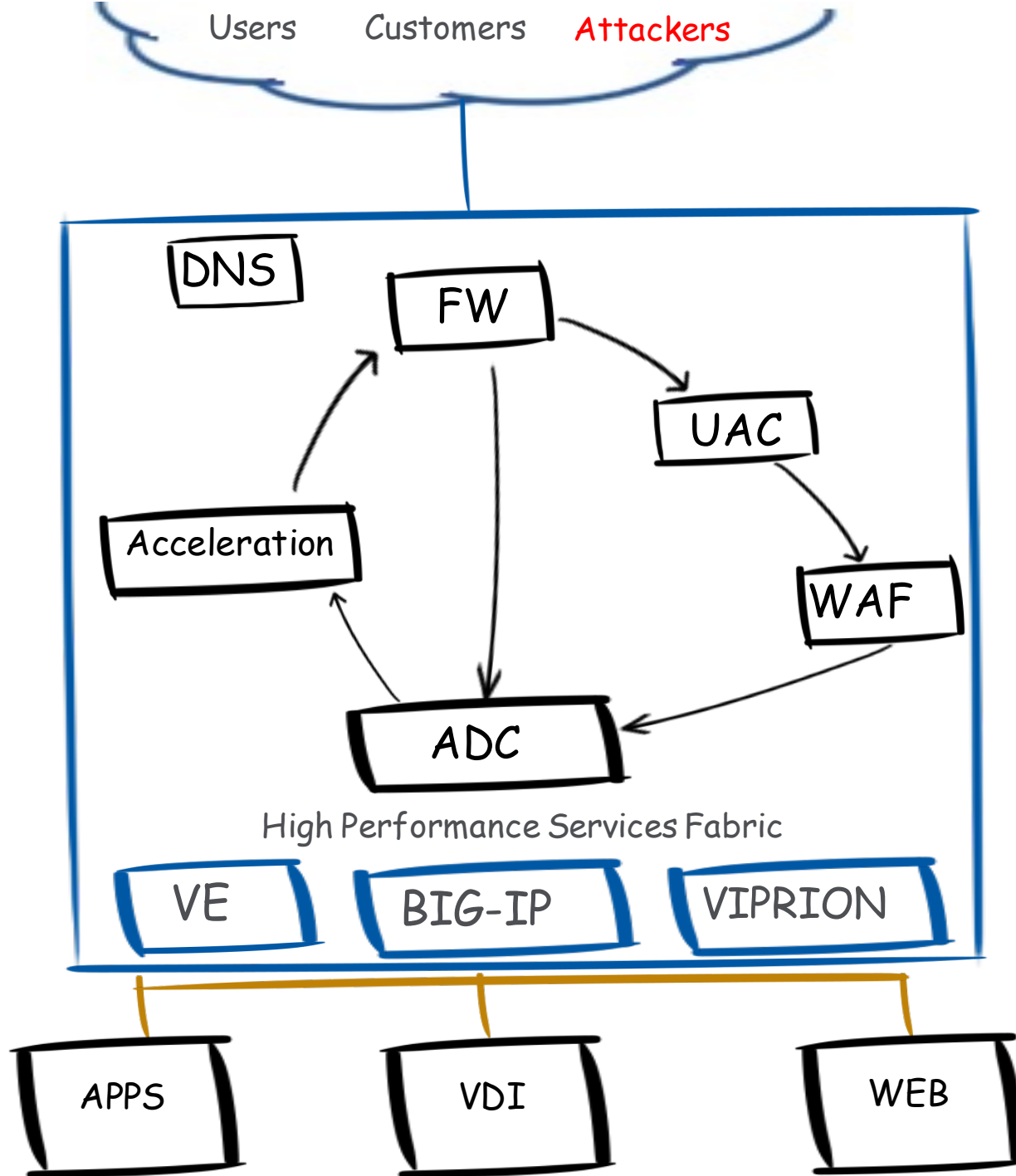
UAC

- Remote Access
- Pre-Authenticacion
- Multi-factor/SSO/Federation
- End Point Inspection

WAF

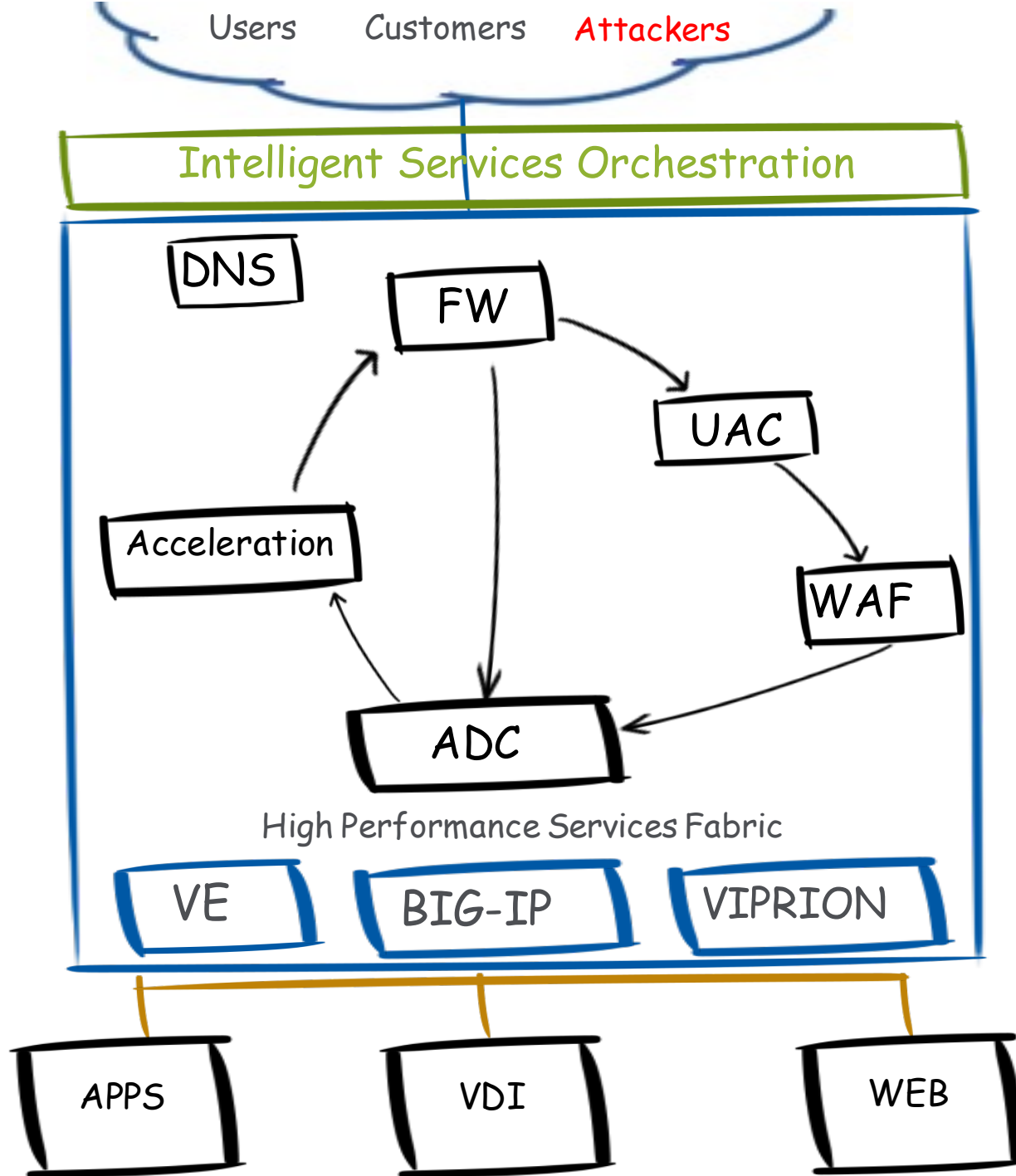
- L7 Firewall
- BOT Detection
- Web Scraping
- Data Leakage
- L7 DoS Mitigation
- PCI Compliance





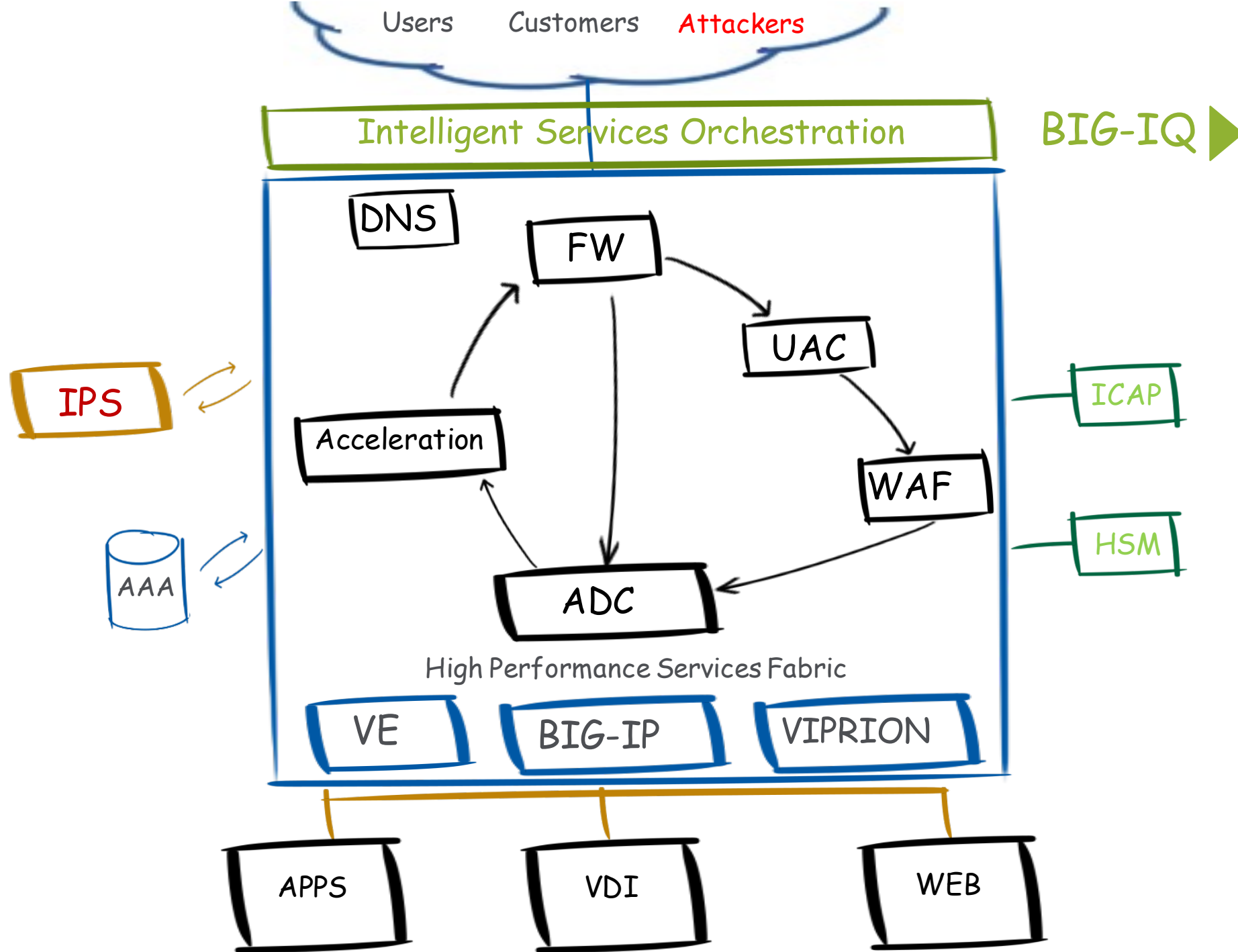
Platform

- Flexibility
- Scalability
- Multi-tenancy
- Programmability
- Custom HW



BIG-IQ ►

- iRules
- iControl
- iCall
- iApps



BIG-IQ ►

- iRules
- iControl
- iCall
- iApps



Solutions for an application world.