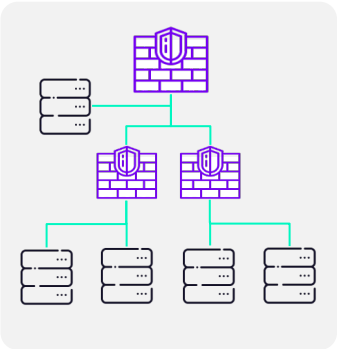
Demystifying modern software-based segmentation

Let's talk about risk..

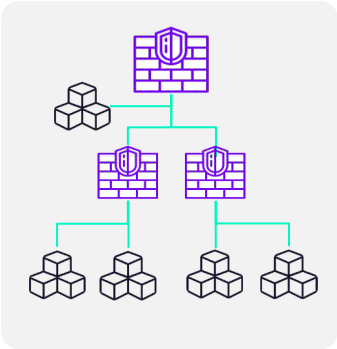
Network segmentation

Data Center



Physical firewall appliances creating network choke points

Cloud

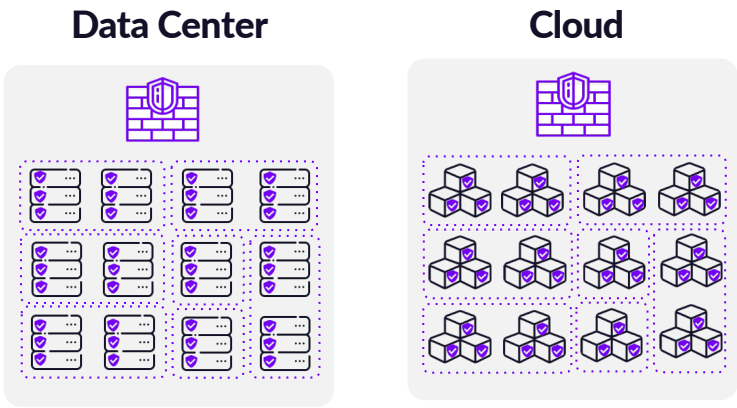


Virtual firewall appliances creating network choke points

Common Issues

- Long lead times to implement changes
- Low visibility into each segment
- Mixed environments and security strategies
- Static, Network-Centric policies
- Difficult to Implement Zero Trust Architecture
- ”Never Finished”

Software-based Segmentation



Software-based policies based on finer-grained attributes
(e.g., process, user, fully-qualified domain name)

What we gain

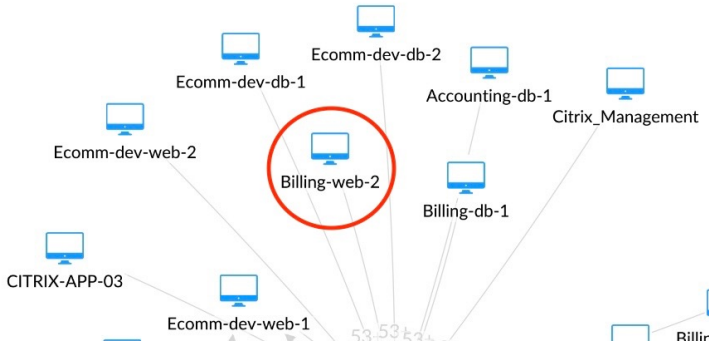
- Granular Visibility
- Map of all assets and applications
- Host level enforcement
- Clear and dynamic policy language
- Zero Trust Architecture

So what's the gist of Software based segmentation?

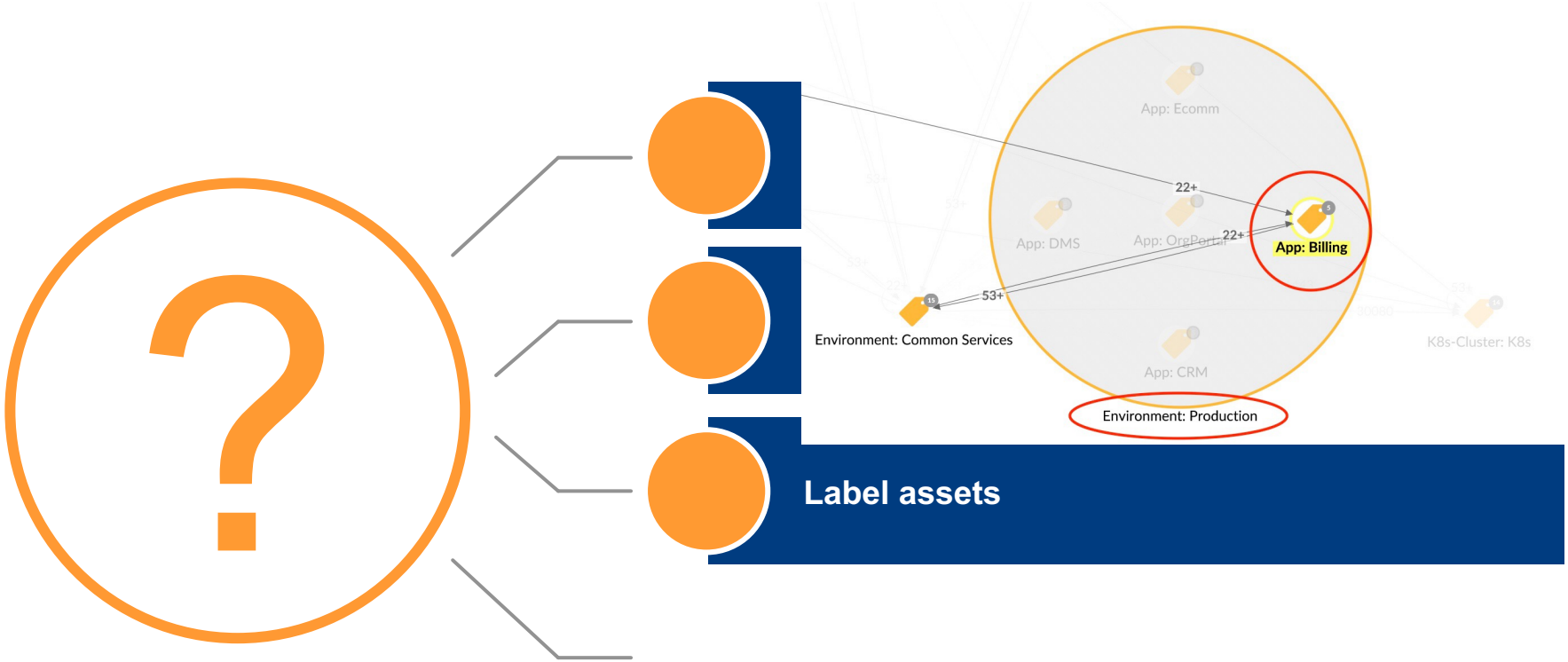
Deploy agent

So what's the gist of Software based segmentation?

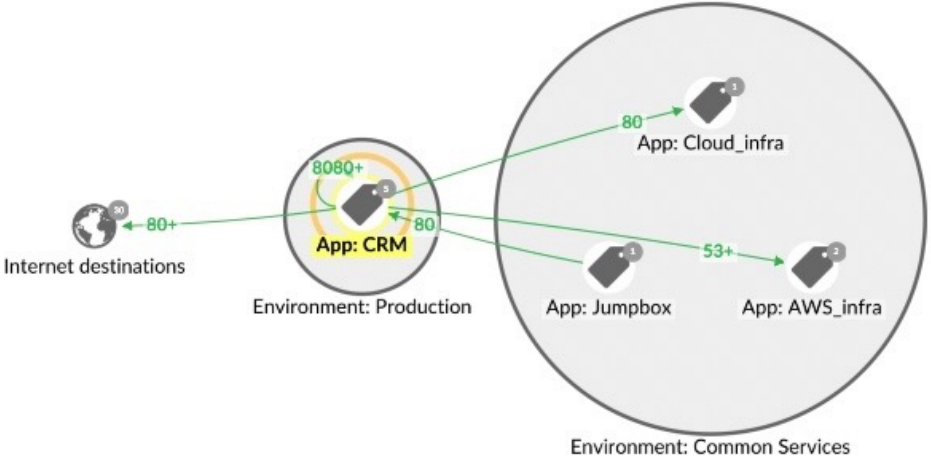
- Deploy agent
- Visualize traffic



So what's the gist of Software based segmentation?

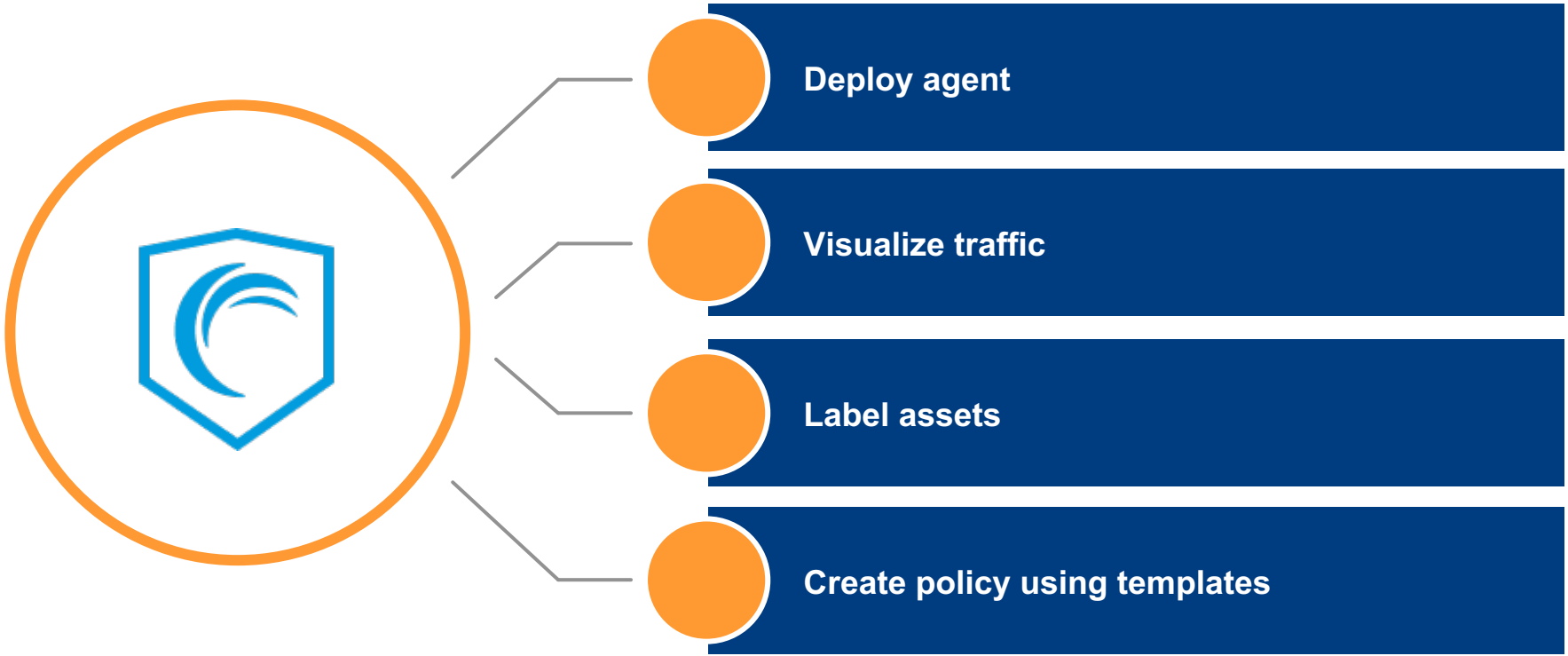


So what's the gist of Software based segmentation?



Create policy using templates

The gist of Software based segmentation



Key drivers

EU Directive

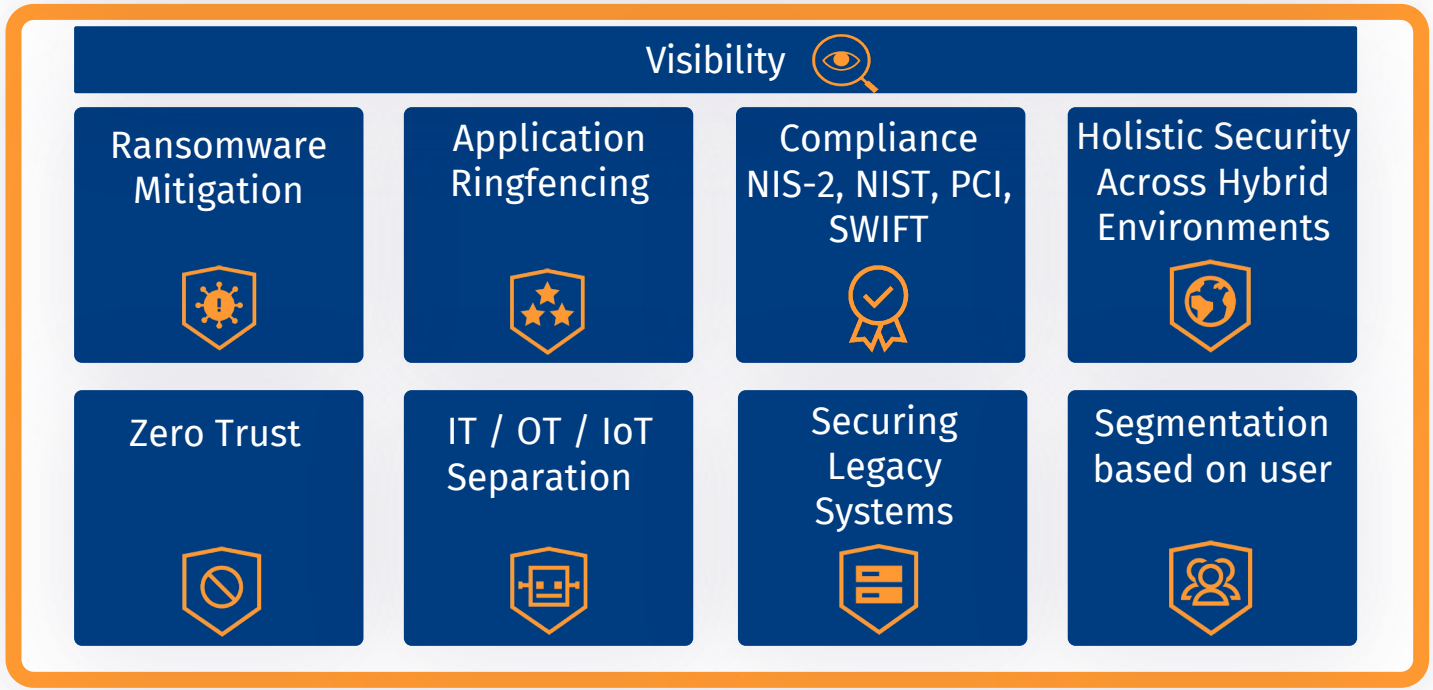
NIS-2

Insurance & Risk

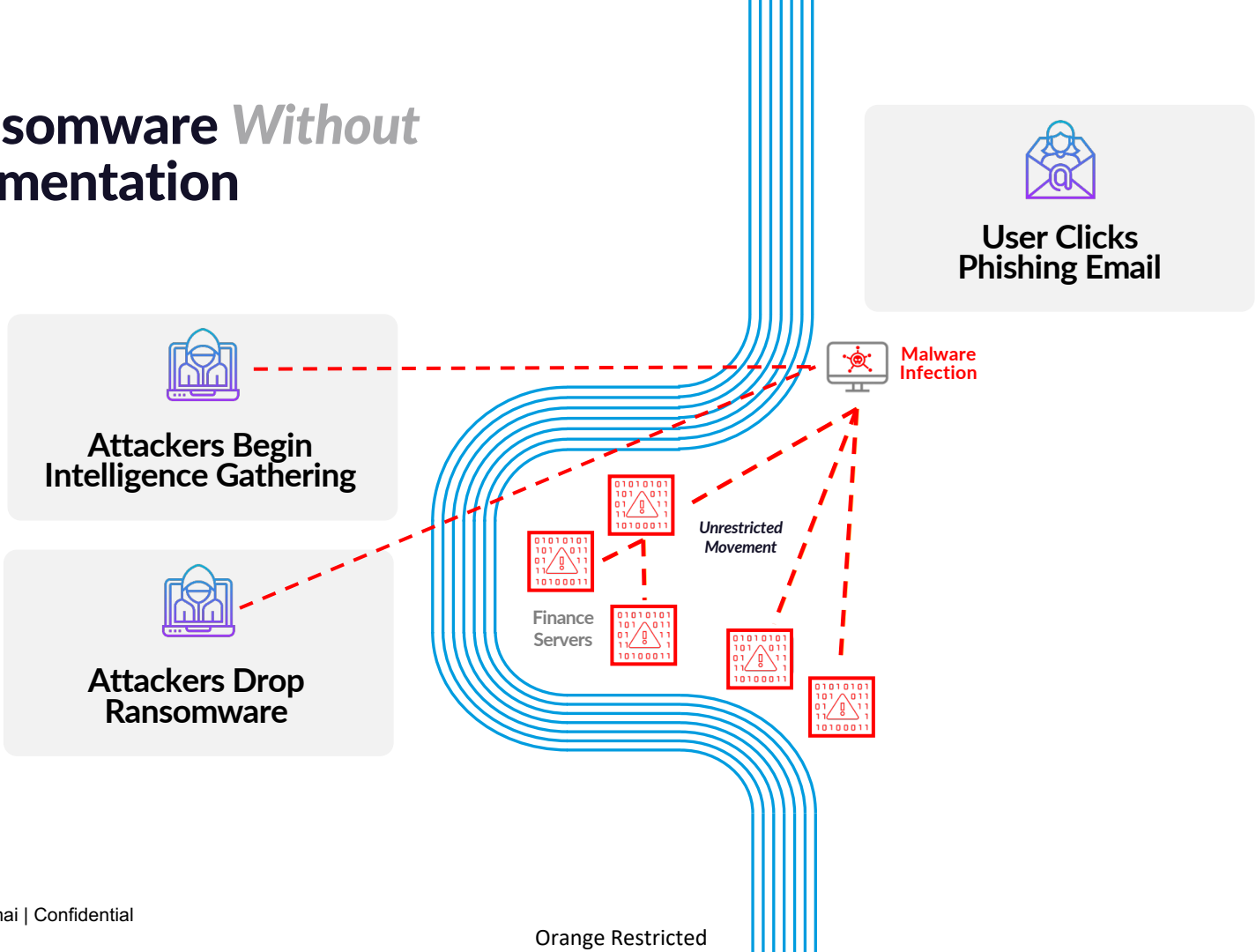
White house

Executive Order on Improving the Nation's Cybersecurity

Usecases

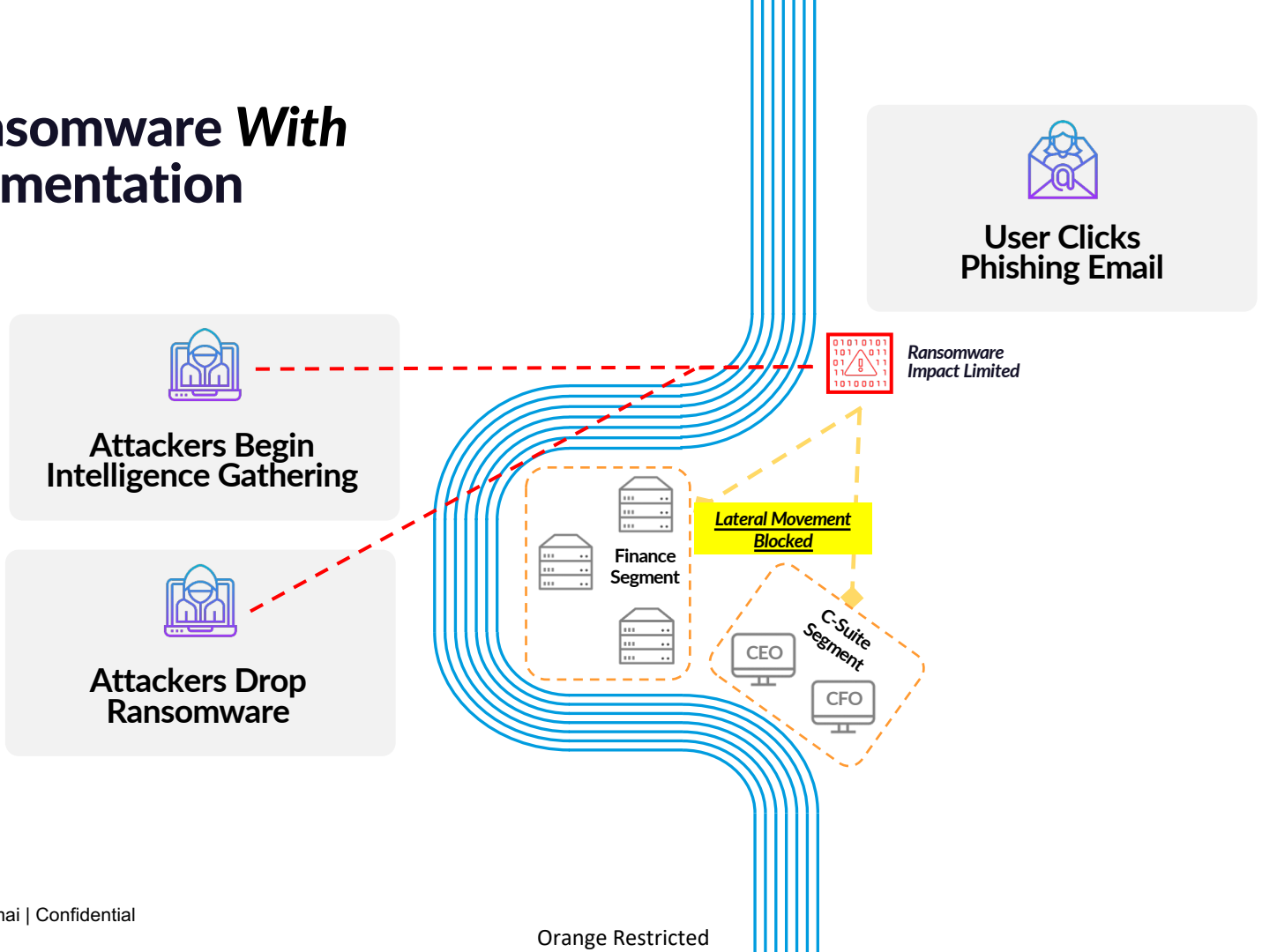


Ransomware *Without* Segmentation



Orange Restricted

Ransomware *With* Segmentation



Summary

Quickly Reduce Risk

Remove Network Complexity

Maintain Business Continuity


CISO after that board meeting where he shows a clear plan of risk reduction and cost savings

Thank You!