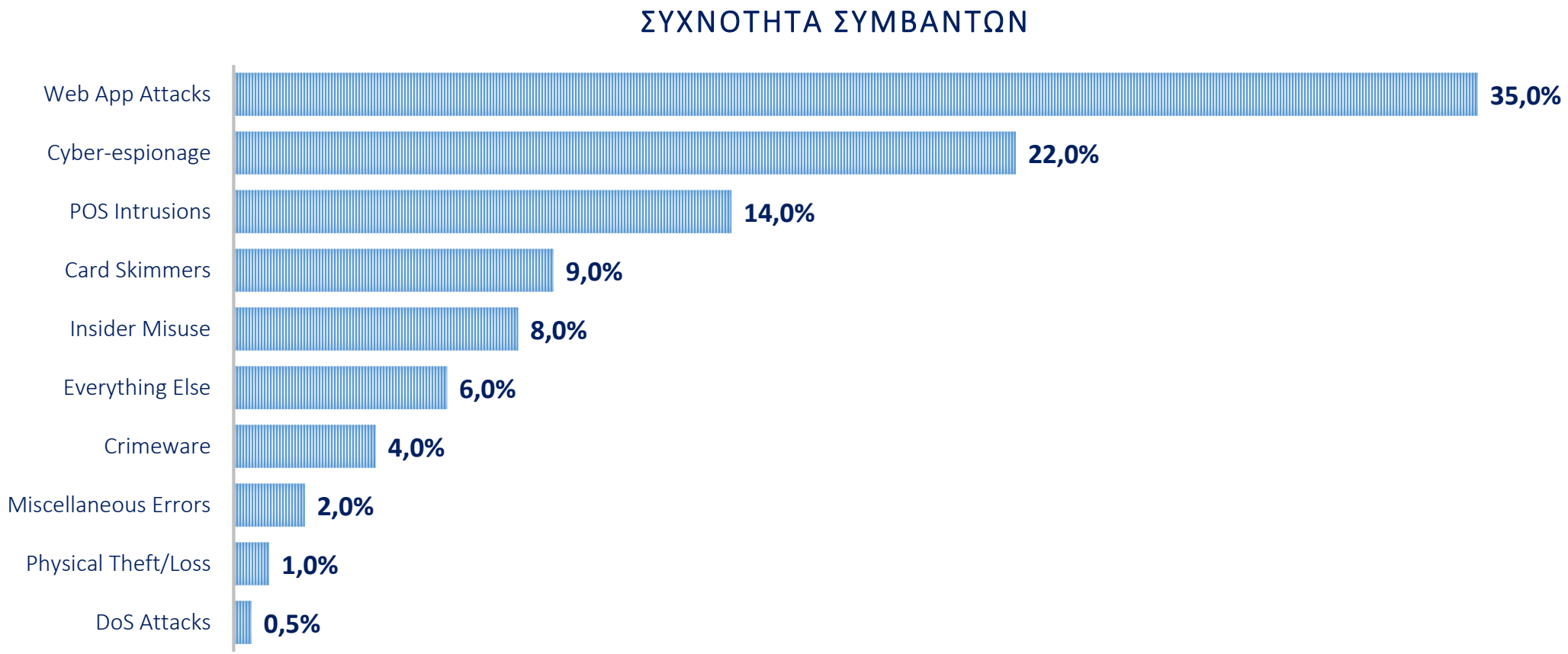
Web Application Firewall

Προστατεύοντας Εφαρμογές και Δεδομένα από προηγμένες απειλές

Καλοχριστιανάκης Αντώνης
Digital SIMA

Τα Websites είναι ο λιγότερο ασφαλής τομέας



Απειλές Web App : ο τομέας με τη μεγαλύτερη ανάπτυξη

80%

Ποσοστό των vulnerabilities που είναι web-based

75%

Ποσοστό των κυβερνοεπιθέσεων που στοχεύουν σε web εφαρμογές

12Δισ

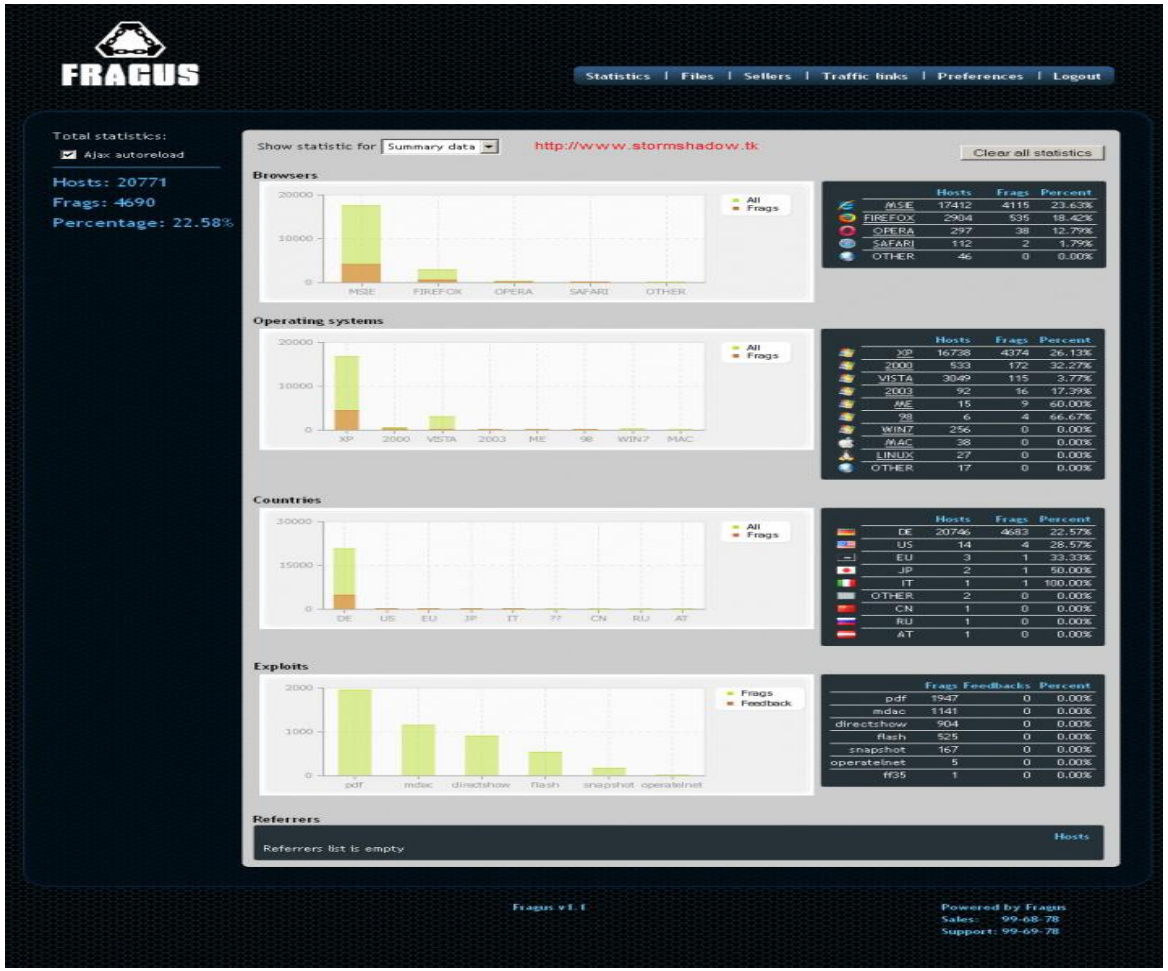
Αριθμός των κακόβουλων εμφανίσεων διαφημίσεων ετησίως

5Εκκ

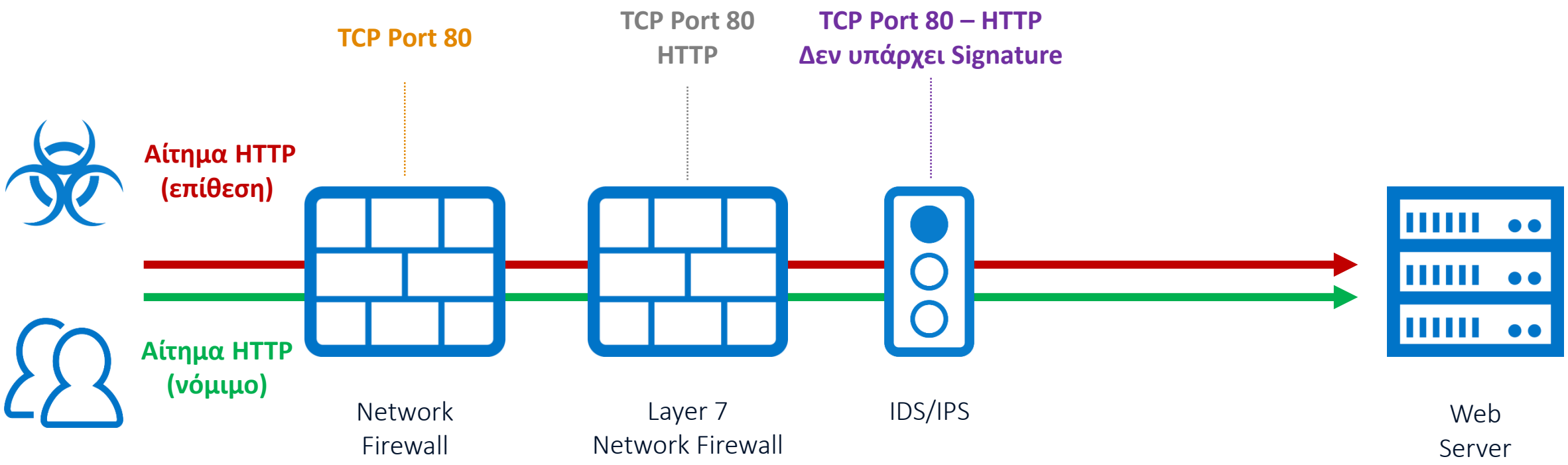
Αριθμός των websites που έγιναν defaced τα τελευταία 5 έτη

Όλοι αποτελούν στόχο…..

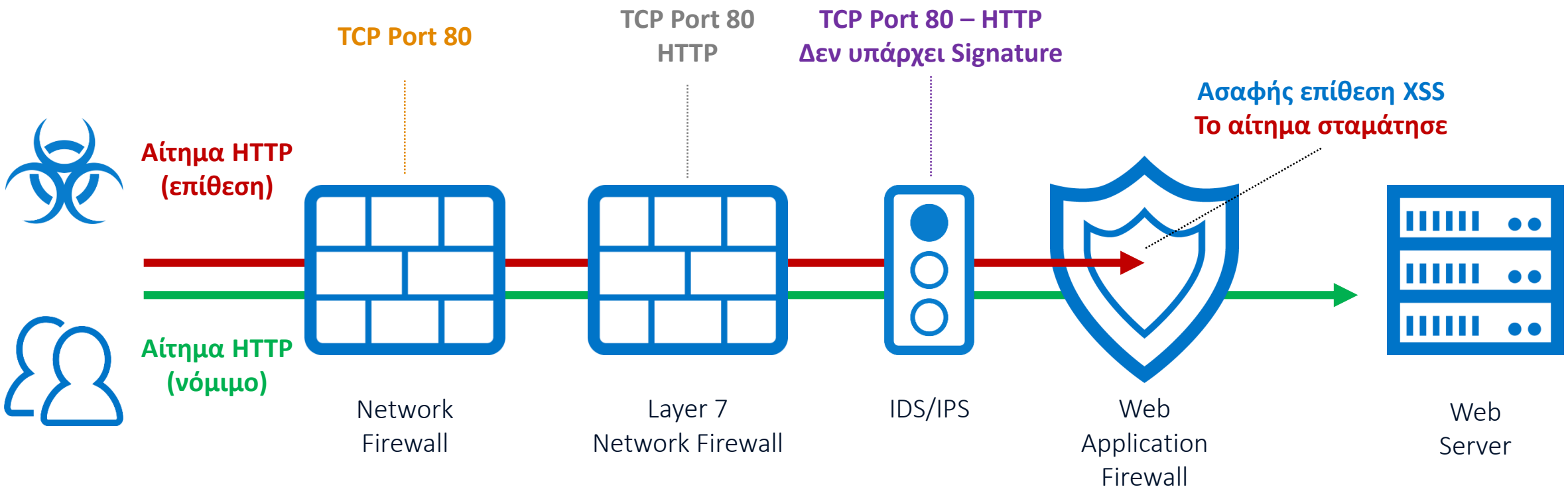
- Εύκολη προμήθεια
- Δεν απαιτείται εξειδίκευση
- Λειτουργούν σαν εταιρείες
- Μπορούν να επιτεθούν σε χιλιάδες servers σε δευτερόλεπτα.



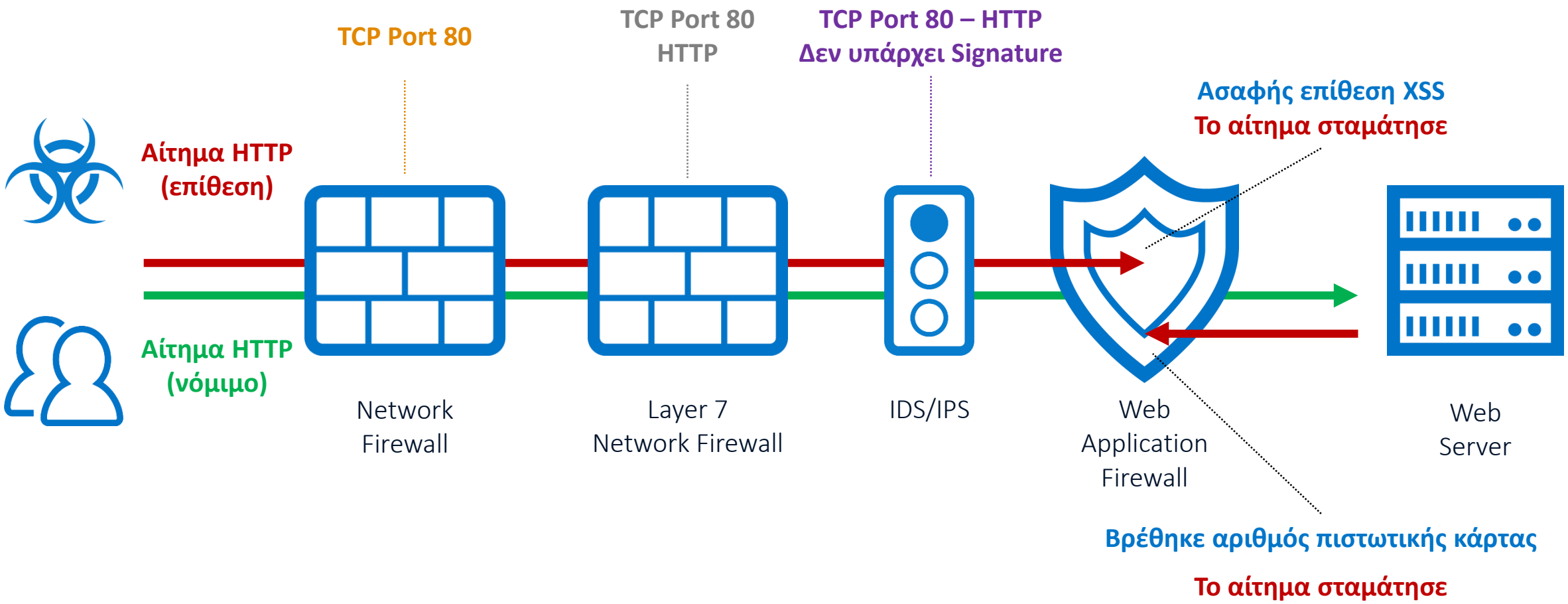
Τα App-Aware Firewalls δεν ασφαλίζουν τις Web Apps



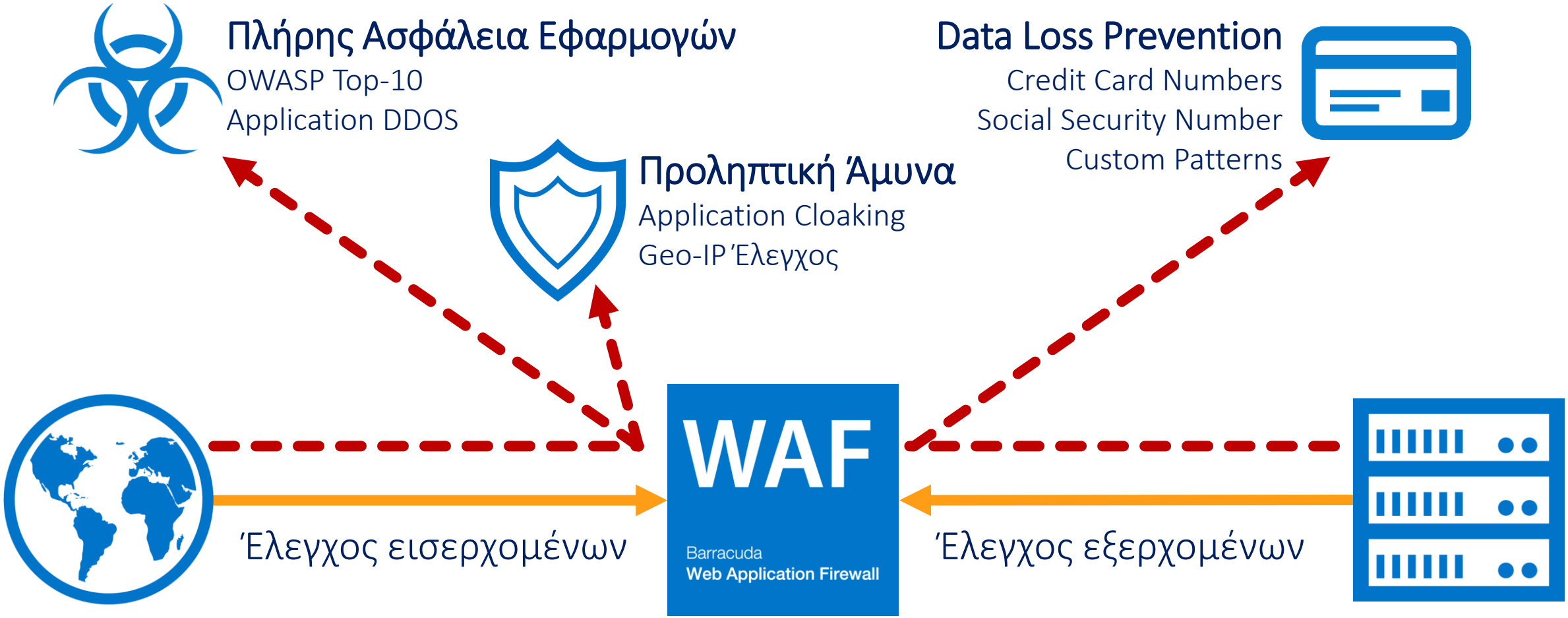
WAFs vs....


TCP Port 80
TCP Port 80
HTTP
TCP Port 80 – HTTP
Δεν υπάρχει Signature
Ασαφής επίθεση XSS
Το αίτημα σταμάτησε
Αίτημα HTTP
(επίθεση)
Αίτημα HTTP
(νόμιμο)
Network
Firewall
Layer 7
Network Firewall
IDS/IPS
Web
Application
Firewall
Web
Server

WAFs vs....


TCP Port 80
TCP Port 80
HTTP
TCP Port 80 – HTTP
Δεν υπάρχει Signature
Ασαφής επίθεση XSS
Το αίτημα σταμάτησε
Αίτημα HTTP
(επίθεση)
Αίτημα HTTP
(νόμιμο)
Network
Firewall
Layer 7
Network Firewall
IDS/IPS
Web
Application
Firewall
Web
Server
Βρέθηκε αριθμός πιστωτικής κάρτας
Το αίτημα σταμάτησε

Το Web App. Firewall Προσφέρει



Barracuda WAF: Πλήρης Ασφάλεια Εφαρμογών

Προστασία επιθέσεων
- SQL, XSS, command injection

CSRF

Web Site Cloaking

Προστασία απώλειας δεδομένων
- Credit card, SSN, custom patterns

Session Protection
- Cookie encryption
- Parameter tampering protection

Integrated Anti-Virus

Positive and Negative Security
- Automated Learning

IP Reputation Blocking
- GeoIP, Tor, Botnets
- Anonymous Proxy

JSON and XML Firewall
- XML schema enforcement
- Web services security
- REST API security
- Mobile apps security

Next-Gen Firewall & IPS vs. WAF

	Web Application Firewall	Intrusion Prevention System	Next-Gen Firewall
Multiprotocol Security	○	●	●
IP Reputation	◑	◑	◑
Web Attack Signatures	●	◑	○
Web Vulnerability Signatures	●	◑	◑
Automatic Policy Learning	●	○	○
URL, Parameter, Cookie, and Form Protection	●	○	○
Leveraging Vulnerability Scan Results	●	◑	○

● Καλό ως πολύ καλό ◑ Μέτριο ως καλό ○ φτωχό

Ενσωματώνονται 4 μηχανισμοί

Acceleration

- SSL-Offloading
- TCP-Pooling
- Caching
- Compression
- Rate Control
- Connection Multiplexing

Application Security

- OWASP Top 10 and beyond
- XML firewall, Cookie Security
- Positive Security Model
- DDoS and Bot protection
- Integrated Anit Virus
- Vulnerability scanner integration

Identity and Access Management

- Authentication & Authorization
- Single Sign On
- SSL Client Certificates
- One Time Passwords
- LDAP/AD, Kerberos, CA-Siteminder
- RADIUS, RSA SecureID

Traffic Management

- Load Balancing
- Session Persistence
- Health Monitors
- Content Routing
- Content Rewrite
- Instant SSL

Ασφάλεια εφαρμογών σε κάθε περιβάλλον

Hardware Appliance

- No per-user or per-feature fees

Virtual Appliance

- VMware
- Citrix Xen Server
- Hyper-V

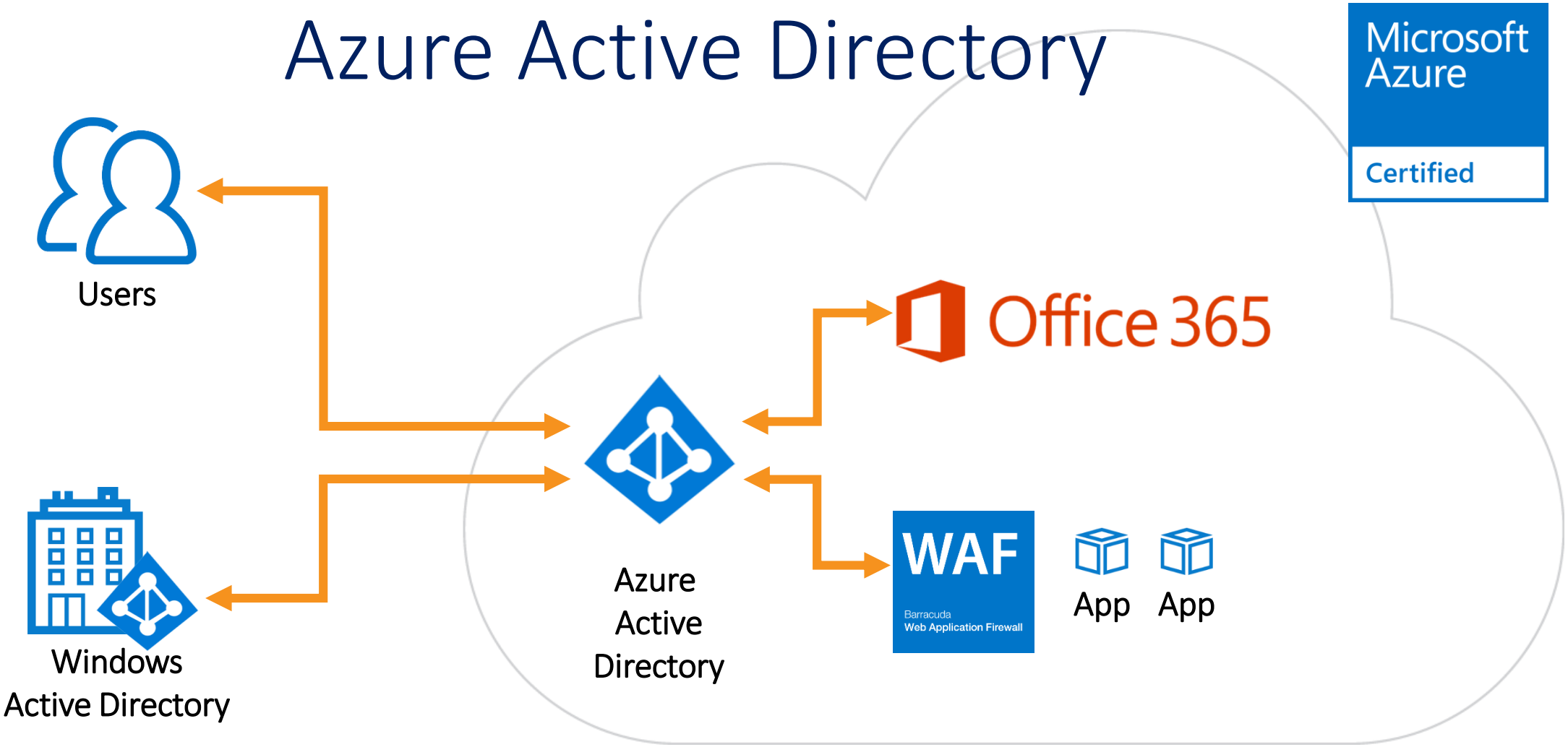
Public Cloud

- Microsoft Azure
- Amazon Web Services

Microsoft Azure Certified

amazon web services Partner Network
ADVANCED TECHNOLOGY PARTNER

Azure Active Directory



Compliance

- Comply with major application-specific requirements like PCI-DSS, HIPAA, FISMA, and SOX
- Directly satisfies section 6.6 of PCI-DSS and assists compliance with built-in PCI compliance reports
- FIPS 140-2 HSM model ensures that applications it protects meets the highest cryptographic standards

NSS Lab Results

99.97%	Highest marks for Security Effectiveness
100%	Score against all evasion techniques
100%	Score in stability and reliability tests
0.715%	False Positive Rate


Thank you!