
cisco Live!
TURN
IT
UP
#CiscoLive

The bridge to possible

Differentiating with NIST Standards and Compliance in a Zero Trust World

Steve Vetter
Senior National Security Strategist
Industry Solutions Group

Tony Winfield
Senior Solutions Architect
Global Public Sector

PSOIND-1003

Agenda

- Introduction
- Criticality of an end-to-end architectural approach!
- The essence of Zero Trust
- The evolution of risk
- NIST's view of Zero Trust
- Cisco's alignment with NIST's Zero Trust Architecture and Cybersecurity Framework

Why are we talking about this today?

Embracing NIST Zero Trust enables a more strategic conversation

Better enable CXO and business/mission outcome conversations

Rise above point product conversations

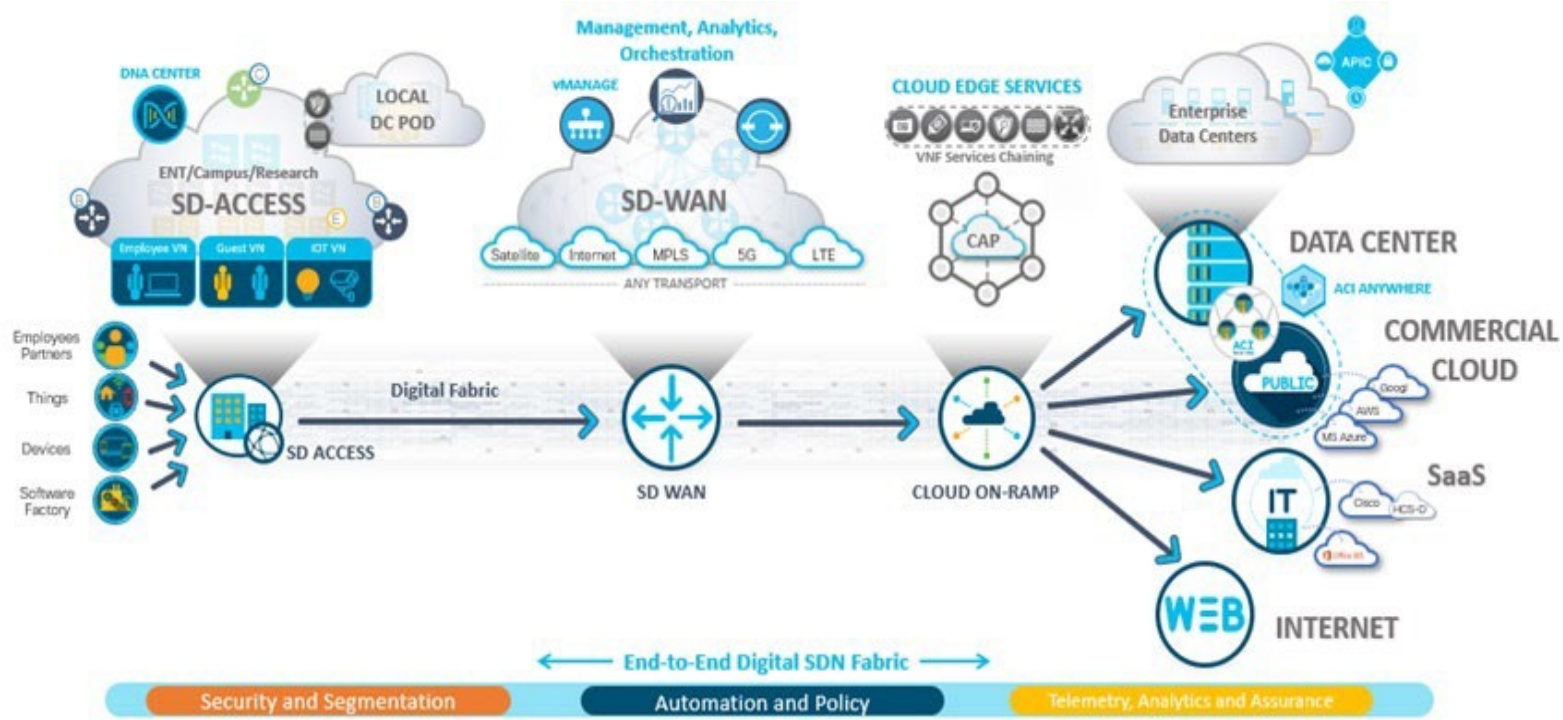
Help clients better understand what vendors can provide

Discuss Zero Trust / IoT in common language

Better enables comprehensive E2E strategy approaches

End-to-End Architectural Approach!

Comprehensive Security Architecture

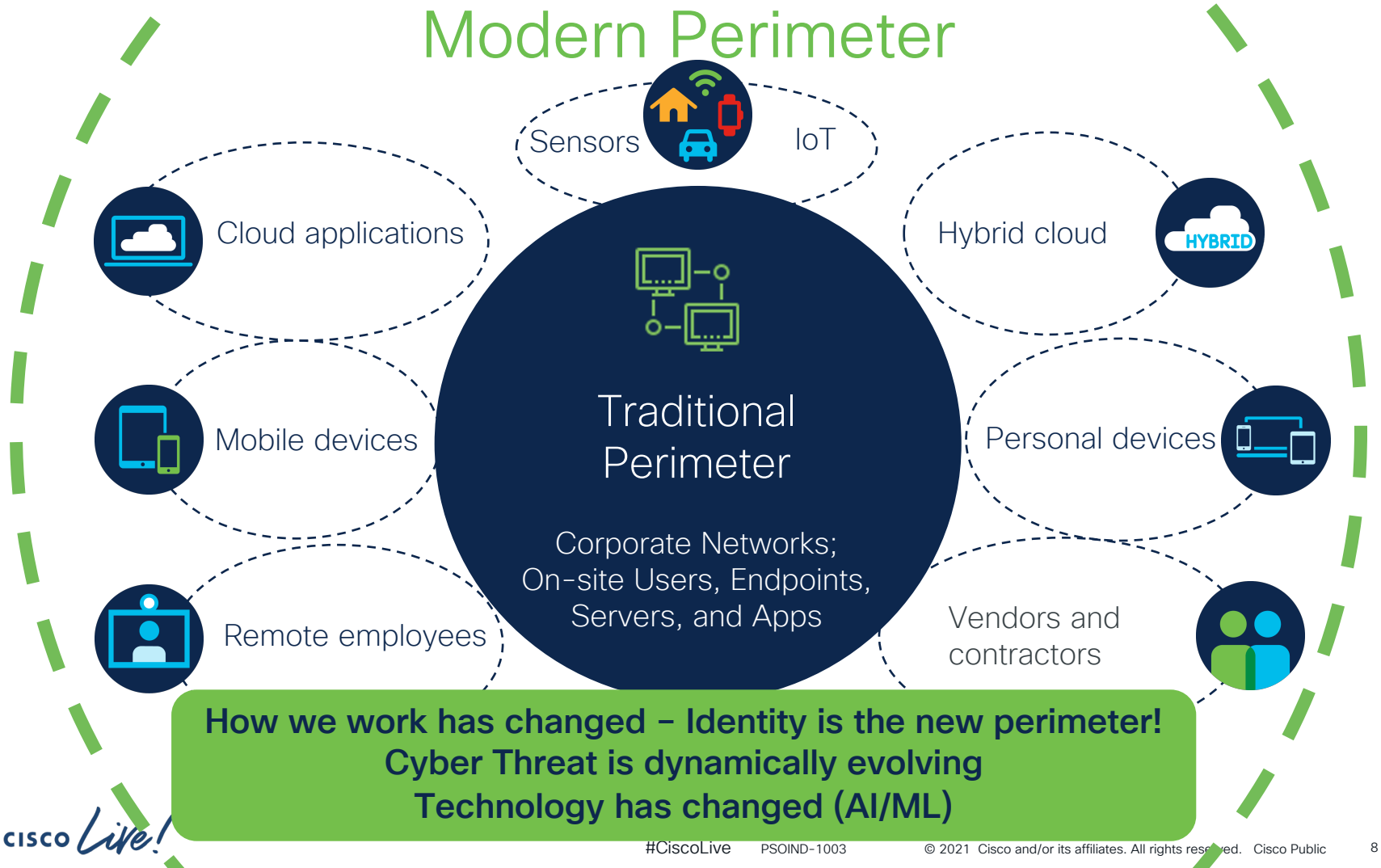


Driven by Zero Trust

The Essence of Zero Trust

cisco Live!

Modern Perimeter



How we work has changed – Identity is the new perimeter!
Cyber Threat is dynamically evolving
Technology has changed (AI/ML)

A bit of Zero Trust history

Jericho Forum | ZT | BeyondCorp | CARTA & ZTX | ZTA

2004 | 2010 | 2014 | 2017 | TODAY

De-perimeterization

An international group of corporate CISOs and vendors (Cisco hosted initial meeting)

Focused on solving “de-perimeterization” problem

Early output calling for “the need for trust”

Multiple Models Emerge

Forrester coined Zero Trust.

Google published their ZT solution as BeyondCorp

Forrester then expands to Zero Trust eXtended Platform

Gartner names their model Continuous Adaptive Risk and Trust Assessment

Generalized

The industry has largely accepted Zero Trust Architecture as the general term

NIST SP800-207

Key to Zero Trust

NO implicit trust – trust is explicitly stated and dynamically calculated based on context and security
And it should be done continuously

The Evolution of Risk

cisco Live!

A Question of Risk

Which policy would you choose?		
Option 1	Liability	$200/Year
Option 2	+ Collision	$300/Year
Option 3	+ Comprehensive	$600/Year

Your Car: 2006 Acura TL
Book Value: $6500

Move to Stronger Risk Management

Compliance

Risk determination based on checklist

Cyber Hygiene

Risk determination based on automated management of assets and accounts

Threat-based Approach

Risk determination based on performance-based measures

Slide courtesy of Department of Homeland Security (DHS)

The NIST CyberSecurity Framework (CSF)

Enables more effective management of cyber risk

- **What:** Prioritized, flexible, repeatable, performance-based, cost-effective approach
- **Goal:** Identify, assess and manage cyber risks
- **Key:** Business drivers guide cyber resources and activities to better manage risk
- **3 Parts:** Framework Core / 4 Maturity-Implementation Tiers / Your Profile

The Core:

- Aligns with risk tolerance, business requirements, organizational resources

- **Adaptable:** to IT / OT / IoT / IIoT / ICS / FRCS / CPS / Critical Infrastructure

It's FLEXIBLE.....and it's NOT a Checklist!!!

NIST Cybersecurity Framework – Functions

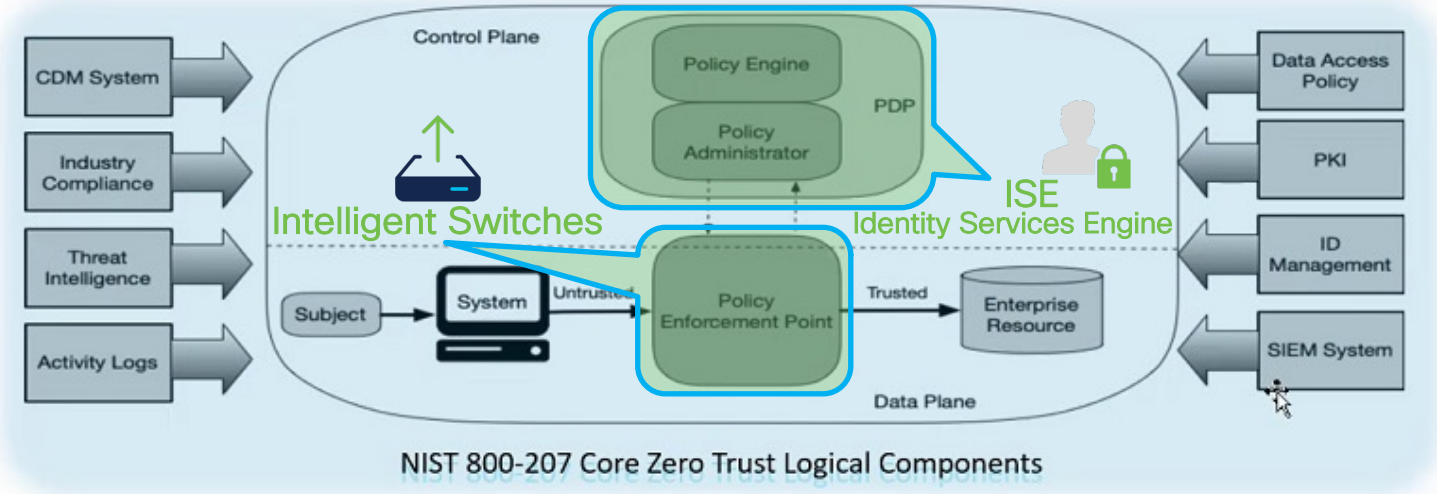
Functions		
ID	Identify	Know what you have
PR	Protect	Secure what you have
DE	Detect	Spot threats quickly
RS	Respond	Take action immediately
RC	Recover	Restore operations

NIST CyberSecurity Framework (CSF) – Categories

Functions		Category	
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

NIST Zero Trust

NIST Zero Trust Architecture – SP 800-207



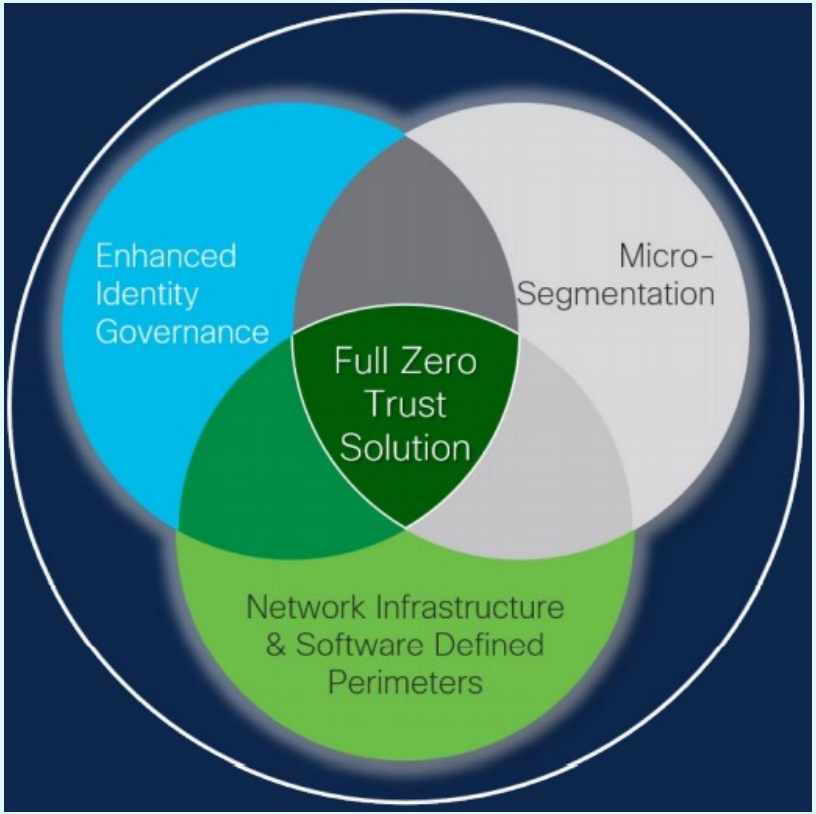
NIST 800-207 Core Zero Trust Logical Components

"The key to a successful Zero Trust journey is taking the first steps, often by leveraging existing enterprise tool investments."

{NIST SP-800-207}

Zero Trust – Holistic visibility

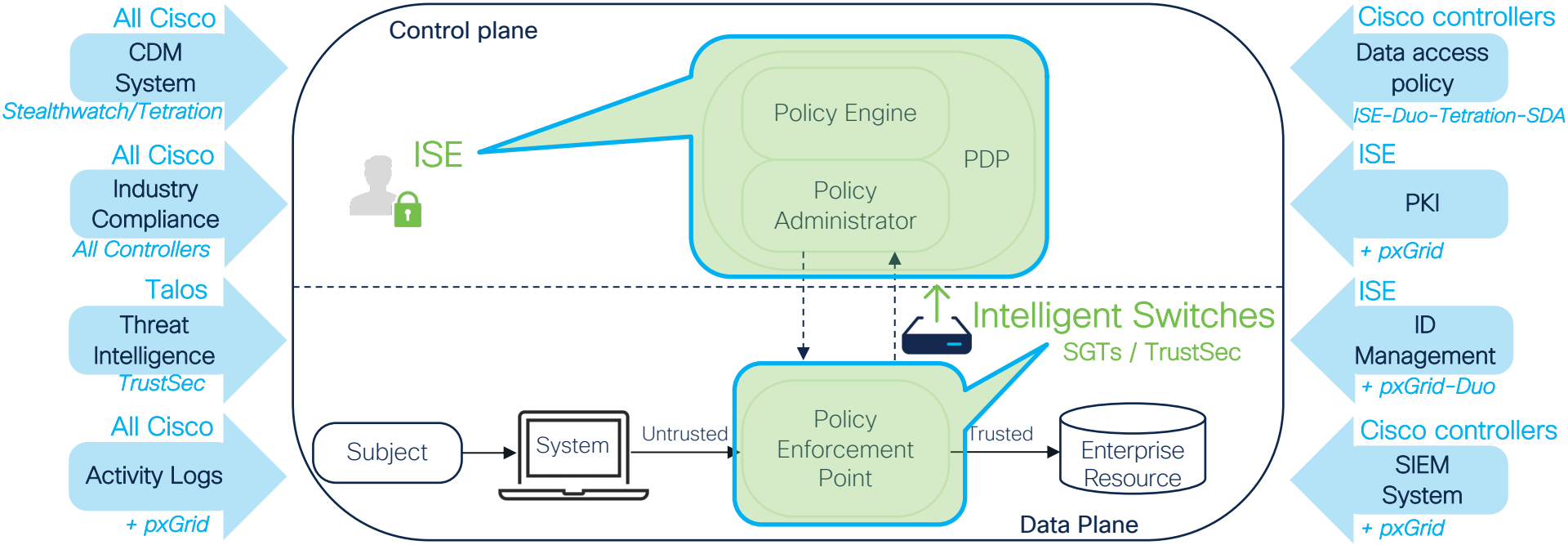
NIST Zero Trust Architecture – SP 800-207 – Approach Variations

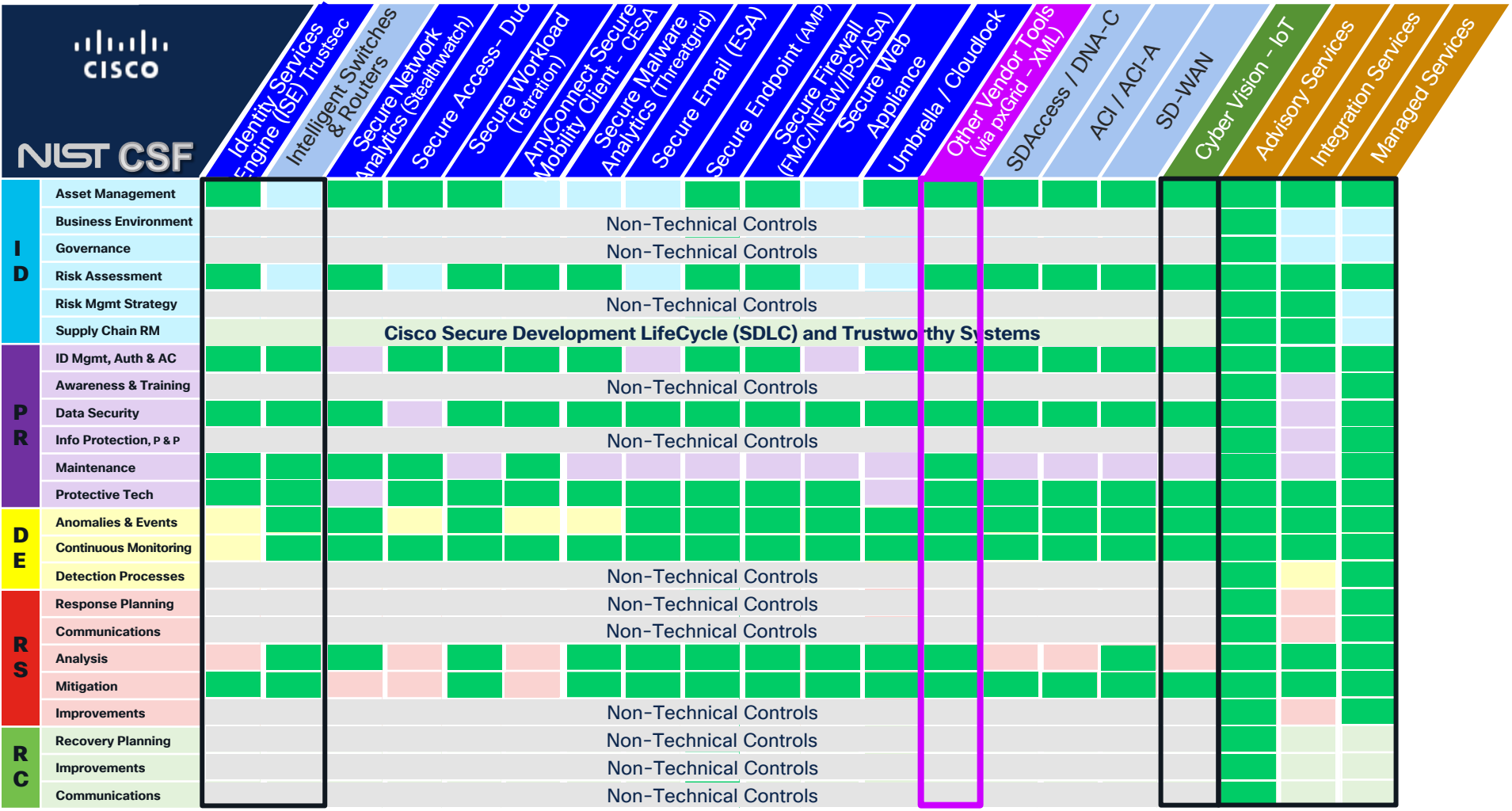


Cisco Alignment with NIST's Zero Trust Architecture and Cybersecurity Framework

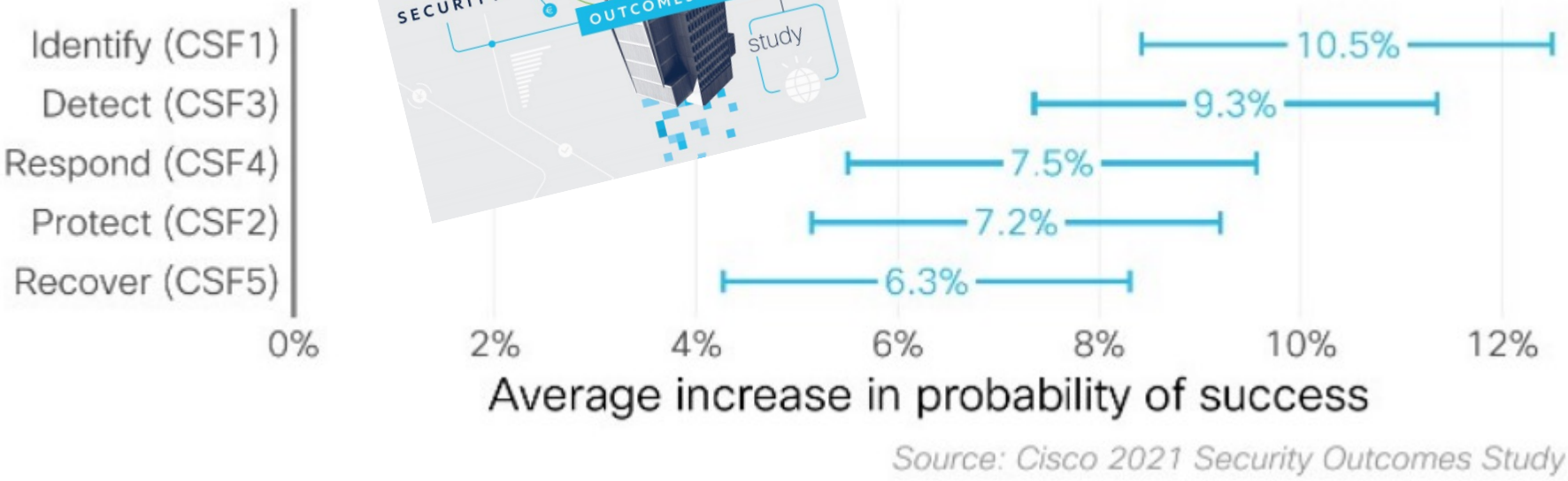
cisco Live!

NIST Zero Trust Architecture – SP 800-207





Value of additional Investments for improving NIST CSF Program Success



Source: Cisco 2021 Security Outcomes Study

Summary

- Comprehensive security is enhanced using an end-to-end architectural approach
- Desired business/mission outcomes, risk tolerance discussions and existing investments will inform your tailored Zero Trust journey
- Cisco's strong alignment with NIST's Zero Trust Architecture and Cybersecurity Framework could be a tremendous help with your cybersecurity efforts

The bridge to possible

Thank you


cisco Live!
TURN
IT
UP
#CiscoLive