Secure now, Secure Forever

Zero-Trust: Beyond the Buzzword to Practical Implementation

Abdullah Al Ghassani- Cyber Security Specialist

1 0 1 1 0 0 1 0 0 0 1 0 1 1 0 0 1 1
1 0 1 0 0 0 1 0 1 0 1 1 0 0 1 0 0 1 1 0

cyber security park
by ODP

Agenda

1- Understanding Zero-Trust Concepts

2- The Modern Enterprise Network Model

3- Adopting Zero Trust: Drivers, Outcomes and Challenges

4- The ZTA Maturity Model

5- A Journey Towards Optimal Zero Trust

6- Assessing Zero-Trust in a Cyber Supply Chain

7- Zero-Trust and the Role of SOC

Understanding Zero-Trust Concepts

What is Zero Trust ?

Zero trust provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.

Understanding Zero-Trust Concepts

What is Zero Trust Architecture (ZTA) ?

ZTA is an enterprise's cybersecurity plan that uses zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a ZTA plan.

Understanding Zero-Trust Concepts

Zero Trust Core Principles

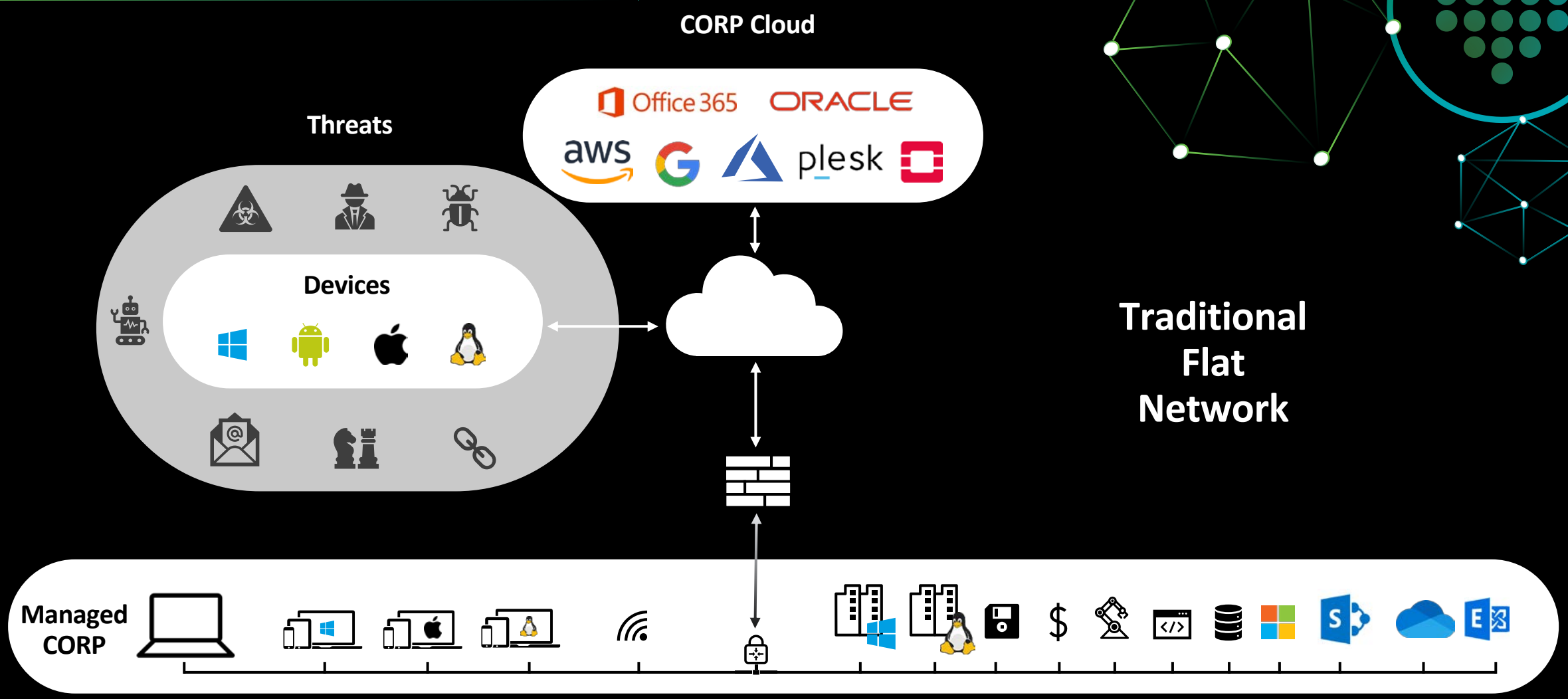
- Never TRUST, always VERIFY
- Least Privilege Access
- Assume Breach

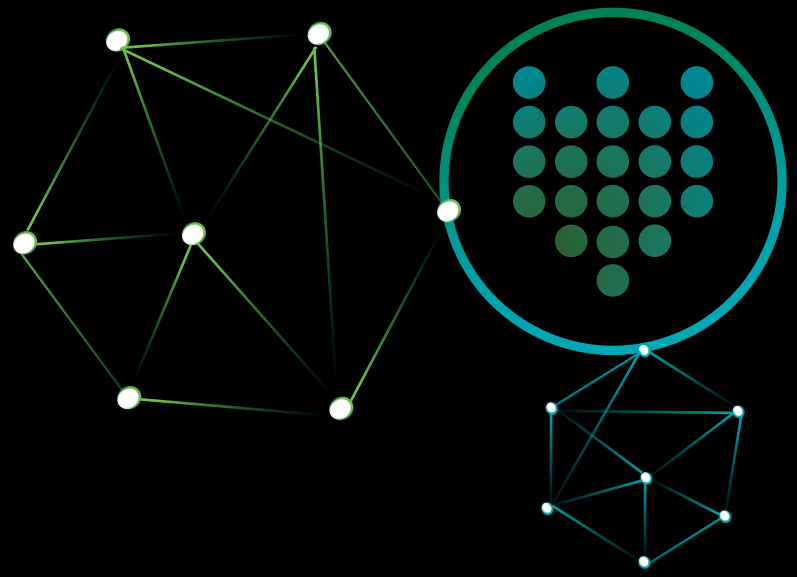
Adopting Zero Trust: Drivers, Outcomes and Challenges

cyber security park by ODP

Drivers	Outcomes	Challenges
The **Rapid Pace of Digitisation** and movement toward **Dynamic Work Environments**	**Architecture and Governance** Contextually-aware, simpler and dynamic enterprise security architecture	**Embracing Change** Zero-Trust must be supported by a Dynamic and Agile Cyber Organization
Increasingly **Complex Network Architecture** and **Supply Chain Activities**	**Security Operations** Predictive Monitoring and Automated Response	**Integrating Solutions** Lack of Zero-Trust standards raises integration challenges between technologies
Adversaries are **more Sophisticated** and are **outmatching current Cyber Defences**	**Policy Management and Integrations** Centralised Security Policy Management and Dynamic Policy Enforcement	**Setting up Zero-Trust Governance** Establishing a Zero-Trust Standard Requires a Security and IAM Mindset

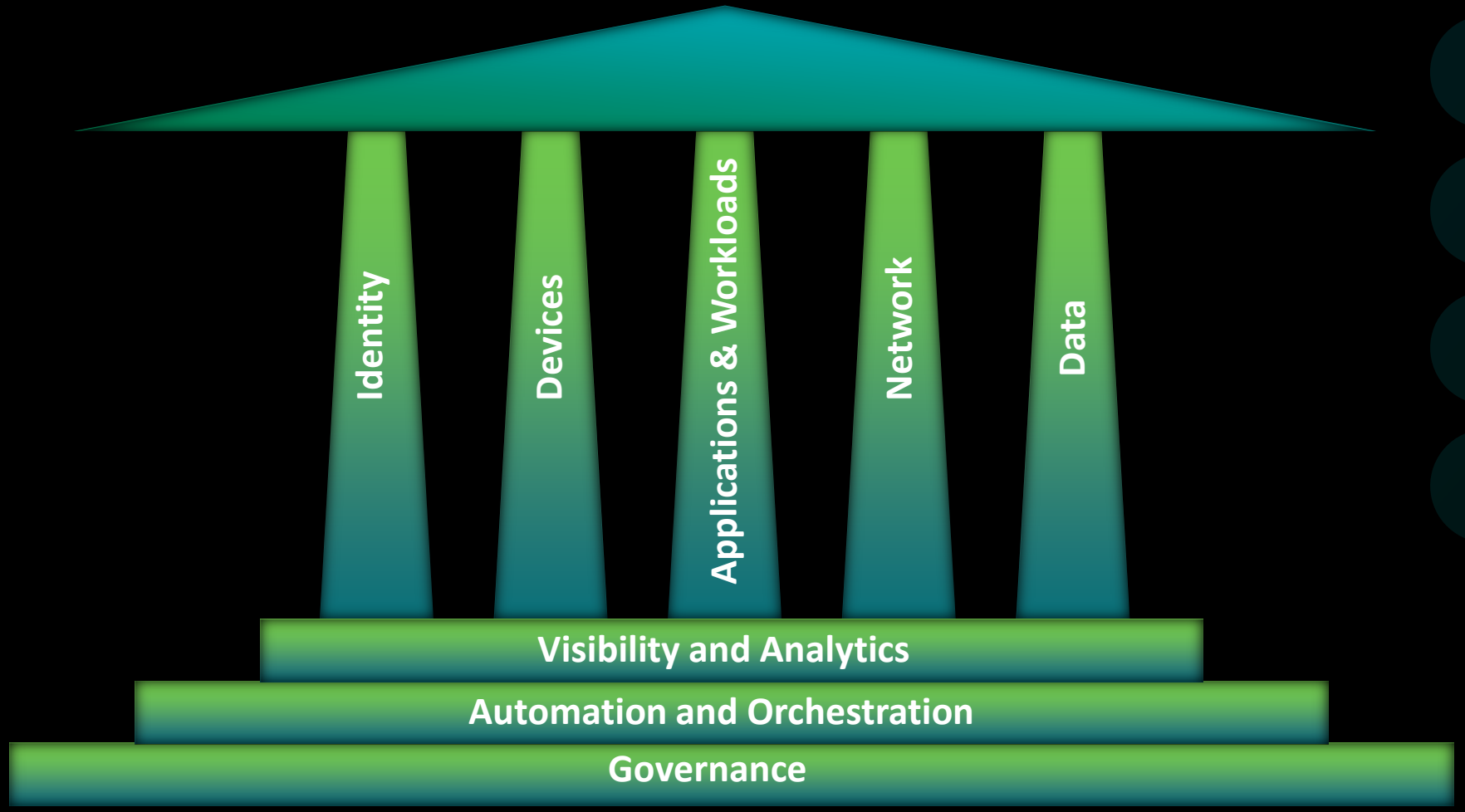
The Enterprise Network Model



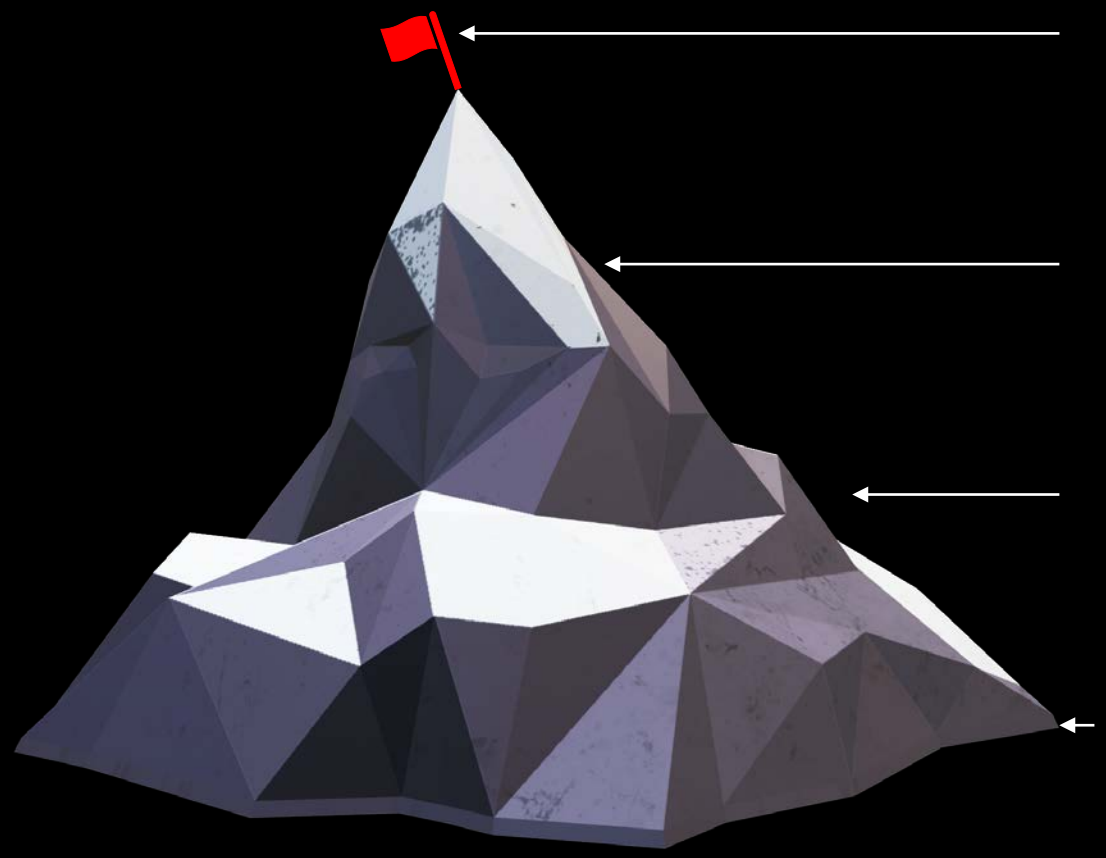


Traditional Flat Network

The Zero-Trust Architecture Maturity Model



A Journey Towards Optimal Zero Trust



1.Optimal:

1. Fully automated lifecycles and attribute assignments.
2. Dynamic policies based on observed triggers.
3. Dynamic least privilege access enterprise-wide.
4. Continuous monitoring with cross-pillar interoperability.

2.Advanced:

1. Automated controls for lifecycle and configuration assignment.
2. Centralized visibility and identity control.
3. Policy enforcement integrated across pillars.
4. Response to predefined mitigations.

3.Initial:

1. Beginning automation of attribute assignment and lifecycle configuration.
2. Initial integration of external systems for policy enforcement.
3. Some responsive changes to least privilege post-provisioning.
4. Aggregated visibility for internal systems.

4.Traditional:

1. Manual configuration of lifecycles and attribute assignments.
2. Static security policies addressing one pillar at a time.
3. Least privilege established only during provisioning.
4. Siloed policy enforcement and manual response/mitigation.

Benchmarking your Zero-Trust Maturity

	Initial	Advanced	Optimal
Identities	MFA with Passwords Self-Managed & Hosted Identity Stores Manual Identity Risk Assessments	Phishing-resistant MFA Consolidation and Secure Integration of Identity Stores Automated Identity Risk Assessment	Continuous Validation and Risk Analysis Enterprise-wide identity integration Tailored Automated Access
Devices	Physical Assets are tracked Limited device based access control Some Automated Protection	Most Physical & Virtual Assets are tracked Enforced compliance integrated with threat protection	Continuous physical & virtual asset and automated supply chain risk management. Resource access on real-time device analytics
Network	Initial Isolation of Critical workloads Dynamic configurations for some portions of the network	Expanded isolation and resilience Mechanisms Automated risk-aware application profile assessments	Distributed micro-perimeters with just-in-time and just-enough access controls Cryptography Agility best practice
Applications & Workloads	Some mission critical workflows have integrated protections Static and Dynamic security testing prior to deployment	All mission critical workflows are integrated with security and context based access control Coordinated teams for development, security and Ops	Protection Against Sophisticated attacks Immutable workloads with security testing integrated throughout lifecycle
Data	Initial Centralized key management Some High Availability Data Stores Initial Data Strategy	Automated Data Inventory with Tracking Consistent, tiered targeted categorization of Data	Continuous Data Inventorying Automated Data Categorization DLP exfiltration blocking Real Time Data Encryption

Visibility & Analytics

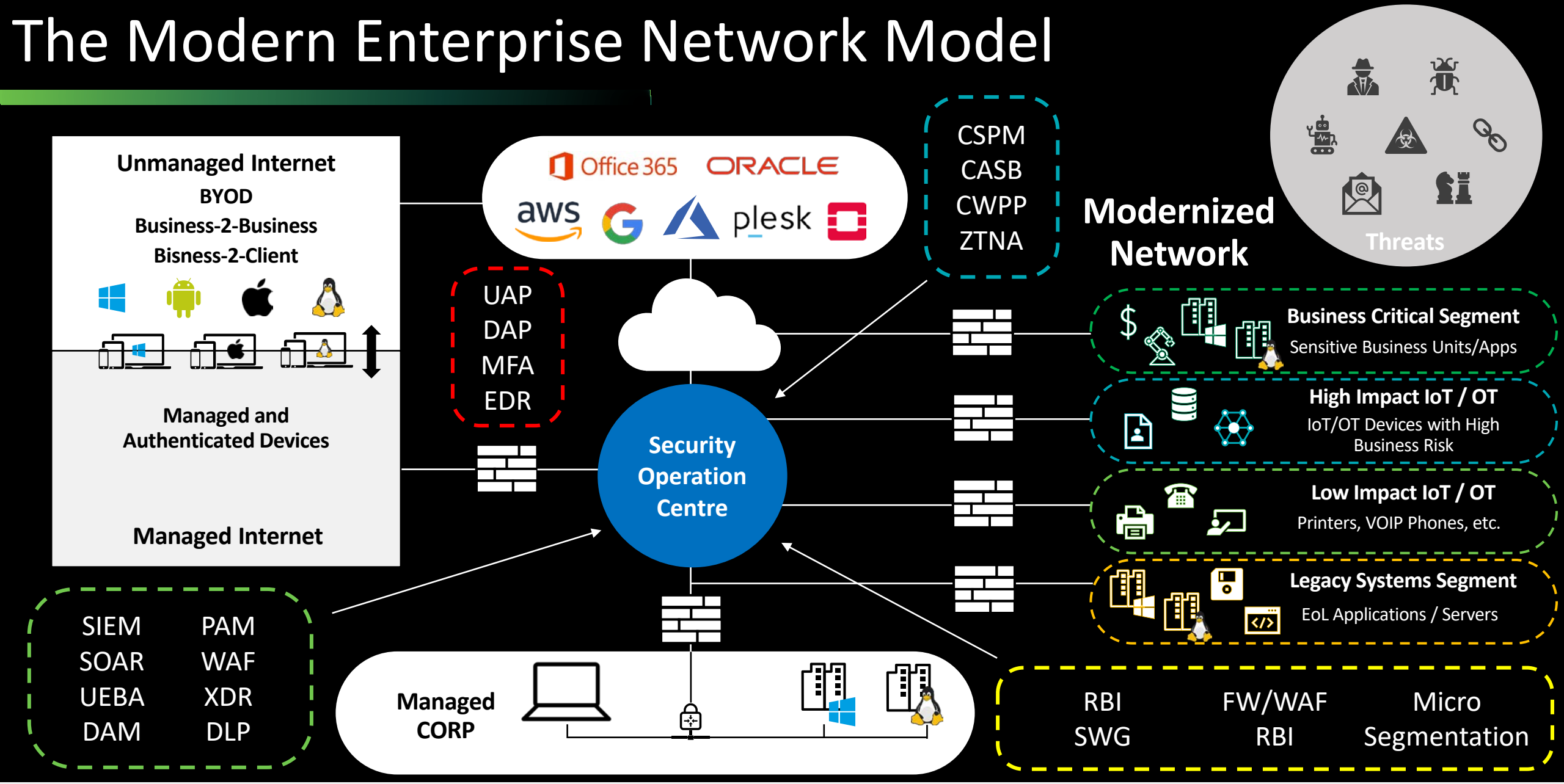
Automation & Orchestration

Governance

Assessing Zero-Trust in a Cyber Supply Chain

	Initial	Advanced	Optimal
Identities	Is there a cyber supply chain risk management policy in place ?	Is there an inventory of suppliers ? Is it possible to verify the authenticity of supply chain components ?	Is the cyber supply chain risk management plan updated frequently based on automatically collected inputs ?
Applications & Workloads	Is there an access policy considering cyber supply chain aspects ?	Is information about maintenance shared taking into consideration aspects of a Zero Trust architecture ?	Are cyber supply chain maintenance activities automated ? Infrastructure Are the maintenances continuously monitored ?
Data	Is there a cyber supply chain information integrity policy in place ?	Do information integrity mechanisms take into account insider threats such as equipment infected by malwares, e.g. ransomware attacks ?	Are techniques implemented to ensure non-repudiation of cyber supply chain information ?
Network	Is there a policy in place to protect communications used in the cyber supply chain ?	Are communications protected in several heterogeneous layers considering possible failures in some mechanisms ?	Are the communication protection mechanisms being continuously monitored and adapted ?
Devices	Is there a contingency plan for the cyber supply chain ? Is there a physical and environmental protection policy in place ?	Is physical access segregated by roles ? Is there a protection against modifications?	Is the organization able to provide alternative services considering aspects of a Zero Trust architecture ?

The Modern Enterprise Network Model



cyber security park
by ODP

Secure now, Secure Forever

cyber security park

by ODP

Thank You