illumio

Take the fast train to NIS2 and DORA compliance with Zero Trust Segmentation

Raghu Nandakumara
Senior Director, Solutions Marketing

October 2023

Key Objectives

DORA

- **Uniform requirements concerning the security of network and information systems supporting the business processes of financial entities, including:**
  - ICT Risk Management
  - Reporting and notifying of major ICT incidents and significant cyber threats
  - Digital operational resilience testing
  - Information sharing in relation to cyber threats and vulnerabilities
  - Measures for the sound management of ICT third-party risk
- **Consistent contractual arrangements between ICT third-party service providers and financial entities for managing ICT risk**
- **Cooperation among competent authorities, and rules on supervision and enforcement by competent authorities**

NIS2

- **Increase the level of cyber-resilience** of a comprehensive set of businesses operating in the European Union across all relevant sectors, by putting in place rules that ensure that all public and private entities across the internal market, which fulfil important functions for the economy and society as a whole, are required to take adequate cybersecurity measures.
- **Reduce inconsistencies in resilience** across the internal market in the sectors already covered by the directive, by further aligning i) the de facto scope; ii) the security and incident reporting requirements; iii) the provisions governing national supervision and enforcement; and iv) the capabilities of the Member States' relevant competent authorities.
- **Improve the level of joint situational awareness** and the collective capability to prepare and respond, by i) taking measures to increase the level of trust between competent authorities; ii) by sharing more information; and iii) setting rules and procedures in the event of a large-scale incident or crisis.


Helping organisations maintain services while under attack
illumio


Contain cyber attacks to prevent access to high value assets
illumio

Implementation Timelines

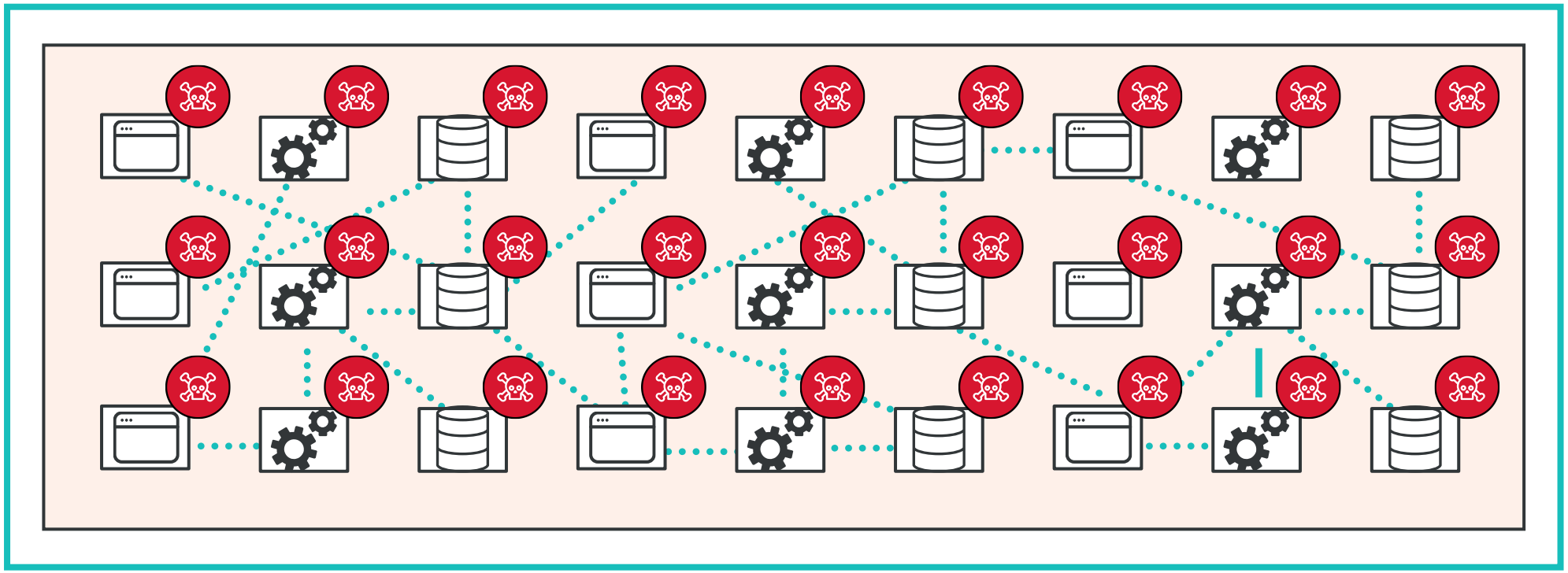
DORA

- **September 2020**: the European Commission published its draft Digital Operational Resilience Act (DORA) as part of the Digital Finance Package (DFP).
- **November 2022:** The European Council adopted DORA
- **January 2023**: DORA entered into force on 16 January 2023.
- **Early 2024**: Multiple regulatory and implementing technical standards are defined and issued by the ESAs. They provide entities with specifications and guidance on how to implement specific DORA requirements.
- **January 2025**: Financial entities will be expected to be compliant with DORA..

NIS2

- NIS 2 is the updated version of the 2016 Network and Information Systems directive
- Like the 2016 NIS directive the specifics for each state are defined by and enforced by the local regulator
- NIS2 needs to be drafted into law in each state by October 2024 with full compliance date set by each state.
- Proof of implementation within 4 years of coming into law – i.e. by 2028.
- Continuous validation every 2 years from there onwards.

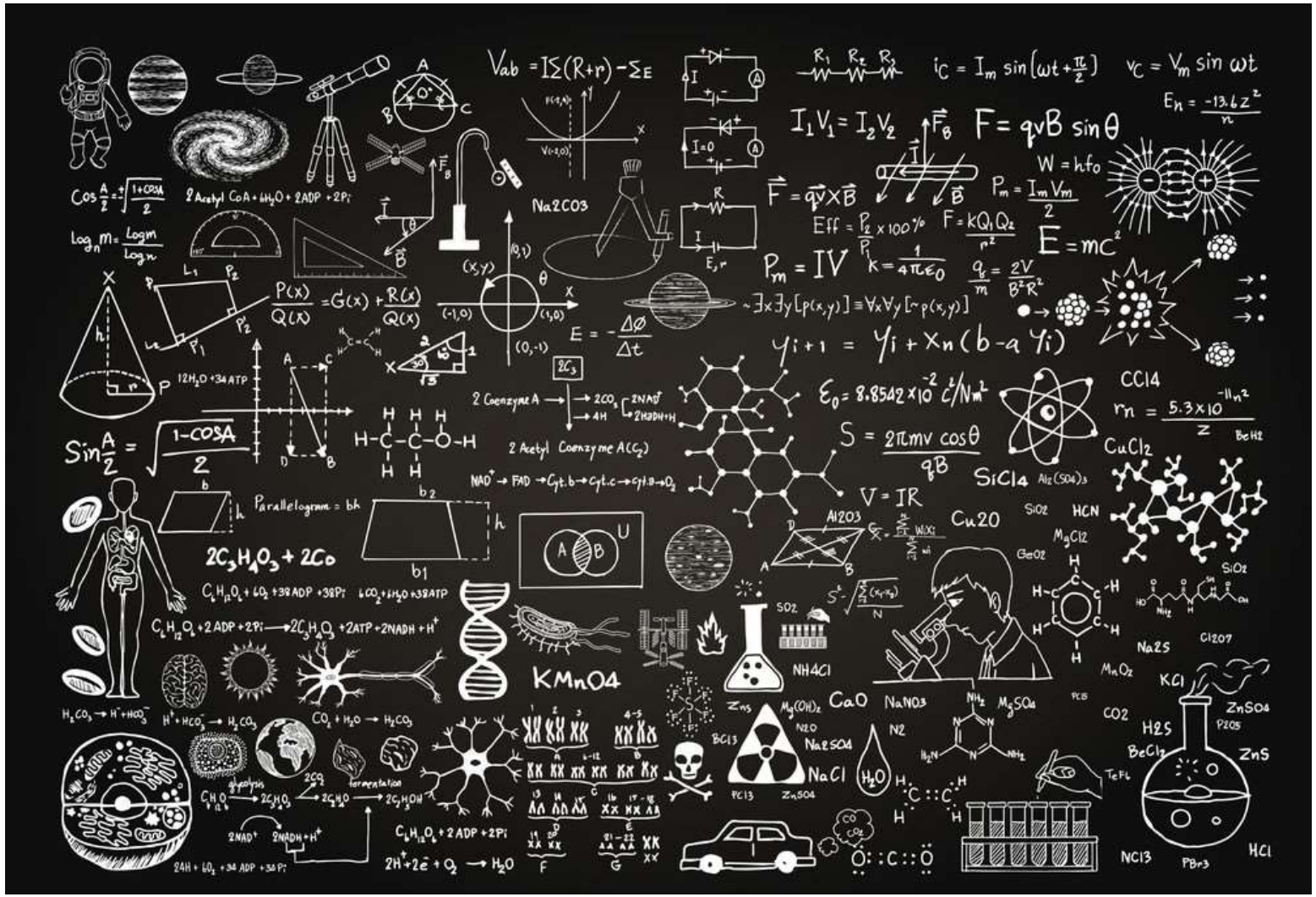
Lateral Movement Reduces Resilience



Use Zero Trust Segmentation to Provide Least Privilege Access to Assets

illumio

Where to Start with Zero Trust?



What is Zero Trust?

"an evolving set of cybersecurity paradigms that move defences from static, network-based perimeters to focus on users, assets, and resources."

National Institute for Standards & Technology (NIST)

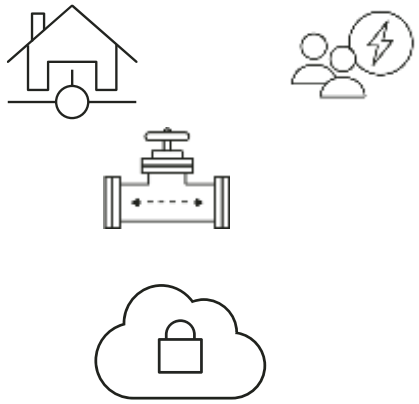
Zero Trust changes the security paradigm.

Instead of trying to identify thousands of **bad** things and stopping them.

Identify the few **good** things and allow them.

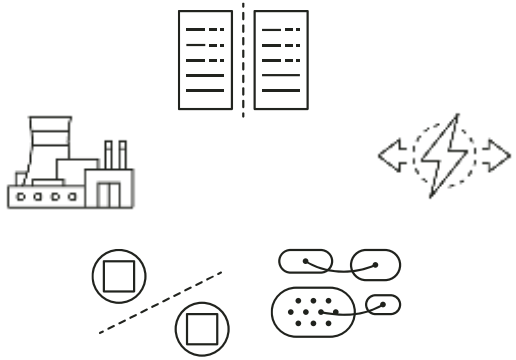
Zero Trust Taxonomy

Zero Trust Network Access



Next generation perimeter to securely identify and verify connectivity based on identity

Zero Trust Segmentation

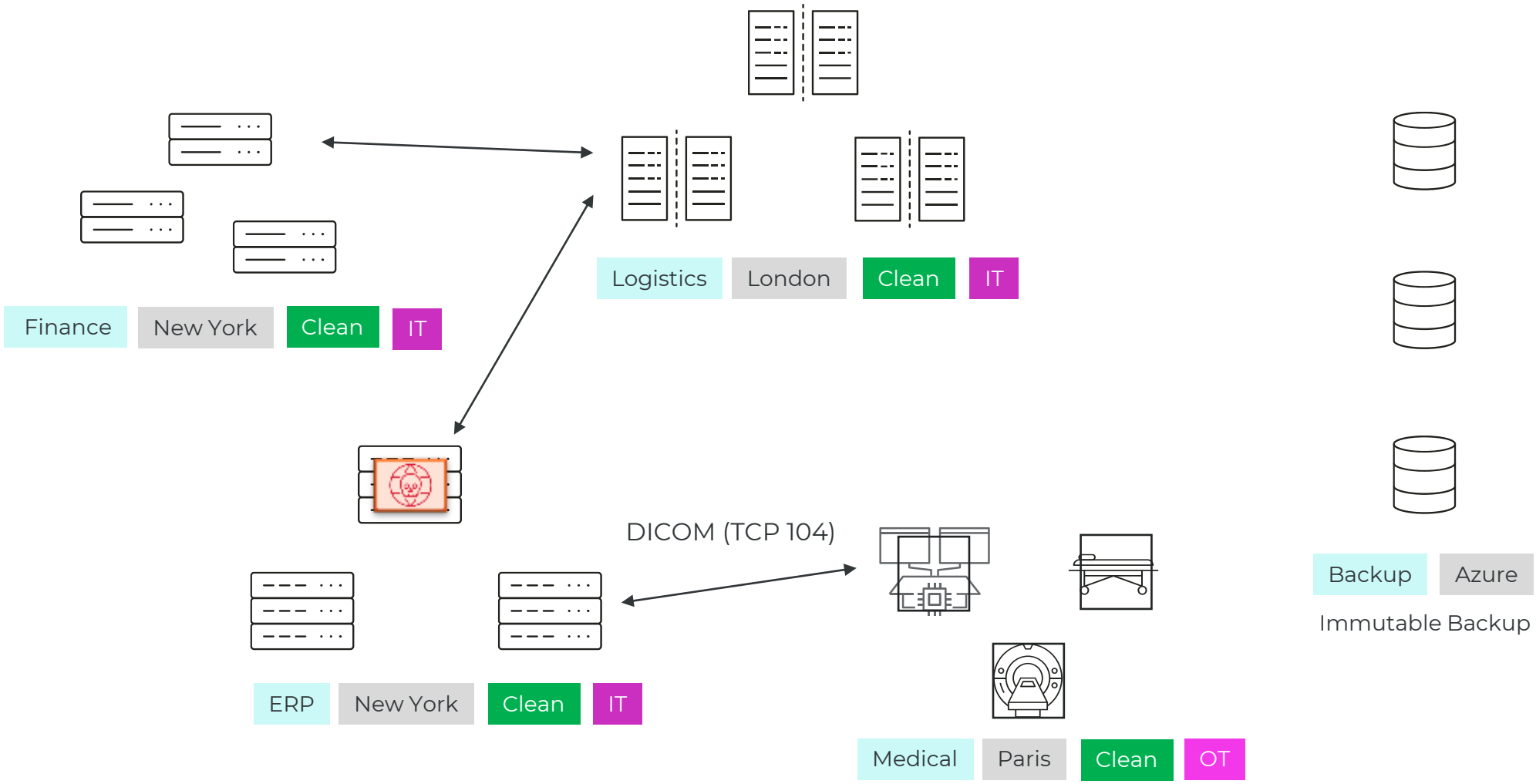


Mapping interdependencies and separating applications, IT & OT systems

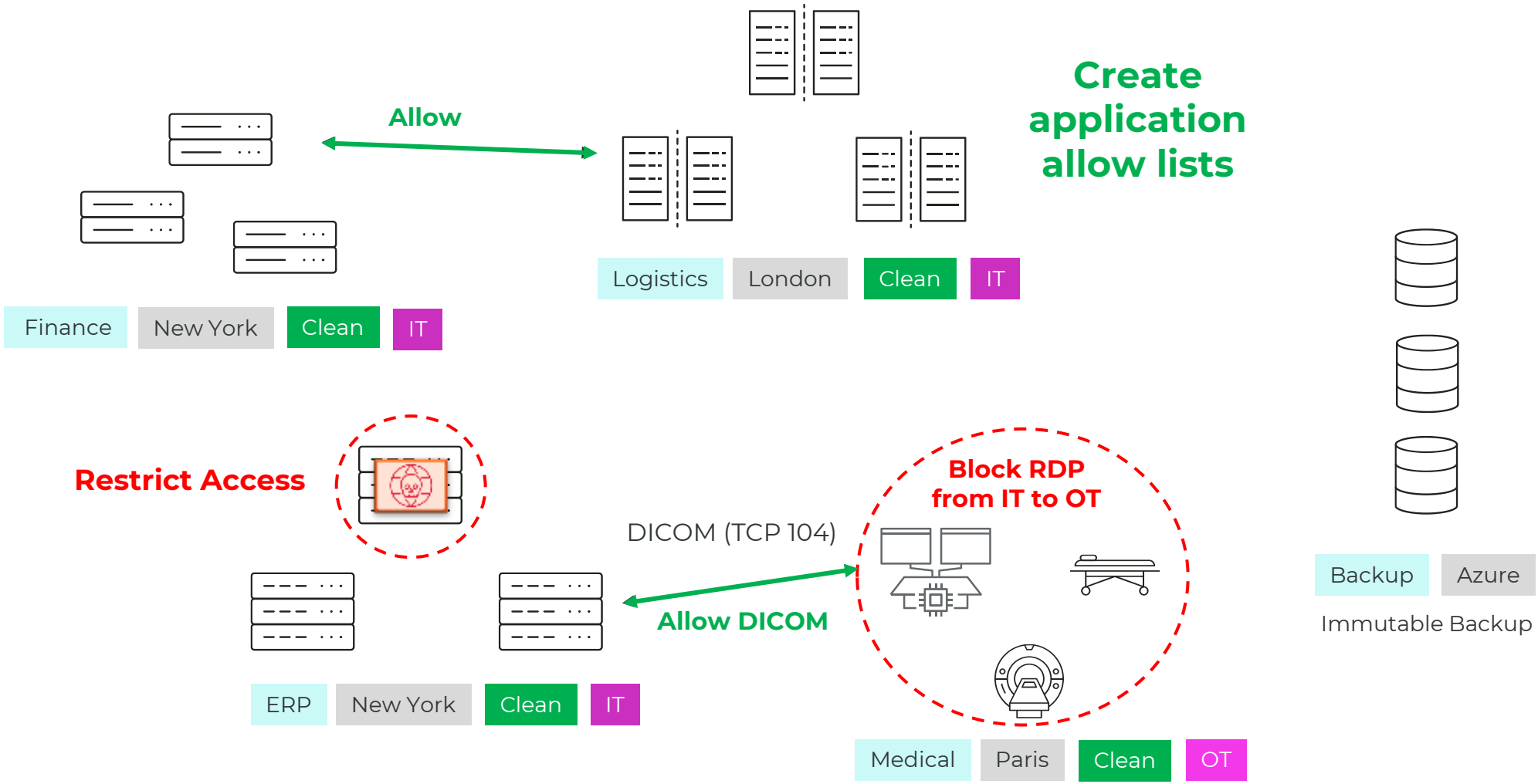
Zero Trust Data Security

Reliable and dependable data backup and restoration

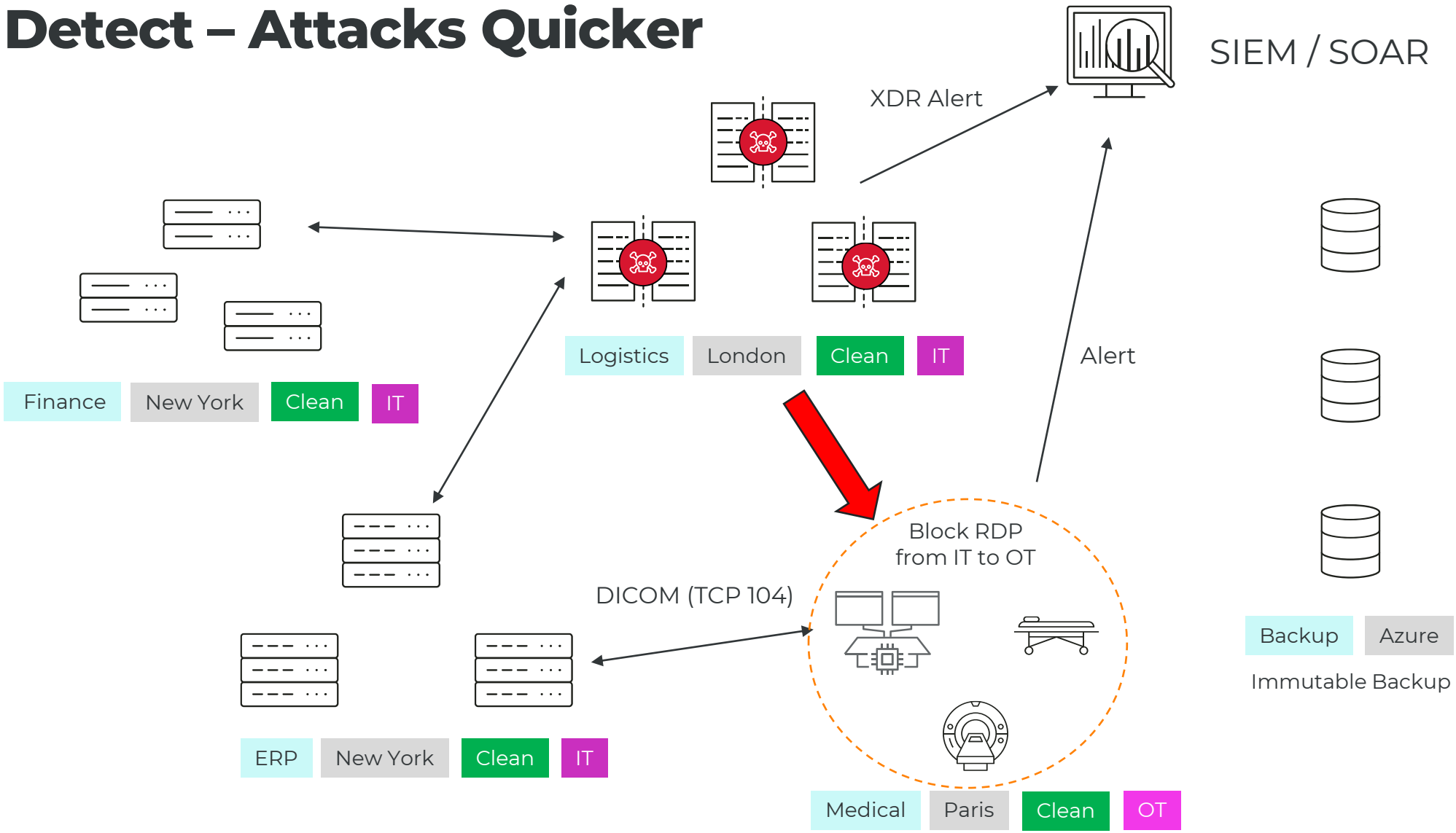
Identify – Assets, Vulnerabilities & Connections



Protect - Drastically Reduce the Attack Surface

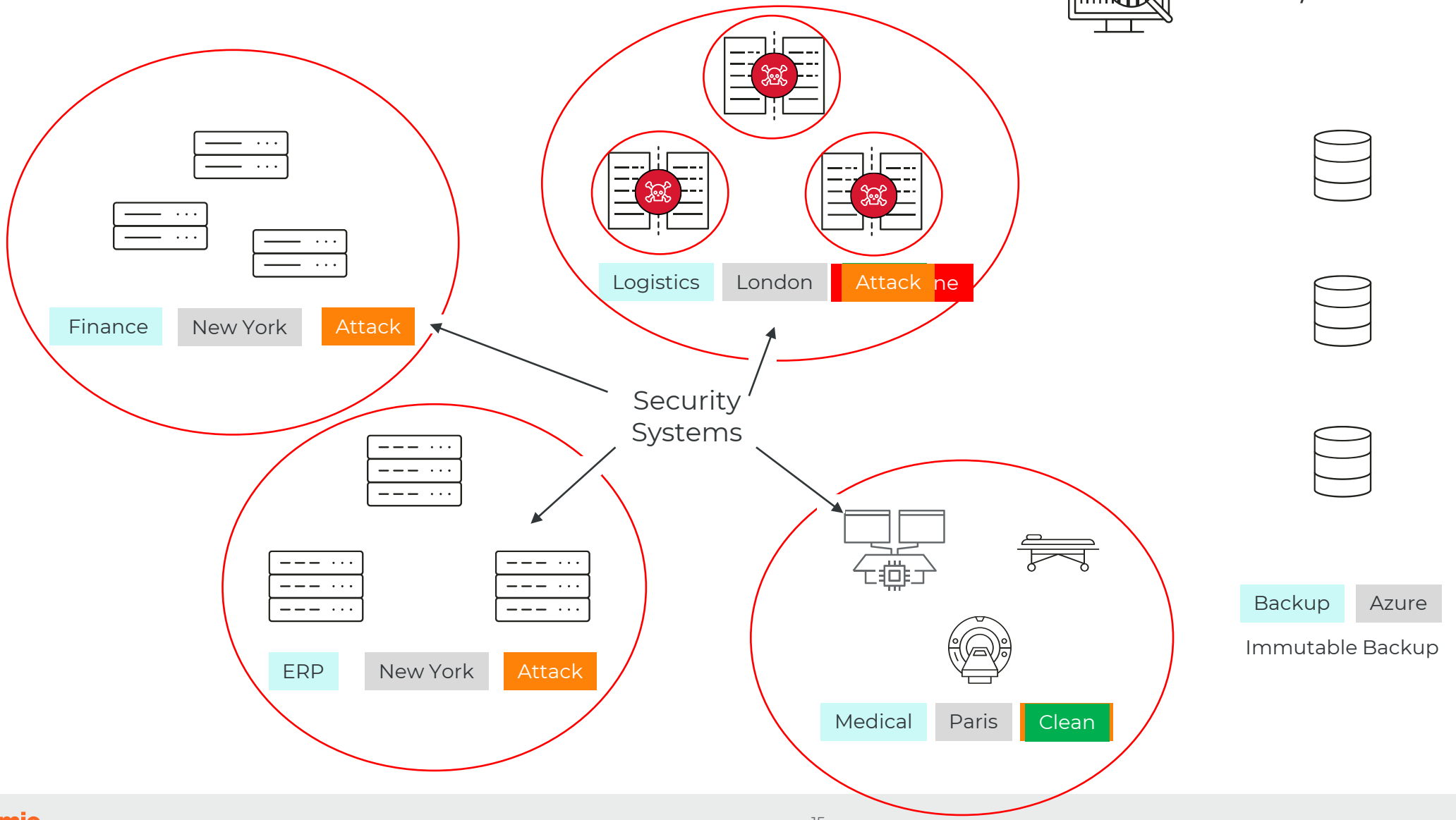


Detect – Attacks Quicker



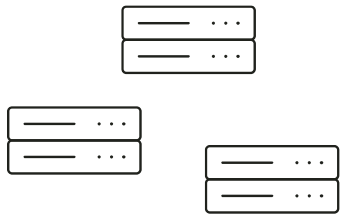
Respond – Contain Instantly

SEIM / SOAR

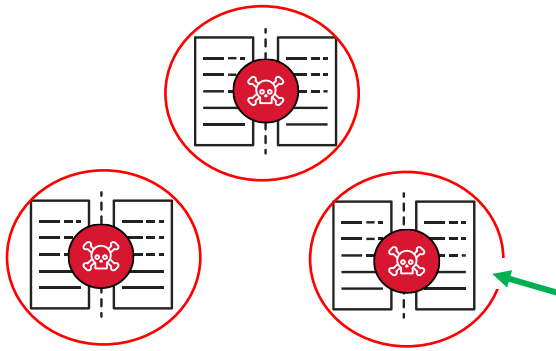


Recover - Securely

SEIM / SOAR

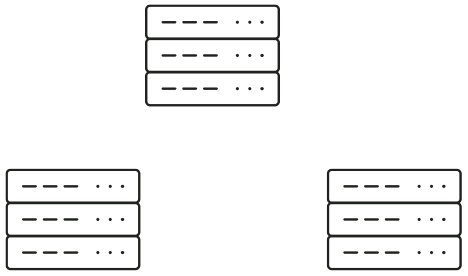


Finance | New York | Clean

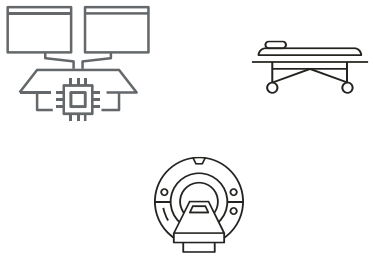


Logistics | London | Clean

NDMP



ERP | New York | Clean

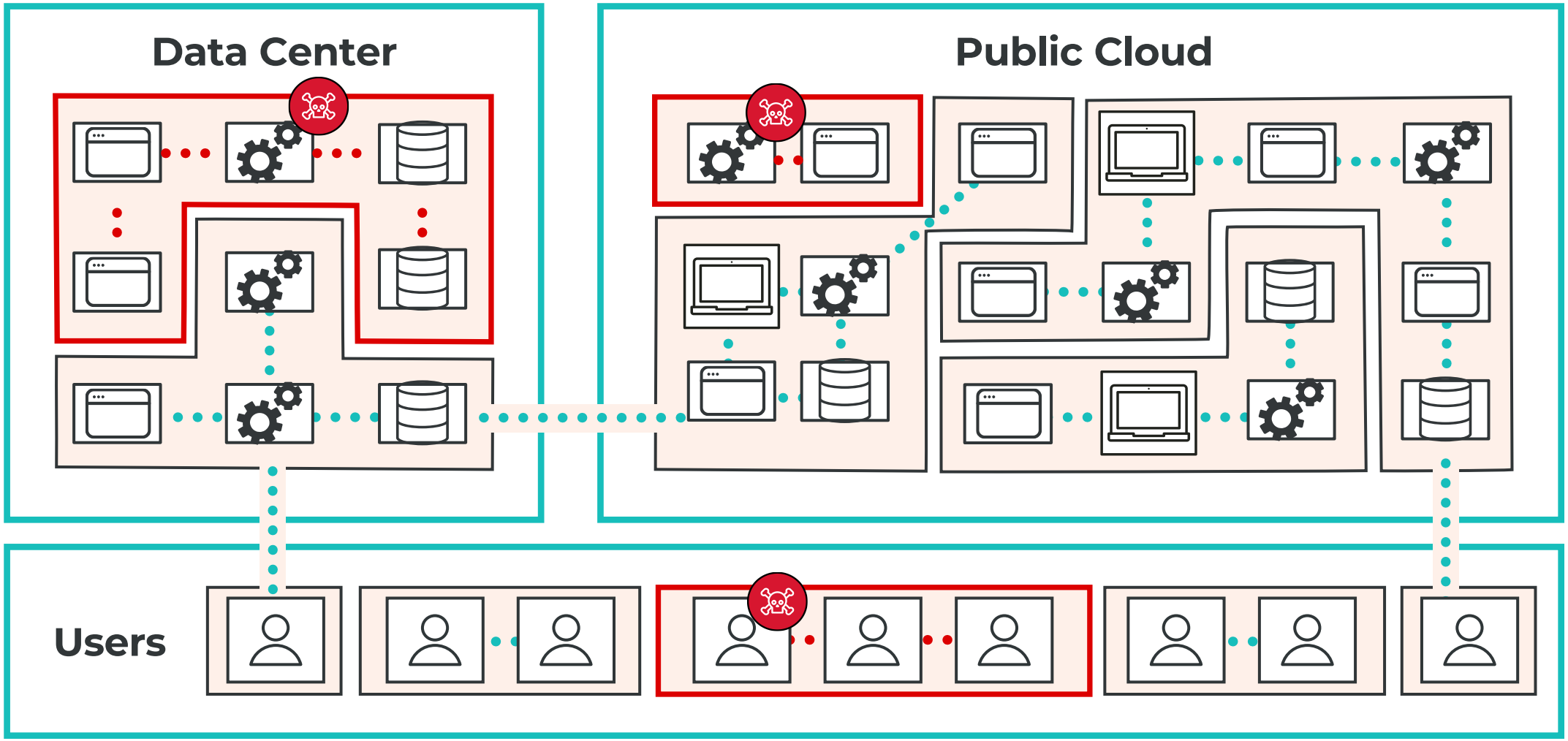


Medical | Paris | Clean

Backup | Azure

Immutable Backup

Maintaining Services



Key Objectives - recap

DORA

- **Uniform requirements concerning the security of network and information systems supporting the business processes of financial entities, including:**
  - ICT Risk Management
  - Reporting and notifying of major ICT incidents and significant cyber threats
  - Digital operational resilience testing
  - Information sharing in relation to cyber threats and vulnerabilities
  - Measures for the sound management of ICT third-party risk
- **Consistent contractual arrangements between ICT third-party service providers and financial entities for managing ICT risk**
- **Cooperation among competent authorities, and rules on supervision and enforcement by competent authorities**

NIS2

- **Increase the level of cyber-resilience** of a comprehensive set of businesses operating in the European Union across all relevant sectors, by putting in place rules that ensure that all public and private entities across the internal market, which fulfil important functions for the economy and society as a whole, are required to take adequate cybersecurity measures.
- **Reduce inconsistencies in resilience** across the internal market in the sectors already covered by the directive, by further aligning i) the de facto scope; ii) the security and incident reporting requirements; iii) the provisions governing national supervision and enforcement; and iv) the capabilities of the Member States' relevant competent authorities.
- **Improve the level of joint situational awareness** and the collective capability to prepare and respond, by i) taking measures to increase the level of trust between competent authorities; ii) by sharing more information; and iii) setting rules and procedures in the event of a large-scale incident or crisis.

illumio

Thank you

Visit our stand: Halle 7 - Standnummer 7-539

Check out our DORA blog: https://www.illumio.com/blog/dora-what-you-need-to-know

Read our NIS2 Solution Brief: https://www.illumio.com/resource-center/nis2-compliance