

The Akamai Edge

Forum Bezpieczeństwa Banków, 3 czerwca 2020



Chmura czy Edge?

Jak Akamai pomaga największym bankom na świecie. Czego uczy nas pandemia?

#finserve AD2020

Co widzimy?

Regulacje, compliance

Przetwarzanie danych

Ciągłość działania

Wiele technologii dostępowych

Rozproszenie użytkowników

Rozproszenie zagrożeń

Wydajność, performance serwisów

Szybko zmieniające się środowisko

Kary



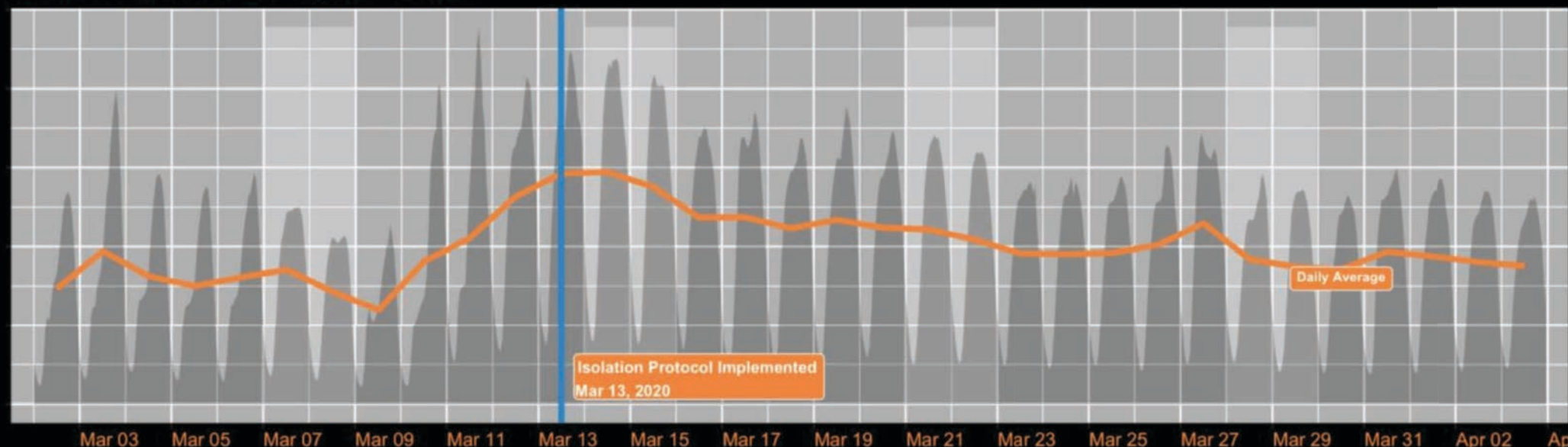
Co zmienił #covid

Nowa rzeczywistość w świecie online

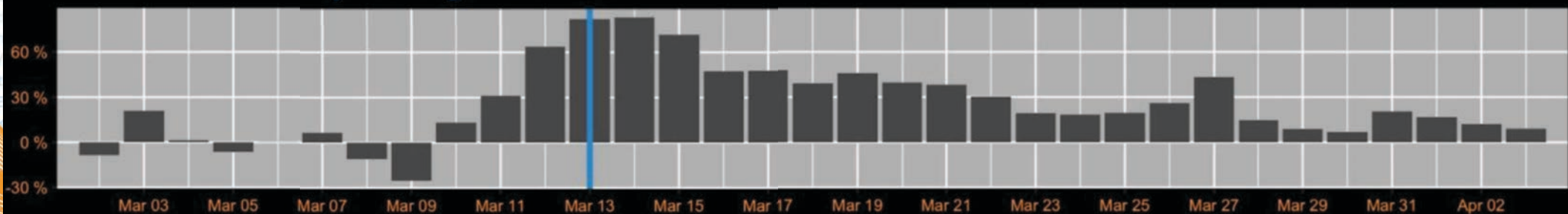


Daily Traffic: Poland

From March 02, 2020 - April 03, 2020

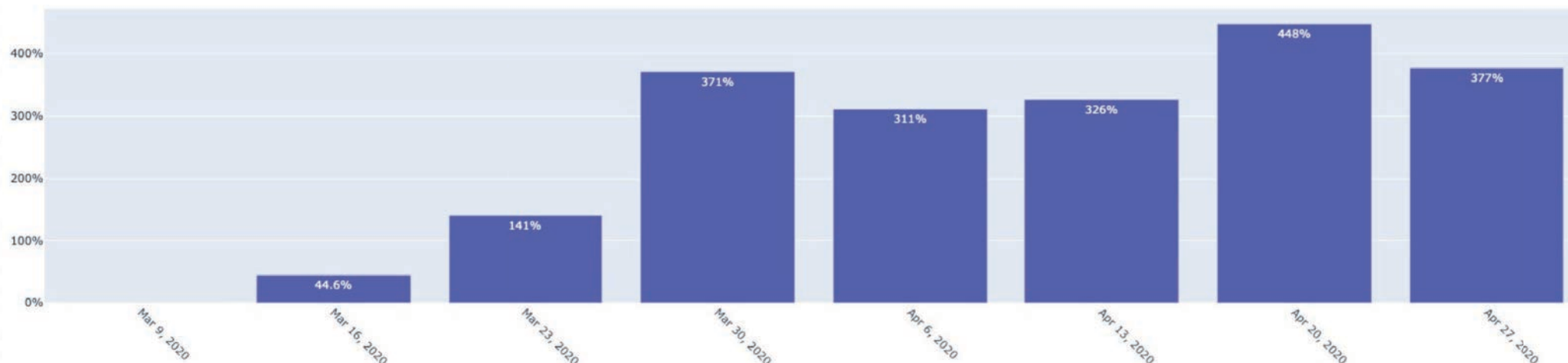


Delta from February Average - Poland



Co zmienił #covid

Nowa rzeczywistość w świecie online



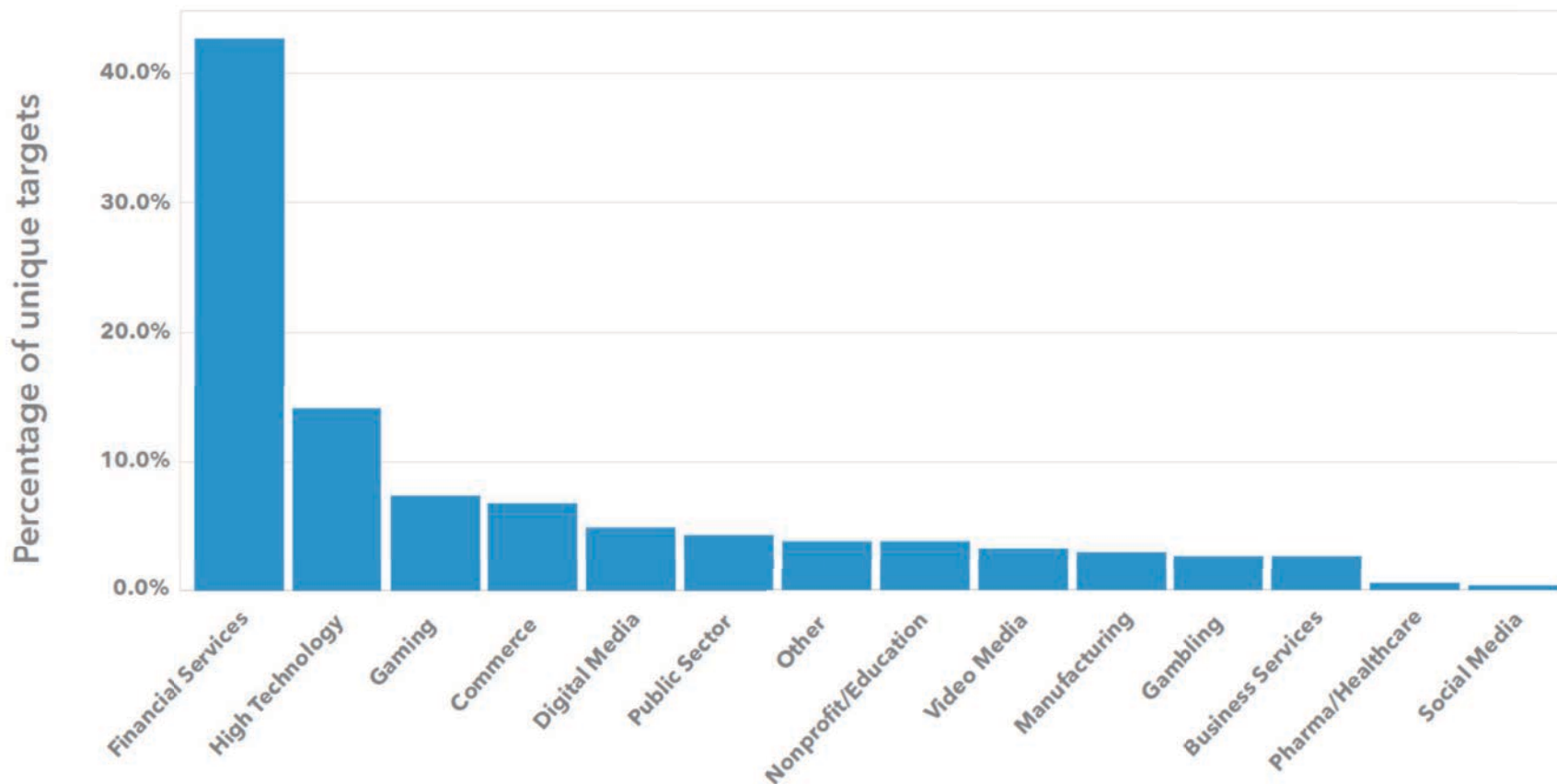
Cumulative change in number of DNS queries to malware-associated websites

Co zmienił #covid

Stare problemy na większą skalę



Unique DDoS Targets by Vertical
December 2017 – November 2019

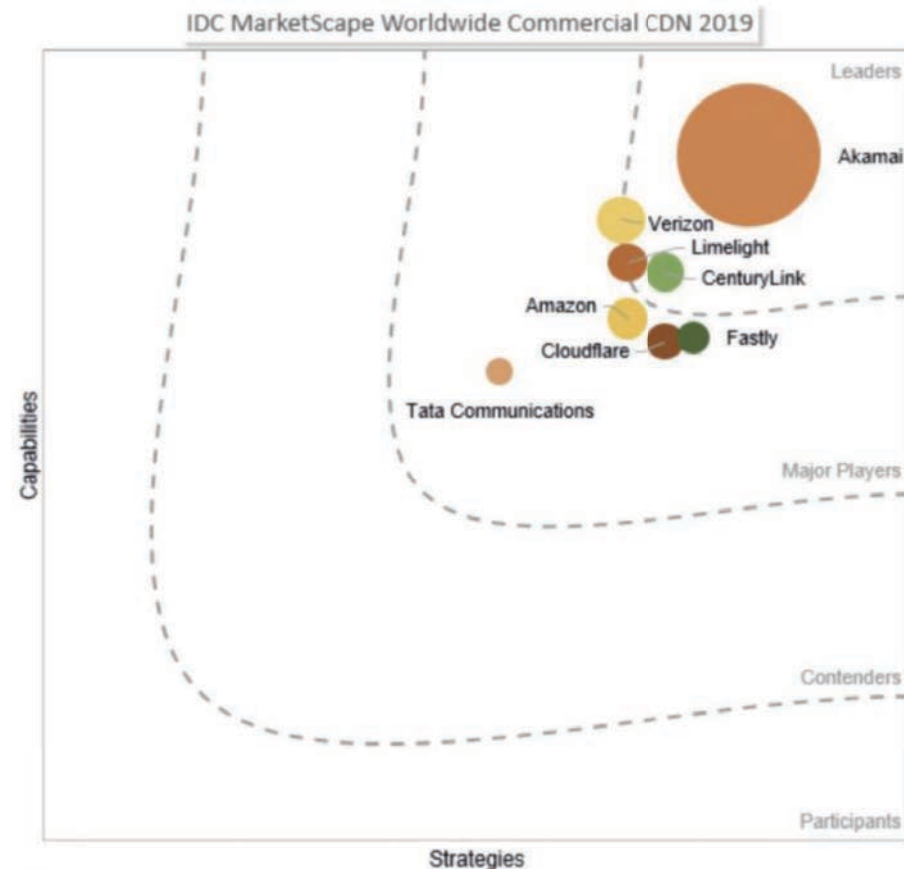


Akamai Edge

Co to jest Edge?



IDC MarketScape Worldwide Commercial CDN Vendor Assessment



Source: IDC, 2019

Akamai Edge

Dlaczego Edge?

Obecność blisko użytkowników -> obecność blisko zagrożeń

Obecność blisko zagrożeń -> trzymanie zagrożeń z dala od nas

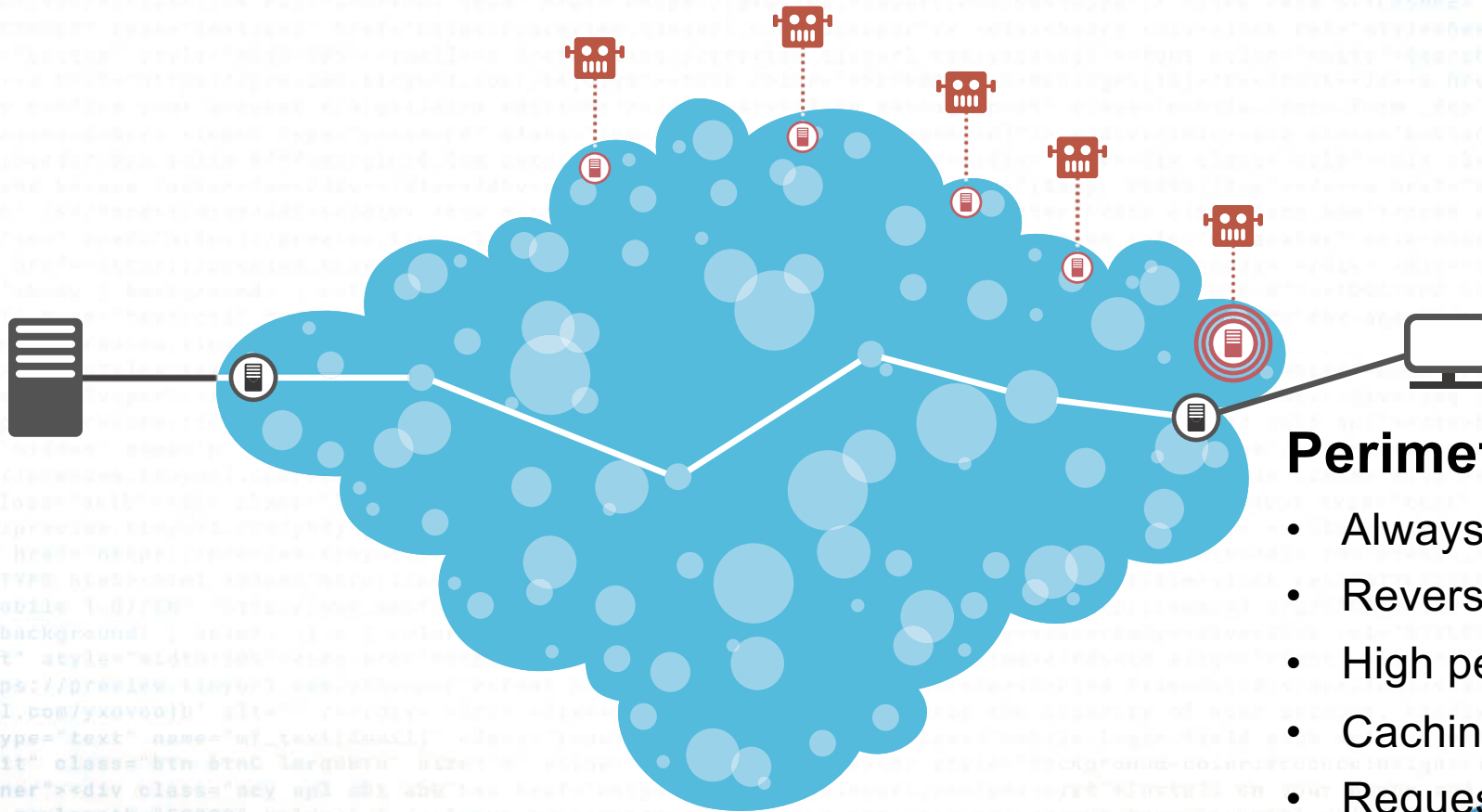
Unikalny threat research z 30% światowego ruchu internetowego

... i 65% ruchu DNS-owego ($\sim 2.2 \cdot 10^{12}$ zapytań DNSowych dziennie)

Skalowalność (peak traffic / DDoS)



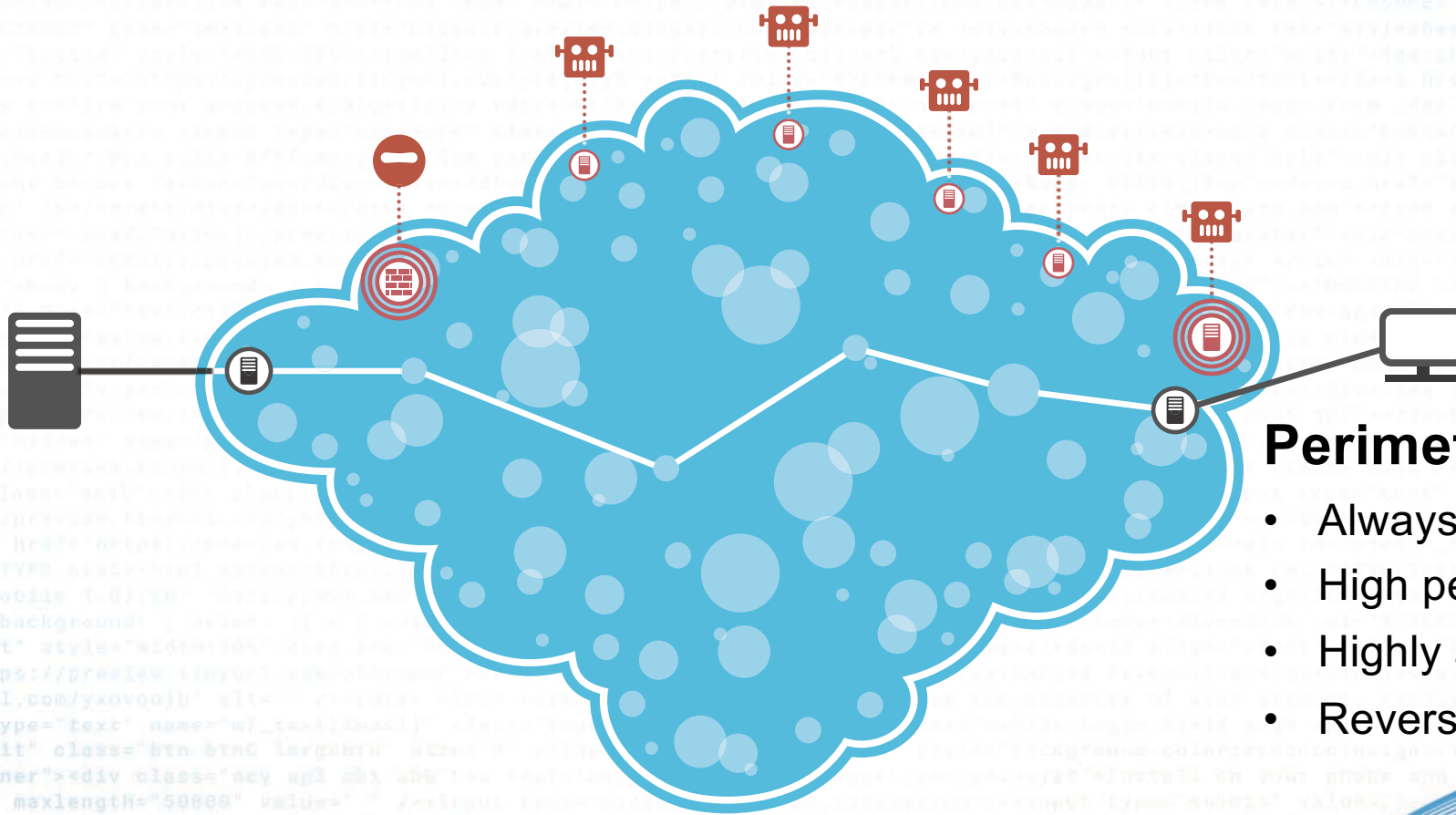
Protecting Multiple Perimeters on the Edge



Perimeter 1 – Web (DDoS)

- Always-on defense
- Reverse Proxy (HTTP / HTTPS)
- High performance
- Caching
- Request Validation

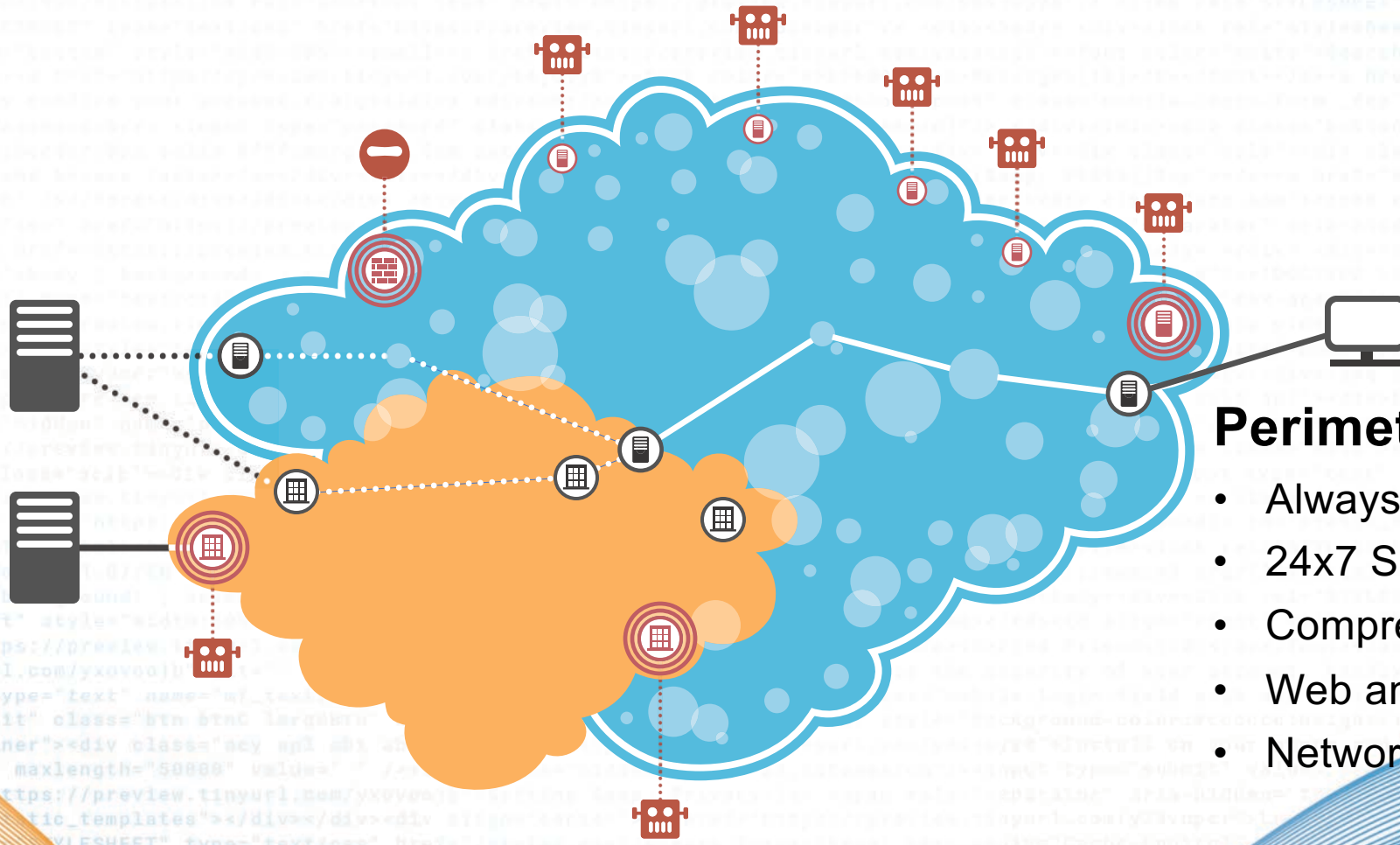
Protecting Multiple Perimeters on the Edge



Perimeter 1 – Web (WAF + CSI)

- Always-on defense against data theft
- High performance and scalability
- Highly accurate (reduced FP, FN)
- Reverse Proxy (HTTP / HTTPS)

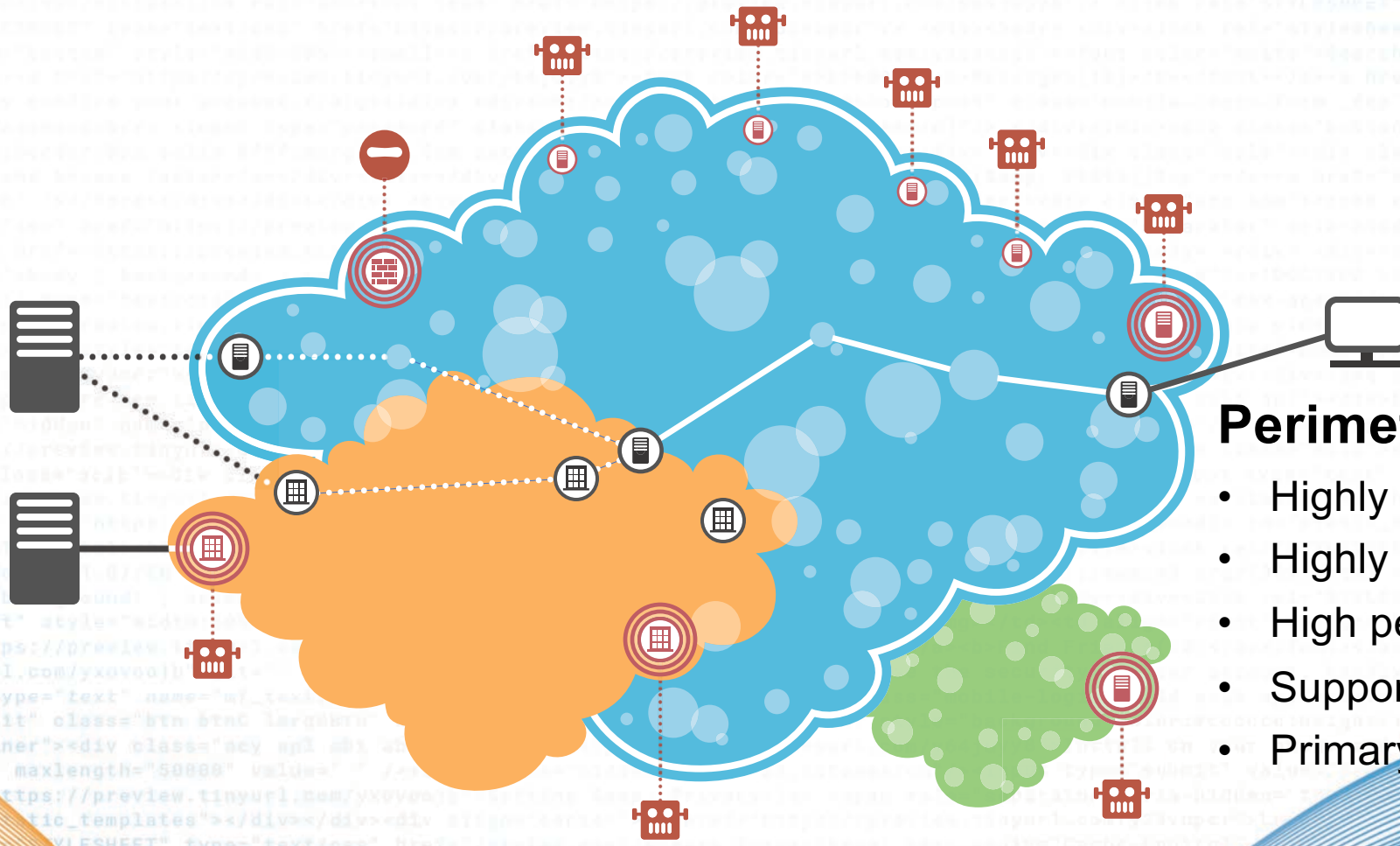
Protecting Multiple Perimeters on the Edge



Perimeter 2 – Origin (DDoS)

- Always-on or on-demand
- 24x7 SOC (5-20 min SLA)
- Comprehensive (subnet granularity)
- Web and IP applications
- Network infrastructure + bandwidth

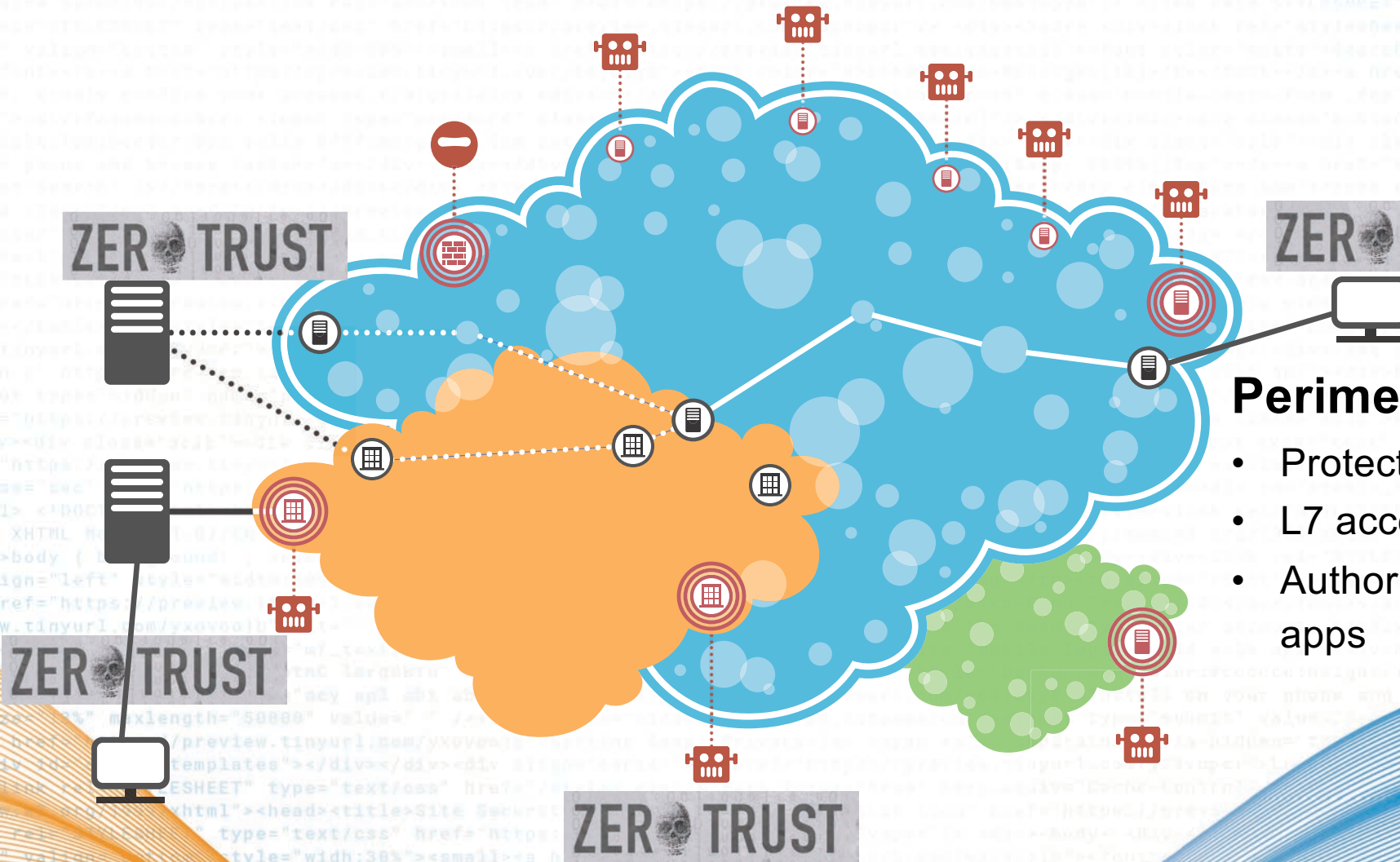
Protecting Multiple Perimeters on the Edge



Perimeter 3 – DNS

- Highly scalable (<1% total capacity)
- Highly available (24x7 SLA)
- High performance (zone apex)
- Supports DNSSEC
- Primary and secondary DNS

Protecting Multiple Perimeters on the Edge



Perimeter 4 – Zero Trust

- Protection organizations from inside
- L7 access to the apps instead of L3
- Authorized access only to required apps