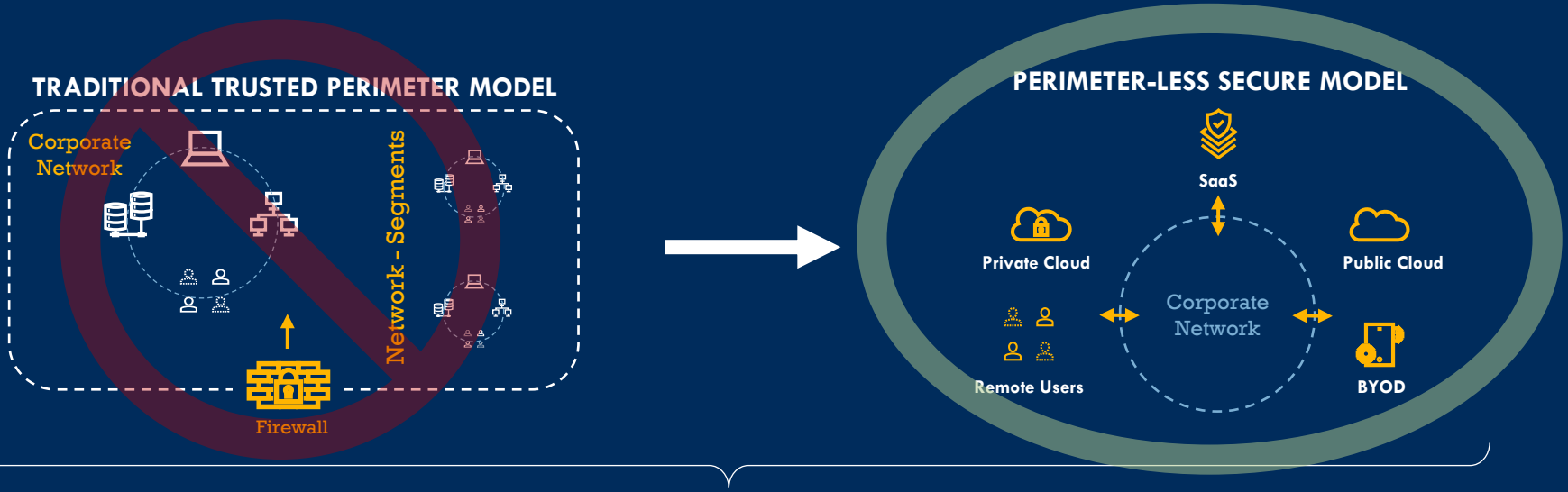
ZERO TRUST JOURNEY CENTRAL ISSA MARYLAND

Where can it take the security of your organization

John Humenick
Client Solutions Analyst

OPTIV

EVOLUTION OF THE TRUSTED PERIMETER



EVOLUTION HIGHLIGHTS

- ✓ **Departure of the traditional** "trusted" network perimeter.
- ✓ Proliferation of **heterogeneous multi-cloud** technology stack.
- ✓ **De-centralized and distributed** nature of assets and identities accessing those assets.
- ✓ **Ubiquity of remote users and devices** due to the adoption of "work from anywhere" business models.

OPTIV

ZERO TRUST DEFINED BY OPTIV

WHAT IT MEANS TO MOVE TO ZERO TRUST

The evolving ecosystem warrants a paradigm shift in the way organizations approach the design and implementation of business processes and technical capabilities aligning them with the Zero Trust architecture. Optiv categorizes this paradigm shift under **three primary components** that can guide the implementation and optimization of Zero Trust capabilities.

Adopt a Context- Based Security Model

An integrated security model that actively consumes risk-based information to secure busines critical assets.

Default to "Trust Nothing"

“Assume breach” - default position that any entity (user or device) is a potential threat actor.

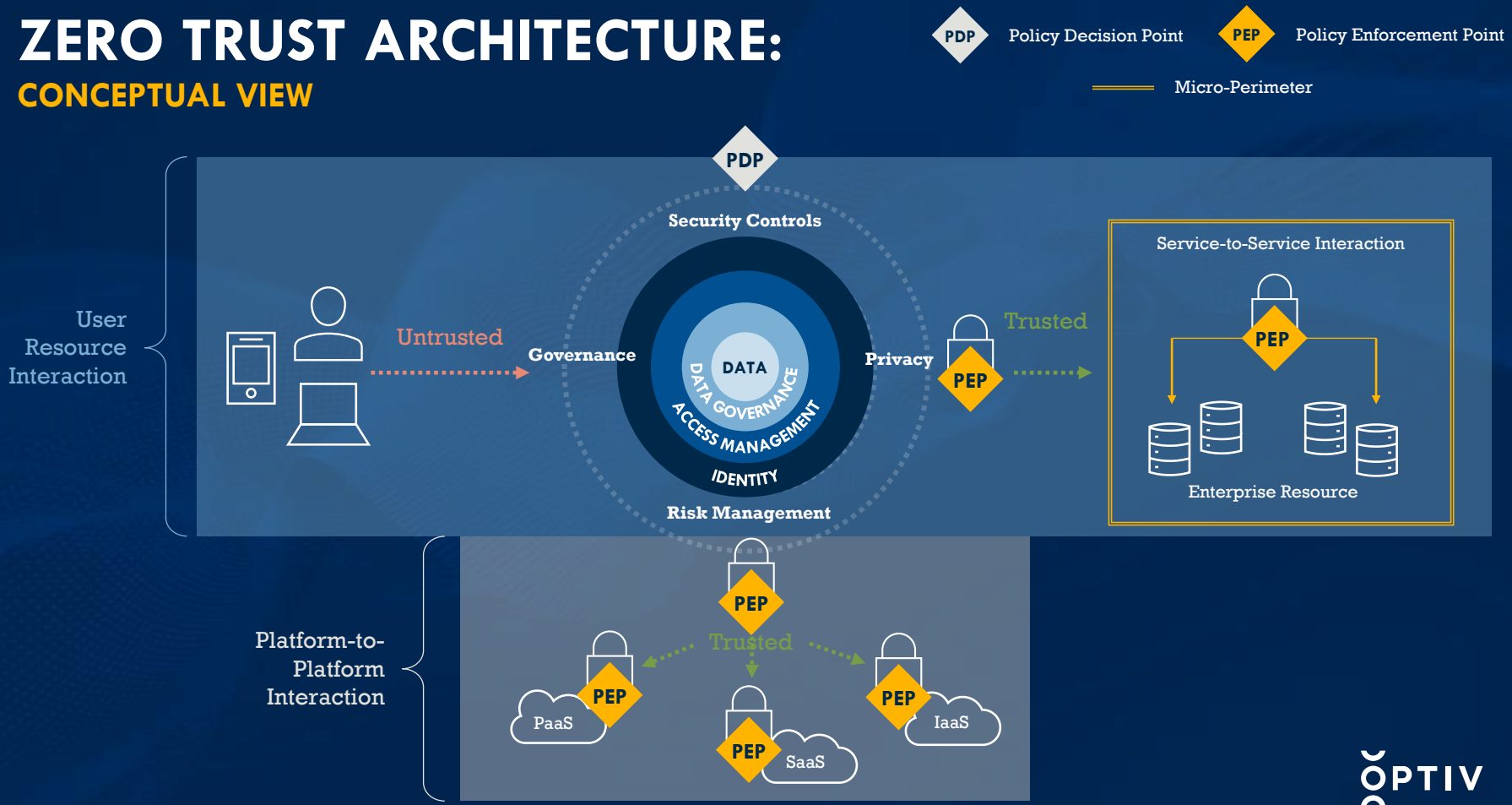
Design Dynamic Micro-Perimeters

Design and implement architectures that create secure and dynamic risk-based perimeters around critical business resources.

OPTIV

ZERO TRUST ARCHITECTURE:

CONCEPTUAL VIEW



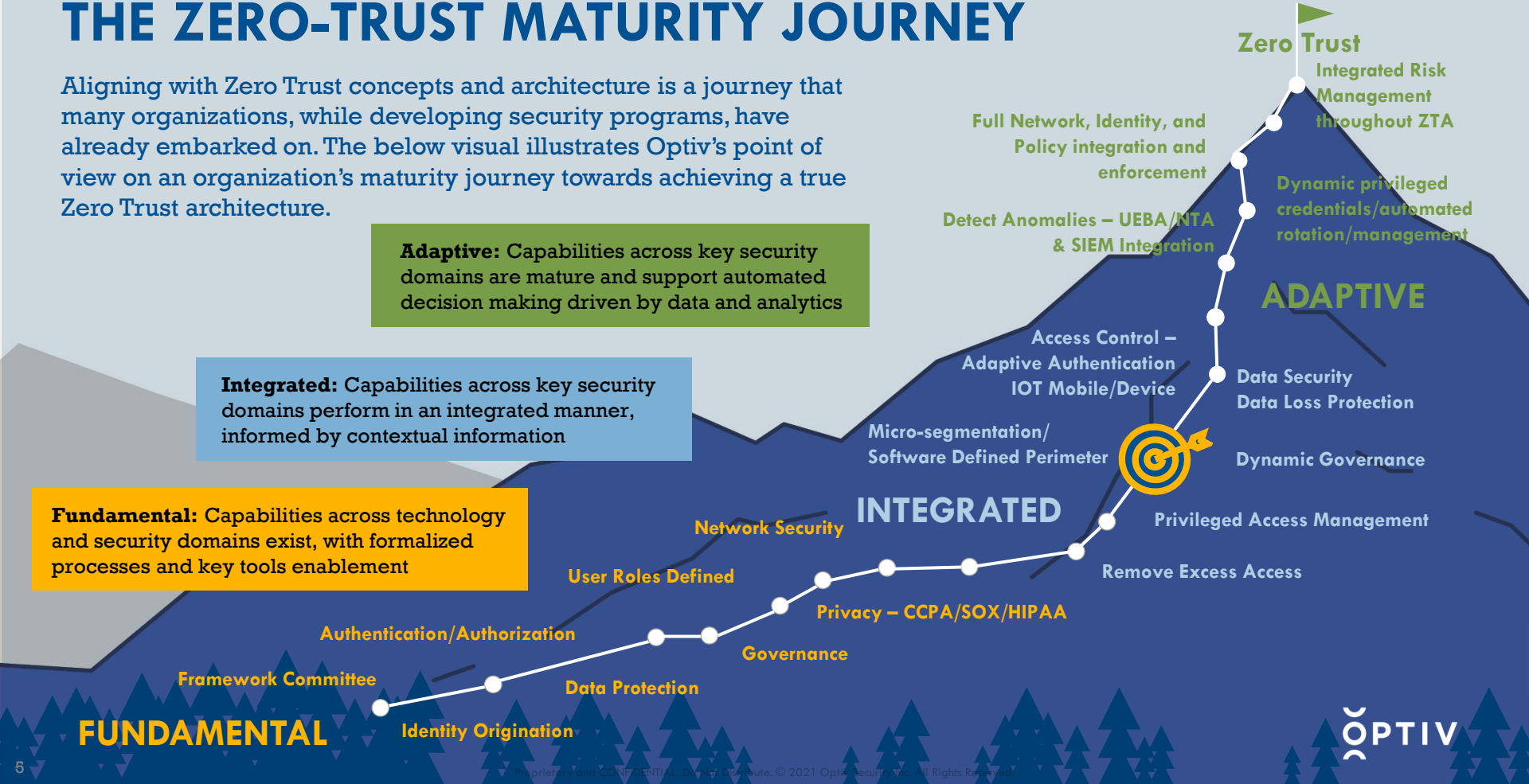
THE ZERO-TRUST MATURITY JOURNEY

Aligning with Zero Trust concepts and architecture is a journey that many organizations, while developing security programs, have already embarked on. The below visual illustrates Optiv's point of view on an organization's maturity journey towards achieving a true Zero Trust architecture.

Adaptive: Capabilities across key security domains are mature and support automated decision making driven by data and analytics

Integrated: Capabilities across key security domains perform in an integrated manner, informed by contextual information

Fundamental: Capabilities across technology and security domains exist, with formalized processes and key tools enablement



OPTIV'S ZERO TRUST CORE PRINCIPLES

Leveraging understanding and expertise across security domain, Optiv has developed **four core** principles to drive an organization's trajectory towards a true **Zero Trust Architecture**.

ESTABLISH A MICRO-PERIMETER

Secure business resources through **"just-in-time" automatic placement of systems** to have access to only permissible services based on security posture.

ESTABLISH A SECURE IDENTITY-BASED CONTEXT TO THE RESOURCE

Contextualize key security events as well as the traffic flow through the micro-perimeter **with specific Identity**.

CREATE ENHANCED SECURITY

Enable additional verification as resources are accessed and managed.

CONTINUOUS REVIEW OF IDENTITY AND SECURE CONNECTION

Maintain security connectivity to the resource, **monitor** activity as the resources are utilized and **respond** to incidents as needed.

Optiv's Zero Trust Principles are aligned to NIST 800-207 (Published NIST Zero Trust Standards)

OPTIV'S APPROACH TO THE ZERO-TRUST JOURNEY

A holistic strategy and approach around Zero Trust adoption has three key stages that enable organizations establishing and maturing their Zero Trust capabilities.

ASSESS AND RECOMMEND

Conduct baseline, and subsequent periodic **assessments** to determine **organizational posture** against the Zero Trust requirements across domains.

REMEDIATE AND BUILD

Based on the current state assessments, remediate the identified gaps by **executing on a maturity roadmap.**

OPERATE AND OPTIMIZE

Operate and continue to enhance the Zero Trust capabilities across the key security domains.

OPTIV

TALK TO US

Let's get you there.