RSACONFERENCE2014
ASIA PACIFIC & JAPAN

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

The Perimeter is Dead! Birth of the Elastic Network

SESSION ID: CDS-W05

John Ellis

Enterprise Security Director
Akamai Technologies
@zenofsecurity

#RSAC

What is De-perimeterisation?

… is not a security strategy

What is de-perimeterisation?

… is a consequence of globalisation by cooperating enterprises

… consumerisation of IT and

… emergence of shadow IT

How did this come about?

Inter-enterprise access to complex applications

Public / externally hosted Cloud services

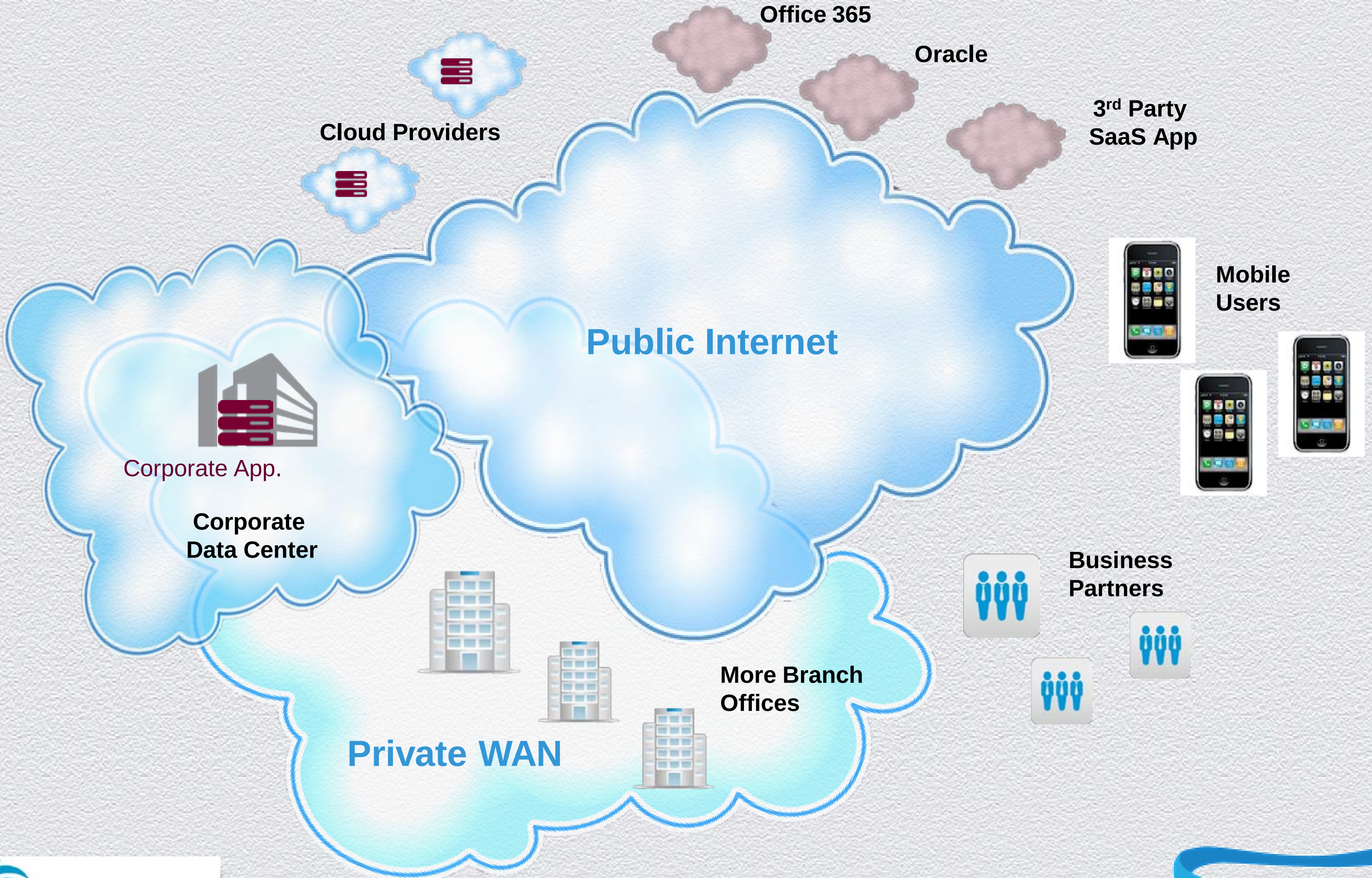
Specifically how did this occur?

Virtualisation of employee location

On site access for non employees

Direct access from external applications to internal application and data resources

Today’s modern enterprise

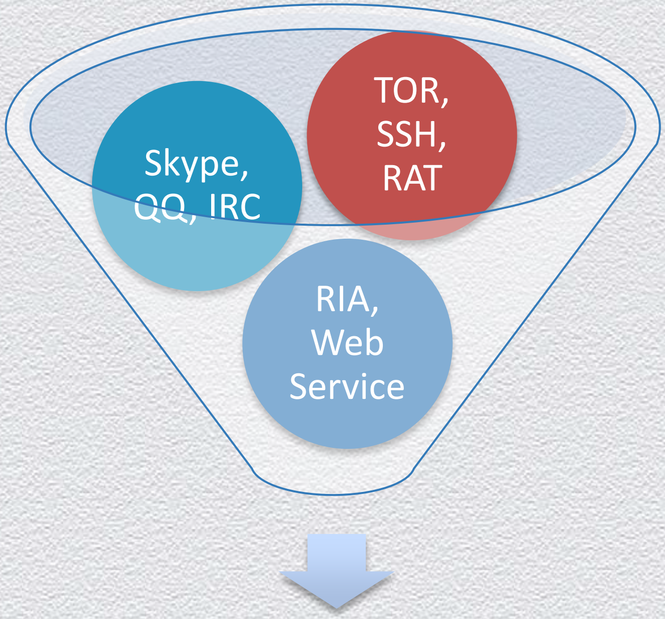


Increased degree of complexity

IaaS
PaaS
SaaS
iOS

- Myriad of devices
- Connection types
- Media formats
- Browser and code

Port 80, 443 - Ports of everything



Ports 80 & 443

- Tunneling through Ports 80 & 443 is SOP
- Old school port = service (wrong)
- New school port + service ID = (service)
- What is the service doing?
- Abstract security away from the network

The impacts?

Network security – failing us?

Default policy of any-any-allow!

Is your firewall just an expensive router?

Network centric designs fail us

AppID is cool but what about the actual application context?

How do you protect cloud resources beyond your data centre?

Federation at the network layer doesn't exist

More to attack

Mobiles are targeted

Third party services are targeted

Expanded attack surface

Trusted connections can serve as a back-channel

Not all Internet connected devices go through the ‘firewall’

Users directly accessing hostile sources

Static defences are easily bypassed

Defences that are static are easily bypassed

54% of malware is Fully Un-Detectable (FUD)

Rules and Signatures aren’t enough

Assuming context for security decisions is dangerous

Threats are evolving,

Users directly accessing hostile sources

Static defences are easily bypassed

Copy – manage Identity Management isn’t scalable

How does a partner trust you and you trust them?

Traditional identity management doesn’t work

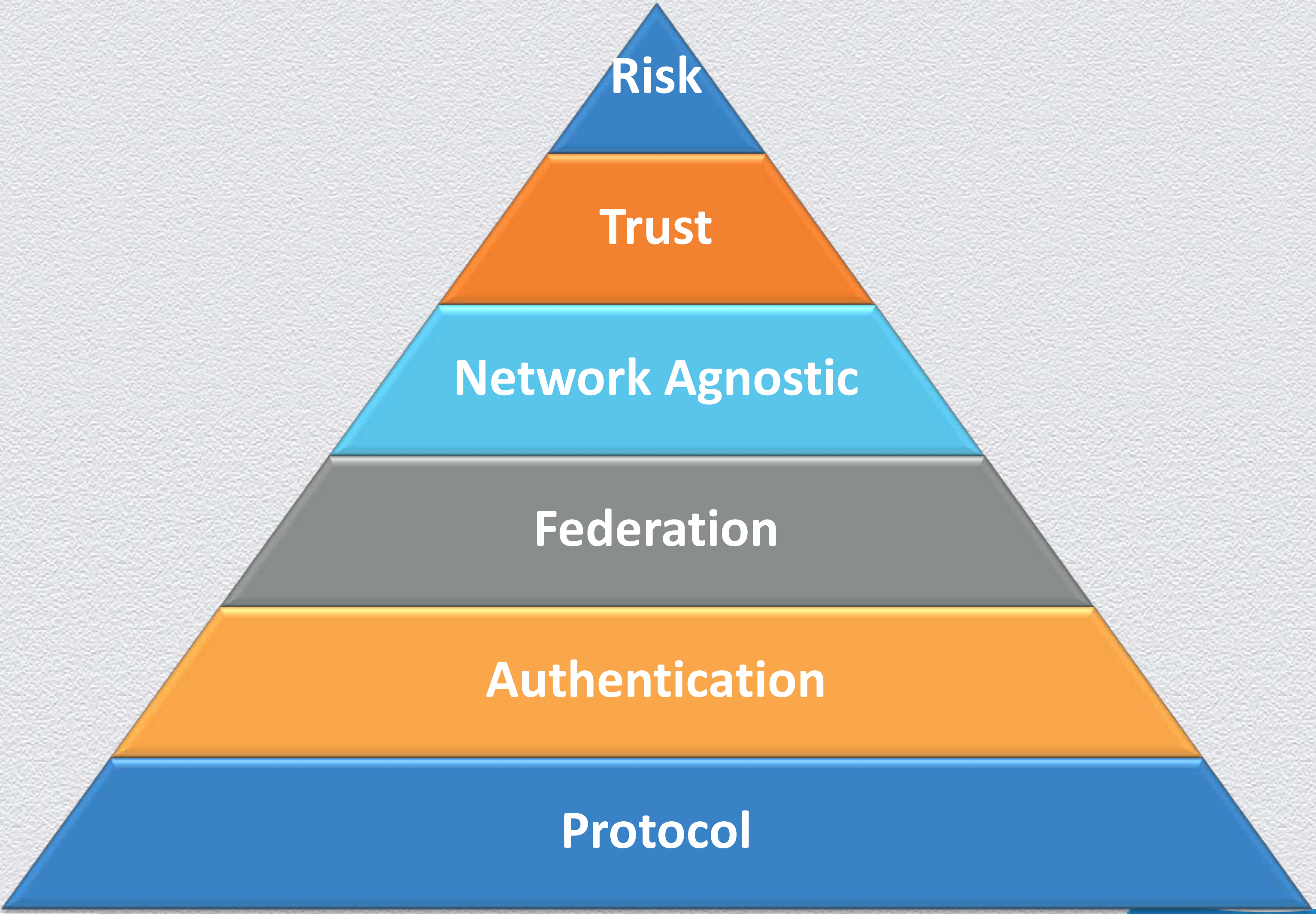
How do employees use ‘their creds’ when accessing cloud services?

How does a resource on a mobile protect itself & enforce your policy?

How do you provision, de-provision, and prevent toxic access?

The solution?

Elements of de-perimeterisation

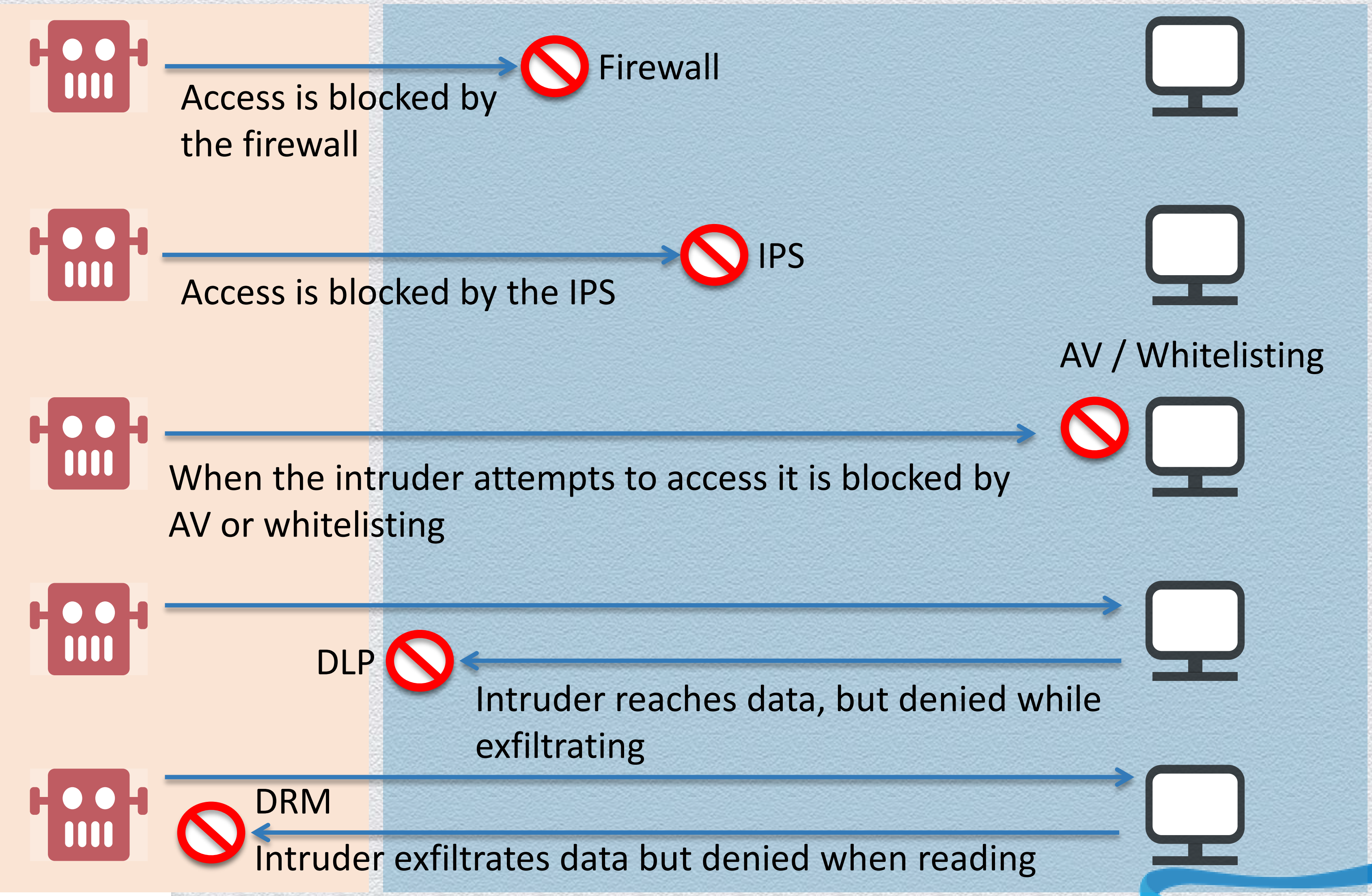


Collaboration Orientated Architecture Elements
http://en.wikipedia.org/wiki/Collaboration-oriented_architecture

The ‘elastic’ network

- Concepts largely based on the work done by Jericho Forum
- Security should be seamless and enable the business in a distributed ecosystem
- Security controls and defences aligned with the resources that you wish to protect
- This model is not for everyone, some ideas may seem rather brazen
- Security controls and defences need to move up ‘the stack’, closer to the resource
- Identity Management, virtualisation, encryption, decentralised Policy Enforcement Points (PEP) and open standards are foundational
- Cloud Security Networks (CSNs) and reputational services provide some exciting opportunities to extend our defences, filtering out noise and preventing untrusted entities from connecting to resources

Blocking, Filtering, and Denying – then!



Firewall

Access is blocked by the firewall

IPS

Access is blocked by the IPS

AV / Whitelisting

When the intruder attempts to access it is blocked by AV or whitelisting

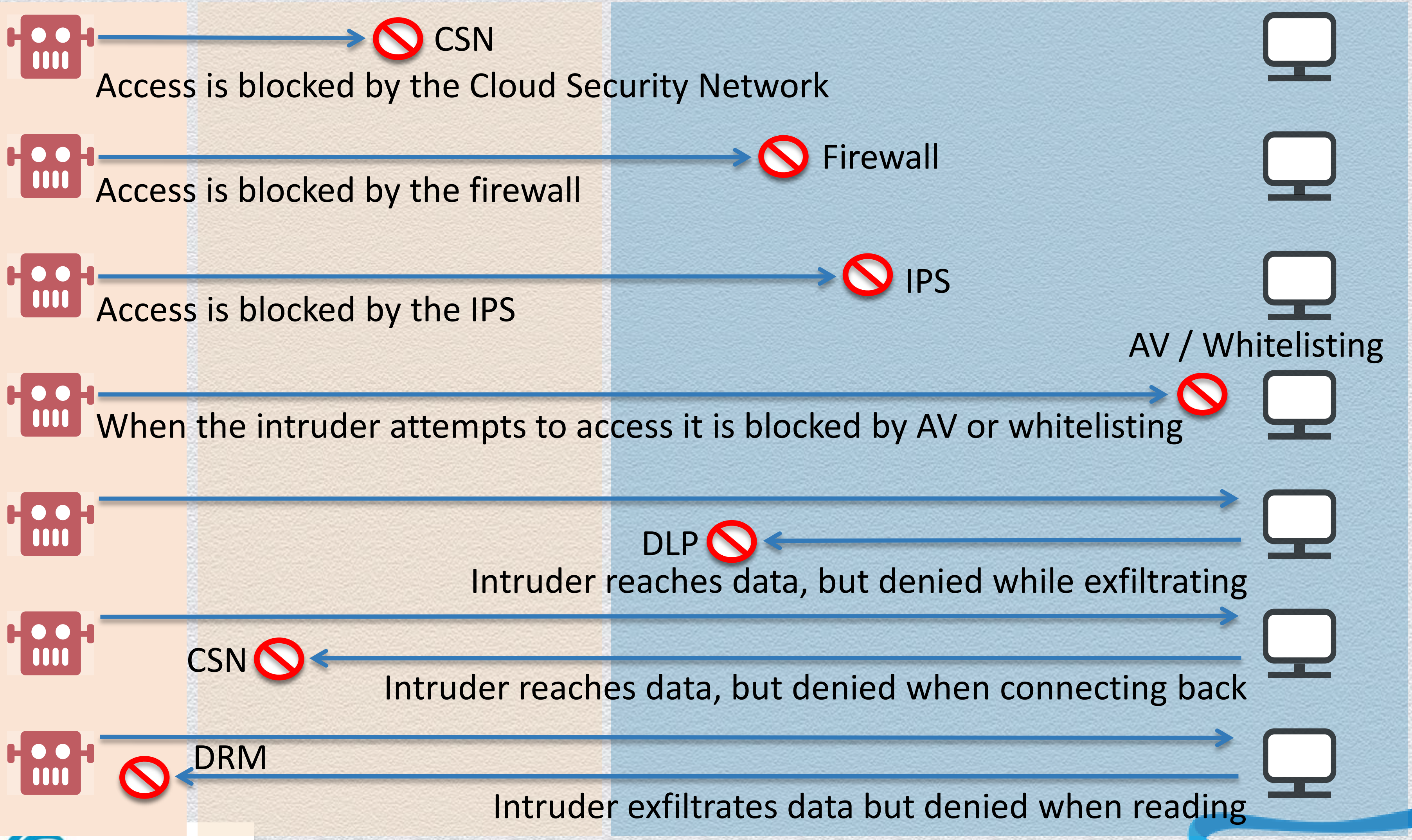
DLP

Intruder reaches data, but denied while exfiltrating

DRM

Intruder exfiltrates data but denied when reading

Blocking, Filtering, and Denying – now!



CSN

Access is blocked by the Cloud Security Network

Firewall

Access is blocked by the firewall

IPS

Access is blocked by the IPS

AV / Whitelisting

When the intruder attempts to access it is blocked by AV or whitelisting

DLP

Intruder reaches data, but denied while exfiltrating

CSN

Intruder reaches data, but denied when connecting back

DRM

Intruder exfiltrates data but denied when reading

Akamai FASTER FORWARD

#RSAC

RSACONFERENCE2014 ASIA PACIFIC & JAPAN

The data is the new perimeter

Encryption necessary but needs careful planning

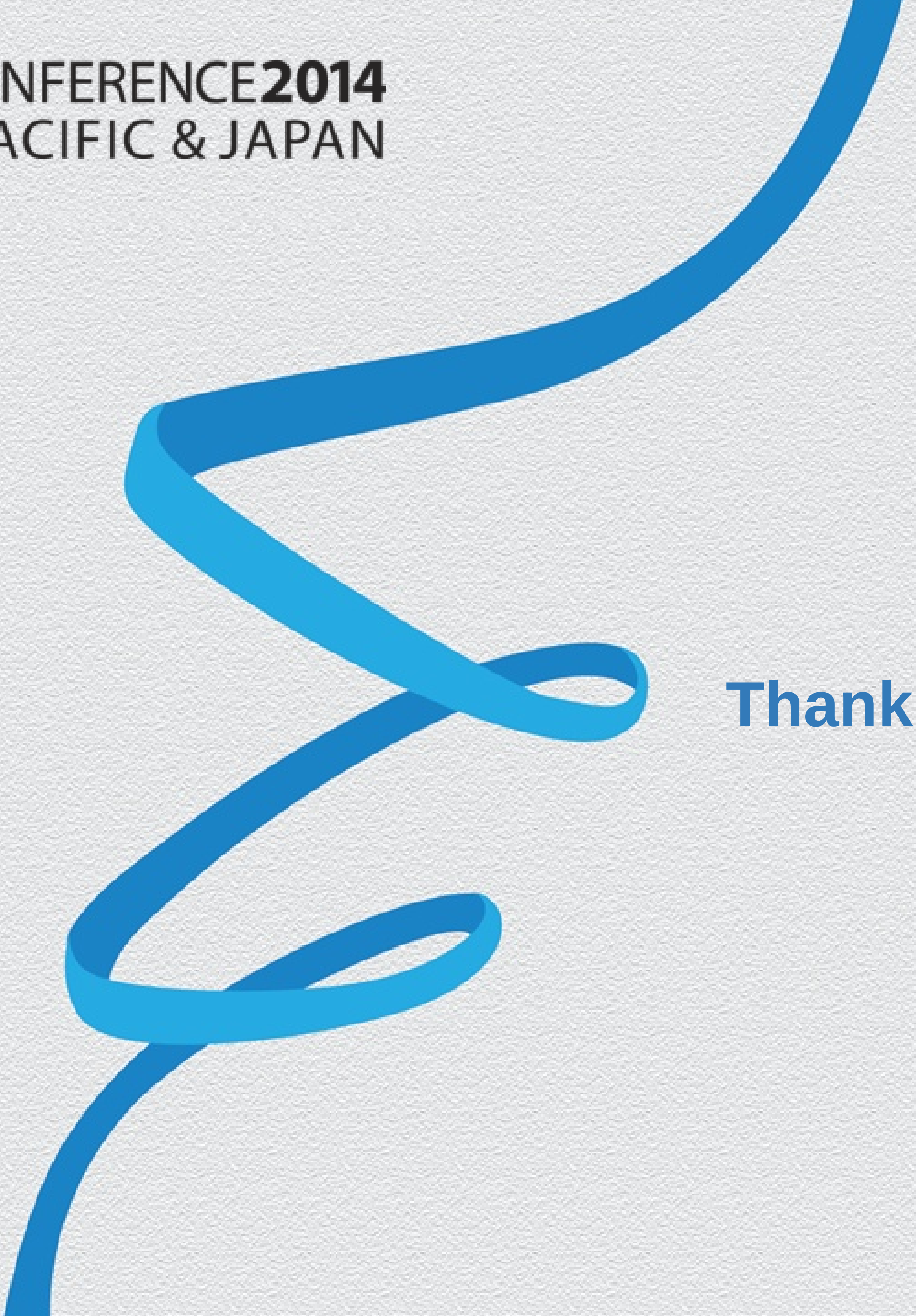
Virtualisation / Sandbox / Containerisation should be considered

Objective: data protection independent of location

Format Preserving Encryption (FPE) is an effective solution for SaaS

Remember, Simple, Scalable, and Manageable

If using cloud, think about HSMs…



Thank You