LSZ Cyber Crime Forum

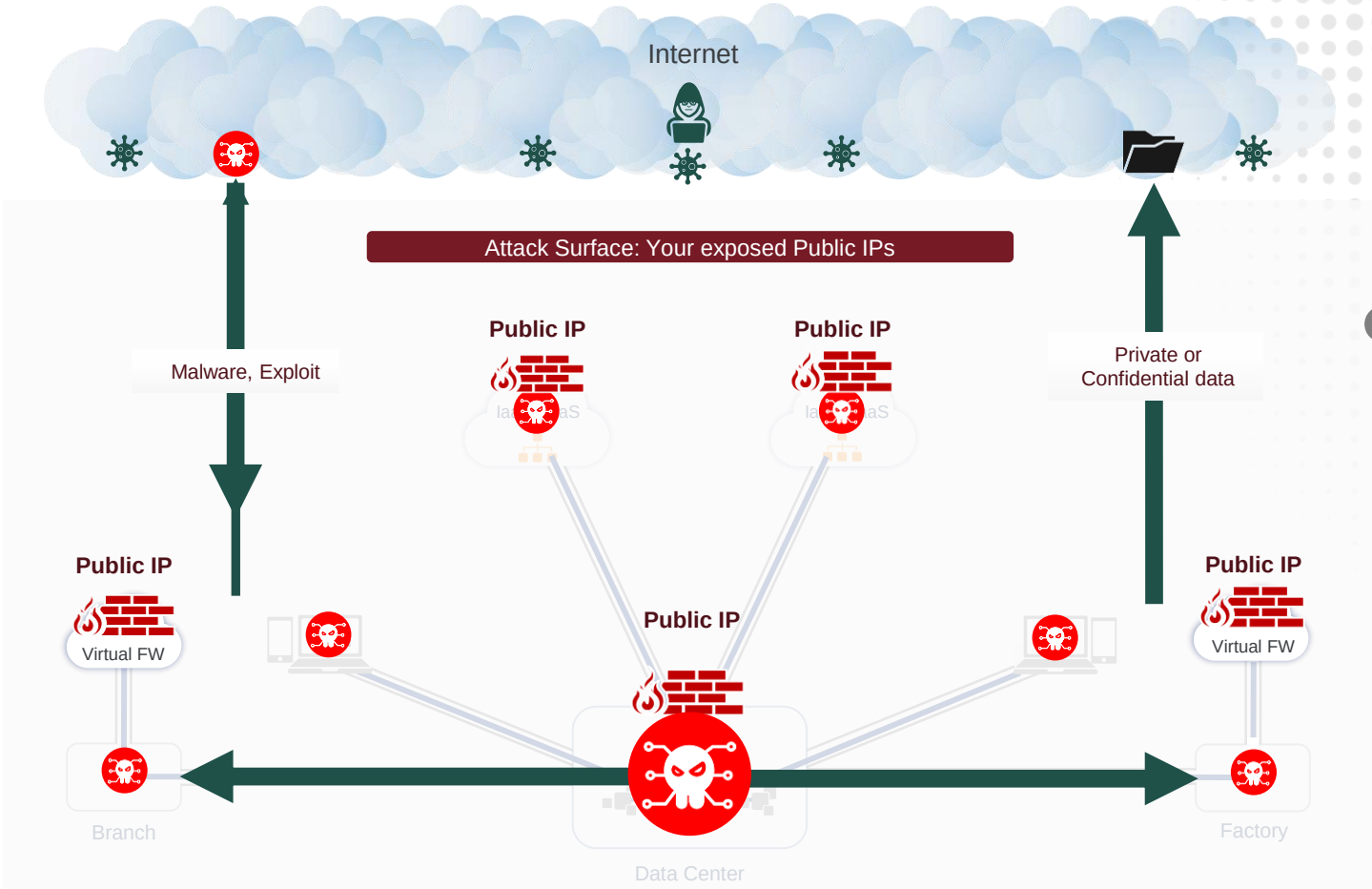
Julian Fleper – Serviceware, Senior Security Consultant
David Etzelstorfer – Zscaler, Sales Engineer

Wien, 20.06.2023

Why legacy security and networks are no longer effective

1 **They find you** your attack surface

2 **They compromise you**
Infect users, devices, workloads



4 **They steal your data**
Avoid firewall detection

Extend the Network
App access requires users and apps to be on the same network

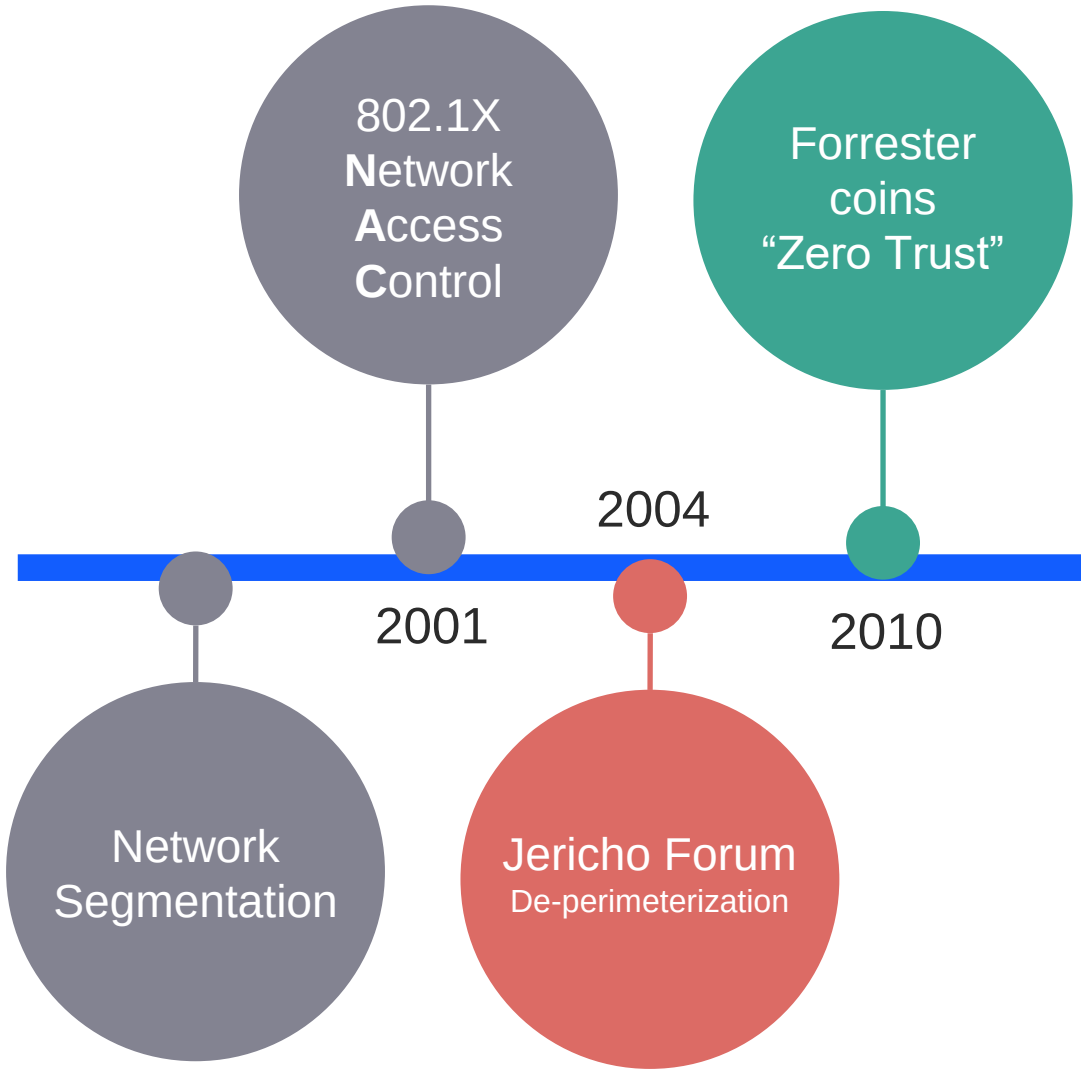
3 **They move laterally** across your routable network to find high-value targets

70% are currently rolling out or planning their zero trust security strategy

21% already have a zero trust security strategy already in place

Source: Zscaler_State of Zero Trust Transformation

“Zero Trust” was Born



Moved auth and security inline

Segmentation of sessions

Moved the perimeter to inside the network

Still focused on network access

Formalising Trust as a Computational Concept

Stephen Paul Marsh

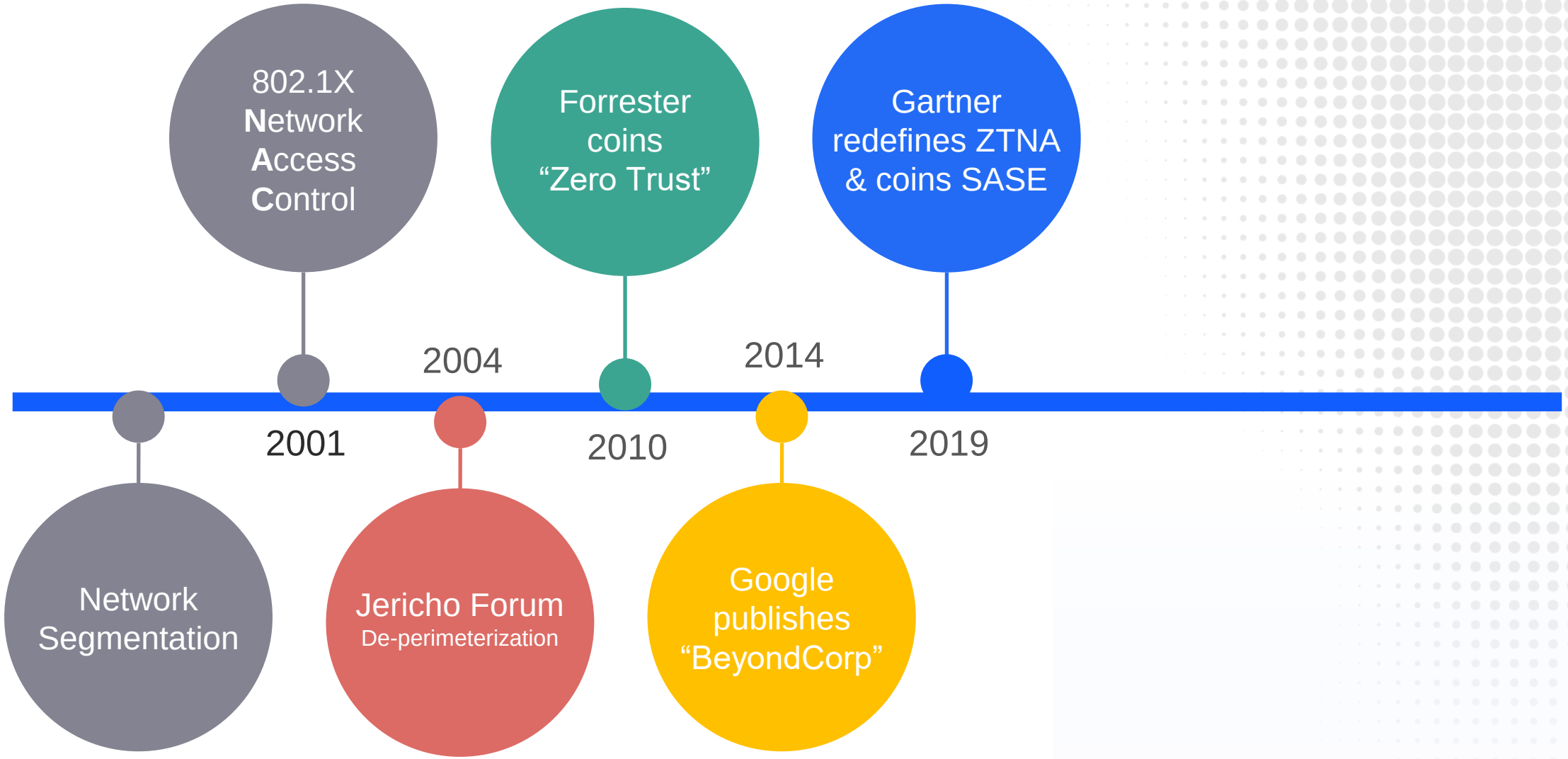
Department of Computing Science and Mathematics

University of Stirling

Submitted in partial fulfilment of
the degree of Doctor of Philosophy

April 1994

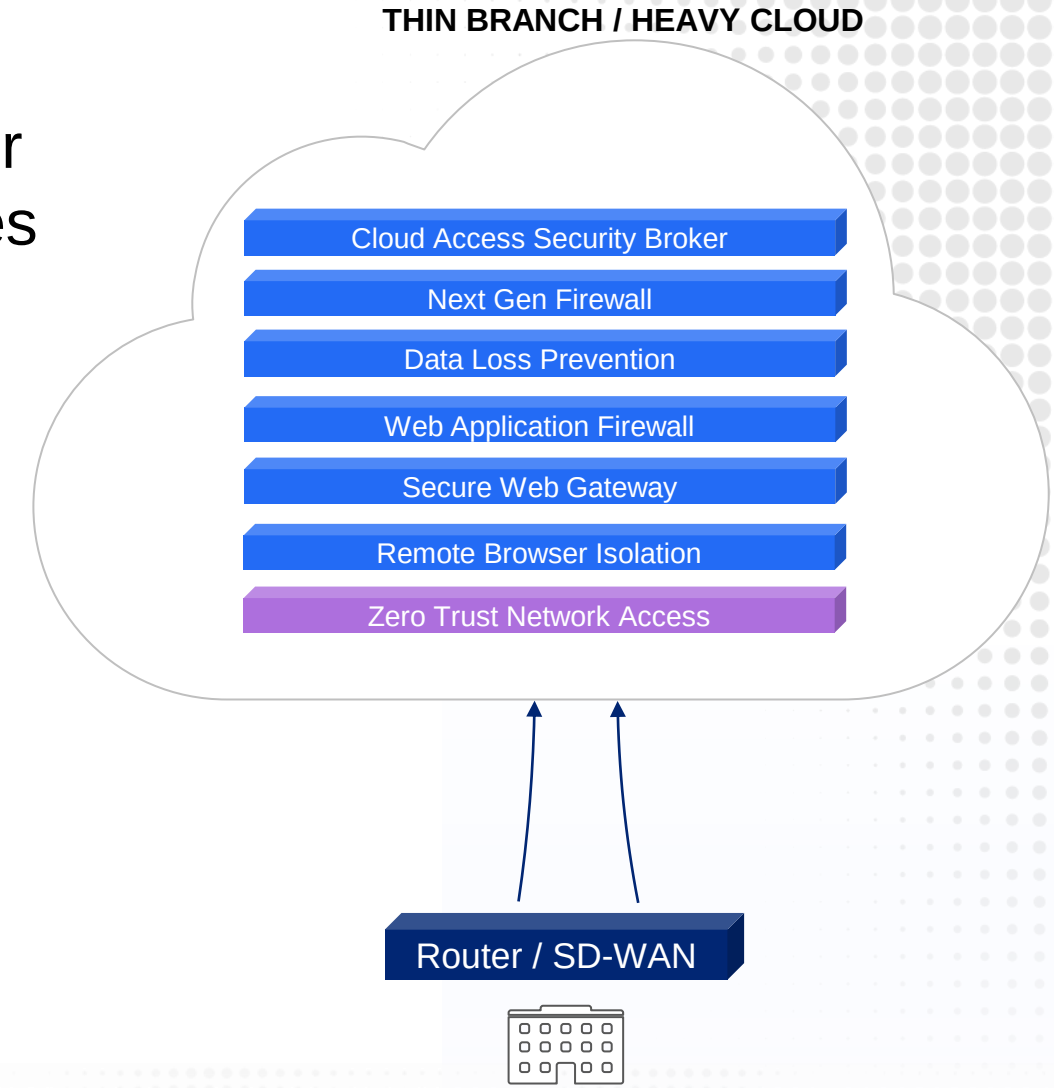
Gartner Got In On the Action



Gartner Secure Access Service Edge (SASE)

A **modern cloud architecture** for securely connecting users/devices to applications

- Initial framework for secure connectivity
- Shift the burden to a heavy cloud while leaving branches & clients thin
- Push security to the edge, as close to the user as possible



Digital Transformation disrupts Traditional Architecture

SERVICEWARE

User Mobility

Flexible, hybrid working. Post-pandemic era

Application Modernization

Apps & Data moving to SaaS / PaaS and IaaS

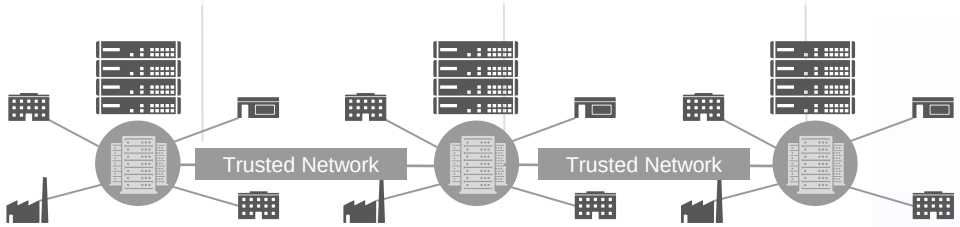
Network Transformation

Direct Internet Access

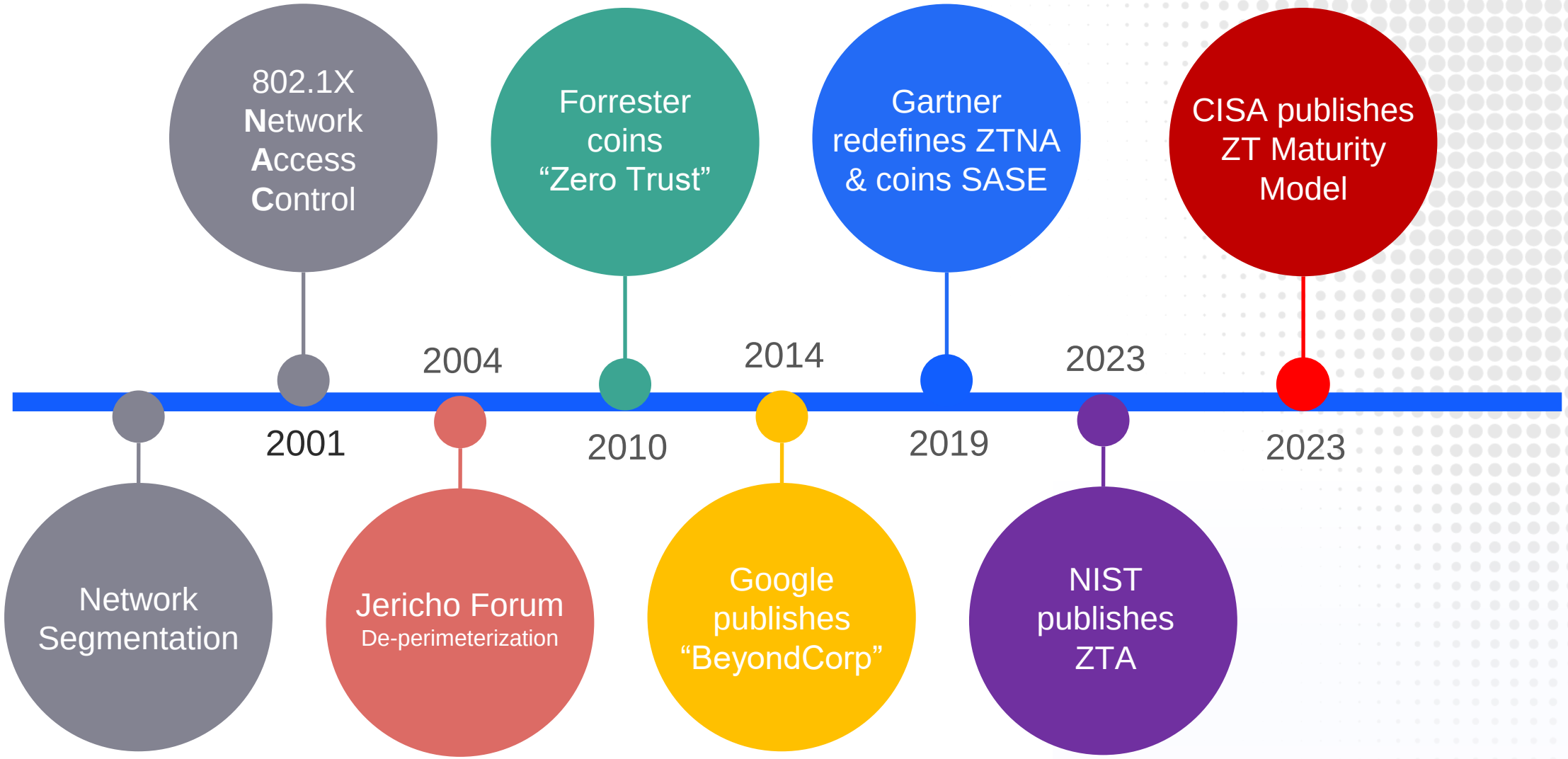
Security Transformation

Which Buzzword will help?!

Business is taking place off your trusted network and outside your security perimeter



One country moves strongly & fast ahead…once again…



So, how do I approach Zero Trust?

Spot the Difference

Architecture Matters

2000 Moving Parts

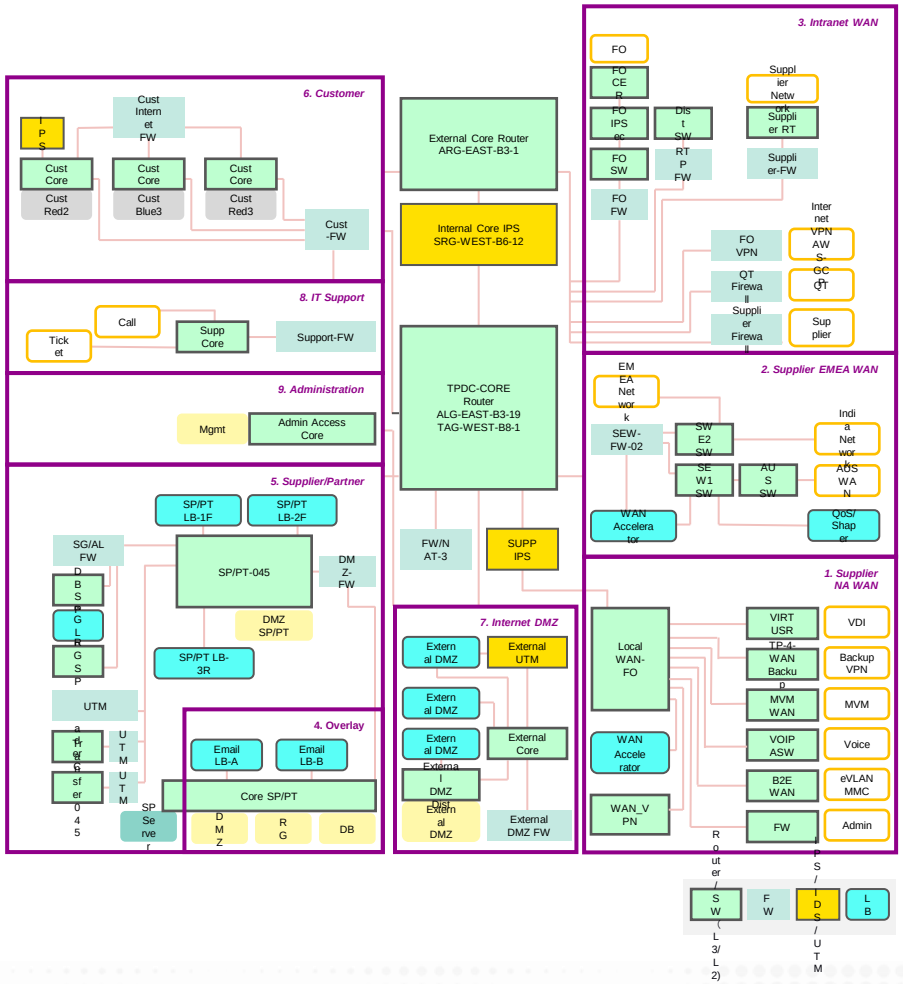
40% Efficient

20 Moving Parts

85% Efficient

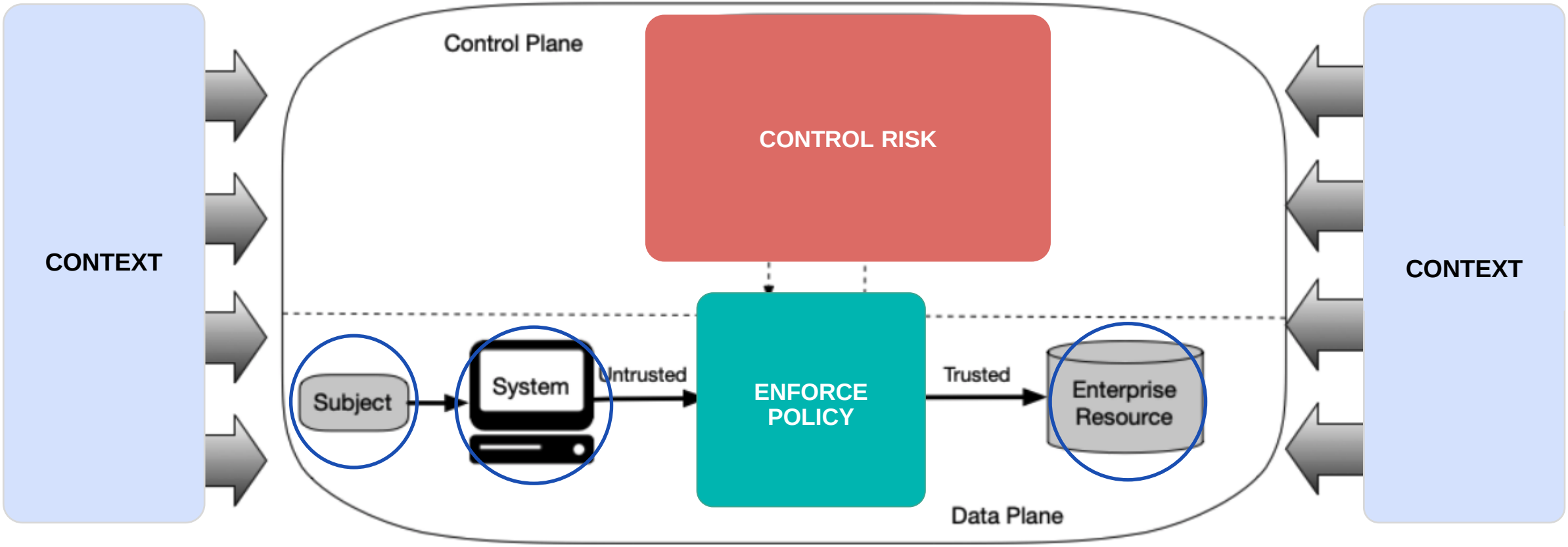
Legacy vs Software Defined Architecture

Castle-and-Moat

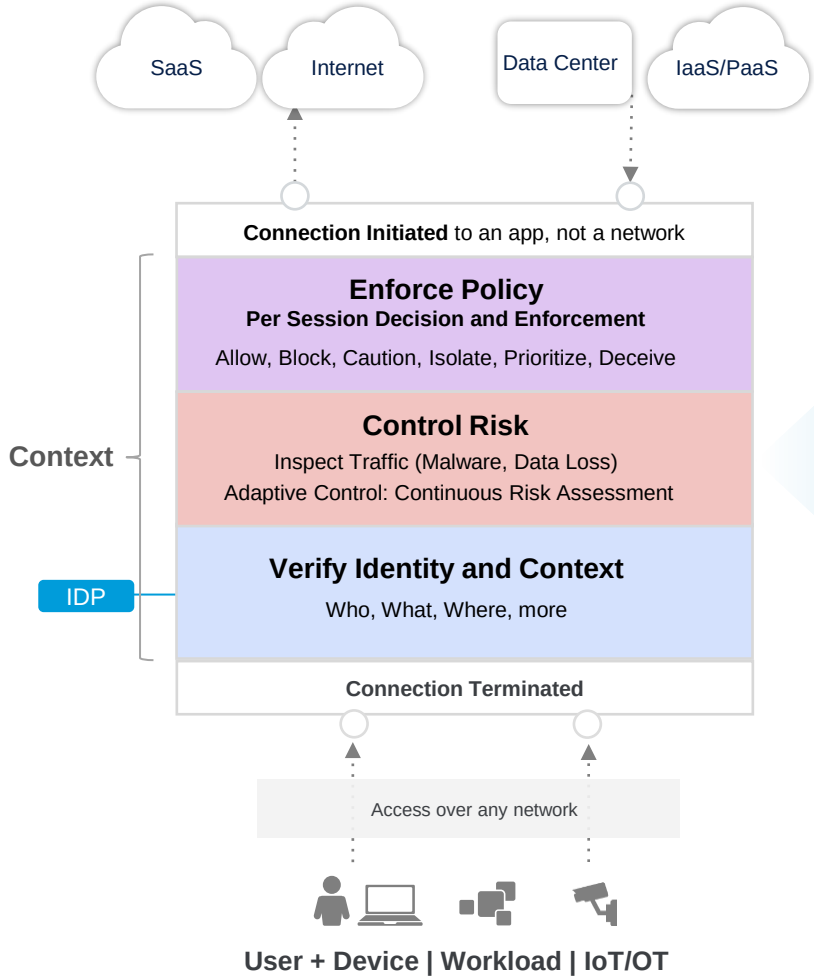


Software Defined

Zero Trust Architecture According to NIST



Zero Trust – A chance…

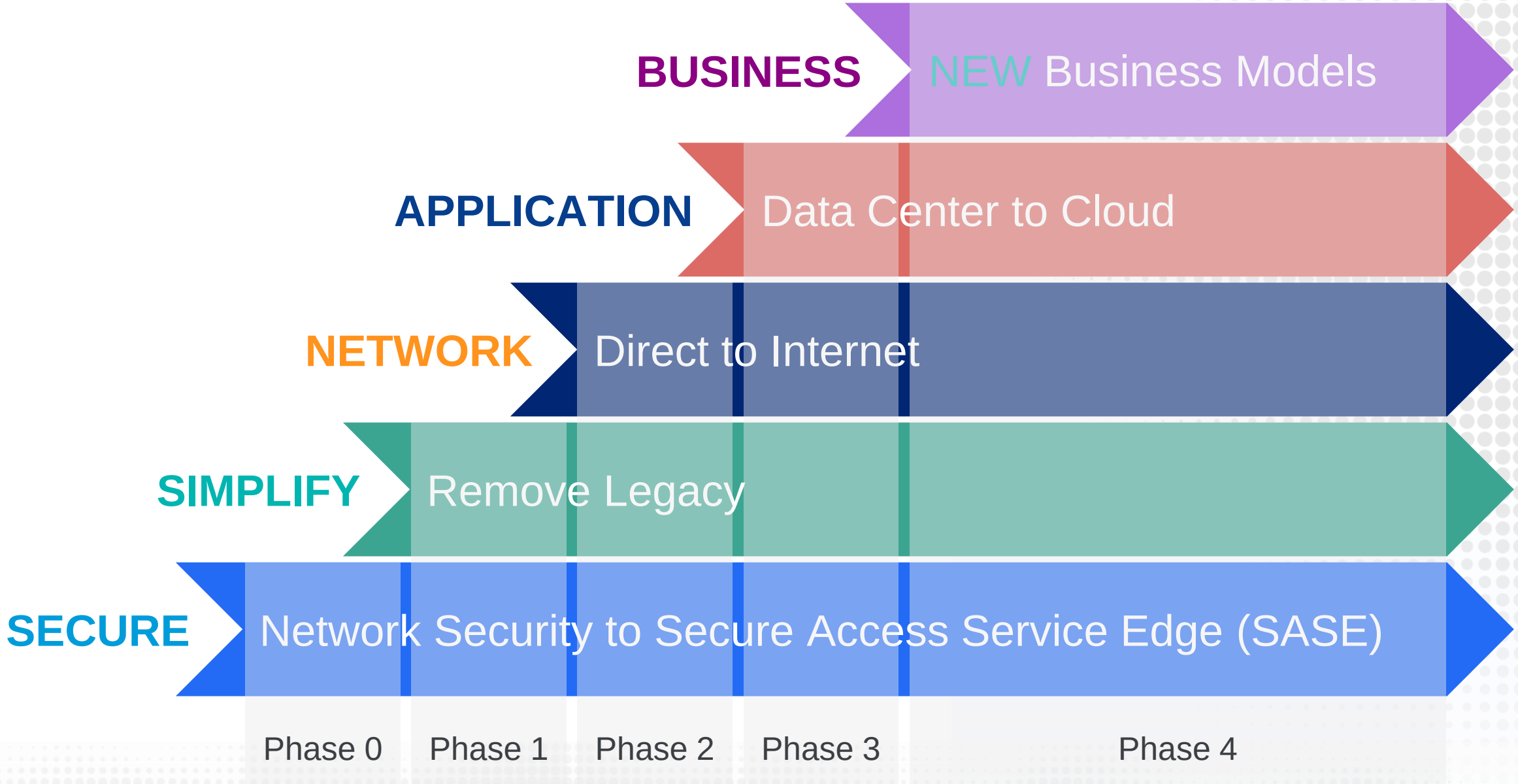


- Security-Transformation
- Network-Transformation
- User-Transformation
- Application-Transformation

Most organizations face one or more of these challenges…

- Don’t have comprehensive application inventory
- Don’t know all the application owners
- Don’t know who needs access to what
- Hard to maintain granular policy
- User-to-app traffic evolves as new use cases arise

The Digital Transformation Journey



What is a Zero Trust target state?

It depends in what you are trying to achieve, many are going with the following:

Identity

Validate users (employees, 3rd Parties, etc.) using **any digital identity** and secure access with defined methods of authentication everywhere.

Visibility of all identities throughout the entire identity lifecycle from registration to deprovisioning

Device

Access of **corporate managed & personal** devices to resources should only happen **after authentication** & the **applicable technical security posture** is validated

Network

Networks are only transit (the Internet acting as the main one) when connecting user/ devices to resources.

Access is granted on **application, files / database level** and not on network segments.

Workload

Define what exactly is “a workload”, for you?

Identify where workloads are located & check how they can be **differentiated or grouped.**

Security should be **embedded** into continuous app development.

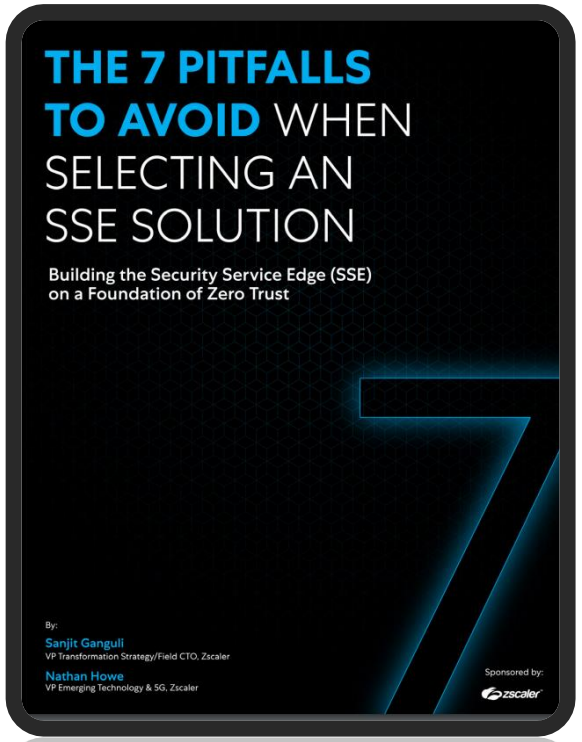
Data

Data is located everywhere and always **protected by granular access control based on business need, data classification and sensitivity.**

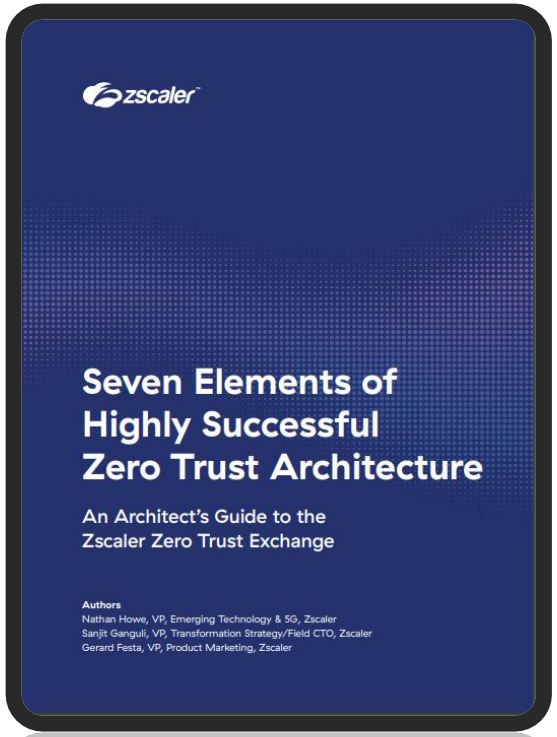
You want to learn more?

The 7 Pitfalls

Learn more about SSE Pitfalls & how to identify the right solution



7 Elements of Highly Successful Zero Trust Architecture



You have additional questions?

Let's follow up at anytime!

Ok, so who is this Zscaler then?

Zscaler Platform Services

SERVICEWARE

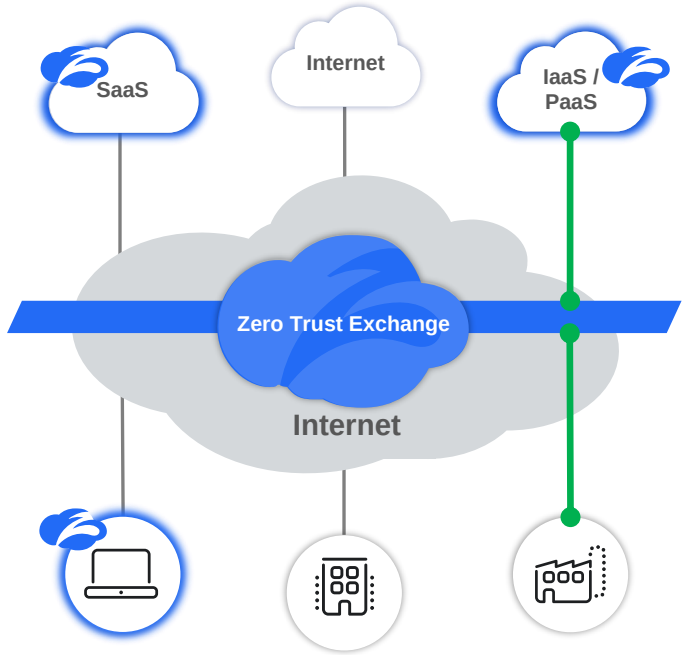
Transform Security

Secure Communication

Entities communicate with each other using business policies

Secure Data at Rest

Secure data in SaaS, IaaS/PaaS, data center and endpoints



Transform Networking

Zero Trust Connectivity

Internet replaces private, routable networks. Branch offices become like a Starbucks.

End-to-End Digital Experience

Visibility from endpoint to app to identify and resolve performance issues

---

Zscaler for **Workforce**

Zscaler for **Workloads**

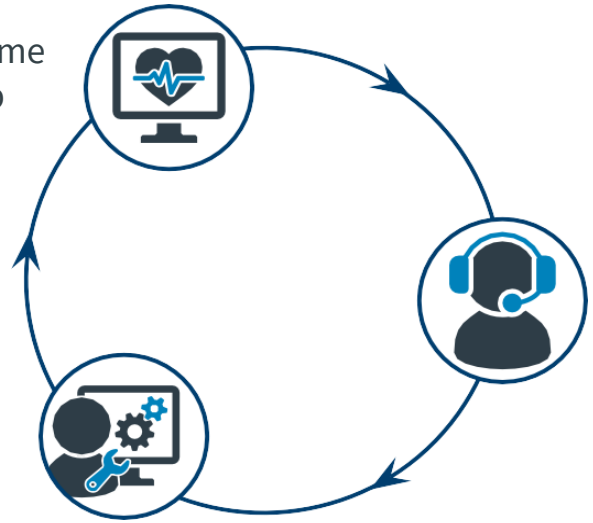
Zscaler for **IOT/OT**

Zscaler for **B2B**

Serviceware und Zscaler

Wir unterstützen in den Bereichen:

1 Bestandsaufnahme
- Anforderungsaufnahme
- Architekturworkshop



2 Proof of Value
- Planung und Durchführung des PoV und seiner Erfolgskriterien
- Komplette Unterstützung des PoV
- Umfassende Dokumentation der Schritte.

3 Support
- Support durch unsere Experten
- Managed Services
- Regelmäßige Healthchecks Ihrer Systemumgebung