devoteam

Roadmap to Zero-Trust

Consultancy

November 2021

Innovative technology consulting for business.

our playground.

Europe, Middle East
& Cloud

Sized for Agility & Trust.

18	7,200	€800M(e)
countries	digital transformakers	*Revenue ambition 2019*

We are a major partner for cutting-edge Cloud companies.

Google Red Hat servicenow

aws salesforce Microsoft

Digital trust and security is our mission.

devoteam
Cyber Trust

Better change is built on trust and resilience.
Embrace a digital journey with trust and confidence in the resilience of your business.

What is Zero-Trust

Microsoft Zero-Trust Principles

Verify explicitly
Always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, data classification, and anomalies.

Use least privileged access
Limit user access with just-in-time and just-enough-access (JIT/JEA), risk-based adaptive polices, and data protection to help secure both data and productivity.

Assume breach
Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses.

Why Zero-Trust ?

Complete Scope

Enabling secure
modern workplace
and cloud adoption

Best Practices

Busines fit
Industry best practices
Standardized platfom

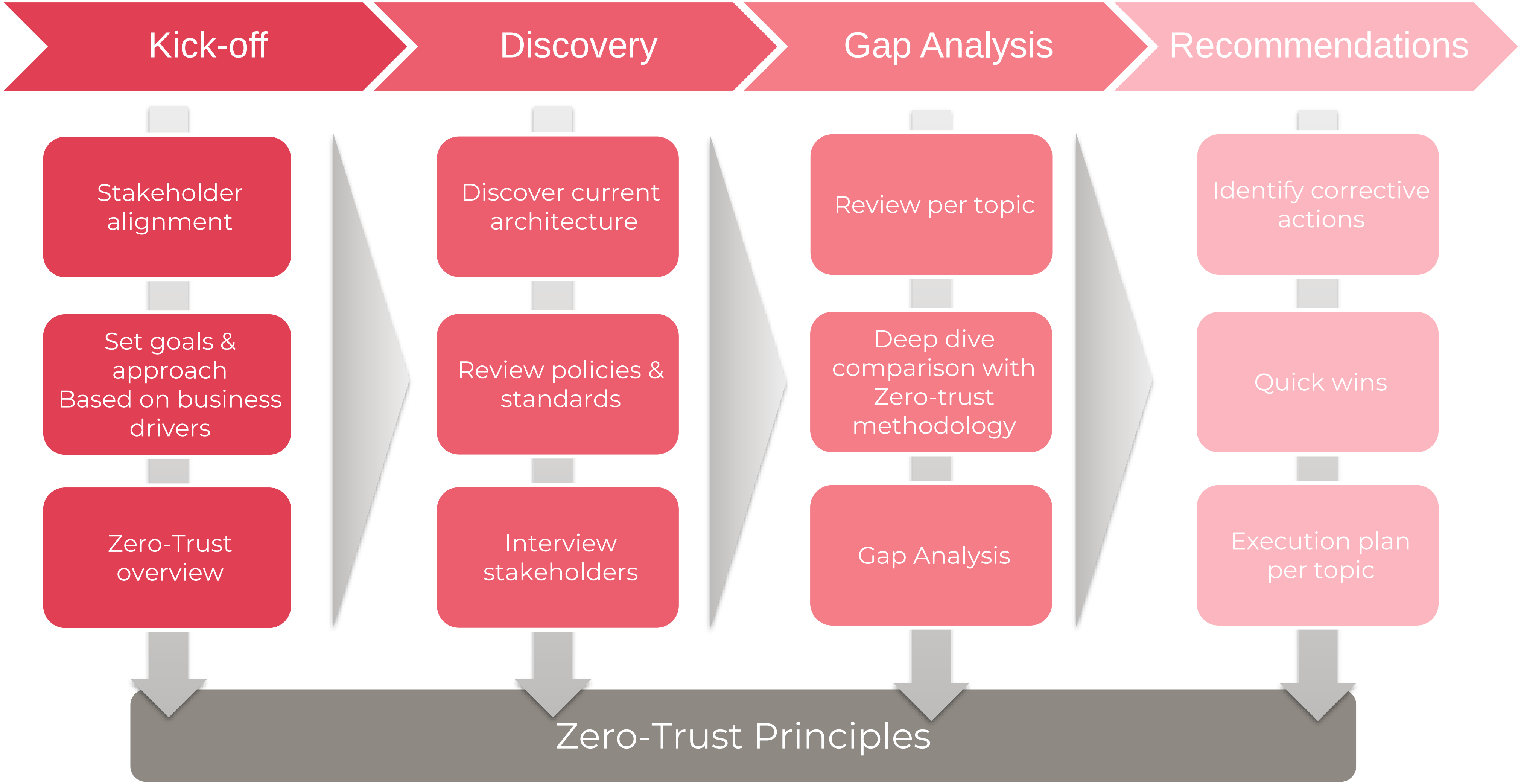
Optimize

Increase value
Optimize cost
Improve efficiency

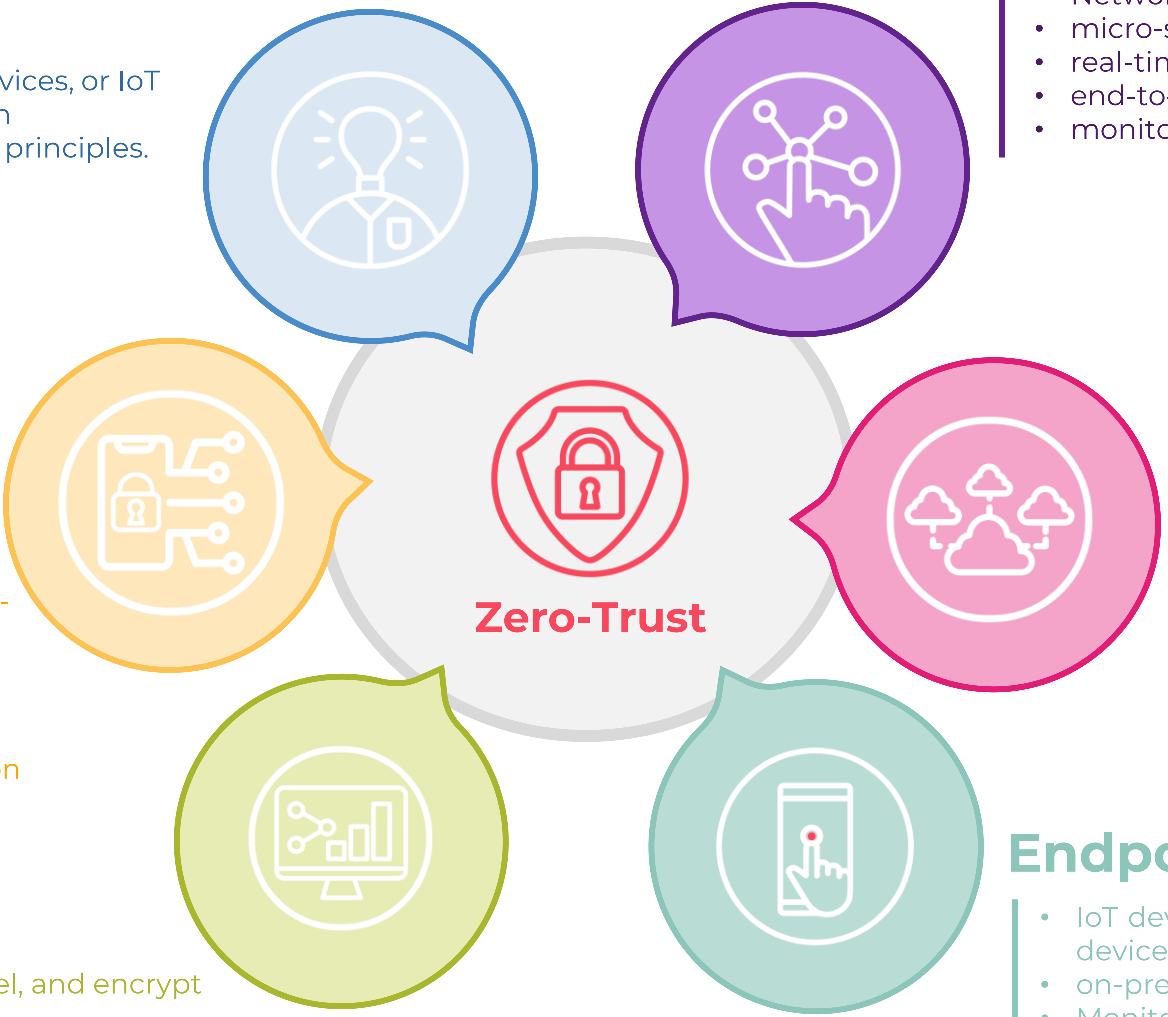
Peace of Mind

Future proof
Supports agility
Reduce risks
Reduce complexity

A Structured Approach to Zero-Trust



Assessment Topics



Identity

- represent people, services, or IoT
- strong authentication
- least privilege access principles.

Network

- Networking controls
- micro-segmentation
- real-time threat protection
- end-to-end encryption
- monitoring, and analytics.

Application

- legacy on-premises, lifted-and-shifted to cloud workloads, or modern SaaS applications.
- discover shadow IT
- Control in-app permissions
- Authorization based on real-time analytics
- monitor for abnormal behavior
- control user actions
- validate secure configuration options.

Infrastructure

- on-premises servers
- cloud-based VMs
- Containers
- micro-services
- harden defense
- Telemetry to detect attacks and anomalies
- Automated remediation

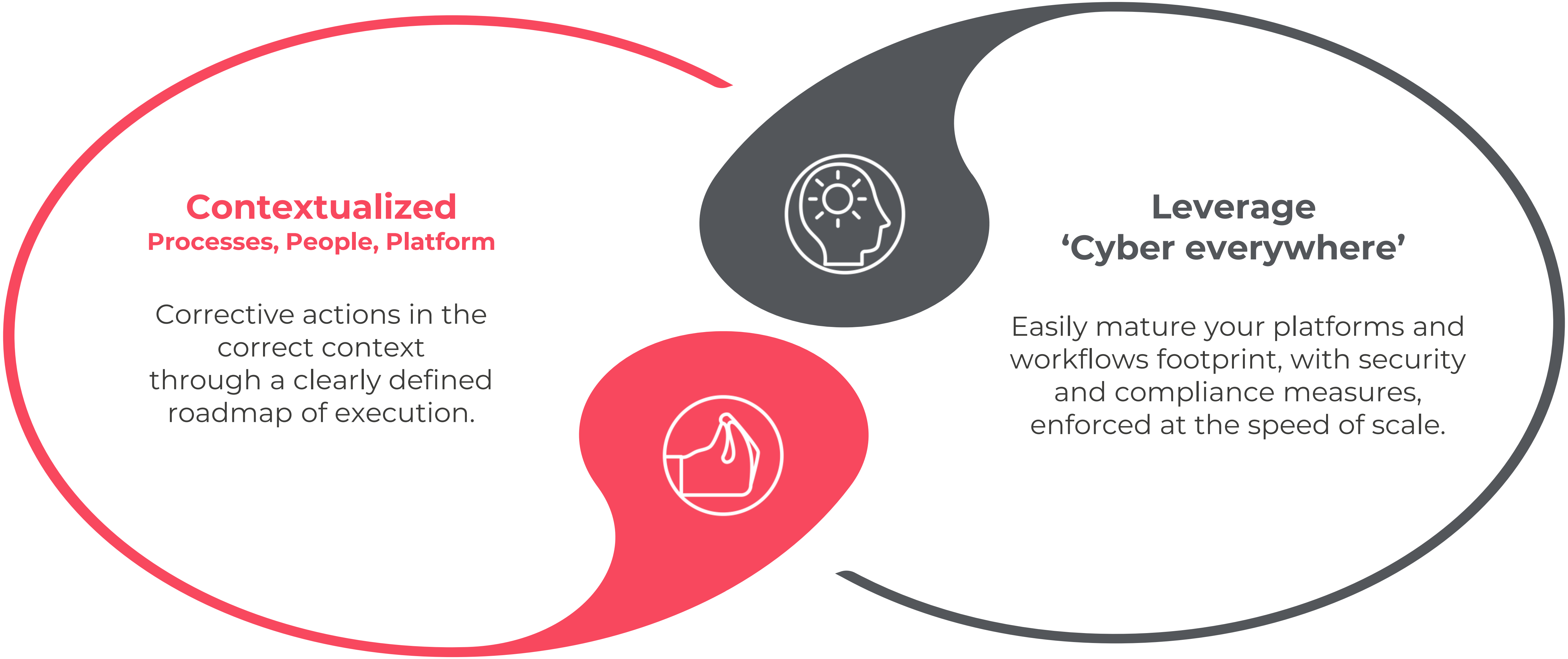
Data

- Classify, label, and encrypt data
- restrict access based on those attributes.

Endpoints

- IoT devices, smartphones, BYOD, partner-managed devices
- on-premises workloads to cloud-hosted servers.
- Monitor and enforce device health and compliance for secure access.

The Outcome



Contextualized

Processes, People, Platform

Corrective actions in the correct context through a clearly defined roadmap of execution.

Leverage ‘Cyber everywhere’

Easily mature your platforms and workflows footprint, with security and compliance measures, enforced at the speed of scale.

Why Devoteam Cyber trust

We consult, advise and use our expertise to develop solutions as part of a design, implementation or managed services with a common goal:
to ensure the resilience of key business transformation initiatives and business functions.

We do this with our top talent team, with high-level certifications in:

devoteam
Cyber Trust

- Application Development Security
- Cloud & DevOps Security
- Risk Management & Assessment
- Compliance & Controls
- Data Privacy & Encryption
- Digital identity
- Access Management
- Security strategy & Governance
- Recovery & Resilience

We are happy to talk about cybersecurity
and share what it takes to build great products.

**Every great journey begins with a plan.
Let's talk about yours today.**