CYBERSECURITY

Zero Trust Model Adoption

MICROSOFT ENTRA ID

MICROSOFT DEFENDER

MICROSOFT PURVIEW

AZURE

MICROSOFT INTUNE

REPLY CLUSTER

ZERO TRUST MODEL

OVERVIEW

The Zero Trust model is a security framework that requires all users and devices to be authenticated, authorized, and continuously validated before being granted access to applications and data, regardless of their location or network connection. It's based on the principle of "never trust, always verify."

KEY PRINCIPLES

ASSUME BREACH

Assume attackers can and will successfully attack anything (identity, network, device, app, infrastructure, data) and protect them accordingly.

VERIFY EXPLICITY

Protect assets against attacker by explicitly verifying that security decisions use all relevant available information and telemetry to grant access to company resources.

USE LEAST-PRIVILEGE ACCESS

Limit user and application privileges with just-in-time and just-enough-access (JIT/JEA) and risk-based polices.

ZERO TRUST MODEL

TRADITIONAL SECURITY MODEL vs ZERO TRUST MODEL

Traditional Security Model

- Perimeter-based security
- Implicit Trust
- Broad access privileges

Zero Trust Model

- Continuous verification
- Network micro-segmentation
- Least privilege access
- Proactive security

MOST COMMON CHALLENGES FOR ZERO TRUST ADOPTION

- Complex integrations and configurations of technologies
- Training of IT staff for new technologies adoption
- Balance between security and usability
- Lack of Asset Inventory and Data Understanding
- Financial investment in new technologies
- User Experience and Operational Impact

REPLY CLUSTER

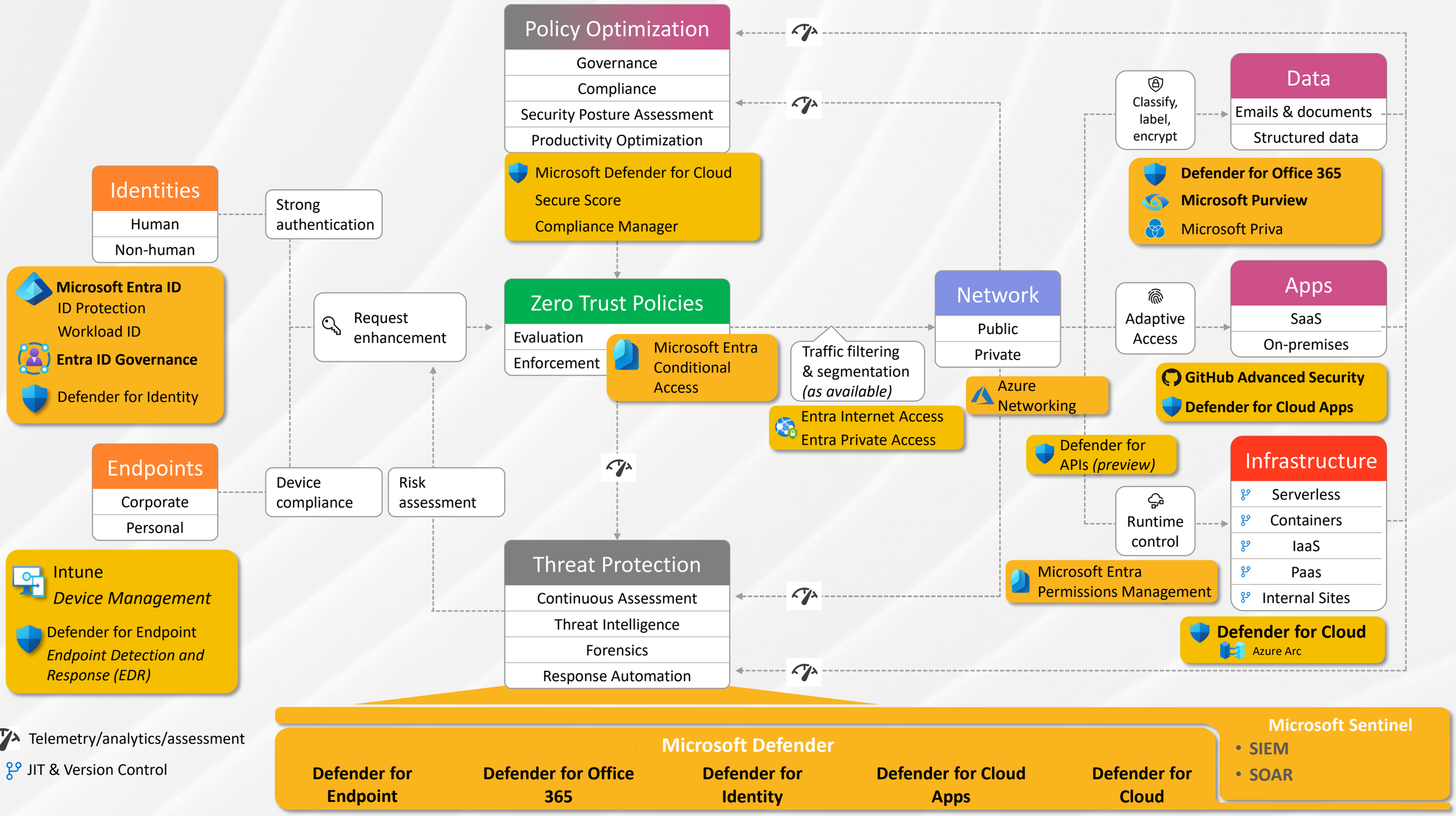
CHALLENGES

HOW MICROSOFT HELPS TO ADDRESS ZERO TRUST ADOPTION CHALLENGES

Complex integrations and configurations of technologies	**Unified platforms for Identity, Security and Compliance**
Balance between security and usability	**Custom configuration to find the right balance for your enviroment**
Financial investment in new technologies	**Single bundle licenses for users to adopt different technologies**
Training of IT staff for new technologies adoption	**Documentation, videos and tutorial to guide the implementation**
Lack of Asset Inventory and Data Understanding	**Automatic inventory recording and data classification**
User Experience and Operational Impact	**Reduce impact by offering seamless authentication, intelligent security analytics, adaptive security policies.**

ARCHITECTURE

MICROSOFT TECHNOLOGIES



Areas of Operation

- Identities and Access
- Infrastructure & Development
- IoT and OT
- Security Operations (SecOps/SOC)
- Data & Governance

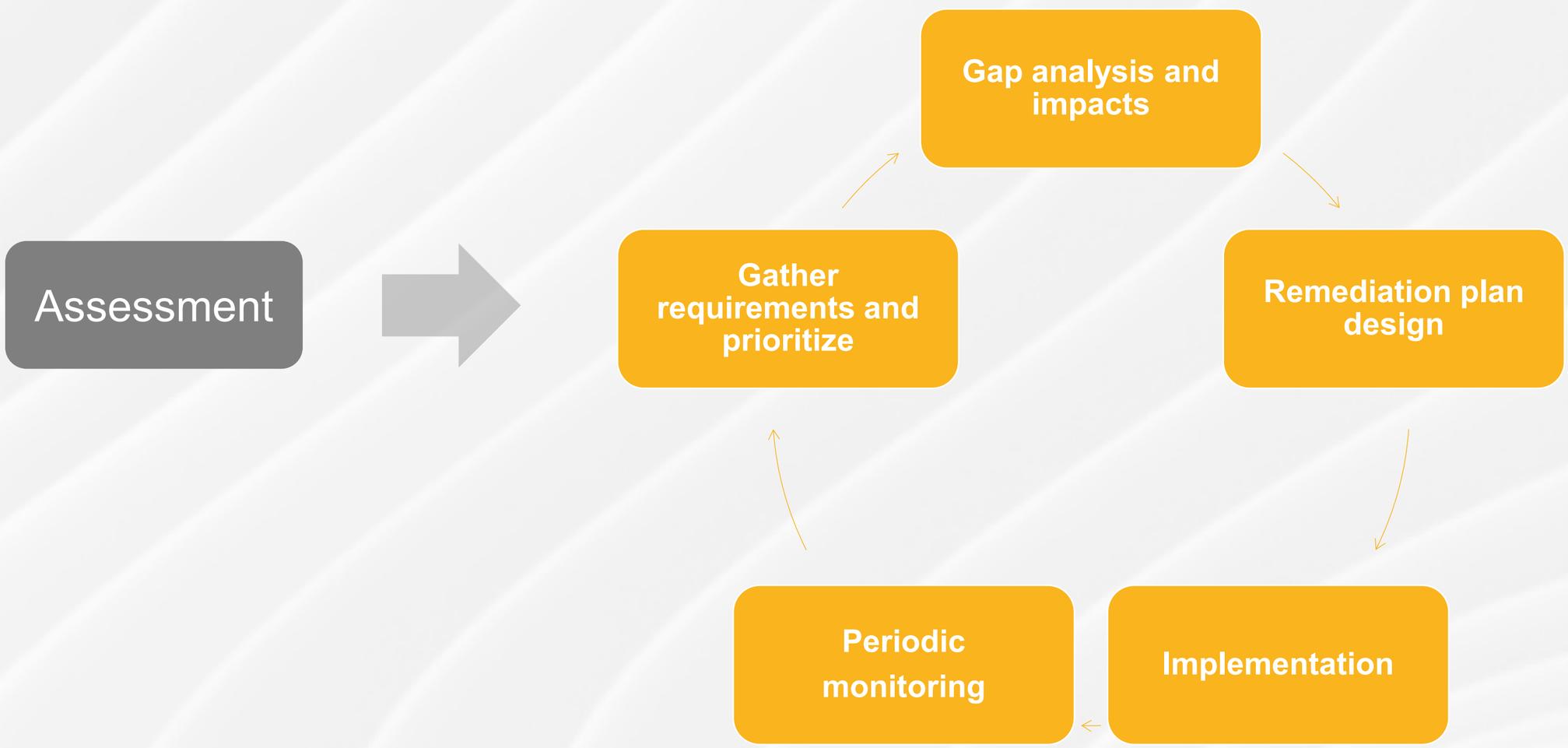
REPLY CLUSTER

ADOPTION STRATEGY

HIGH-LEVEL PLAN

Adoption of Zero Trust Model requires a structured approach and a well-defined adoption plan since from the first phases (environment assessment) continuing with a remediation plan design and implementation.

ADOPTION PATH



CONCLUSIONS

The Zero Trust model offers a paradigm shift in security, prioritizing continuous verification and least privilege access. By adopting a Zero Trust approach, organizations can significantly enhance their security posture and mitigate the risks associated with traditional security models.

KEY TAKEAWAYS

Zero Trust is a fundamental shift	It challenges the traditional perimeter-based security model.
Continuous verification is crucial	Constantly validate user identities and device health.
Least privilege access is essential	Grant only necessary permissions to users and applications.
Micro-segmentation is vital	Divide the network into smaller segments to limit the impact of breaches.
Proactive security is essential	Implement robust monitoring and threat detection mechanisms.

CYBERSECURITY

REPLY
CLUSTER

Contact us!

Davide Cassetta
d.cassetta@reply.it

Gennaro Casolaro
ge.casolaro@reply.it

WWW.CLUSTERREPLY.IT