WAVESTONE

Security in 2025: how to adapt your approach to cope with full-cloud and agile-at-scale

Mike NEWLOVE
mike.newlove@wavestone.com

Gérôme BILLOIS
gerome.billois@wavestone.com
@gbillois

Florian POUCHET
florian.pouchet@wavestone.com
@poulti

In a world where permanent evolution is key to success, we enlighten and partner with business leaders through their most critical decisions

Tier one clients leaders in their industry

2,800 professionals across 8 countries

Among the leading independent consultancies in Europe

BUSINESS FUNCTIONS

Strategy

Innovation management & funding

Marketing, sales & customer experience

People & change

Finance, risk & procurement

Operations & supply chain

INDUSTRIES

Financial services

Telecom, media & entertainment

Consumer goods & retail

Manufacturing

Energies & utilities

Transportation & travel

Real estate

Public sector & international institutions

TECHNOLOGY

Digital & IS strategy

Digital & emerging technologies

IT & data architecture

Cybersecurity & digital trust

Paris | London | New York | Hong Kong | Singapore* | Dubaï* | São Paulo*
Luxembourg | Madrid* | Milano* | Brussels | Geneva | Casablanca | Istanbul*
Lyon | Marseille | Nantes

* Partners

Cybersecurity & Digital Trust practice

Building digital trust in your organisation is an essential enabler for success in the race for digital transformation

Examples of our engagements…

One international team of 500+ consultants

/ International cyber-crisis management exercise (6 countries, 80+ participants, over 11 hours)

High-level view to deep expertise

/ Cyber-framework definition and oversight on a £800m cybersecurity programme

/ Definition of APIs security governance and implementation of token generation platform

Outcomes focused

/ TOM design and change management for DevSecOps at scale

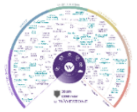
Independence

/ Support for RFP processes for selection of SOC MSSP, EDR, xAST, PAM, IAM, etc.

Some of our unique assets…

CERT-Wavestone

AMT Methodology



CISO Radar

Start-ups Radar

Many and various R&D projects with results shared at international conferences

2017: DEF CON, Black Hat Europe, BruCON, HTIB, BsidesLV…

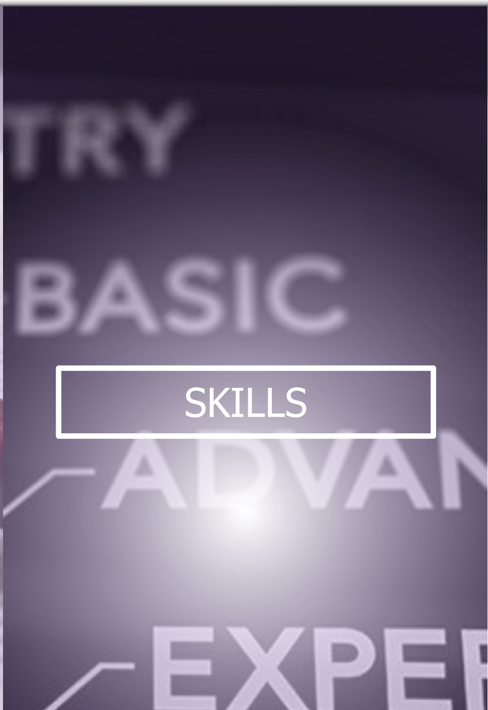
2018: DEF CON, HITB, GreHack, Bsides Lisbon…

Let’s *state* THE OBVIOUS

CONNECTIVITY

THREAT

REGULATIONS

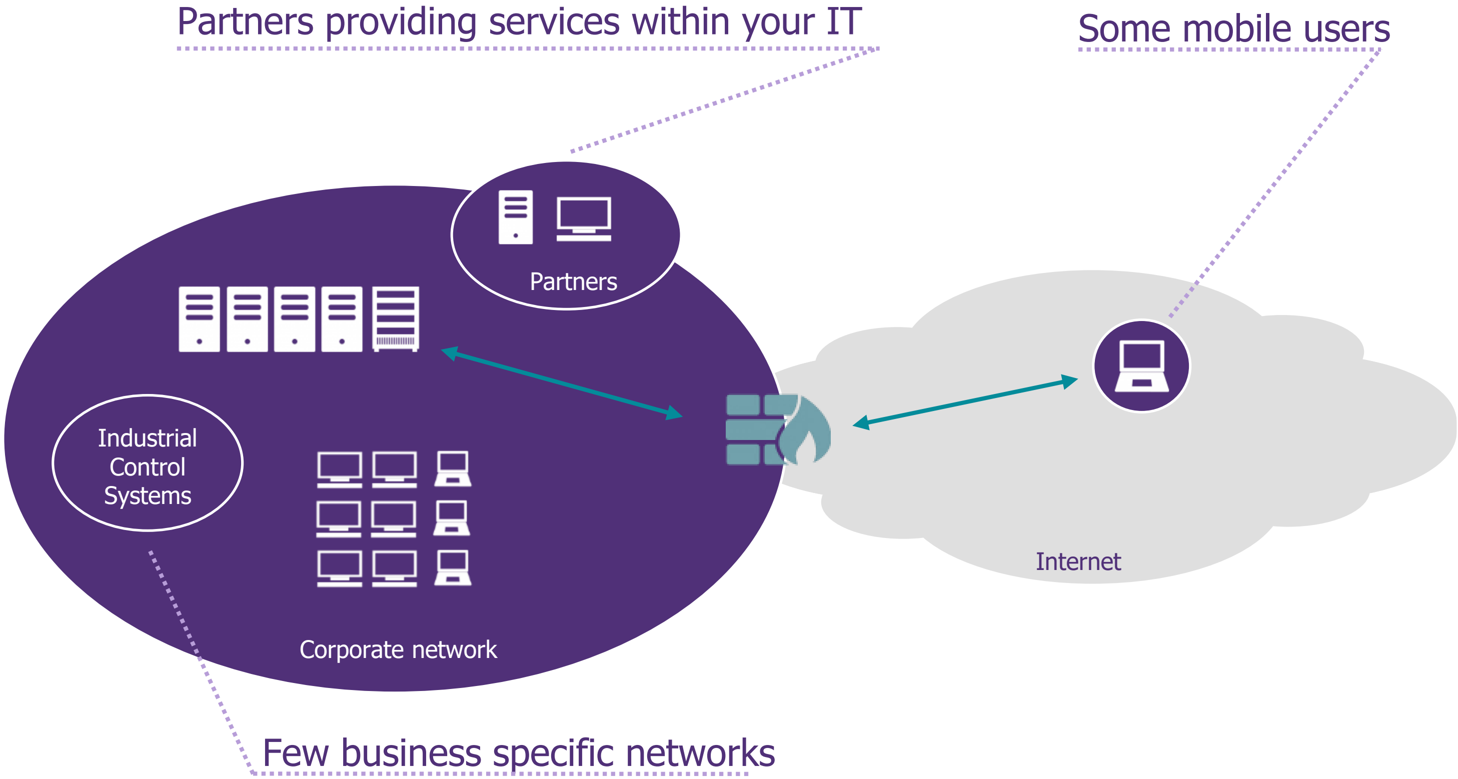


SKILLS

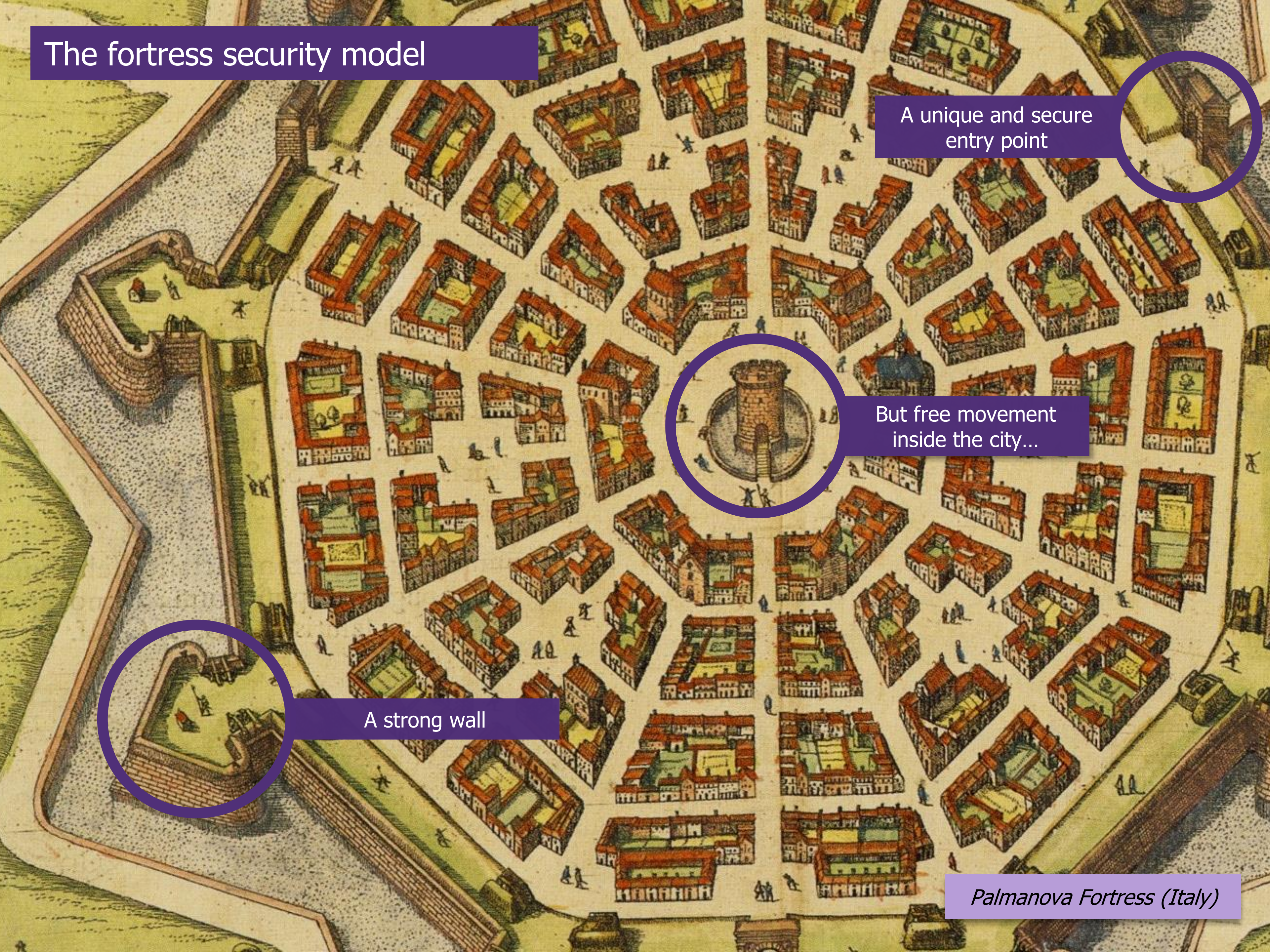
What *we have done* **SO FAR**

PREVIOUS SECURITY MODEL

1995 - 2005: A centralised IT estate


Partners providing services within your IT
Some mobile users
Partners
Industrial Control Systems
Internet
Corporate network
Few business specific networks

The fortress security model



A unique and secure entry point

But free movement inside the city…

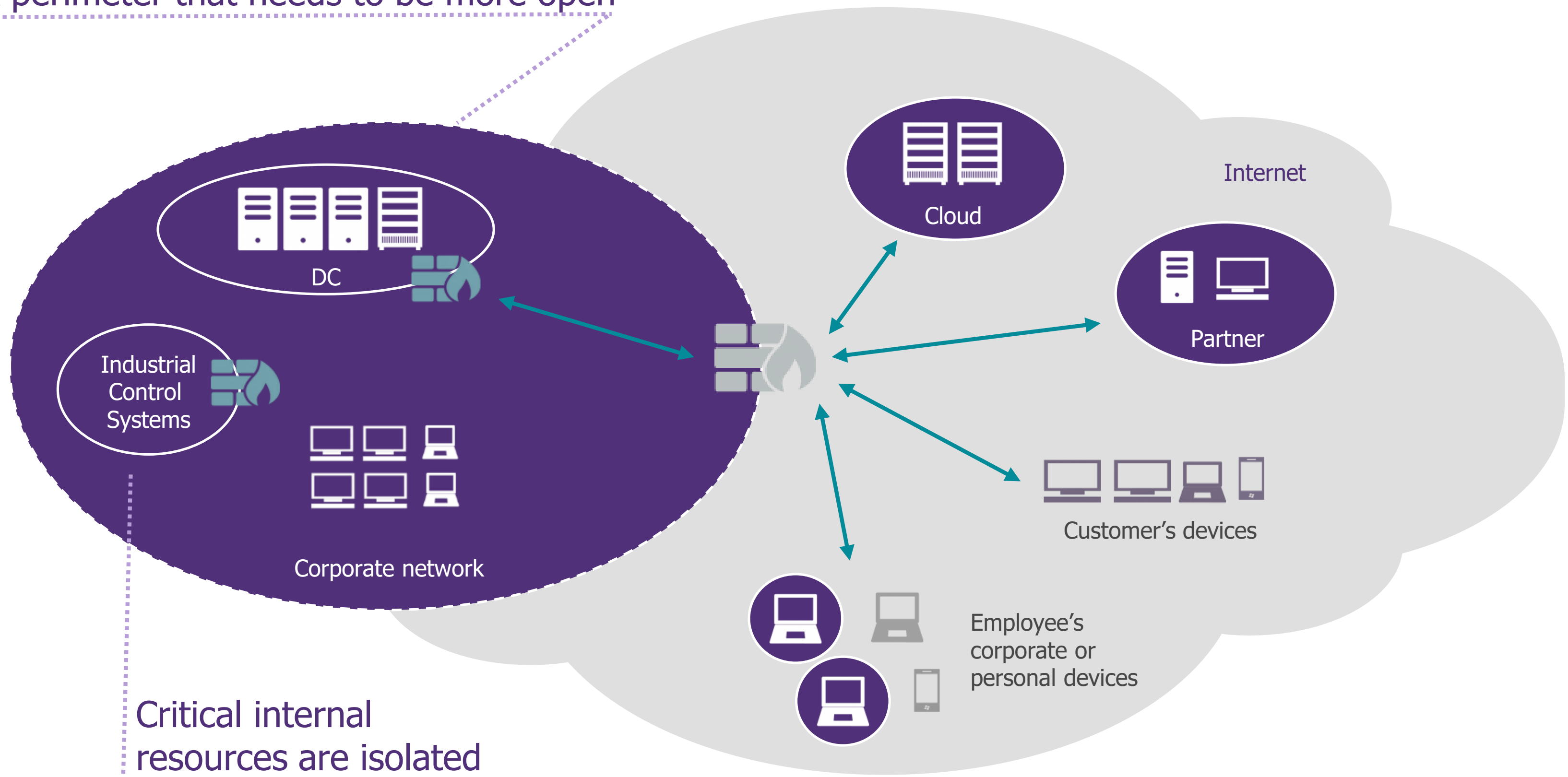
A strong wall

Palmanova Fortress (Italy)

PREVIOUS SECURITY MODEL

2005-2015: An increasingly open IT estate

A perimeter that needs to be more open


DC
Industrial Control Systems
Corporate network
Cloud
Internet
Partner
Customer's devices
Employee's corporate or personal devices

Critical internal resources are isolated and tightly secured

The Airport security model

Additional controls to reach the aircrafts

Critical zones are highly controlled

Airport hall is open by default

Gatwick Airport (UK)

Why *we need to* CHANGE

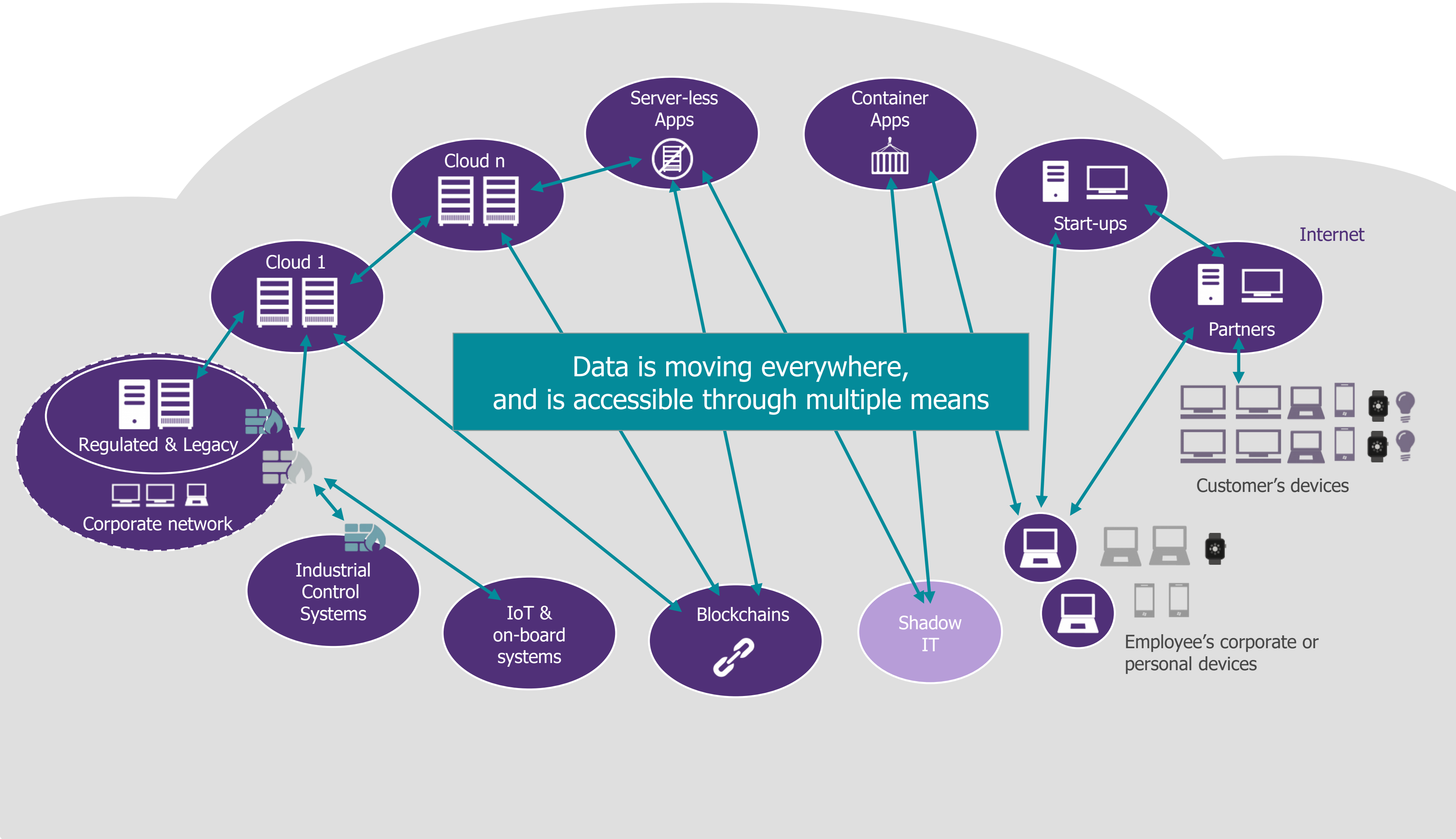
Towards 2025

Cloud is a reality,
even for critical
business applications

Agile methods and
DevOps are a reality

**Current security approaches
aren’t keeping pace with this new paradigm**

Towards 2025: a decentralised IT estate



A new model

With data everywhere

With apps executed by many third parties

Where you keep the responsibility to detect incidents and respond globally

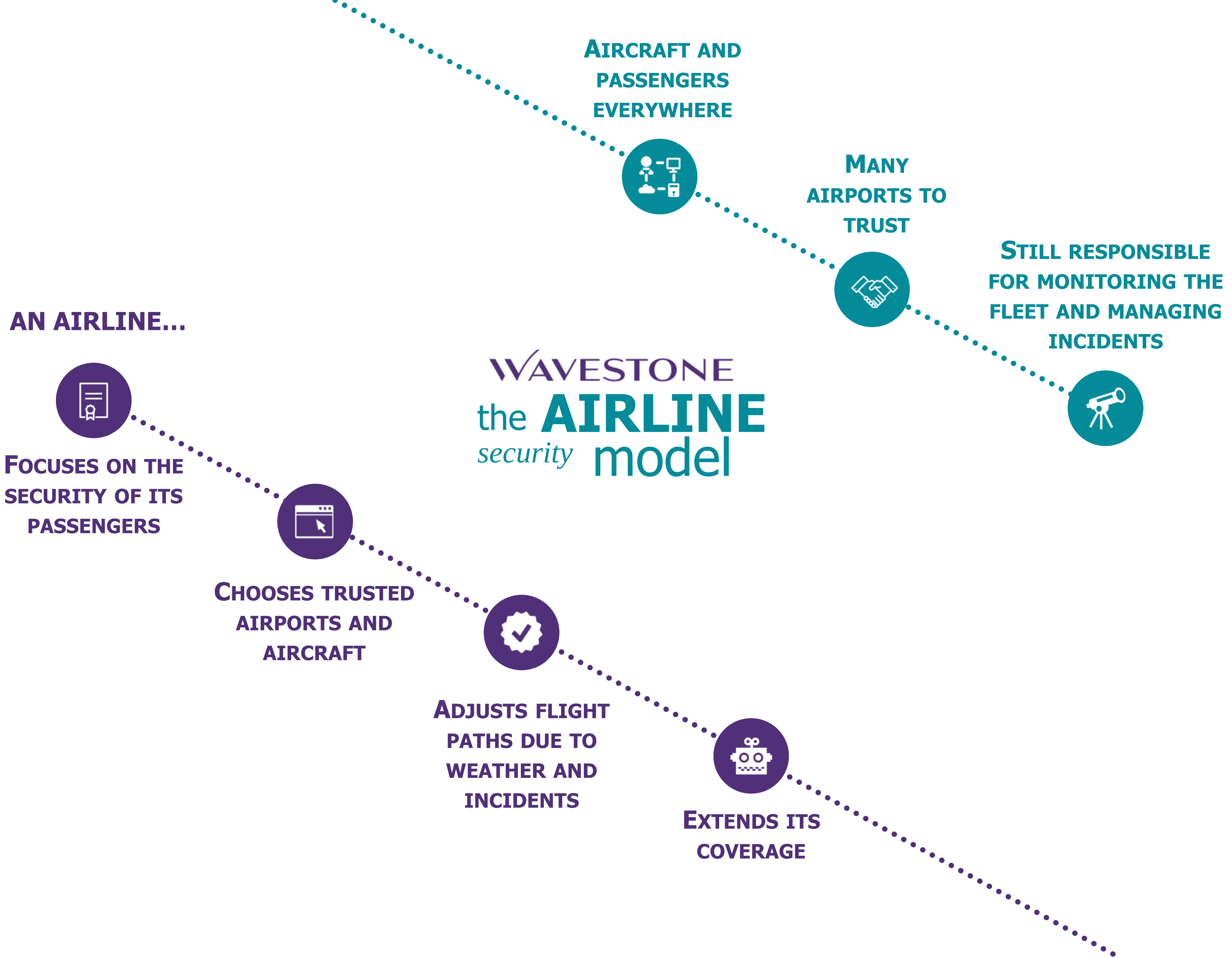
A new security model: the Airline

With aircraft and passengers everywhere

Where you trust an airport to manage your passengers and your aircraft

Where your operations centre monitors your fleet and manages incidents and crises

Embrace *the* AIRLINE MODEL



WAVESTONE

the AIRLINE *security* model

AN AIRLINE…

Focuses on the security of its passengers

Chooses trusted airports and aircraft

Adjusts flight paths due to weather and incidents

Extends its coverage

Aircraft and passengers everywhere

Many airports to trust

Still responsible for monitoring the fleet and managing incidents

1 An airline focuses on the security of its passengers

1 Focus on **critical & regulated assets**

Identify key assets and data

- Ask your senior management and lawyers for the TOP 10
- Empower the business with the ability to identify sensitive data (user-based labelling, etc.)

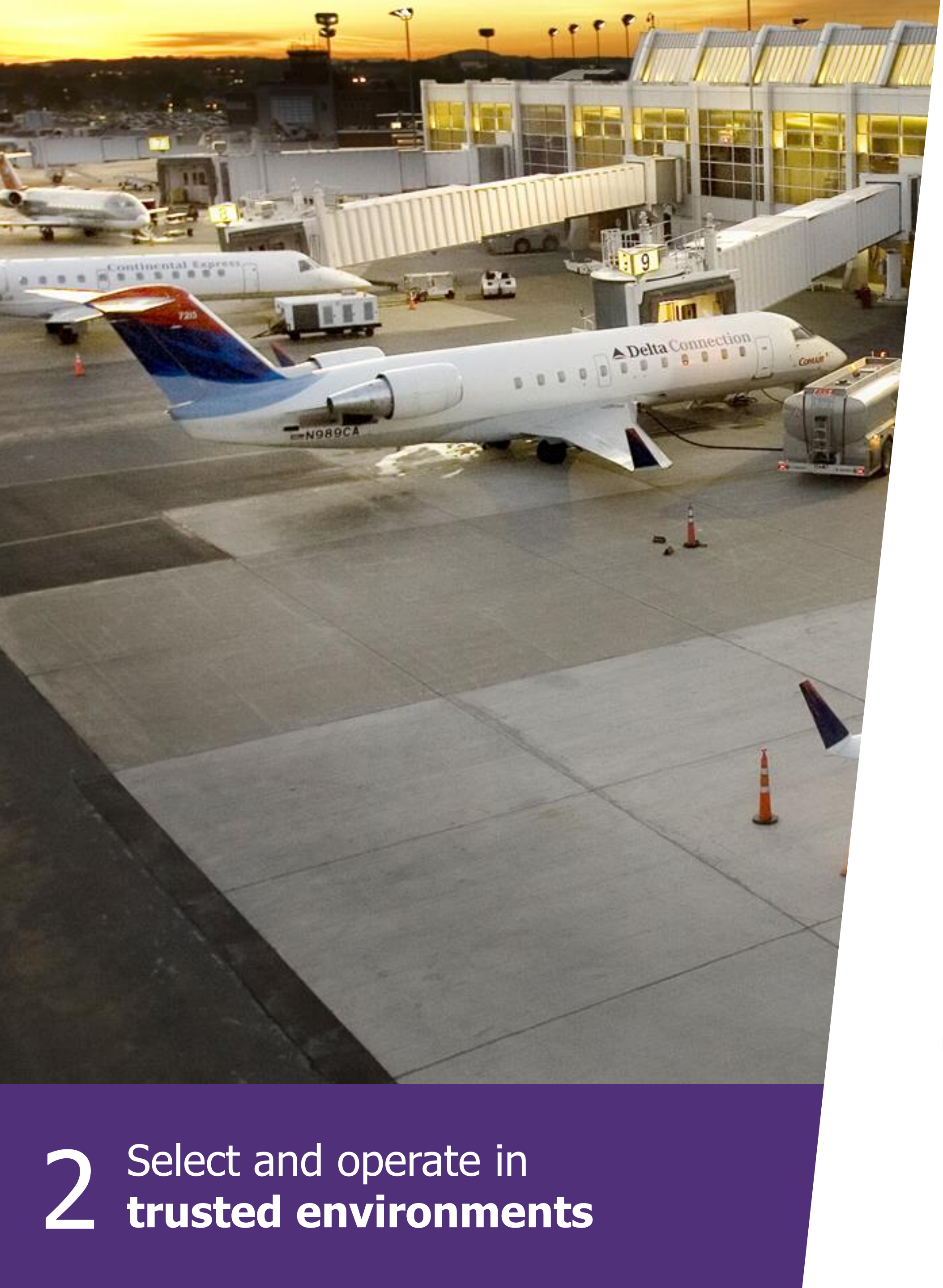
Anticipate and understand security regulations

- Build a regulation champion and watch cell
- Facilitate regulatory compliance by adapting your current projects

Protect your data closely as possible

- Enforce protection automatically measures on labelled data (eDRM, etc.)
- Take control of the generation and lifecycle management of encryption keys (CertaaS, KMS, Blockchain trust services, etc.)

2 An airline chooses trusted airports and aircraft



2 Select and operate in **trusted environments**

Establish trust with Cloud providers

- / Assess trustworthiness with standard certifications (ISO, SOC etc.)
- / Consider CSA CCM initiatives

Build your trusted environments for applications

- / Leverage cloud providers security packages and stores (Amazon/Azure, etc.)
- / Offer an API security platform using standard protocol (token broker etc.) to enable a secure micro-service model – or use a CASB

Control and audit continuously

- / Mix red and blue: grow a Purple Team
- / Consider Bug Bounty

3 An airline adjusts flight paths due to weather and incidents

Extend identity and access management to all users and objects

/ Define API security governance framework to manager APIs lifecycle

Measure device conformity

/ Deploy conformity agents (MDM-like) on IT estate (end-point and servers alike)

Evolve your Operation Centre

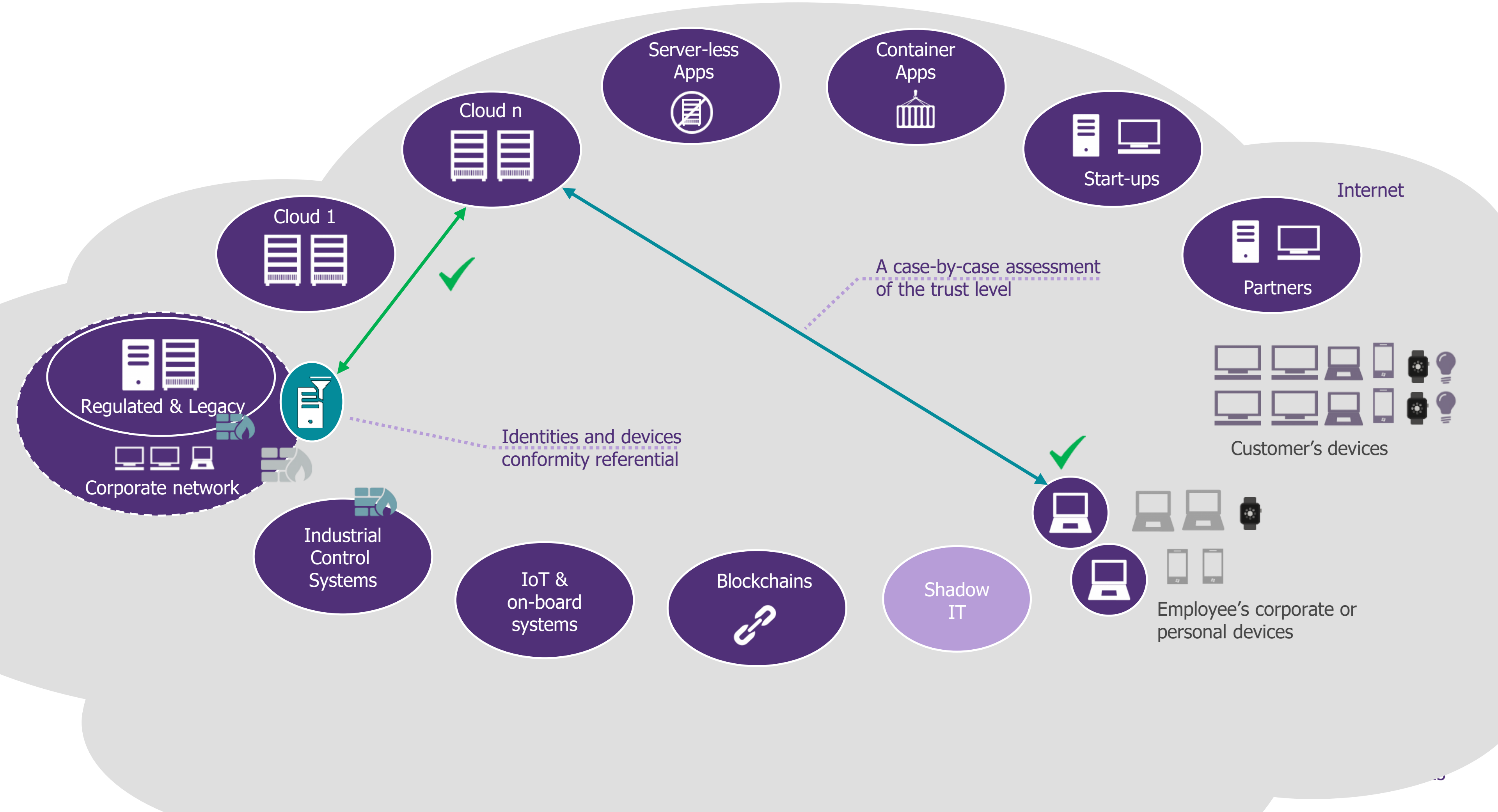
/ Fusion your usual xOC and augment it with anti-fraud-like reactivity

/ Enforce just-in-time access control based on identity, conformity, location, time, accessed data, etc. – and defined policy

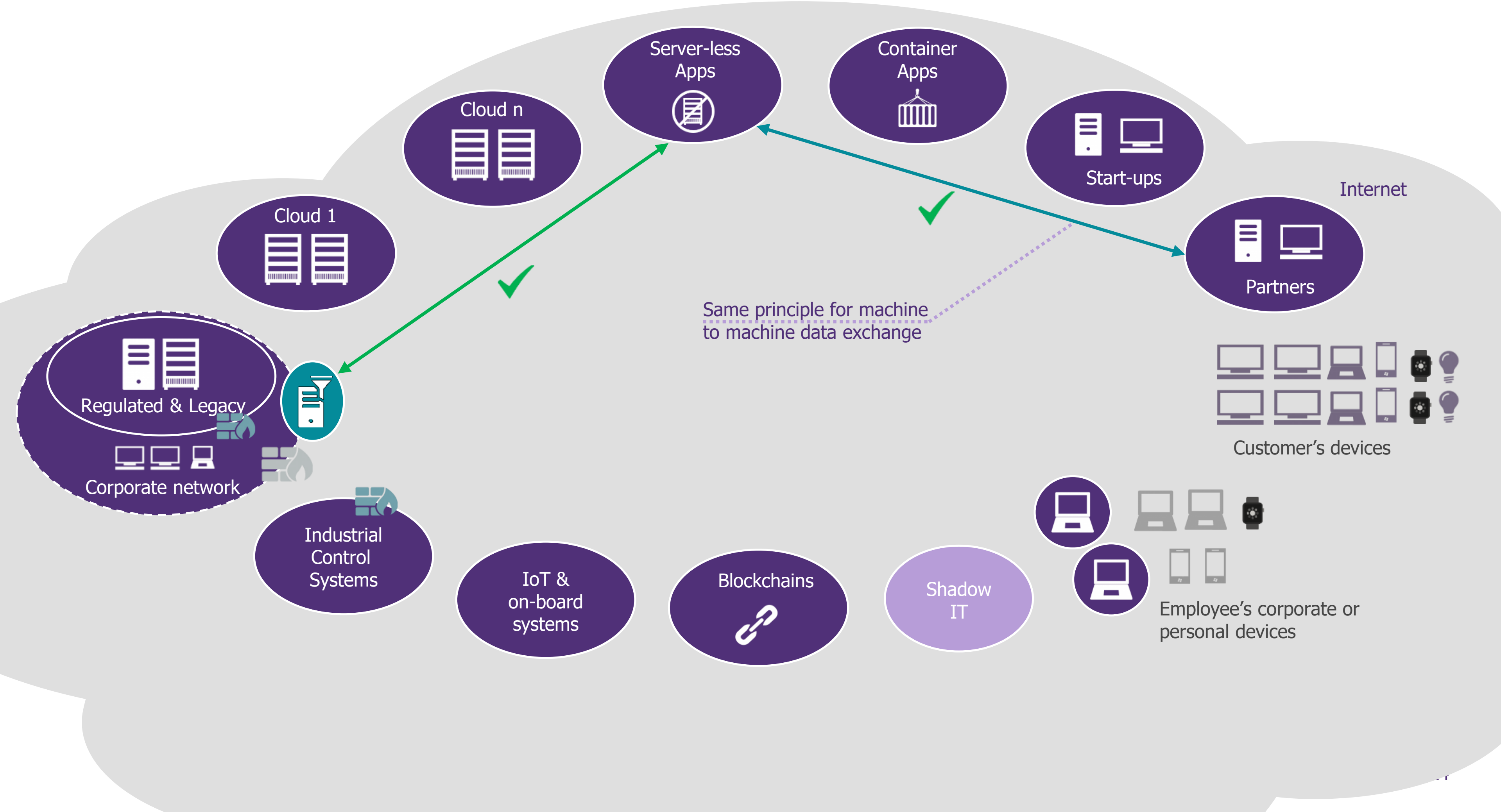
3 Protect **dynamically**

THE AIRLINE SECURITY MODEL

Applications dynamically allow processing depending on the trust level



Applications dynamically allow processing depending on the trust level



4 An airline expands its fleet and coverage

4 Scale up your operating model and automate

Move away from a consulting-based approach

/ Define and implement Agile/DevSecOps Target Operating Model and tools (security guild, evil user story, X team etc.)

Keep up with detection and response

/ Improve and automate detection (EDR, UBA, Machine/Deep Learning, etc.)

/ Improve and automate response (SOAR, etc.)

Prepare to be cyber-resilient

/ Prepare to work without IT for 10 days

/ Reinforce crisis management capabilities (backup communication tools, floodgates, etc.) – and train

/ Prepare to have what it takes to rebuild

/ Test, test and test

It’s not just a model…

We redefined the **strategy of an international bank** on

the ***airline model***

4
Years

80
Projects

£40M
Budget

WAVESTONE

the AIRLINE security model

DATA EVERYWHERE

MANY THIRD-PARTIES

RESPONSIBILITY TO DETECT INCIDENTS AND RESPOND GLOBALLY

FOCUS ON CRITICAL AND REGULATED ASSETS

ESTABLISH TRUSTED ENVIRONMENTS

PROTECT AND RESPOND DYNAMICALLY

SCALE UP YOUR OPERATING MODEL AND AUTOMATE

Mike NEWLOVE	mike.newlove@wavestone.com	
Florian POUCHET	florian.pouchet@wavestone.com	@poulti
Gérôme BILLOIS	gerome.billois@wavestone.com	@gbillois

Images credits:
www.icons8.com
www.flaticon.com