accendnetworks®

Security

Cisco ISE

Part I- Intro to Cisco ISE , Profiling, Posturing, and Integrations

Paula Wong, CEO/Founder, CCIE#13062,
Senior Security Architect/Network Engineer

TABLE of Contents

1 Introduction to Cisco Identity Identities Engine (ISE)

2 CHAPTER 1 Understanding the Cisco Identity Services Engine

3 CHAPTER 2 What you need for your ISE Deployment

4 CHAPTER 3 ISE Deployment Options

5 CHAPTER 4 ISE Profiling

6 CHAPTER 5 Cisco ISE Integrations

7 CHAPTER 6 Cisco ISE Profiling and Posturing

8 CHAPTER 7 How to configure Profiling Probes

9 CHAPTER 8 Posturing

10 CONTACT US!

CHAPTER-1

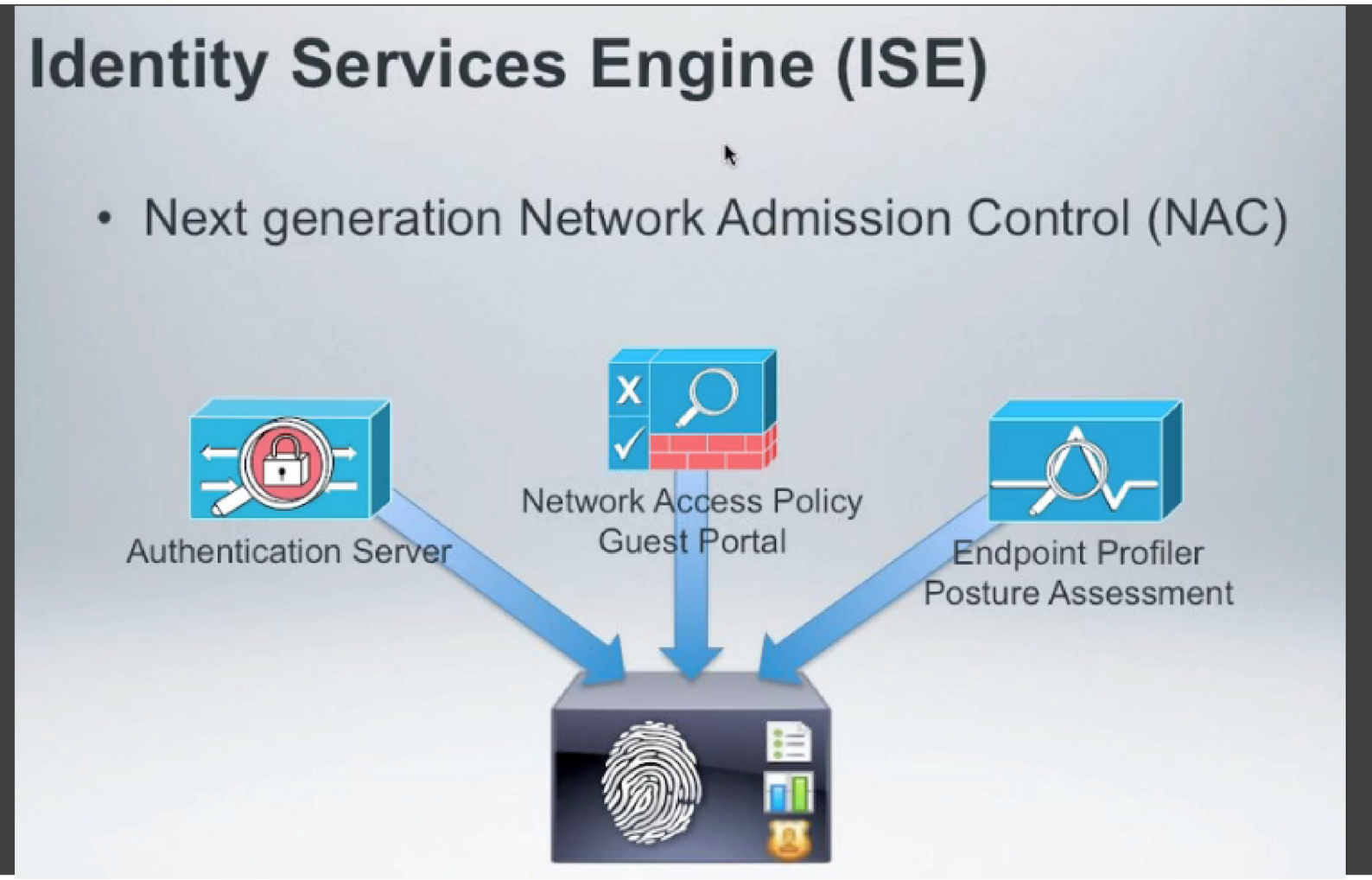
INTRODUCTION TO CISCO ISE

An overview of Cisco Identity Services Engine (ISE)

INTRODUCTION

AN OVERVIEW OF CISCO IDENTITY SERVICES ENGINE (ISE)

- Understanding the Cisco Identity Services Engine (ISE).
- What you need for your ISE deployment
- ISE Deployment Options
- Profiling
- Cisco ISE Integration



SEGMENTATION AND ZERO TRUST

SECURE ZERO TRUST

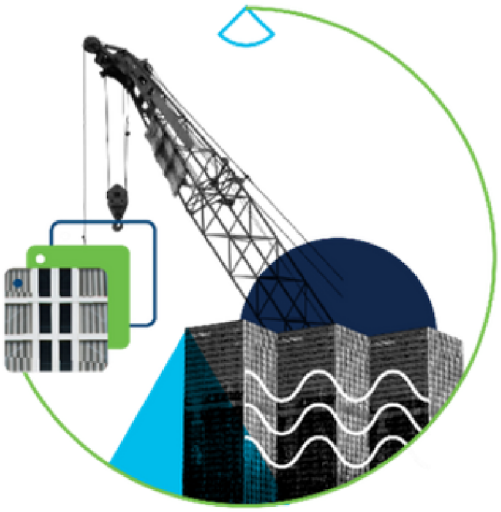
A comprehensive approach to securing all access across your people, applications, and environments.

Workforce

Ensure only the right users and secure devices can access applications.

Workplace

Secure all user and device connections across your network, including IoT.

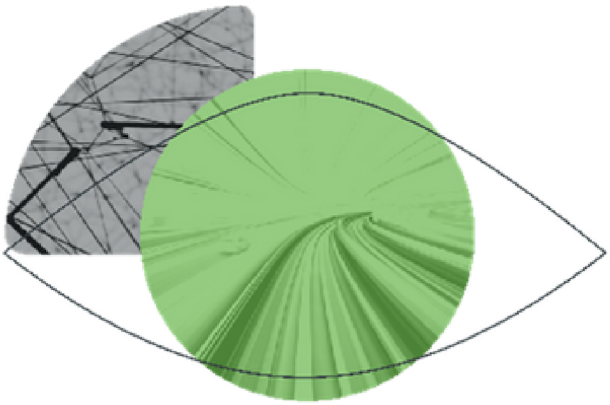


Workloads

Secure all connections within your apps, across multi-cloud.

THE FOUNDATIONS OF ZERO TRUST

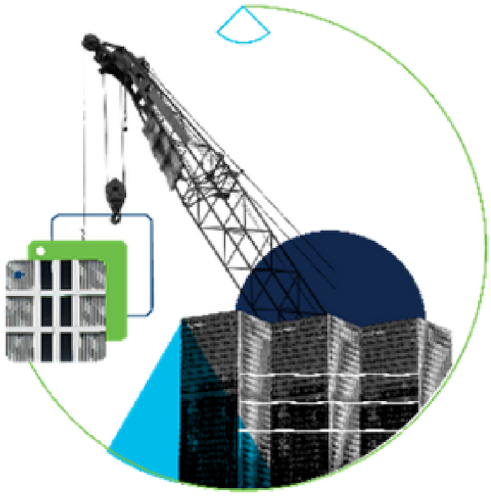
VISIBILITY



Grant the right level of network access to users across domains

SEGMENTATION

Shrink zones of trust and grant access based on least privilege



CONTAINMENT

Automate containment of infected endpoints and revoke network access

WHY WORKPLACE IN CISCO'S ZERO-TRUST?

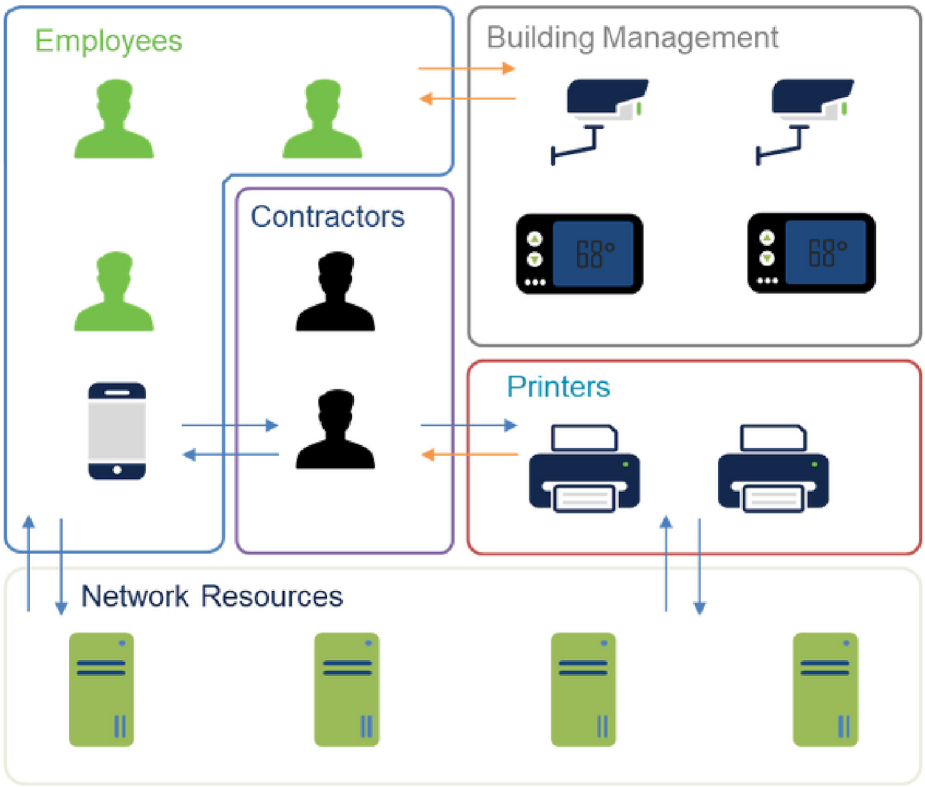
Visibility and control doesn't stop at the end user

THREATS	ZERO TRUST SOLUTION
Unauthorized endpoints or devices with unhygienic posture can disrupt productivity	No network access until endpoint trust is evaluated (authenticate and evaluate system health)
Noncritical assets with unrestricted access can make the entire infrastructure vulnerable	Provide confined access to essential services through macro and micro-segmentation
Compromised endpoints can infect other assets in the network through lateral movements	Continuously evaluate trust and apply adaptive controls to isolate threats in the real-time

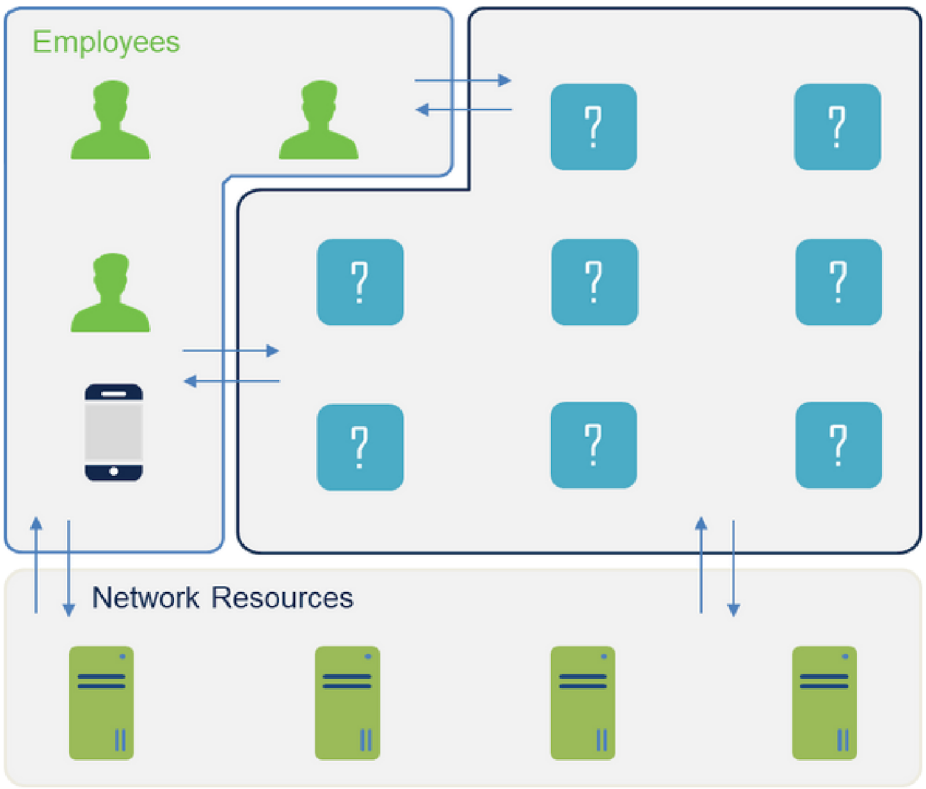
INTRODUCING ISE

LEAST PRIVILEGE ACCESS

EXPECTATION



VS. REALITY



HOW IDENTITY SERVICES ENGINE ENFORCES ZERO TRUST

Connecting trusted users and endpoints with trusted resources

Endpoint Request Access

•Endpoint is identified and trust is established

•Posture of endpoint verified to meet compliance

Trust continually verified

•Continually monitors and verifies endpoint trust level

•Vulnerability assessments to identify indicators of compromise

•Automatically Updates access policy

Endpoint classified, and profiled into groups

•Endpoints are tagged x/SGTs

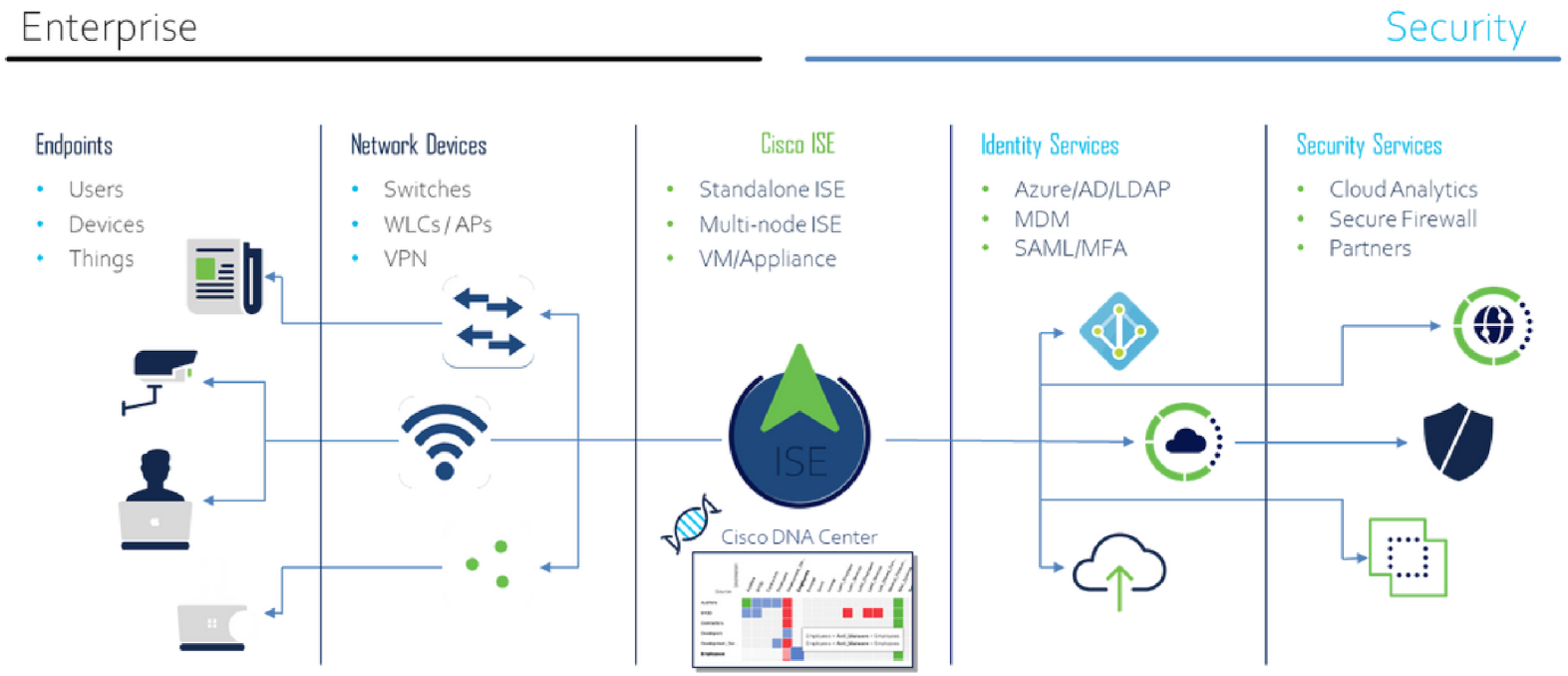
•Policy applied to profiled groups based on least privilege

Endpoint authorized access based on least privilege

•Access granted

•Network segmentation achieved

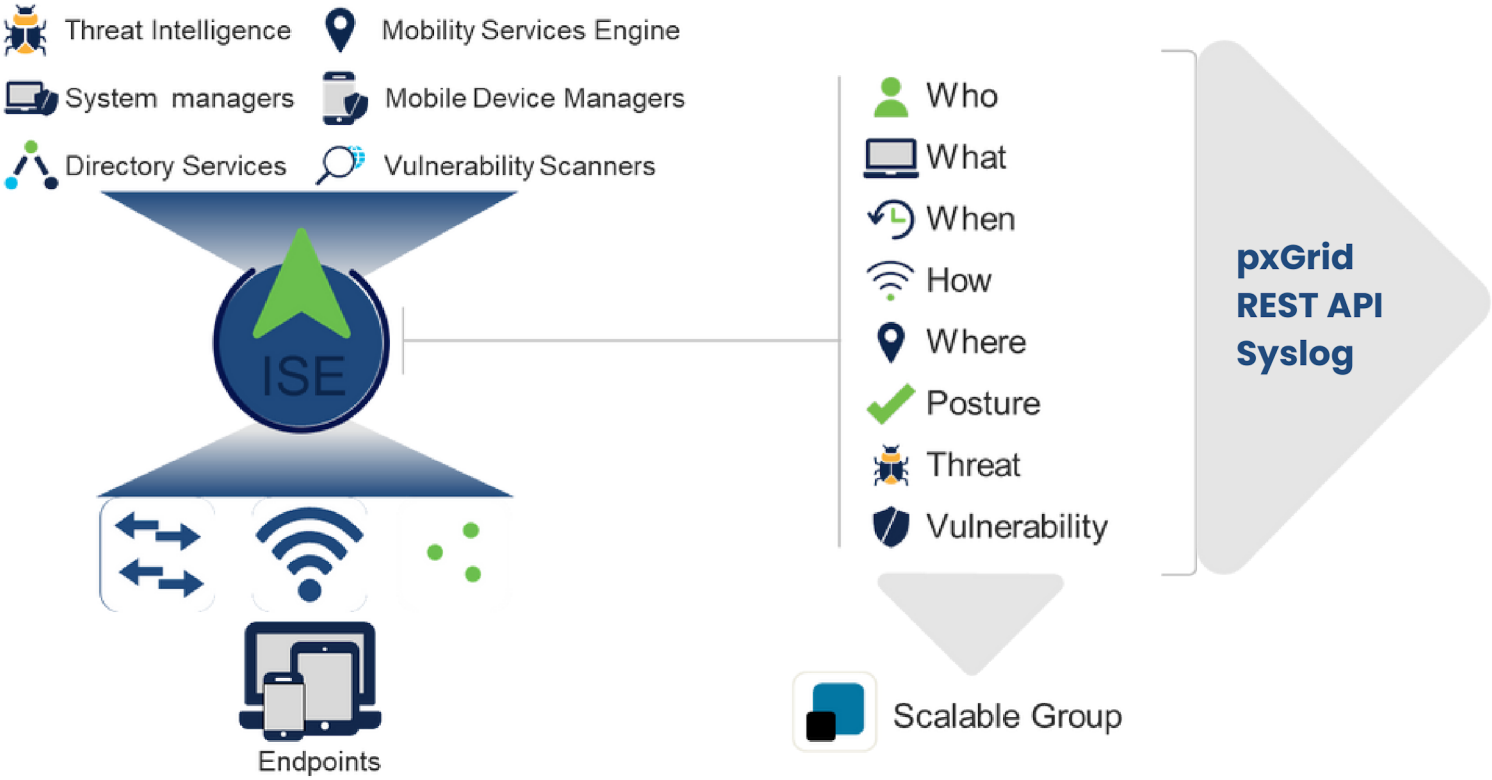
ISE PROVIDES ZERO TRUST FOR THE WORKPLACE



CONTEXT BUILD, SUMMARIZE, EXCHANGE

VISIBILITY AND ACCESS CONTROL

ISE builds context and applies access control restrictions to users and devices



CONTEXT REUSE

by eco-system partners for analysis & control