CISCO
SECURE

CISCO The bridge to possible

Zero Trust
There I said it – Now what?

Oregon Cyber Resilience Summit

Peter Romness
Cybersecurity Principal
US Public Sector CTO Office

October 2021

US PUBLIC SECTOR
MT&G
MARKET TRANSFORMATION & GROWTH

You may be wondering...

How can I protect

Users,

Devices,

Data and

Applications

When they are Everywhere?

~~Deperimeterization~~

~~Borderless Network~~

Zero Trust

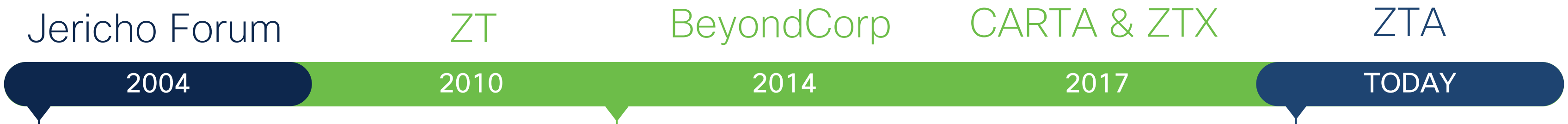
"Assume everything is bad
until proven otherwise"

Zero Trust

- Is not something you buy
- Assumes NO security perimeter
- NO automatic access once “inside”
- Trust must be earned for access to every asset, every time

It’s really more like “earn trust”
But that wouldn’t sound so cool!

A little bit of Zero Trust history



Jericho Forum — 2004

ZT — 2010

BeyondCorp — 2014

CARTA & ZTX — 2017

ZTA — TODAY

De-perimiterization

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

Focused on solving “de-perimiterization” 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

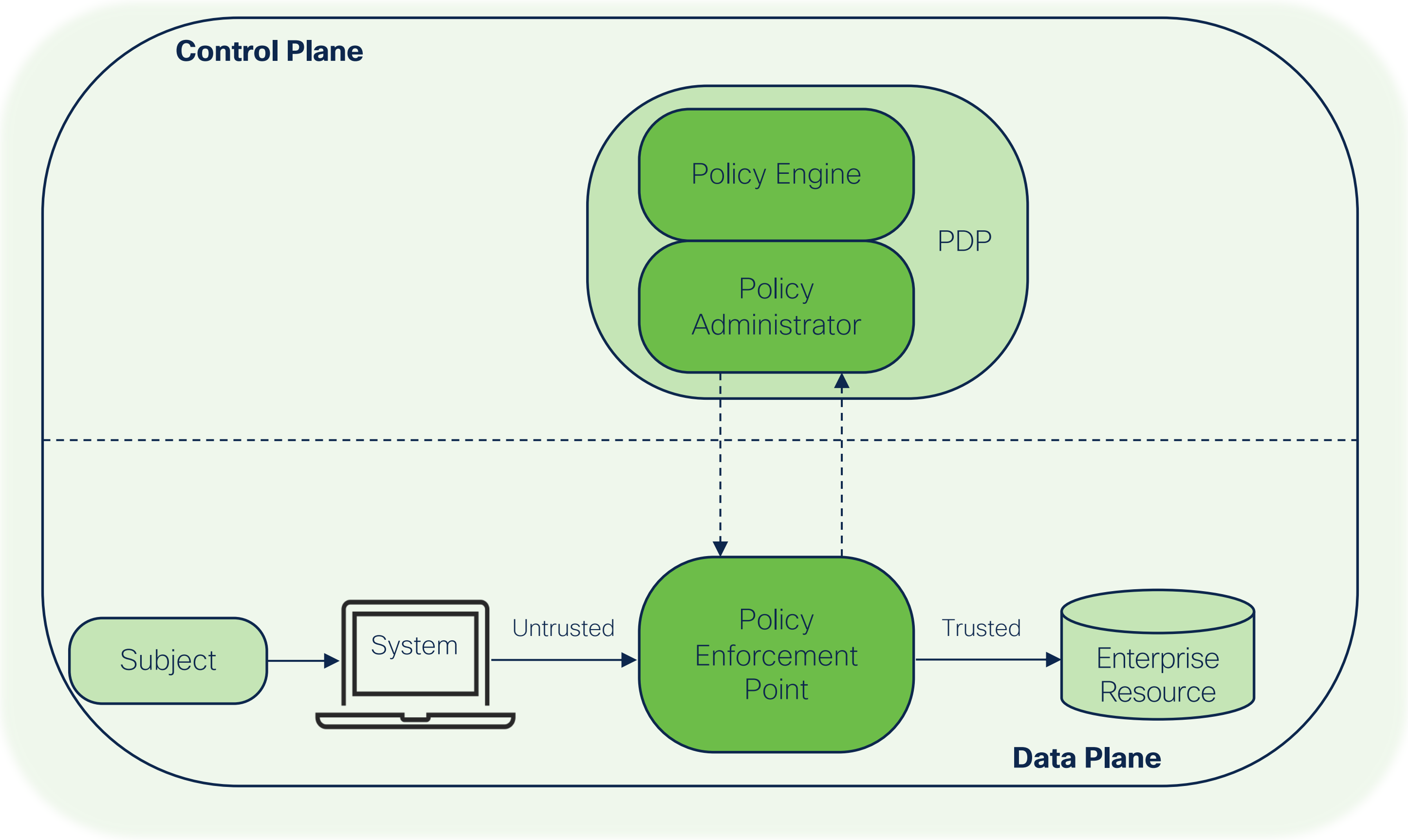
Gartner names their model Continuous Adaptive Risk and Trust Assessment

Generalized

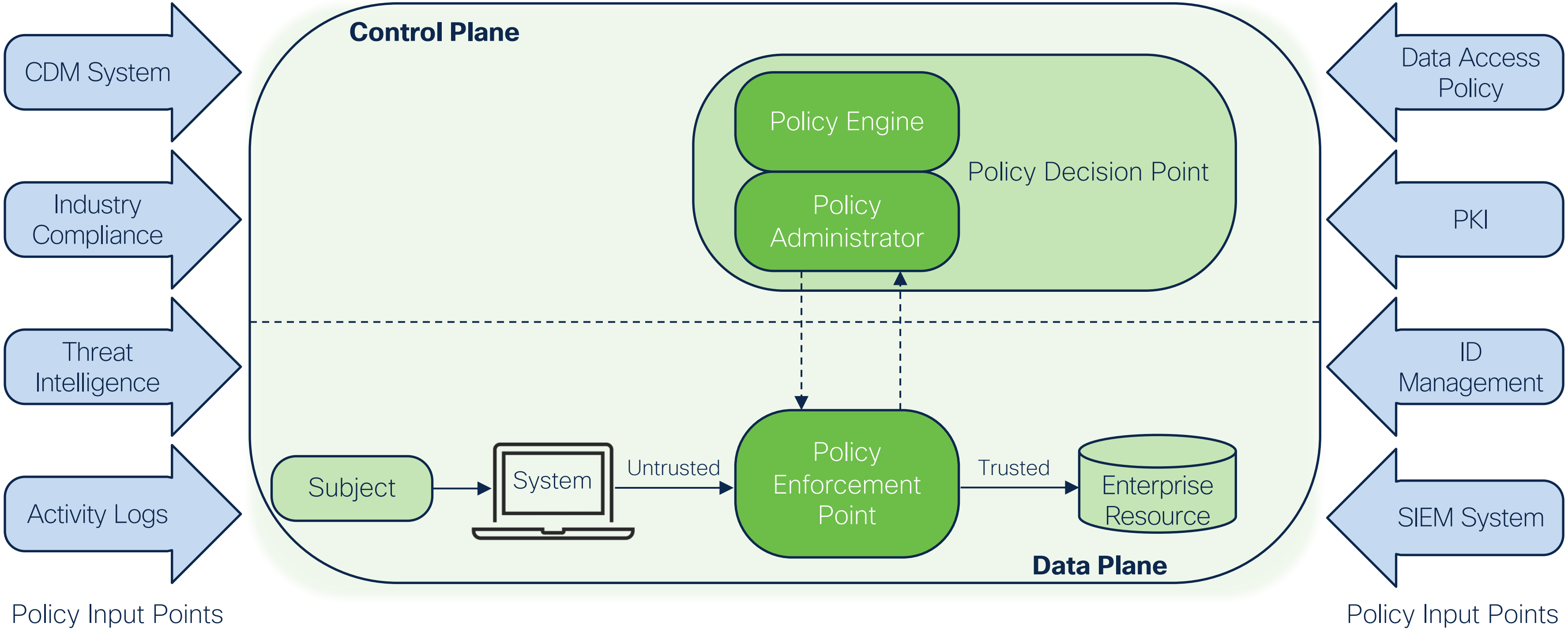
The industry has largely accepted Zero Trust Architecture as the general term

NIST SP800-207

The Heart of NIST Zero Trust Architecture – SP 800-207



NIST Zero Trust Architecture – SP 800-207

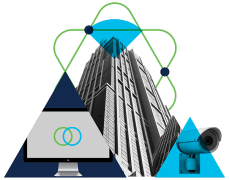


Cisco's Approach
The 3 W's

How can I protect

Trusted Workforce

Users



Devices

Trusted Workplace

Applications
& Data

Trusted Workload

What we’re protecting:

WorkFORCE

Employees

Contractors

Partners

Vendors

Auditors

Customers

WorkPLACE

IoT

APIs

Scripts

Printers

Cameras

Containers

Microservices

OT-Equipment

Virtual Machines

Medical Equipment

Point-of-Sale Systems

WorkLOAD

VPCs

Portals

APIs

Network

Servers

Databases

Containers

Applications

NW Segment

Micro-Services

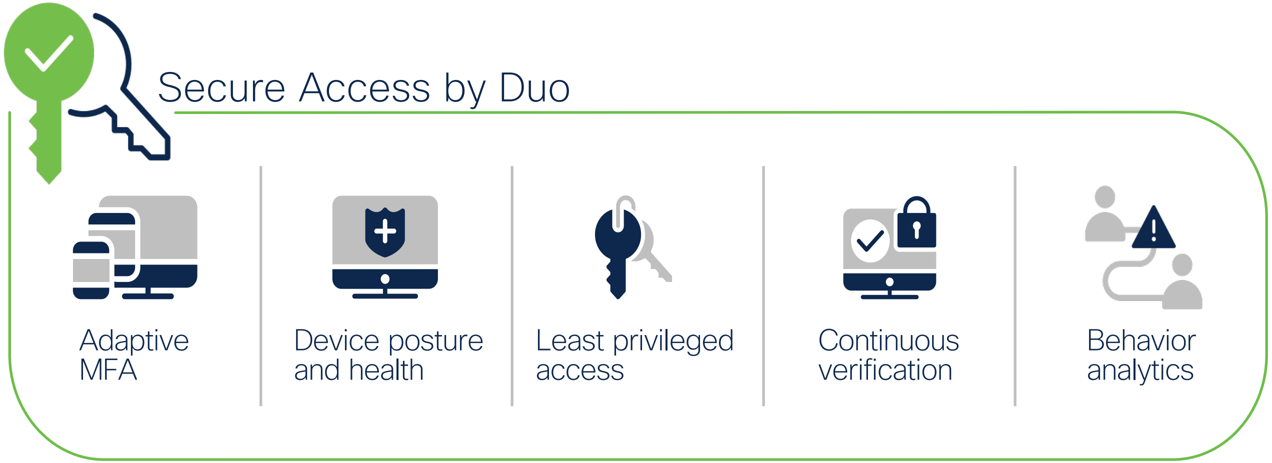
Duo for Workforce

Ensure only the right users and secure devices gain access

- Verify user identity with multi-factor identification
- Check device security posture
  - ✓ Pass code on device
  - ✓ Device software up-to-date
- Assure trust to every application
  - ✓ On-Prem
  - ✓ Cloud

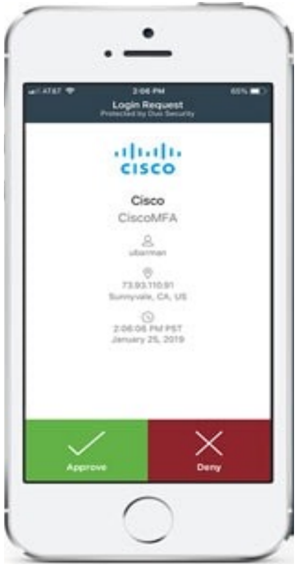
Secure Access Duo

World’s easiest and most secure MFA



Secure Access by Duo

- Adaptive MFA
- Device posture and health
- Least privileged access
- Continuous verification
- Behavior analytics

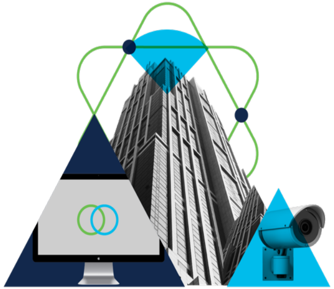


Login Request
Protected by Duo Security

Cisco
CiscoMFA
ubarman
73.93.110.91
Sunnyvale, CA, US
2:06:06 PM PST
January 25, 2019

Every user. Every device. Every application… And it’s easy

Verify the identity of all users before granting access to applications



SDA for Workplace

Cisco
TrustSec,
ISE,
Meraki

Secure all user and device connections across your enterprise

- Authenticate & Authorize users & devices
- Grant granular access only as approved
  - ✓ For Hardware, Apps & Data
  - ✓ Based upon Who, What, When, Where, How of connection
- Micro-Segmentation to the individual port
- Monitor & Control access as needed

Establish Trust with SD-Access

Establish Trust

Discover and classify devices

WITH

IoT device profiling

BYOD lifecycle management

User device Posture

Enforce Trust-Based Access

Context-based network access control policy for users and things

WITH

Dynamic precise policies

Group-based (SGT)

Continuous Trust Verification

Continuous security health monitoring of devices

BY

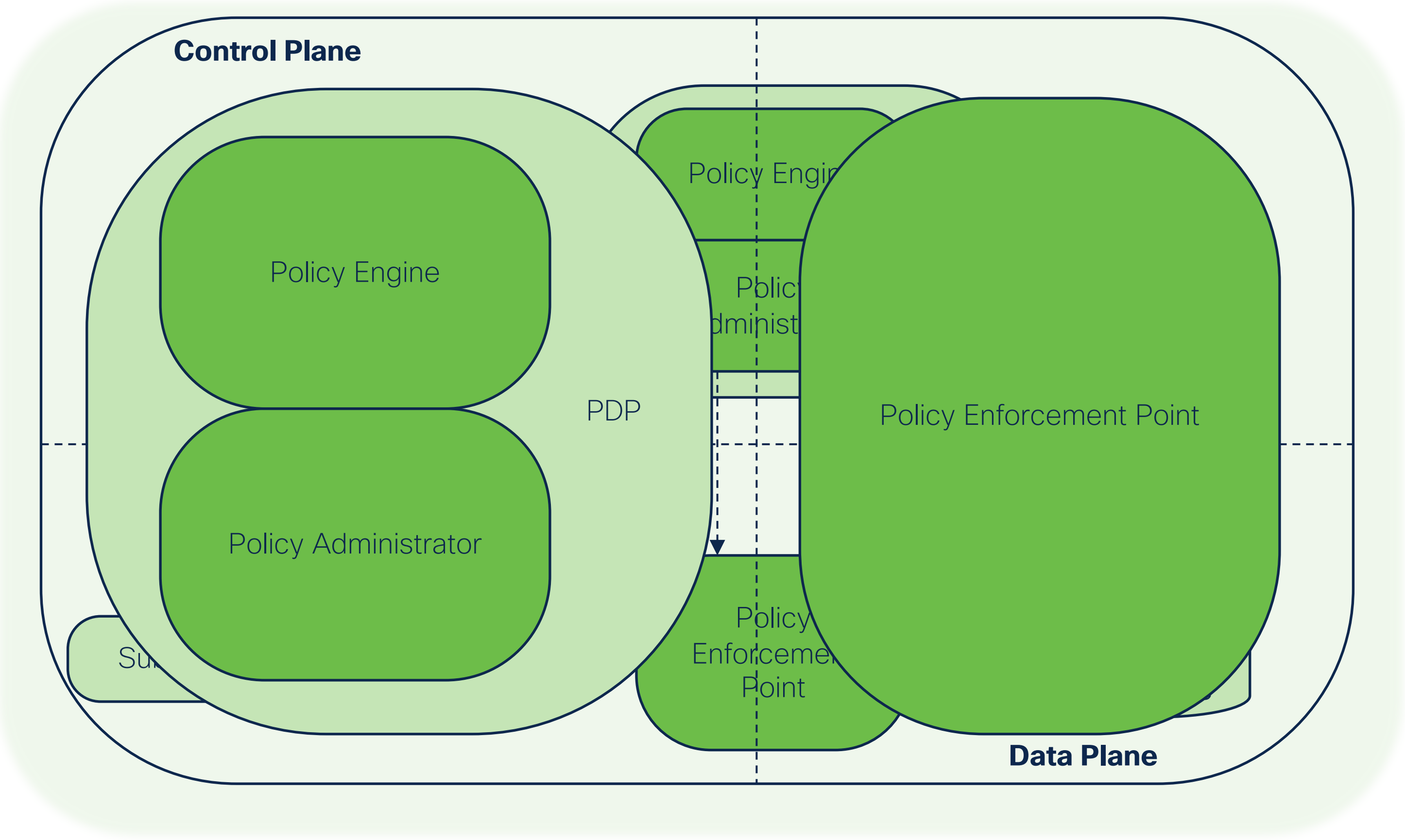
Continuous Posture

Vulnerability assessments

Indications of compromise

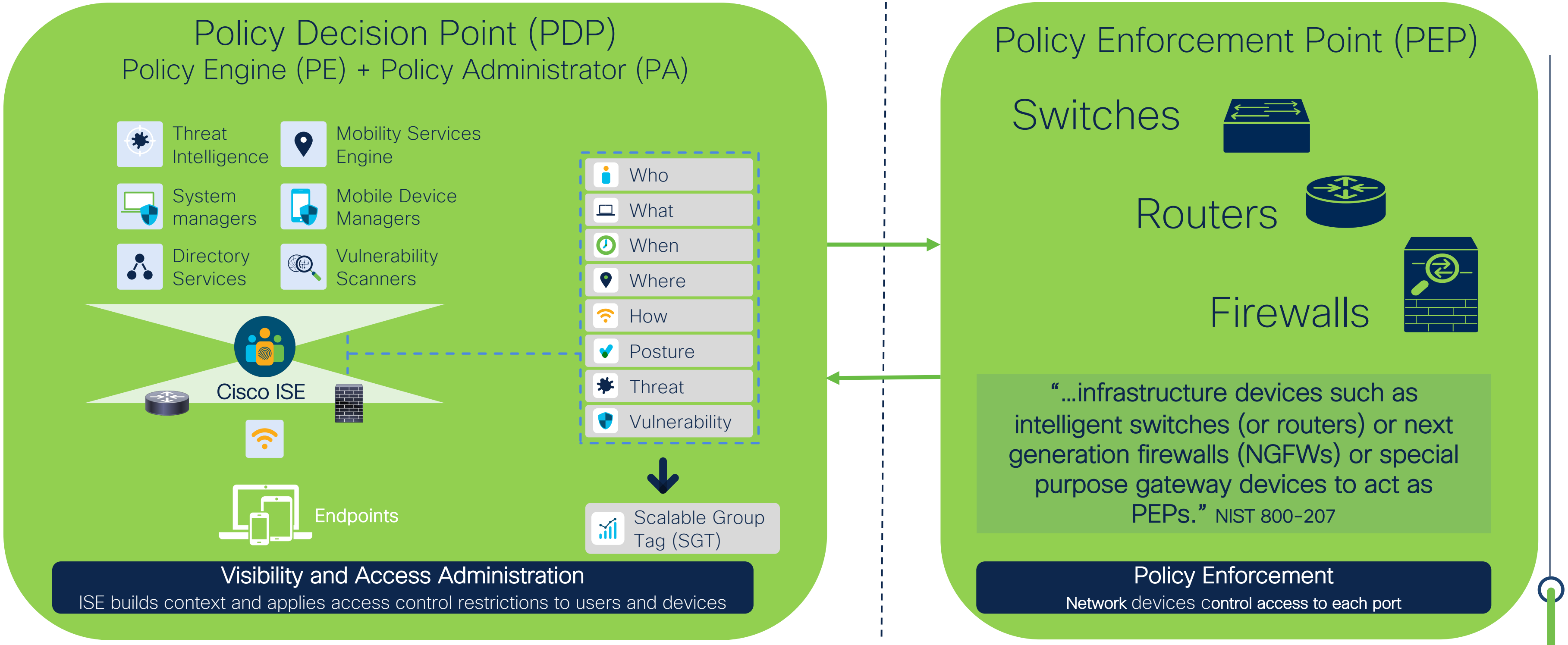
SECURE

From NIST Zero Trust Architecture – SP 800-207



Identity Services Engine

Network Devices



Policy Decision Point (PDP)

Policy Engine (PE) + Policy Administrator (PA)

Threat Intelligence	Mobility Services Engine
System managers	Mobile Device Managers
Directory Services	Vulnerability Scanners

Cisco ISE

Endpoints

- Who
- What
- When
- Where
- How
- Posture
- Threat
- Vulnerability

Scalable Group Tag (SGT)

Visibility and Access Administration

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

Policy Enforcement Point (PEP)

Switches

Routers

Firewalls

"…infrastructure devices such as intelligent switches (or routers) or next generation firewalls (NGFWs) or special purpose gateway devices to act as PEPs." NIST 800-207

Policy Enforcement

Network devices control access to each port

SECURE

Secure Workload (Tetration) for Workload

Secure all connections within your apps, across multi-cloud

- Secure hybrid, multicloud workloads
- Contain lateral movement with application segmentation
- See and control dependencies within databases and applications.

Secure Workload

Secure Workload (Tetratrion)

Apply Zero Trust to Workloads (Apps, Data, VM’s, Containers, etc)

- Generates unique policy per workload
- Pushes policy to all workloads
- Workload securely enforces policy
- Continuously computes policy from identity and classification changes

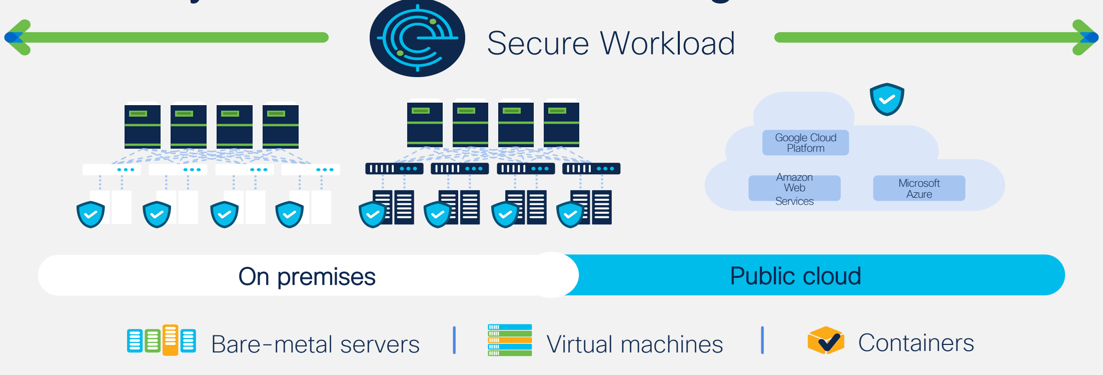
Contain lateral movement

Continuously track security compliance

Identify behavior anomalies

Reduce attack surface

Unify visibility and enable automation



On premises | Public cloud

Bare-metal servers | Virtual machines | Containers

Cisco Secure Zero Trust

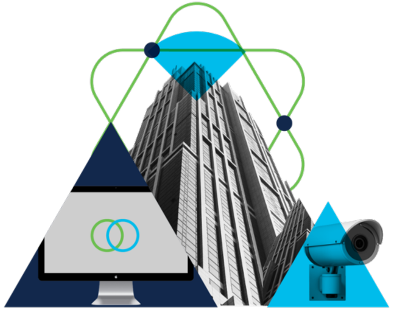
A comprehensive approach to securing all access across your networks, applications, and environment.

Workforce

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

Workloads

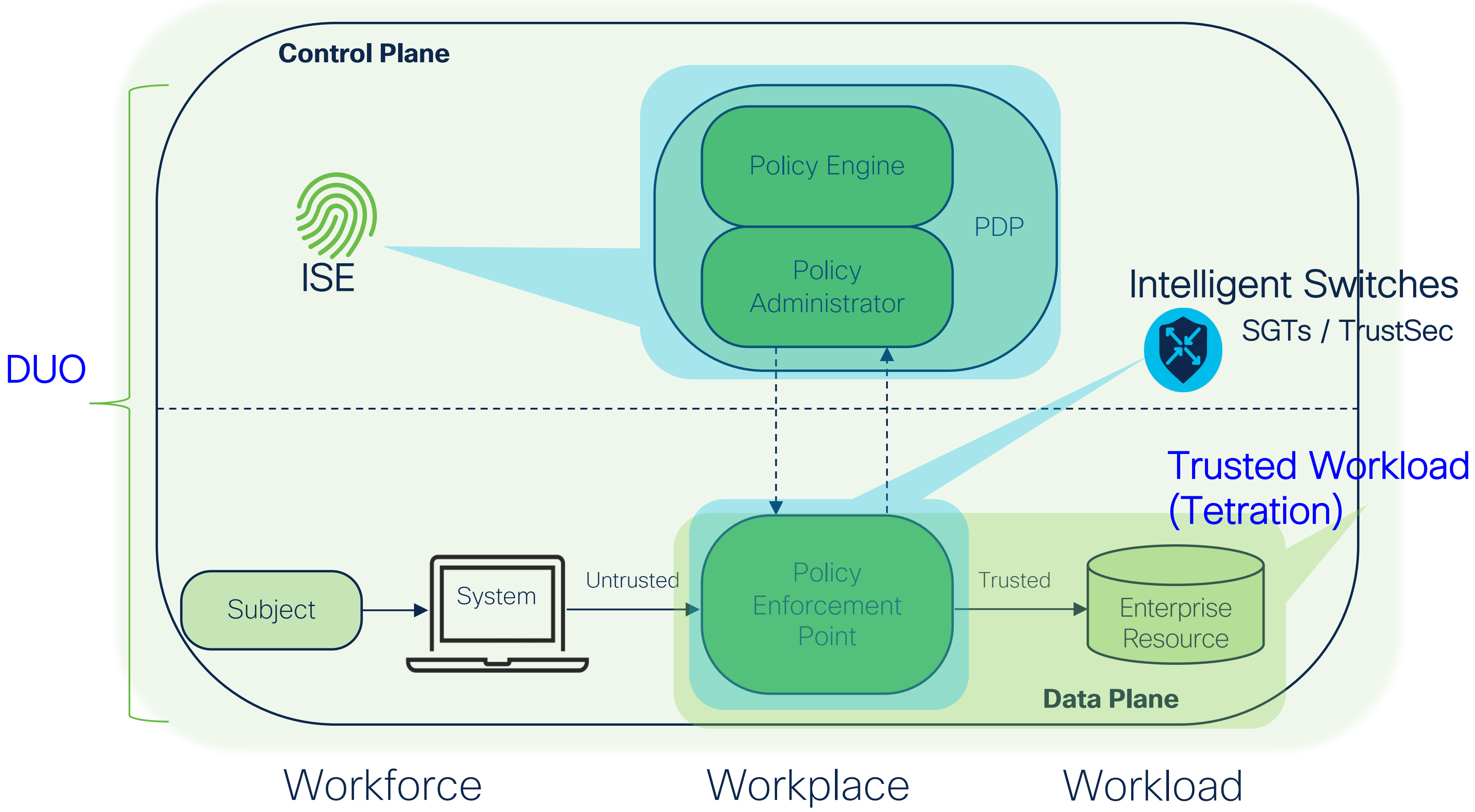
Secure all connections within your apps, across multi-cloud.



Workplace

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

NIST Zero Trust Architecture – SP 800-207



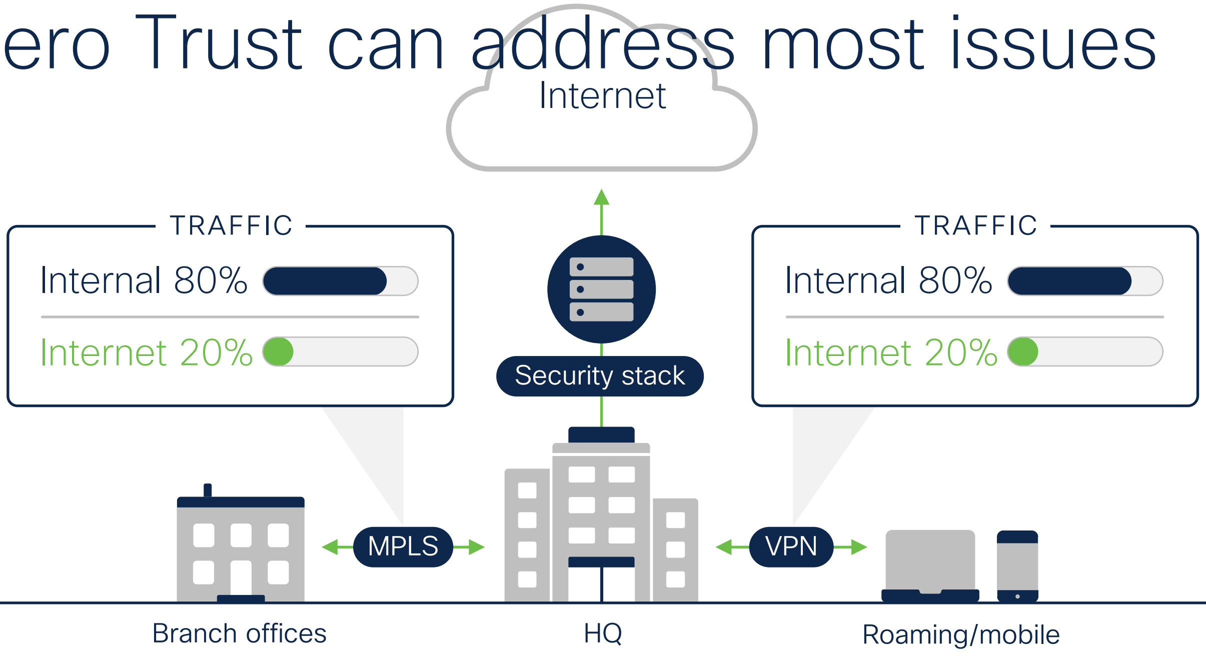
Historic traffic flows

Led to the age of perimeter-based security and networking

Appling Zero Trust can address most issues

Network:
Centralized

Security:
Single, on-premise
security stack



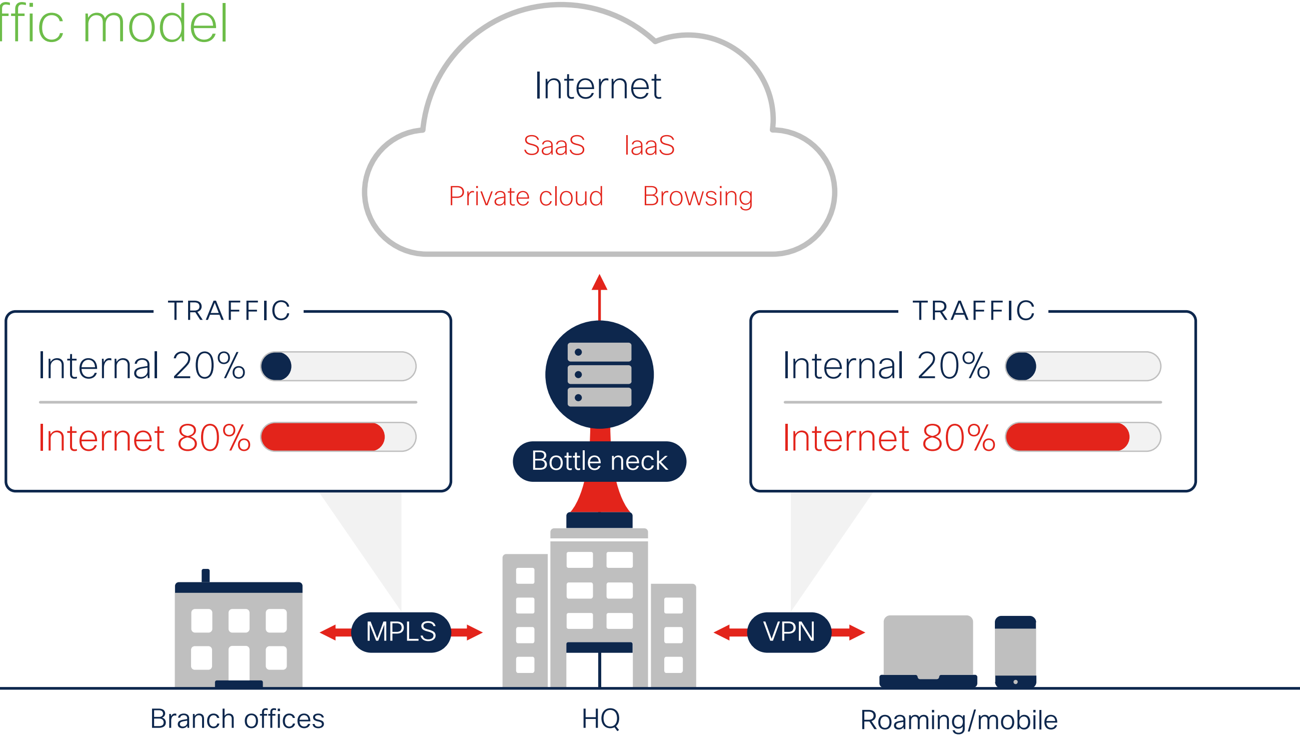
SECURE

Changes in the types of traffic and destinations

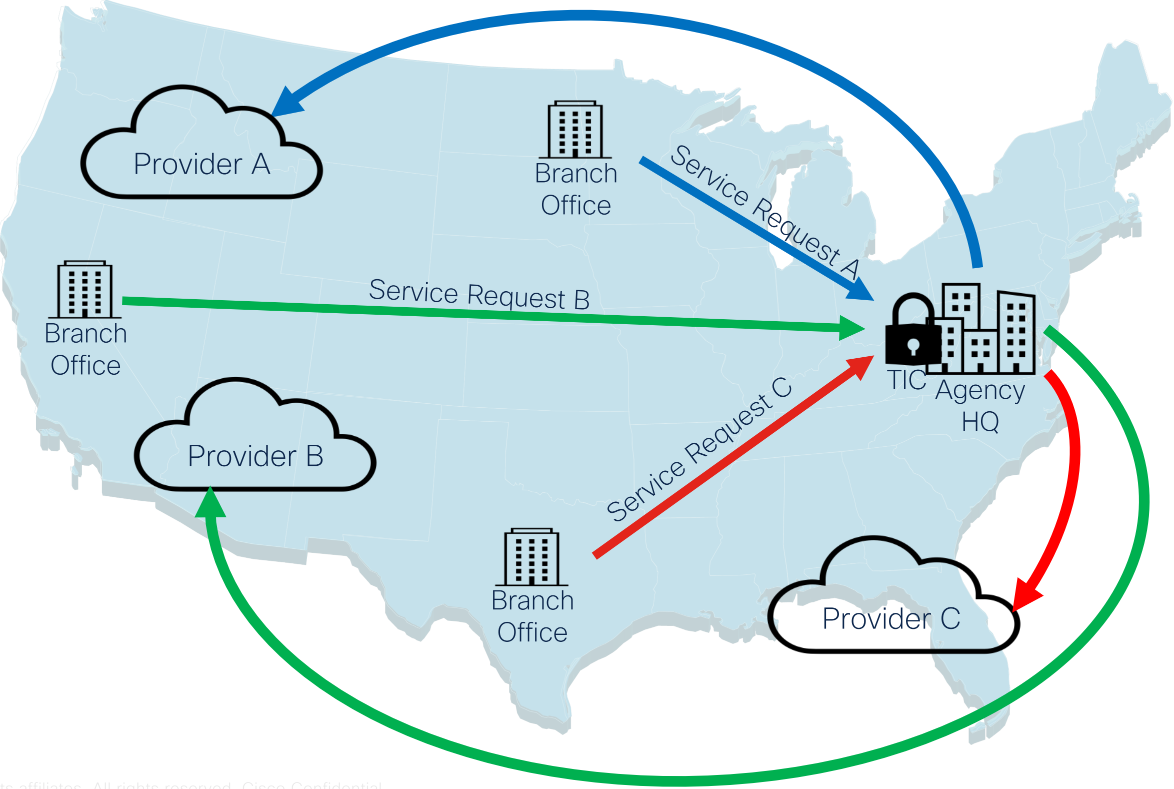
Have inverted the traffic model

Problems:

- Costs
- Performance
- # Tools/vendors
- Integrations
- Maintenance



In Federal Government, This is TIC

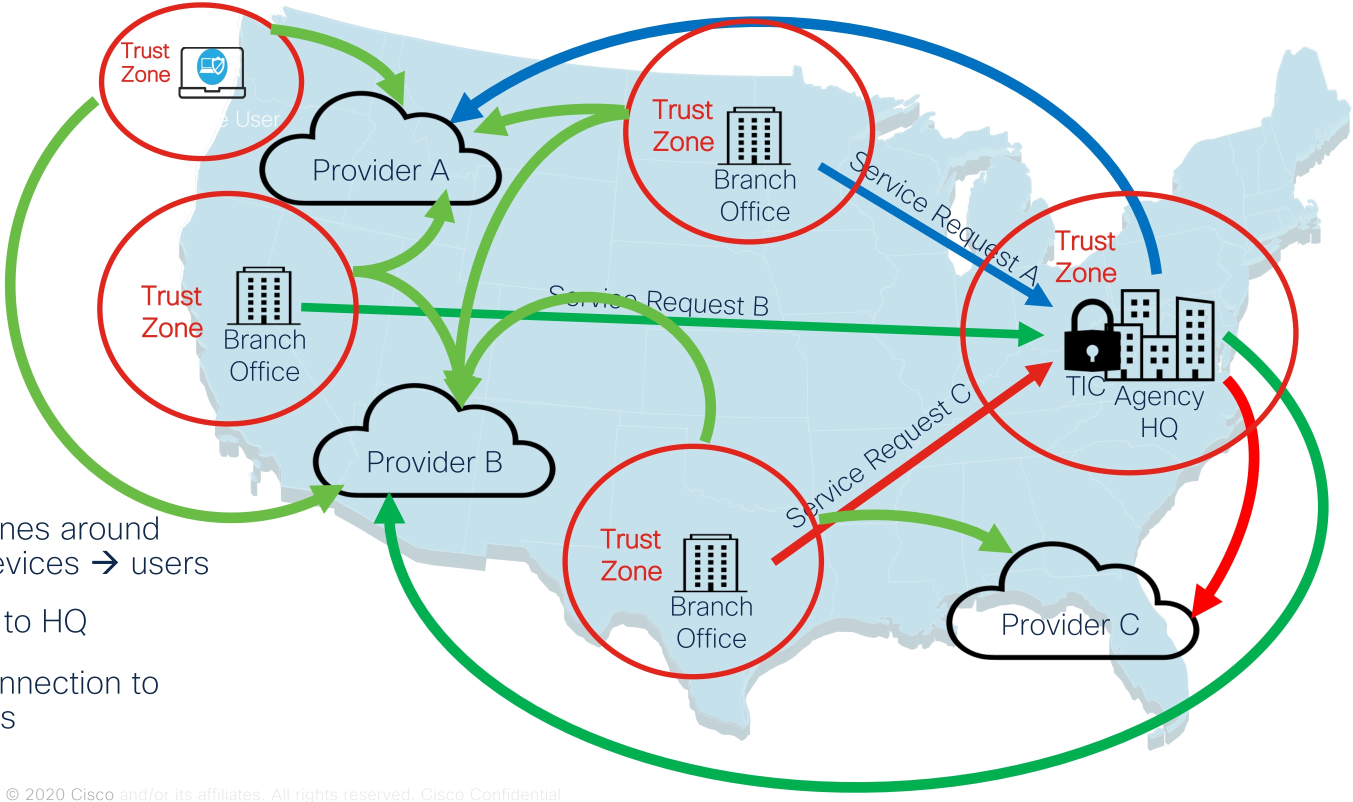


Flexibility of TIC 3.0

TIC 3.0 is an implementation of Zero Trust Principles

- Supports the creation of trust zones
- Trust zones create additional network boundaries
- Allows additional security capabilities to give agencies greater visibility into their network, leading to operational and fiscal efficiencies
- Maintains feed to DHS (“Einstein”) for cross-government threat intelligence
- Guidance → Not a mandate

From “TIC Tax” to TIC 3.0



- Create trust zones around branches → devices → users
- Maintain traffic to HQ
- Allow direct connection to “trusted” clouds

This Photo by Unknown Author is licensed under CC BY-NC

Next, reduce complexity and improve performance by unifying connectivity, security and identity

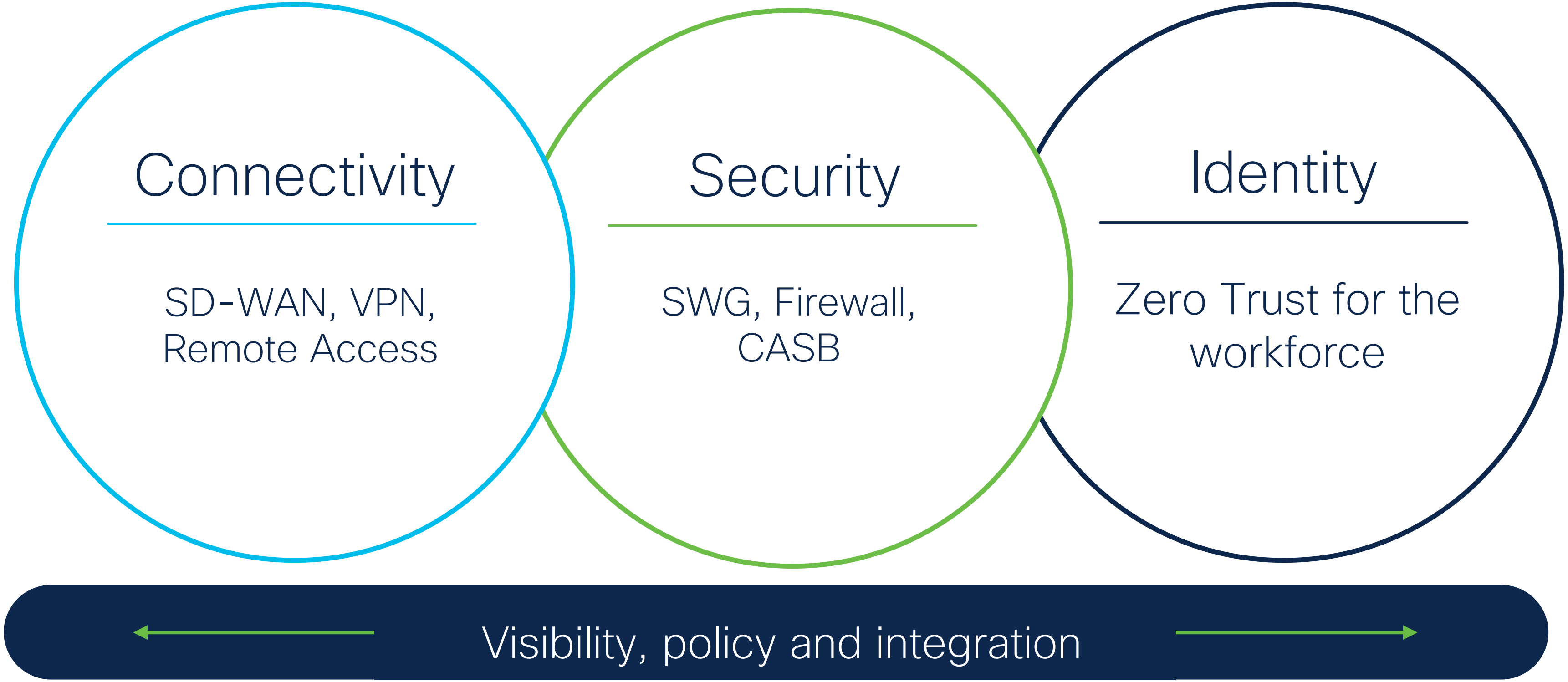
There are many names for this multi-function approach…

Gartner®	Secure Access Service Edge (SASE)
FORRESTER®	Zero Trust Edge
ESG Enterprise Strategy Group	Elastic Cloud Gateway

> “a **network architecture** that combines **VPN and WAN capabilities with cloud-native security** functions like secure web gateways, cloud access security brokers, firewalls, and zero-trust network access”
>
> – Gartner

…but full agreement on the move to cloud-native aggregation

SASE includes much more than security



Connectivity

SD-WAN, VPN,
Remote Access

Security

SWG, Firewall,
CASB

Identity

Zero Trust for the
workforce

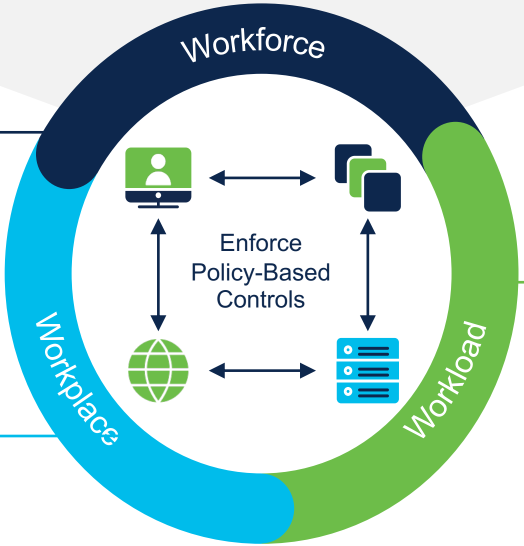
Visibility, policy and integration

SASE and Zero Trust

Secure access for your workforce, workloads and workplace

Cloud transition focuses on workload, workforce, and workplace

Ensure only the right users and secure devices can access applications

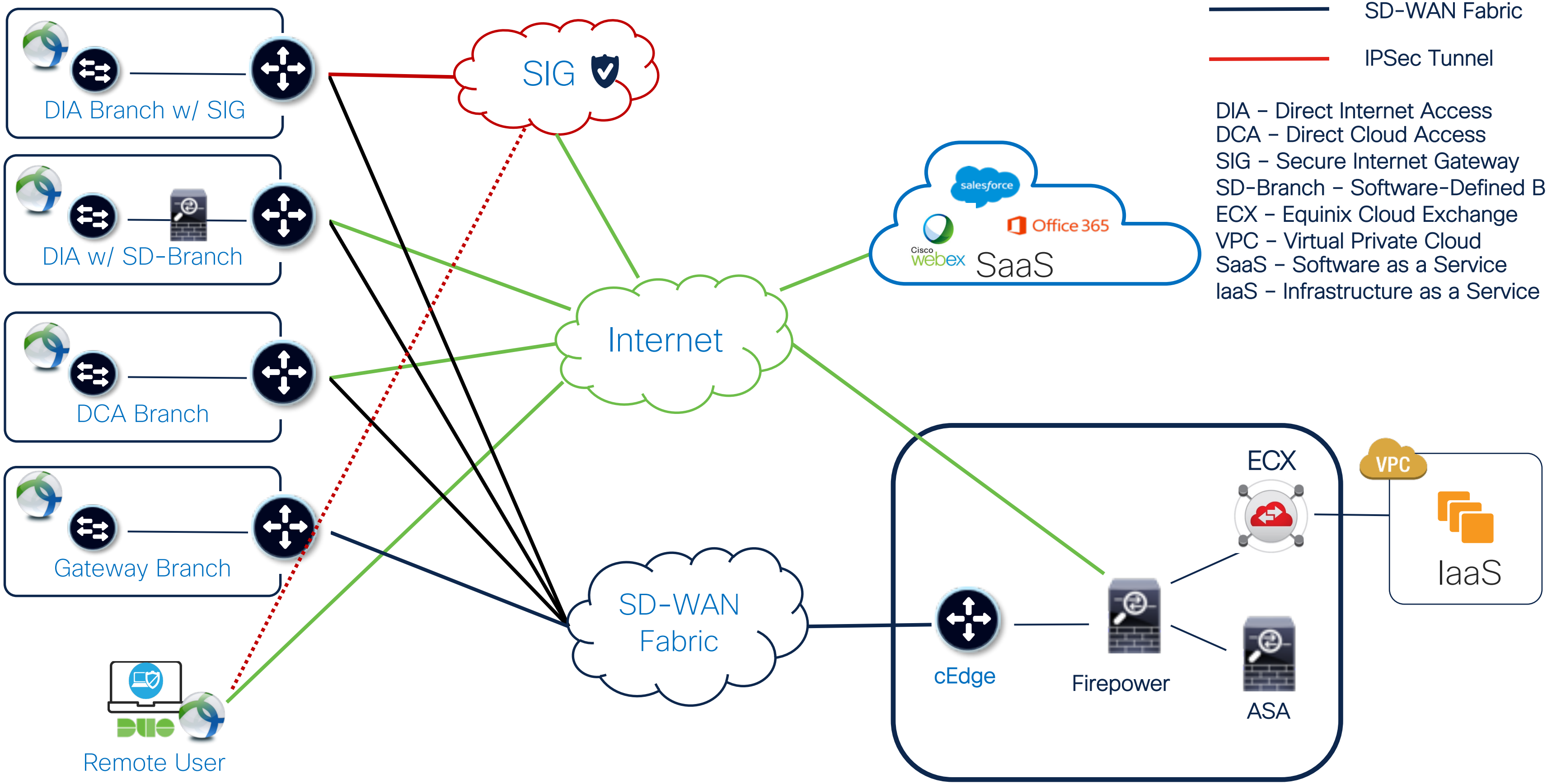


Secure all connections within your apps,
across multi-cloud

Secure all user and device connections across your network, including 5G.

Cisco Sample SASE/TIC 3.0 Architecture

For Use Cases



Direct Internet Access

SD-WAN Fabric

IPSec Tunnel

DIA – Direct Internet Access
DCA – Direct Cloud Access
SIG – Secure Internet Gateway
SD-Branch – Software-Defined Branch
ECX – Equinix Cloud Exchange
VPC – Virtual Private Cloud
SaaS – Software as a Service
IaaS – Infrastructure as a Service

AnyConnect – Not your grandfathers VPN

Think of it as a Security Connector

- Basic VPN
- Advanced VPN
- Endpoint Compliance
- Enterprise Access
- Cloud Edge
- Threat Protection
- Network Visibility

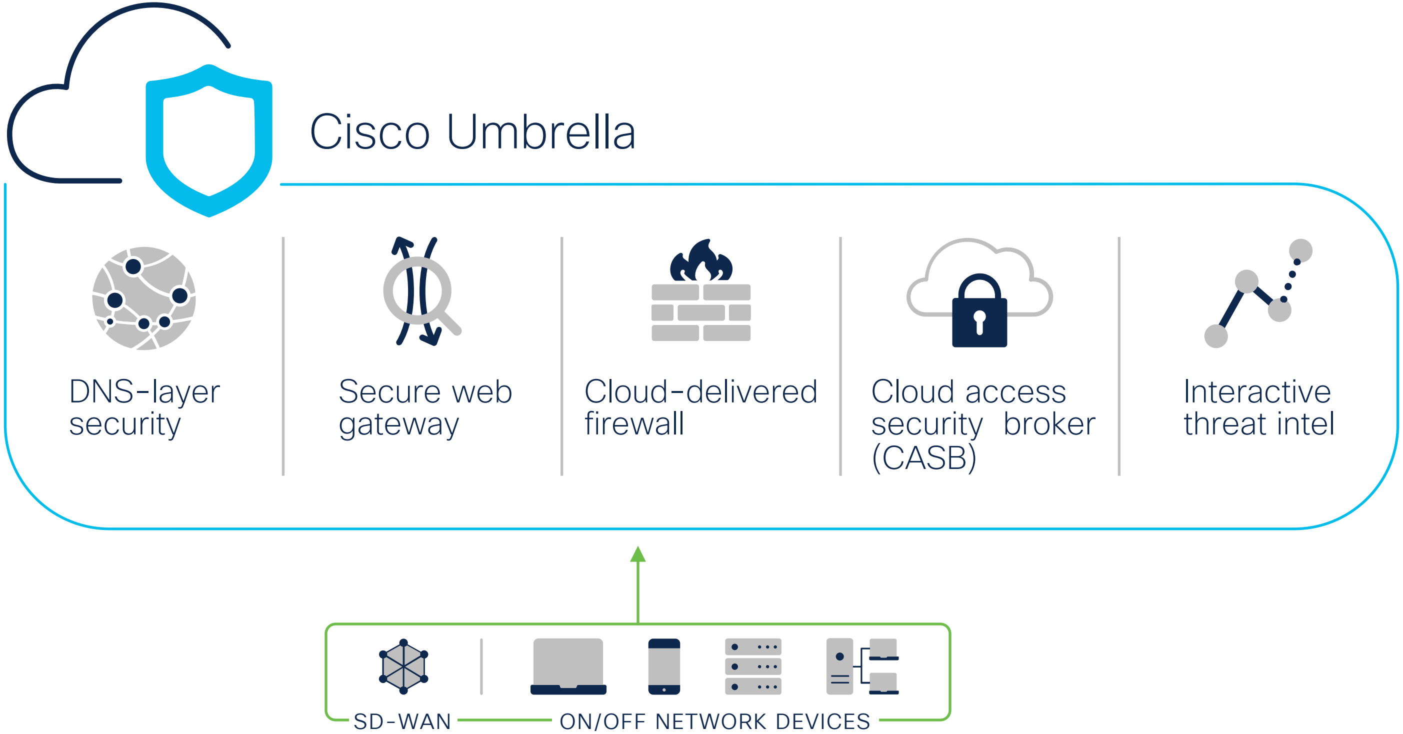
Cisco AnyConnect

Integration with other Cisco solutions

- ISR
- ASR / CSR
- Secure Firewall
- Cisco Identity Services Engine
- Cisco Umbrella
- Switches and Wireless Controllers
- Secure Endpoint
- Stealthwatch & NetFlow Collectors

The Umbrella multi-function security solution

Cisco's Secure Internet Gateway (SIG)



Cisco Umbrella

DNS-layer security

Secure web gateway

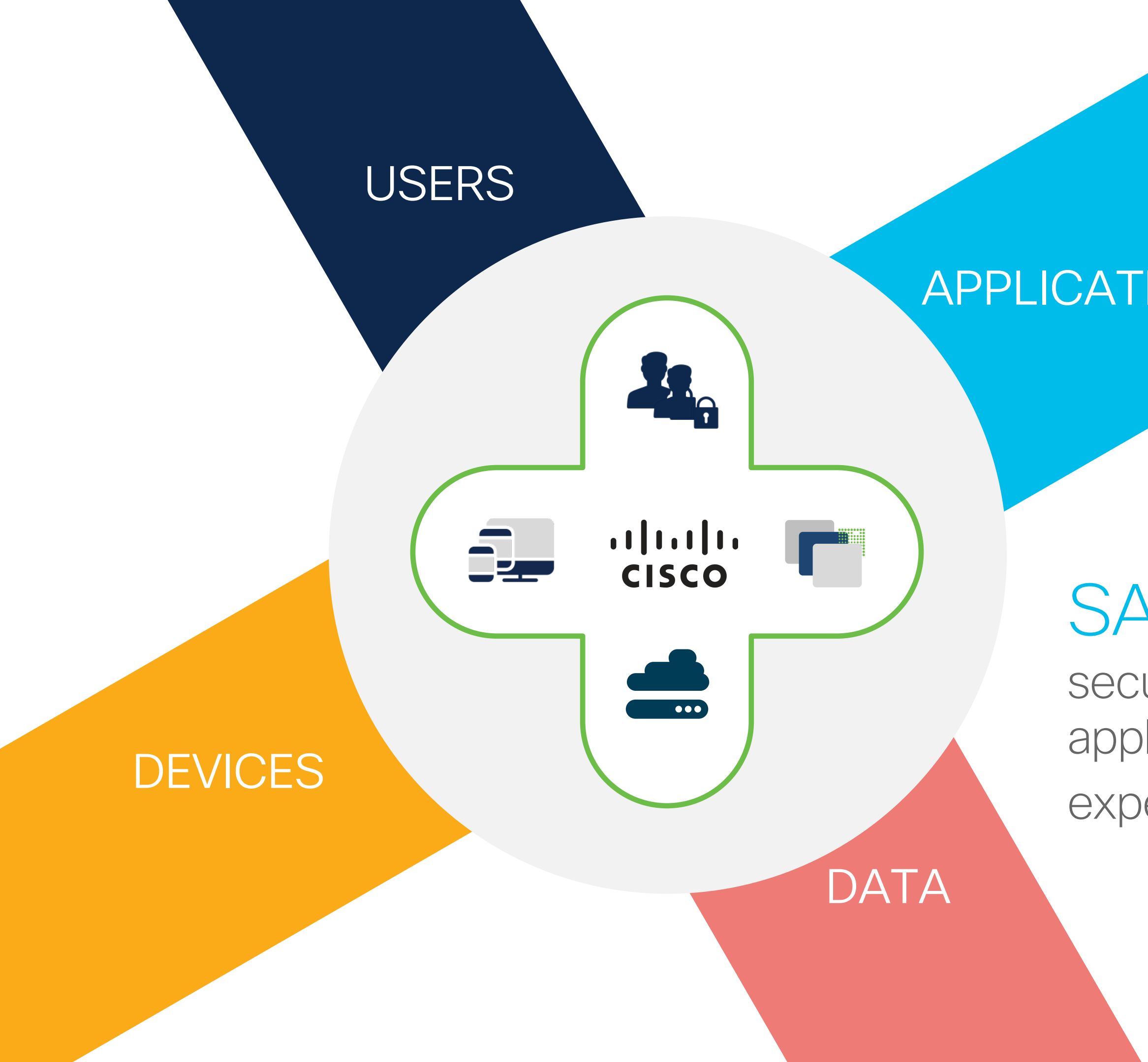
Cloud-delivered firewall

Cloud access security broker (CASB)

Interactive threat intel

SD-WAN

ON/OFF NETWORK DEVICES



USERS

APPLICATIONS

DEVICES

DATA

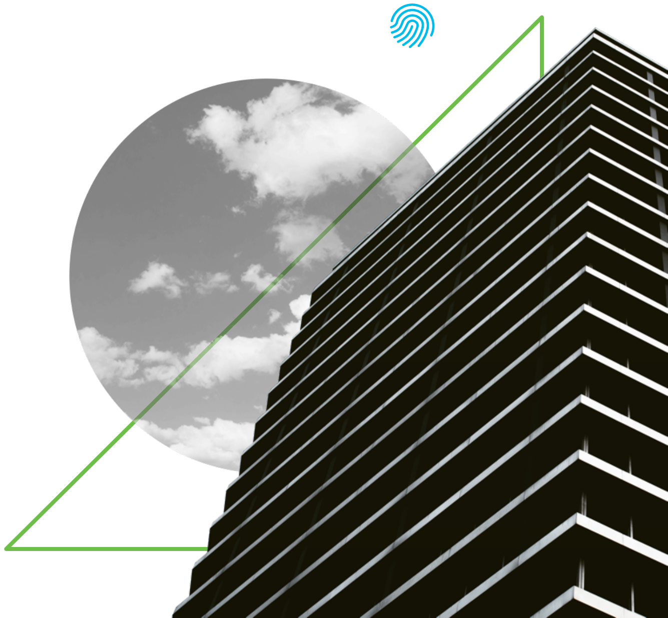
SASE Architecture

securely connect any user to any application with the best user experience

CMMC – Who’s Effected?

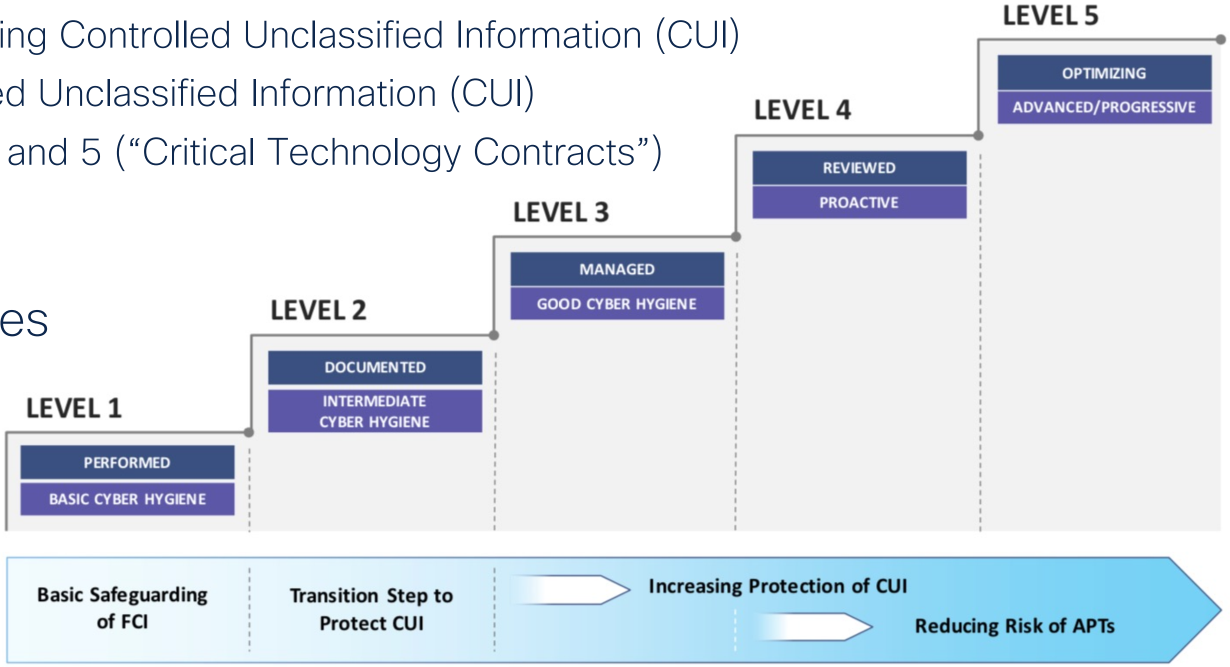
- Federal Systems Integrators (FSI)
- Federal Contractors and Sub-Contractors
- University Affiliated Research Center (UARC)
- Federally Funded Research and Development Centers (FFRDC)
- Any part of the Defense Industrial Base (DIB)

Any organization pursuing a contract or funding from DoD (and likely others)



What is CMMC?

- A requirement for future DoD contracts
- Based mainly on:
  - FAR 52.204-21 for Federal Contract Information (FCI)
  - DFARS 252.204-7012 Protecting Controlled Unclassified Information (CUI)
  - NIST SP 800-171 for Controlled Unclassified Information (CUI)
  - NIST SP 800-172 for Levels 4 and 5 (“Critical Technology Contracts”)
- 5 Levels of Maturity
- 17 Domains – 171 Practices
- It’s a Certification!



LEVEL 1
PERFORMED
BASIC CYBER HYGIENE

LEVEL 2
DOCUMENTED
INTERMEDIATE CYBER HYGIENE

LEVEL 3
MANAGED
GOOD CYBER HYGIENE

LEVEL 4
REVIEWED
PROACTIVE

LEVEL 5
OPTIMIZING
ADVANCED/PROGRESSIVE

Basic Safeguarding of FCI

Transition Step to Protect CUI

Increasing Protection of CUI

Reducing Risk of APTs

Image Credit: Carnegie Mellon University and The Johns Hopkins University Applied Physics Laboratory LLC.

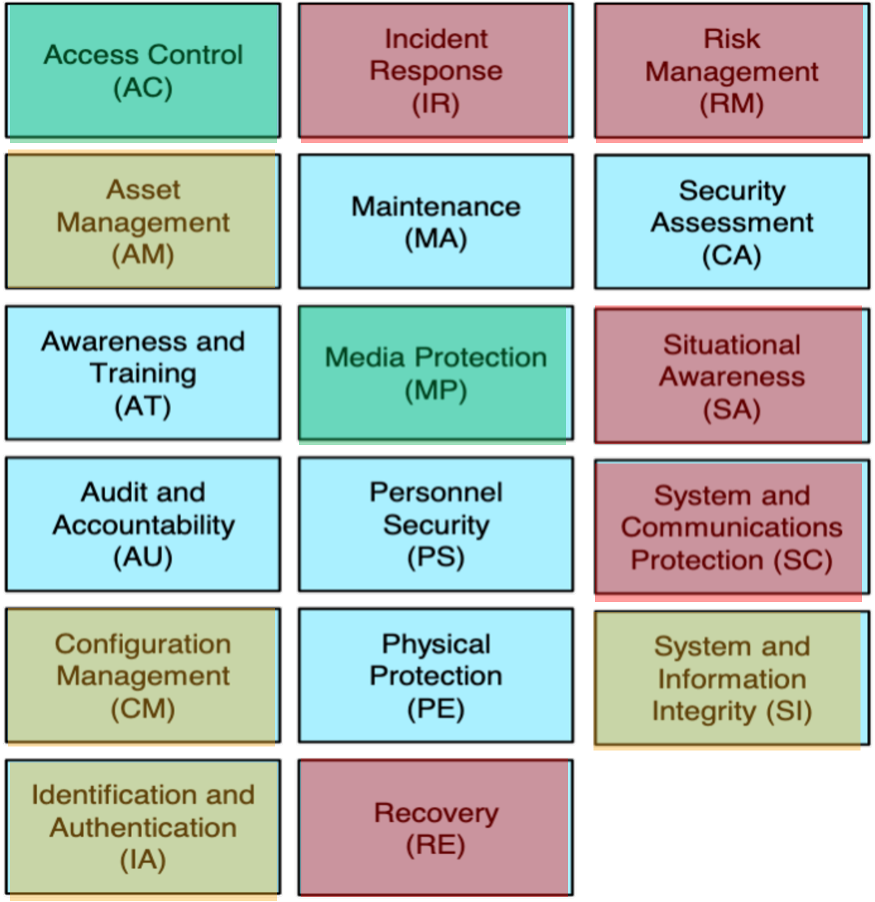
cisco SECURE

CMMC

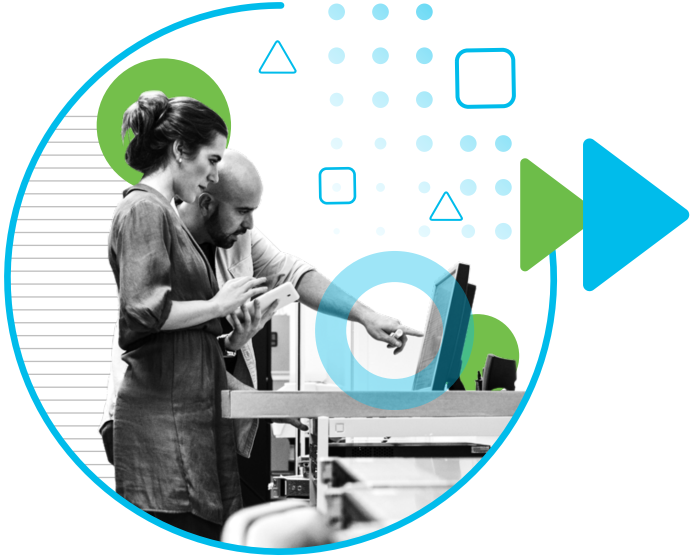
17 Capability Domains

Zero Trust Overlap

ZTA Core	🟩
ZTA Policy Input	🟨
ZTA Core & Policy Input	🟥



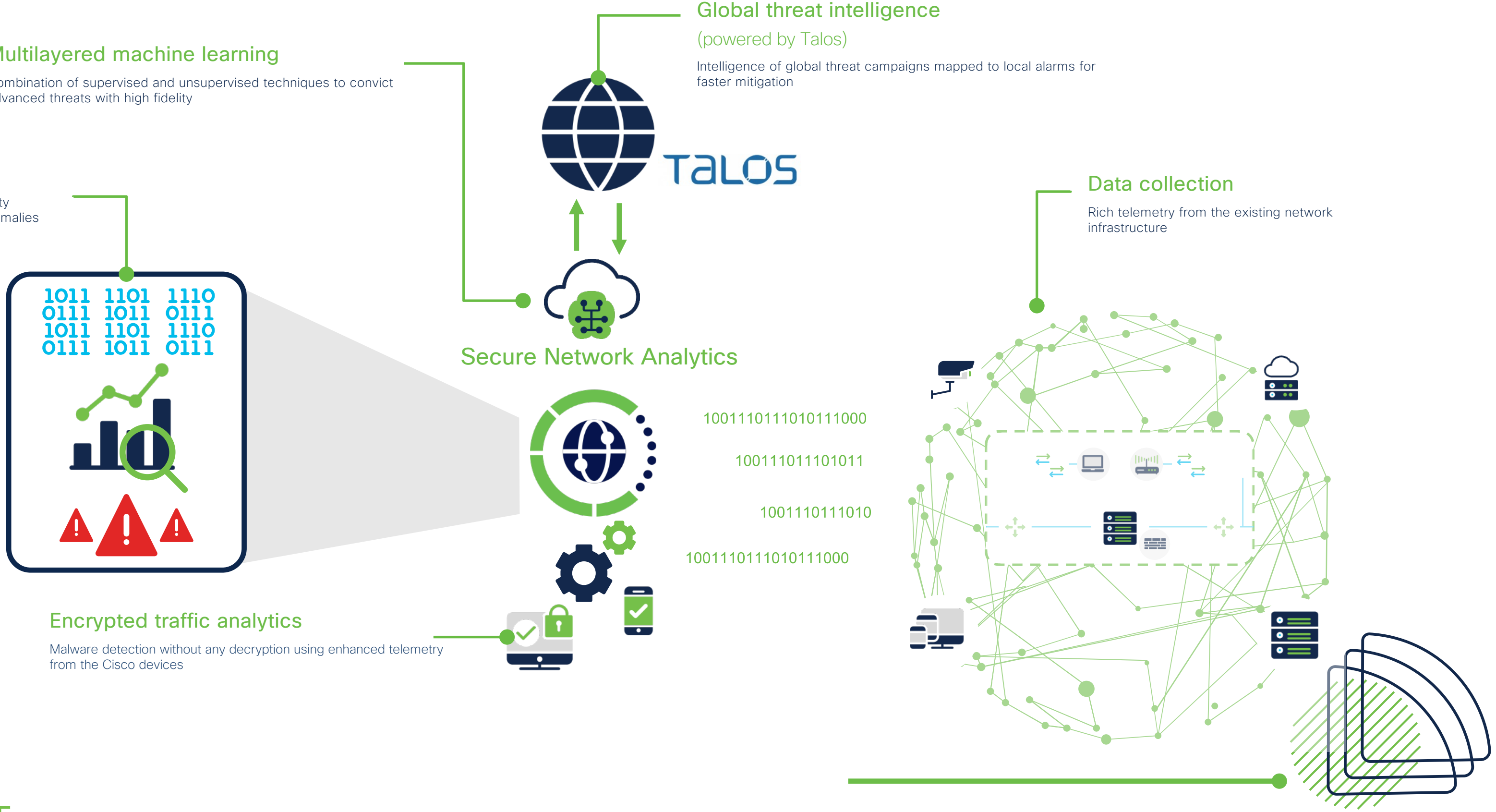
Access Control (AC)	Incident Response (IR)	Risk Management (RM)
Asset Management (AM)	Maintenance (MA)	Security Assessment (CA)
Awareness and Training (AT)	Media Protection (MP)	Situational Awareness (SA)
Audit and Accountability (AU)	Personnel Security (PS)	System and Communications Protection (SC)
Configuration Management (CM)	Physical Protection (PE)	System and Information Integrity (SI)
Identification and Authentication (IA)	Recovery (RE)	



Zero Trust Critical Capabilities

- Trusted Access
- Micro-segmentation
- Automation
- Continuous visibility & enforcement
- Threat intelligence

Secure Network Analytics (Stealthwatch)



Multilayered machine learning

Combination of supervised and unsupervised techniques to convict advanced threats with high fidelity

Global threat intelligence

(powered by Talos)

Intelligence of global threat campaigns mapped to local alarms for faster mitigation

Behavioral modeling

Behavioral analysis of every activity within the network to pinpoint anomalies

Data collection

Rich telemetry from the existing network infrastructure

Secure Network Analytics

Encrypted traffic analytics

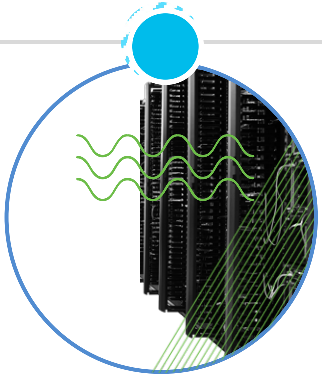
Malware detection without any decryption using enhanced telemetry from the Cisco devices

Secure Endpoint (AMP)

Global Intelligence and Retrospective Detection

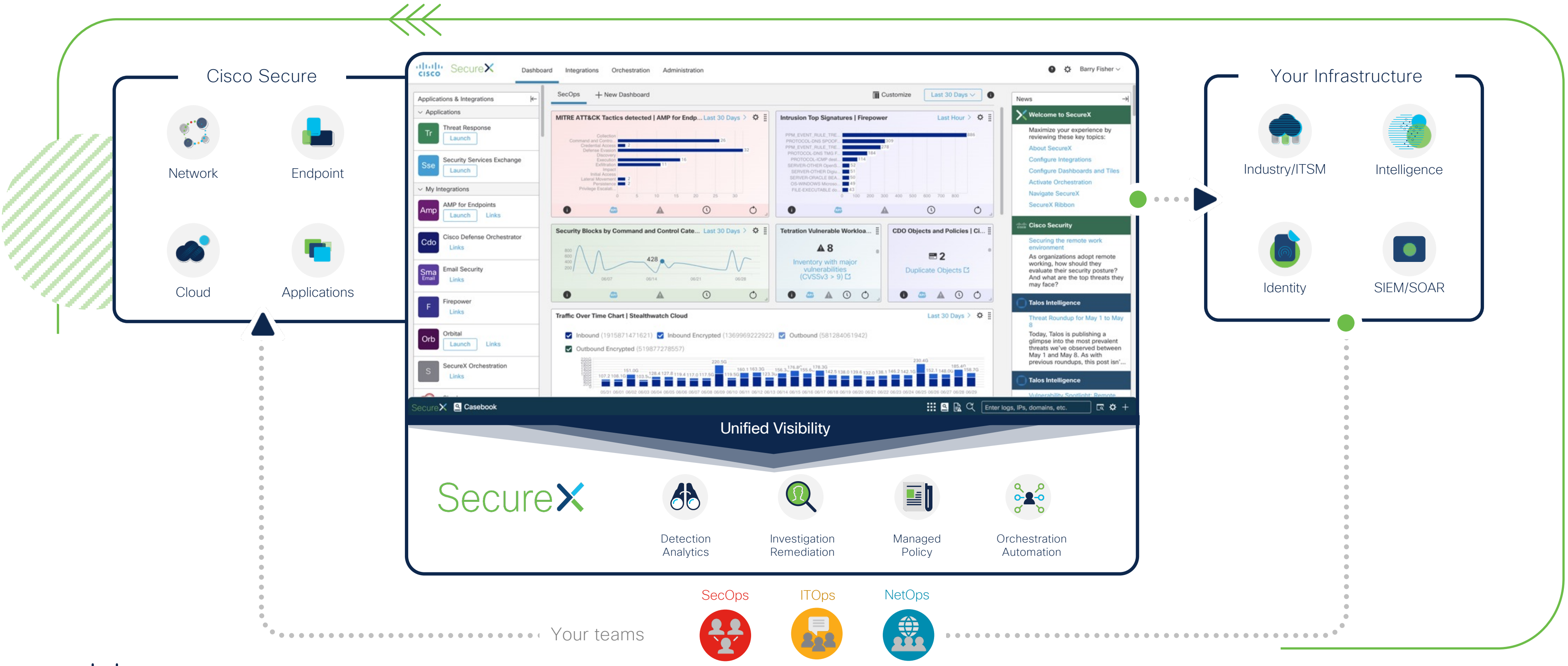
Proactive protection to block even the most advanced threats

Detect and respond to threats continuously with advanced EDR



Leverage global threat intelligence via Cisco Talos

SecureX



Maximize your experience by reviewing these key topics:

As organizations adopt remote working, how should they evaluate their security posture? And what are the top threats they may face?

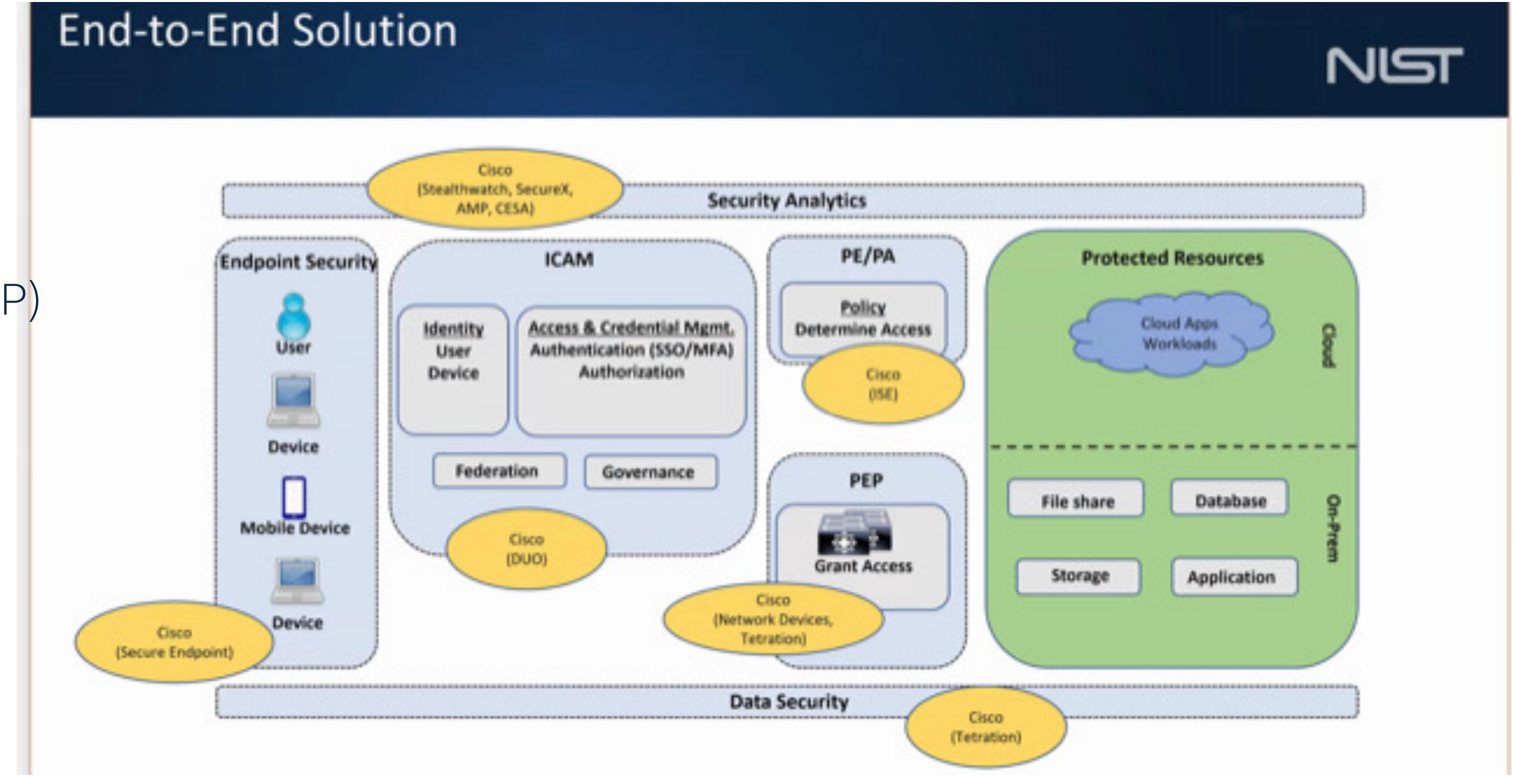
Today, Talos is publishing a glimpse into the most prevalent threats we've observed between May 1 and May 8. As with previous roundups, this post isn'...

NIST Zero Trust Lab Schematic

For creation of SP1800 document

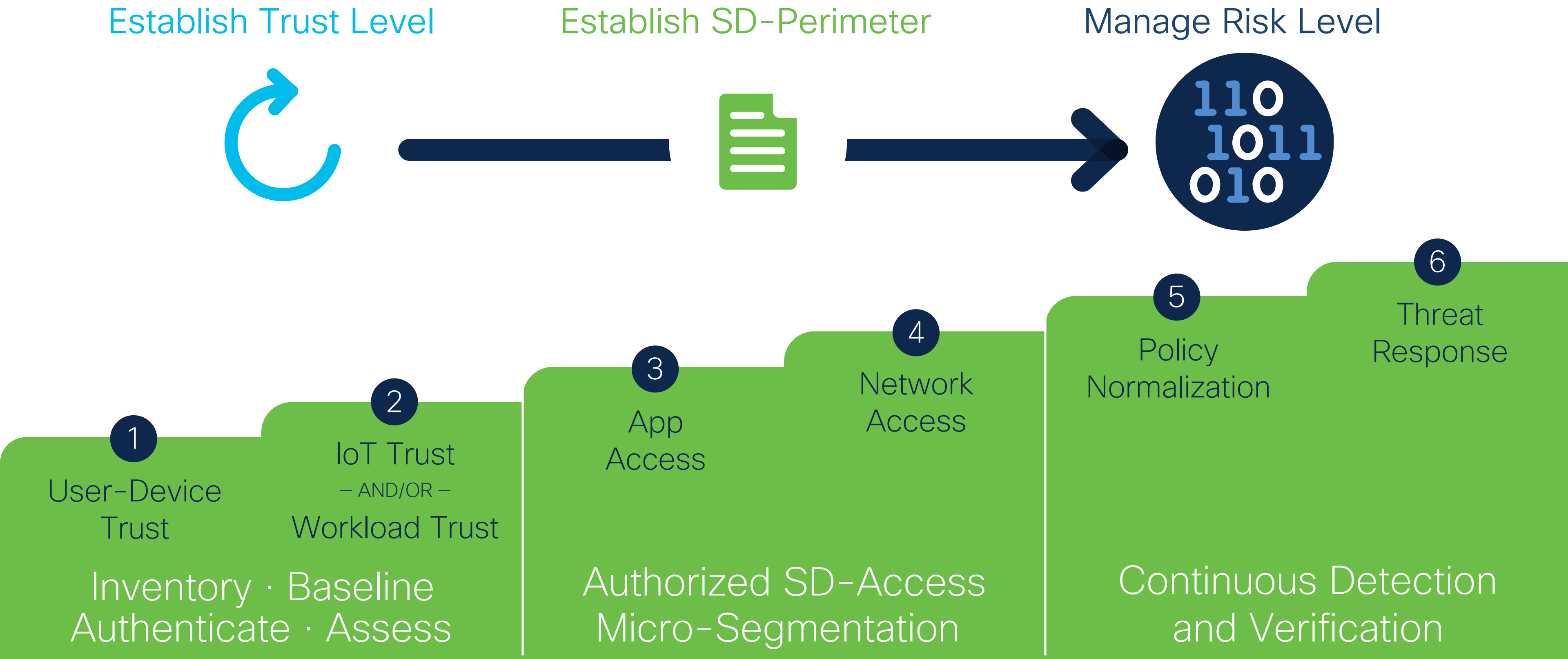
Included Cisco Solutions

- ✓ Duo
- ✓ Secure Endpoint (AMP)
- ✓ CESA
- ✓ ISE
- ✓ Network Devices
- ✓ Stealthwatch
- ✓ Tetration
- ✓ SecureX



Zero Trust – Getting Started

A journey with incremental enforcement based on context



Establish Trust Level

Establish SD-Perimeter

Manage Risk Level

1 User-Device Trust

2 IoT Trust
– AND/OR –
Workload Trust

Inventory · Baseline
Authenticate · Assess

3 App Access

4 Network Access

Authorized SD-Access
Micro-Segmentation

5 Policy Normalization

6 Threat Response

Continuous Detection
and Verification

Additional Thoughts on Getting Started

- Assess and develop a plan
- Use best practices and requirements
- Look for quick time to value
- Think cloud smart
- Demand integration and automation

cisco SECURE

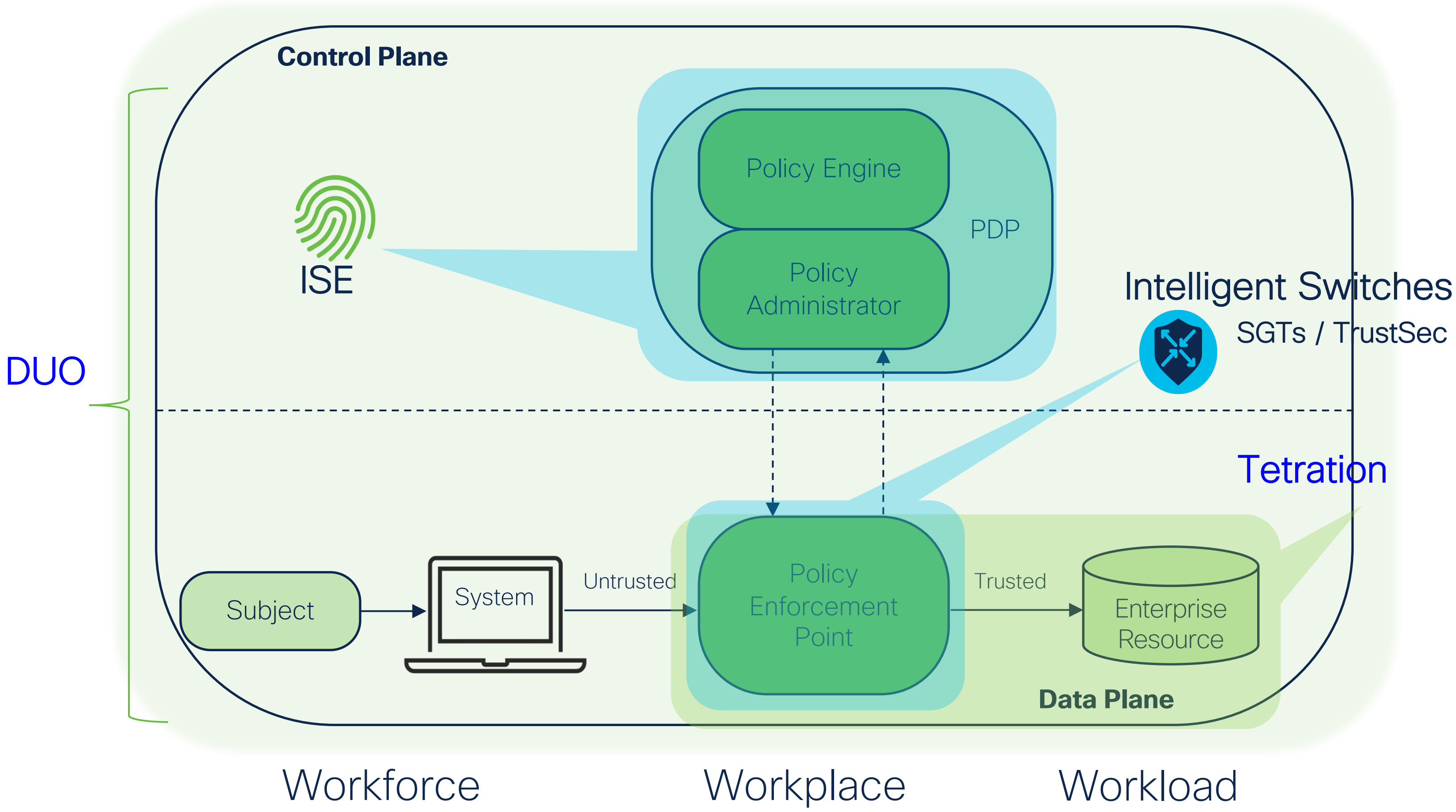
Secure Remote Work/Learning

- Block fraudulent emails before users ever see them
- Protect users whenever and wherever they click
- Stop malware if it ultimately reaches your endpoints
- Thoroughly inspect all internal email too
- Prevent user accounts from being hijacked
- Make everything work together as a team

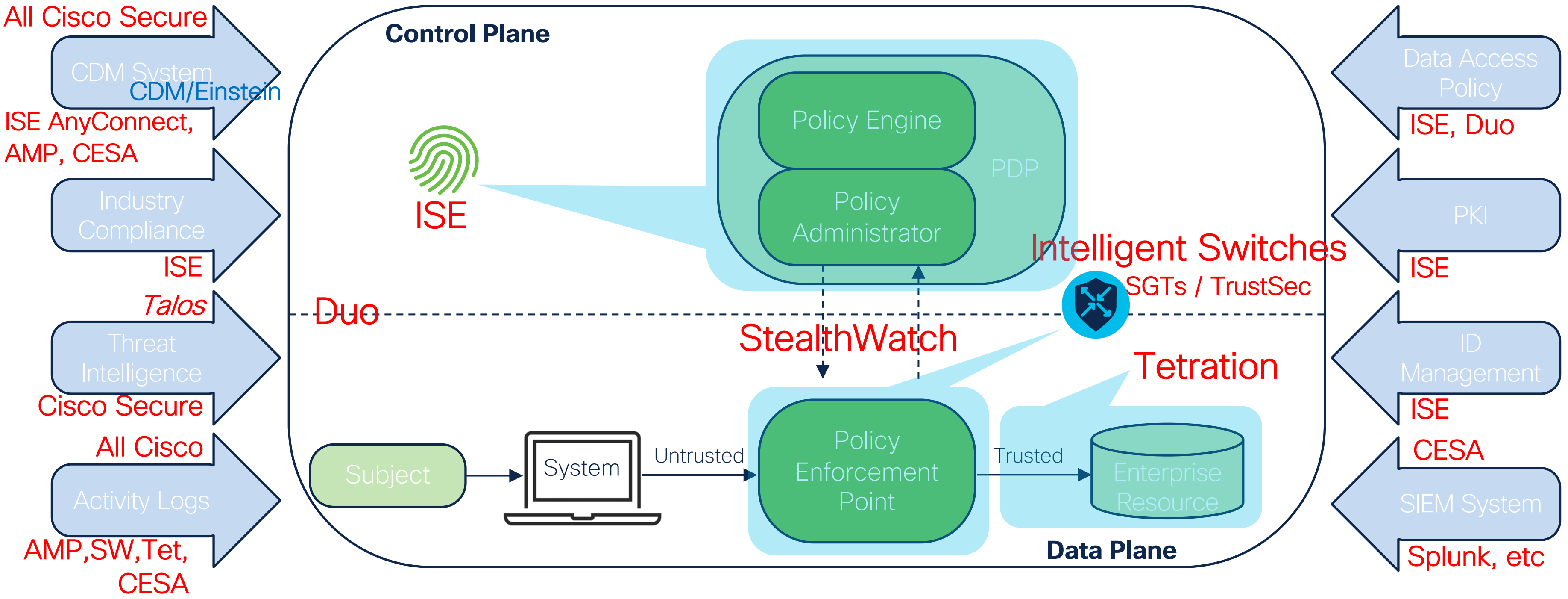
Secure Remote Work/Learning

Block fraudulent emails before users ever see them	Secure Email w/ Adv. Phishing Protection	✓
Protect users whenever and wherever they click	DNS Protection (Umbrella)	✓
Stop malware if it ultimately reaches your endpoints	Secure Endpoint (AMP for Endpoints)	✓
Thoroughly inspect all internal email too	Cloud eMail Defense (Cloud Mailbox Defense)	✓
Prevent user accounts from being hijacked	Multi Factor Authentication (Duo)	✓
Make everything work together as a team	Visibility, Integration, Response (SecureX)	✓

NIST Zero Trust Architecture – SP 800-207



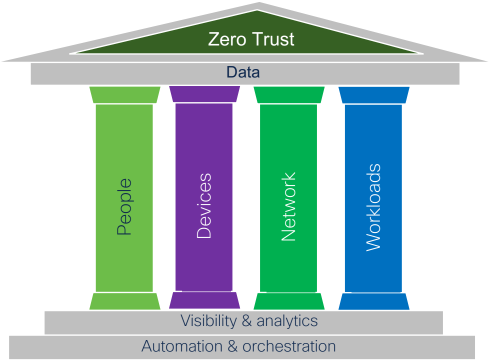
NIST Zero Trust Architecture – SP 800-207



Zero Trust

Popularized by Forrester - ZT and ZTX

- What: A security strategy based on "least-privilege" to address the modern "perimeter-less" IT environment
- Intent: Assumes all environments are hostile - no access until proven trusted
- Tenants: All users, devices, applications, data, and network flows encrypted, authenticated and authorized
- Enablement: Visibility and automation systems are what allow a zero trust network to be built and operated
- Adaptable to: All environments
- Missing: Threats



Zero Trust is a strategy and design approach - not a checklist or a thing you buy

AnyConnect - More than a traditional VPN

Think of it as a Security Connector

Always-on protection

Constant protection, including data encryption

Proactive threat defense

Integrates with advanced malware protection

Web protection for remote workers

Includes built-in web security and malware threat protection

Automated head-end deployment

Supports VPN ‘burst’ scenarios where remote access volume suddenly increases

Integrated compliance

Integrates with Cisco ISE to deliver world-class compliance

Multiple access options

Access control via MFA options across different environments

Zero Trust

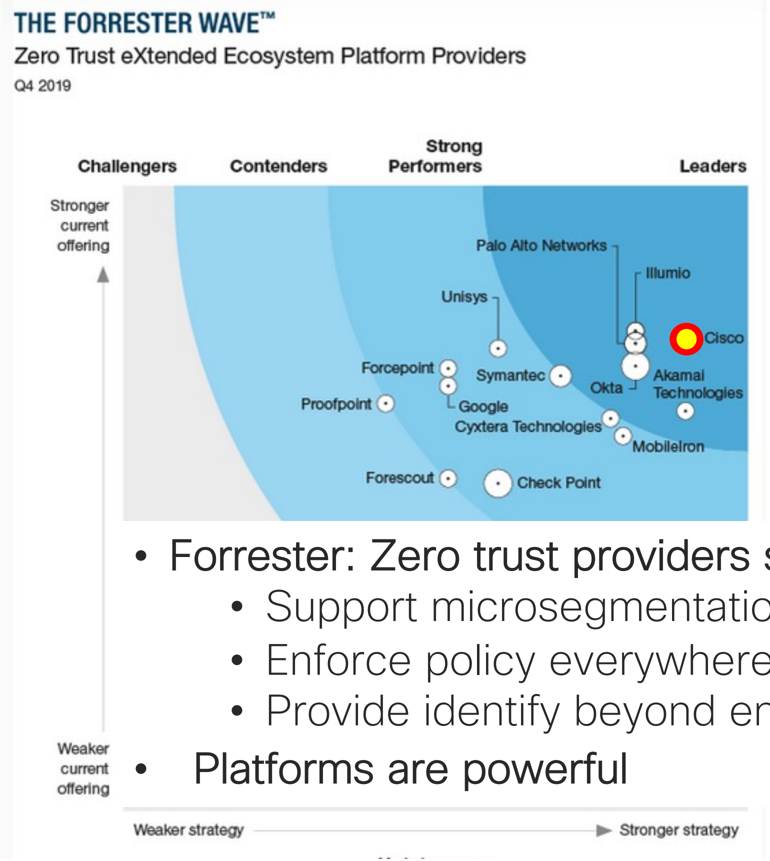
It’s NOT something you buy
It’s a way of thinking

It’s more than “Least Privilege”
It’s more like “Earn Privilege”

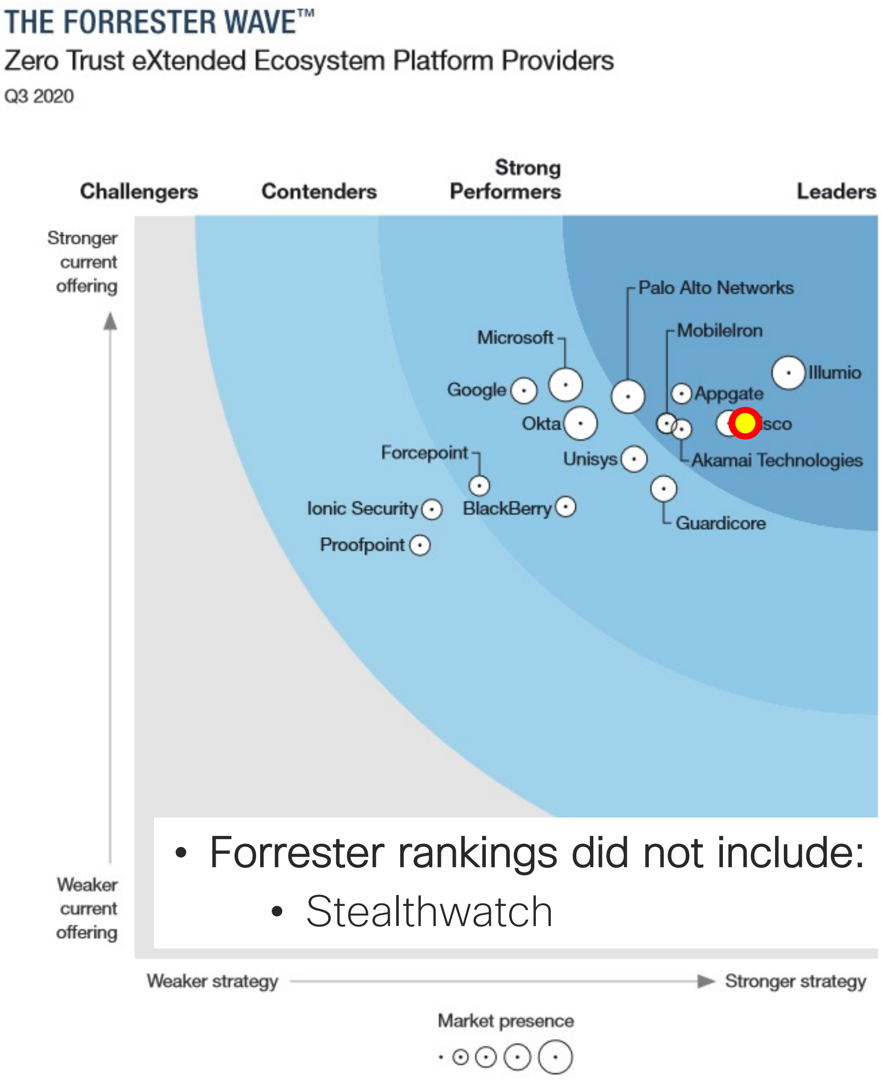
Earn Trust AND…

…Continuous trust verification

Zero Trust – The Rankings



- Forrester: Zero trust providers should:
    - Support microsegmentation
    - Enforce policy everywhere
    - Provide identify beyond end-user
- Platforms are powerful



- Forrester rankings did not include:
    - Stealthwatch

CISCO SECURE

Disclaimer: The Forrester WaveTM is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave are trademarks of Forrester Re spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the For

CESA Closes the Endpoint Visibility Gap

CESA: Closing the Endpoint Visibility Gap

The Endpoint Visibility Gap

Associating detailed user/endpoint behavior with its network activity

Associating detailed user/endpoint behavior
with its network activity

Network Security Analytics

e.g. Stealthwatch, Darktrace, etc.

Sees traffic once it enters the network

Analyzes behavior on the network

EDR & EPP

e.g. AMP, CrowdStrike, Symantec, etc.

Operates within the endpoint

Malware detection, file analysis, file revocation, app/process termination

Zero-Trust Abuse

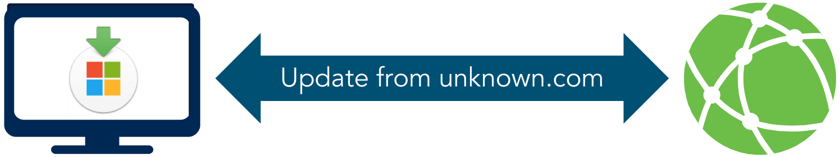
Data Loss

Endpoint Blindness

Endpoint Visibility Gap – Before & After CESA

A Real Example:

Microsoft Background Intelligent Transfer Service (BITS) often gets exploited to make malware downloads look like legitimate traffic/software.



BEFORE – many screens, attack missed

EDR/EPP	“No known malware detected”
Network Analytics	“BITS traffic – nothing strange about that”
Domain Reputation	“Unknown.com – neutral reputation”

AFTER CESA – in 1 pane of glass

“ALERT: bits.exe has never talked to unknown.com in my environment”

Activity detected during C2 contact/download phase

Traced down to file path on endpoint

Found other affected endpoints

Blocked domain in Umbrella

How Cisco Customer Experience (CX) helps with your security transformation requirements

Reliable, secure design

Seamless integration

Holistic approach to preventing and containing security breaches

Cultural and architectural philosophy shift

Network architecture analysis

Comprehensive segmentation and beyond-border security

Cisco® CX and partner services
help you accelerate your transformation

Cisco Zero Trust AS Solutions use cases

Use cases

User Access Control

Contextual Policy and Enforcement

Network Access Integrations

Multifactor Authentication

Endpoint Compliance and Posture

Plan and design services to start your Cisco Zero Trust journey

Zero Trust Strategy and Analysis AS Solutions

Cisco Zero Trust Strategy and Analysis Advanced Services Solutions can tune integrations and components as needed to meet your unique needs for Zero Trust plan and design.

Service components

- Zero Trust strategy and analysis development (plan and design)
- Current technical capabilities assessment
- Security policy and access analysis
- Project management

Deliverables

- Solution Requirements/Design Document
- Security Plan Document
- Strategy and Analysis Report
- Knowledge transfer

Advantages

- Workshops and interviews help you understand your business and how to best make Zero Trust work for your organization.
- You may elect customized service for multiple sites and architectures.
- The number of site visits for analysis, strategy, and technical capabilities can be modified to meet your unique needs and delivered on site and/or remotely.

Zero Trust Advanced Services Solutions deliverable highlights

Accelerating value

Needs Analysis Report

- Identifies the required future state
- Maps this against the current position
- Considers more than just technology
- Highlights the value of moving to that future state

Strategic Roadmap

- Multiyear strategy is provided, identifying key milestone projects that bring alignment to Zero Trust
- Recommendations for year one are easier to achieve, boost security, and deliver quick wins

Executive Readout

- Key facets of the report presented to an executive audience
- Designed to highlight the value of moving to a Zero Trust model and how to reach it
- Builds senior support for the initiative

Environment Types

- Strategy covers up to four environment types (e.g., enterprise network, data center, IoT, off premises), covering a single site/instance of each