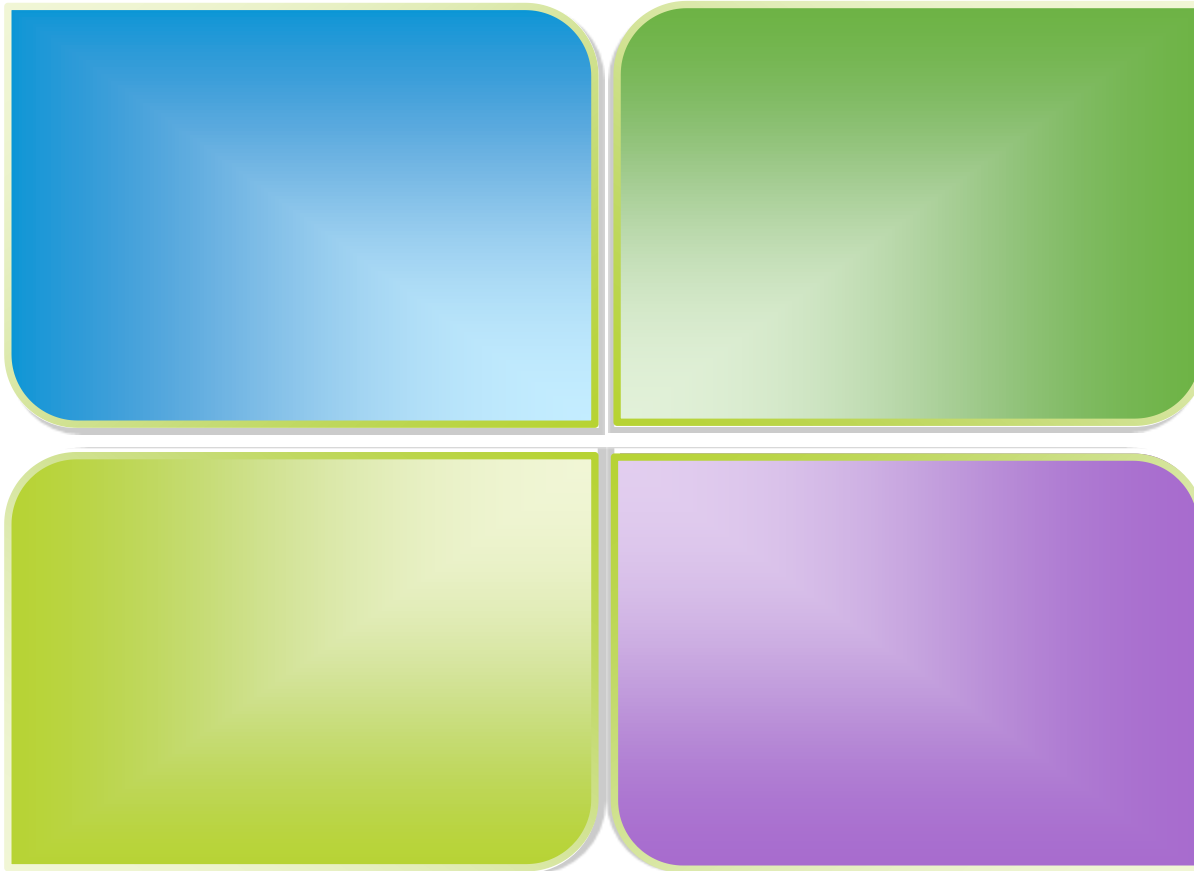




# Cisco TrustSec

Tadas Urmonas

# Complex Environment



The Network is No Longer Static

# The Traditional Model



# Mobile Applications and Data

## The Network



Desktop



DMZ

# Mobile Applications and Data



The Network



Desktop



DMZ



# The Network



# Complexity Creates Challenges

**How do I control all of this?**



# Administrative Challenges

- How do I manage multiple devices?
- How do I manage a workforce in motion?
- Where do I make policy decisions?
- Where and how do I enforce policy?
- How do I ensure consistency?
- How can I scale this across my distributed network?





# It's Not Just Theoretical

## Common Regulatory Requirements

- Control access to information, applications, records, etc.
- Control ingress/egress of data
- Ensure privacy for groups and individuals
- Segment certain classes of users
- Control access to devices, servers, and management platforms by both users and devices
- Manage and inventory IP-enabled devices, and controlling their behavior based on policy
- Enforce access policy beyond the ingress point
- Monitor, record, and audit users and devices

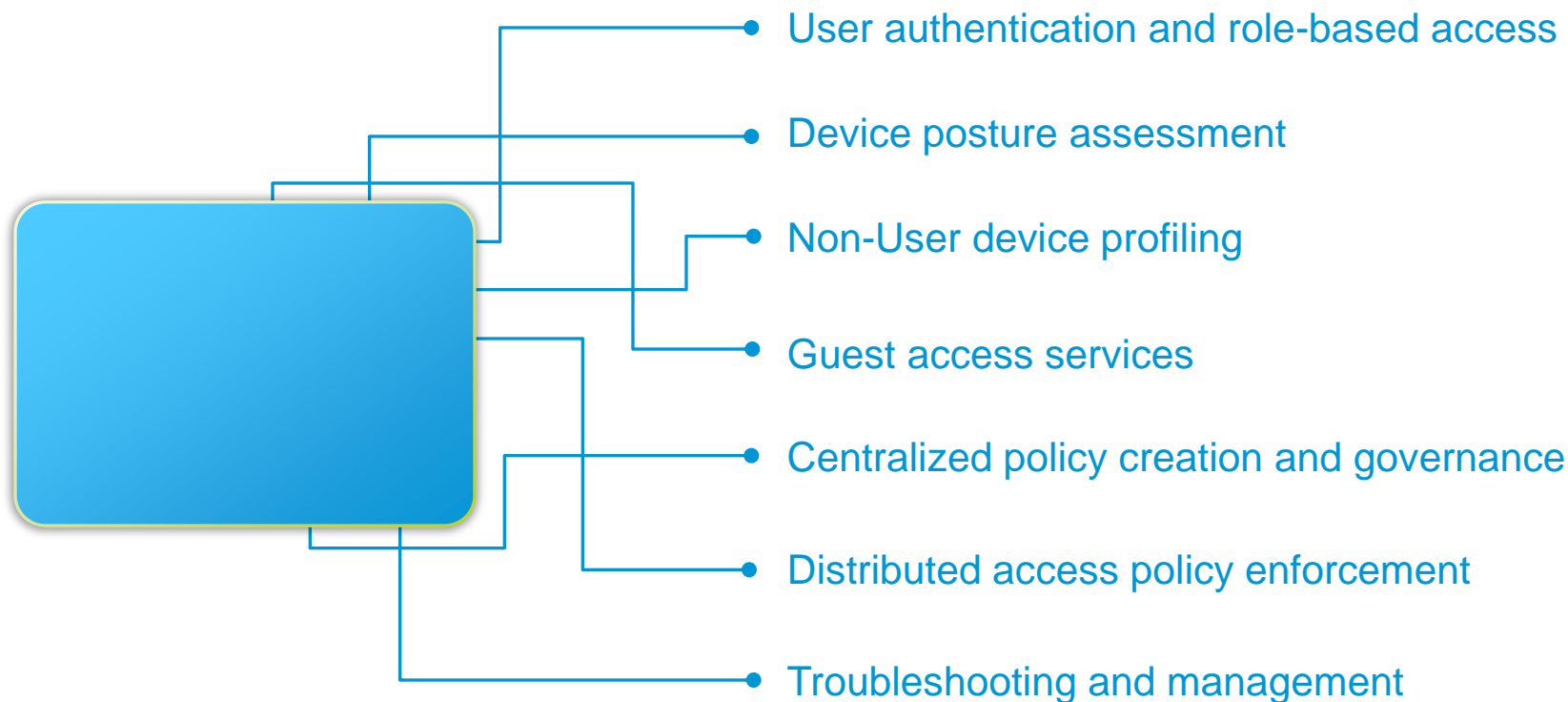


# Need For A Comprehensive Solution

- Scalable approach
- Leverages existing network investment
- Centralized, unified policy
- Distributed enforcement
- Secure by design
- Deployment options

# Cisco TrustSec

- TrustSec builds and enforces centralized identity-based access policies for users and devices and secures critical data



# Two TrustSec Deployment Options

## An appliance-based overlay solution

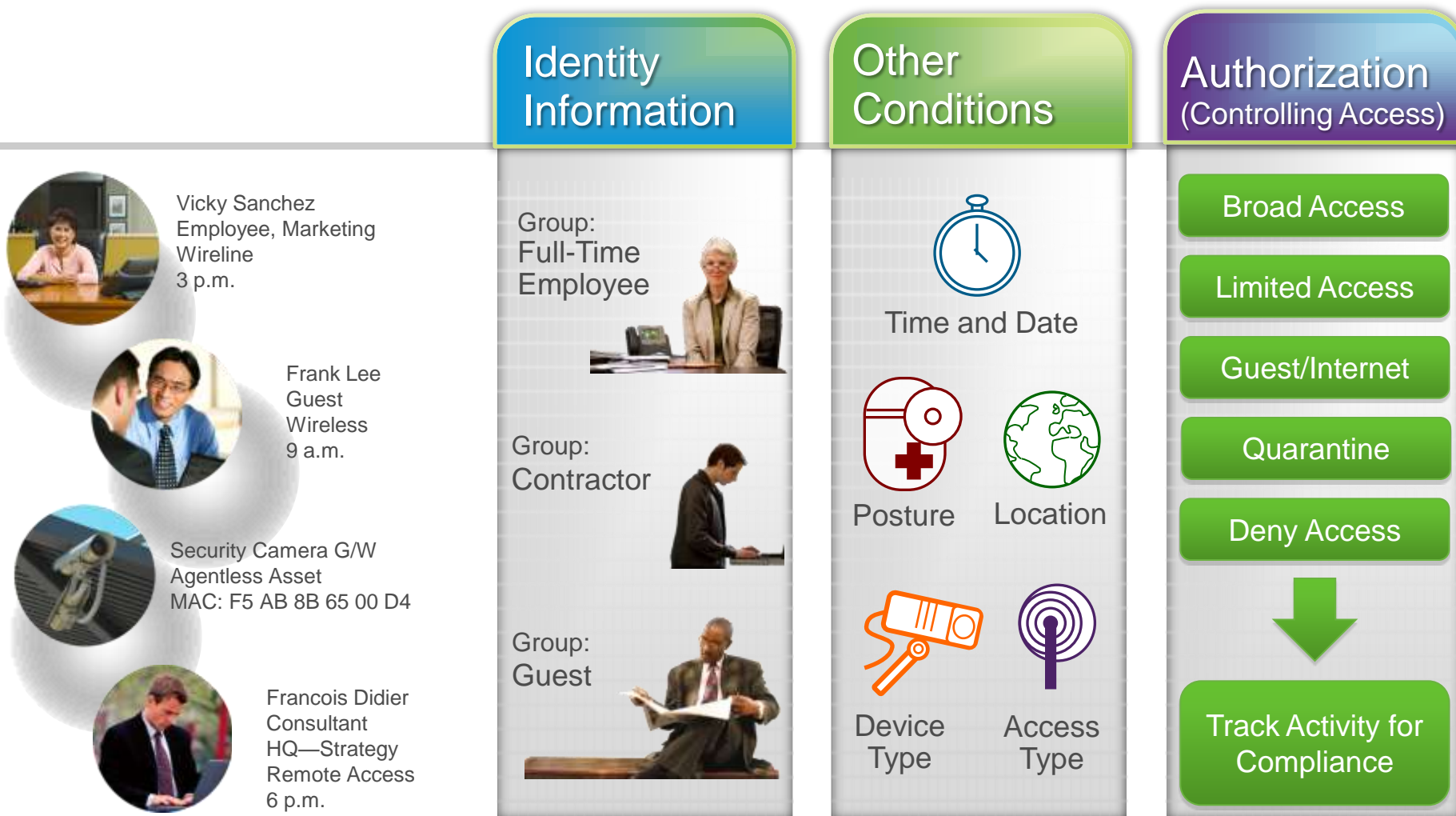
- Ideal for heterogeneous environments
- Scalable, easy-to-deploy solution
- In-band and out-of-band deployment options

## A Cisco network–integrated solution

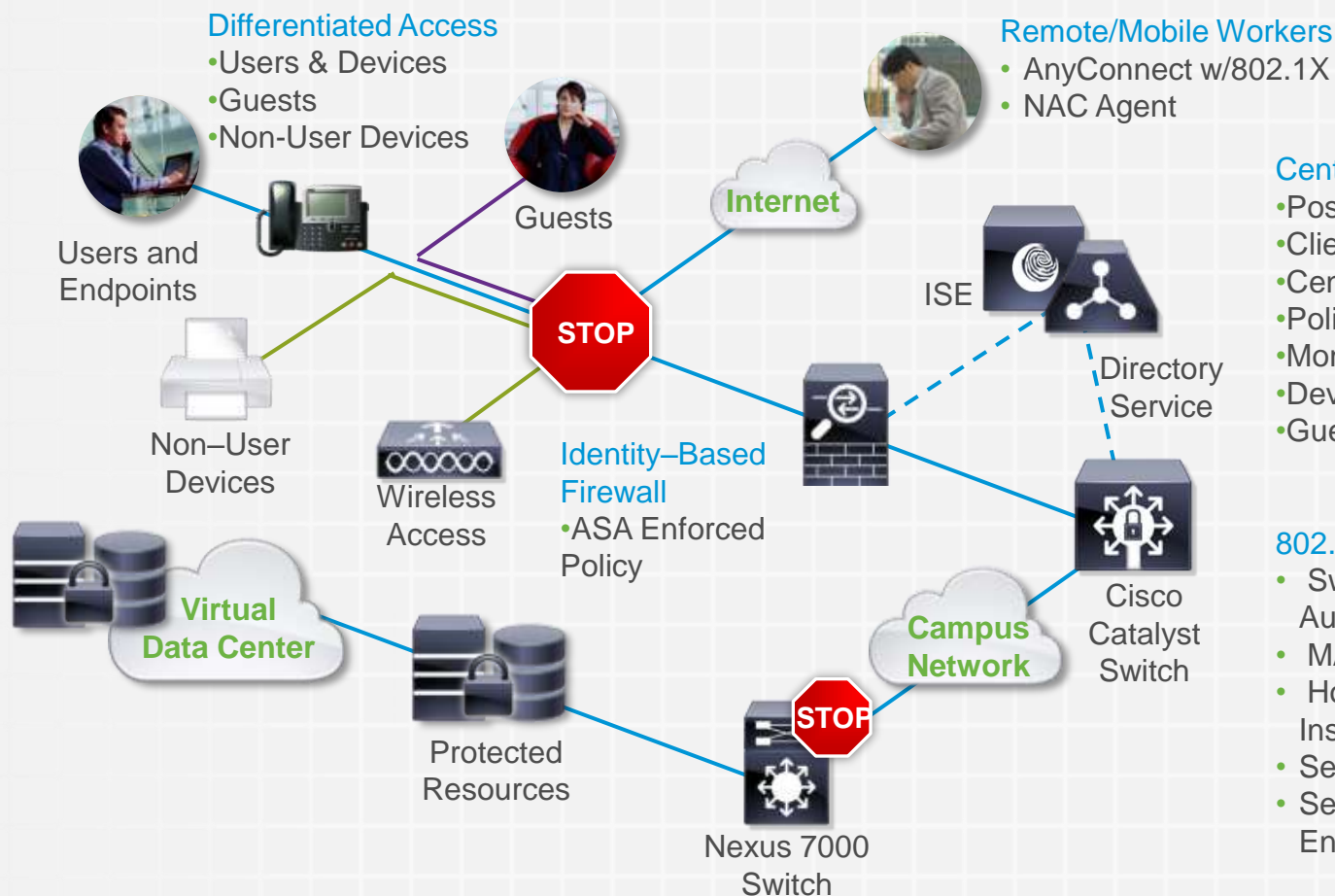
- Leverages the existing switch infrastructure
- Provides dynamic access control across the entire network
- Access policy enforcement across the entire data path
- Data protection through MACsec encryption

# Cisco TrustSec—802.1X

# Authentication and Authorization



# 802.1X Identity Overview



# TrustSec 802.1X Components

- Cisco's 802.1X-based TrustSec approach leverages the Cisco infrastructure and the new ISE appliance for a network-integrated access control solution



AnyConnect  
Client

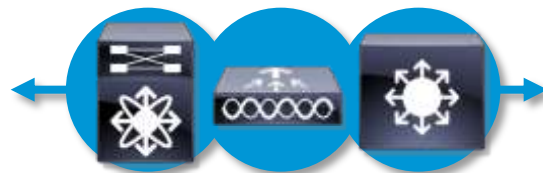


802.1X  
Supplicant

## 802.1X Endpoint Supplicants

Several client options:

- Any standards-based supplicant
- Cisco no-cost CSSC
- Cisco AnyConnect Client (also provides VPN tunneling and MACsec support)



## Cisco 802.1X– enabled infrastructure

Cisco Catalyst and Nexus switches and wireless access points communicate with the ISE for policy

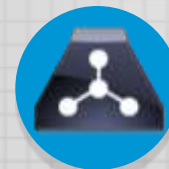
- Posture assessment
- Access services
- Policy enforcement
- MACsec support



## Identity Services Engine

Centralized multi-function policy creation and administration appliance

- Policy creation and governance
- Policy distribution
- Device profiling
- Guest access services
- Centralized administration
- Monitoring and reporting
- Troubleshooting





## Active Directory




# TrustSec 802.1X Benefits

- With a Cisco TrustSec solution in place, organizations are able to:

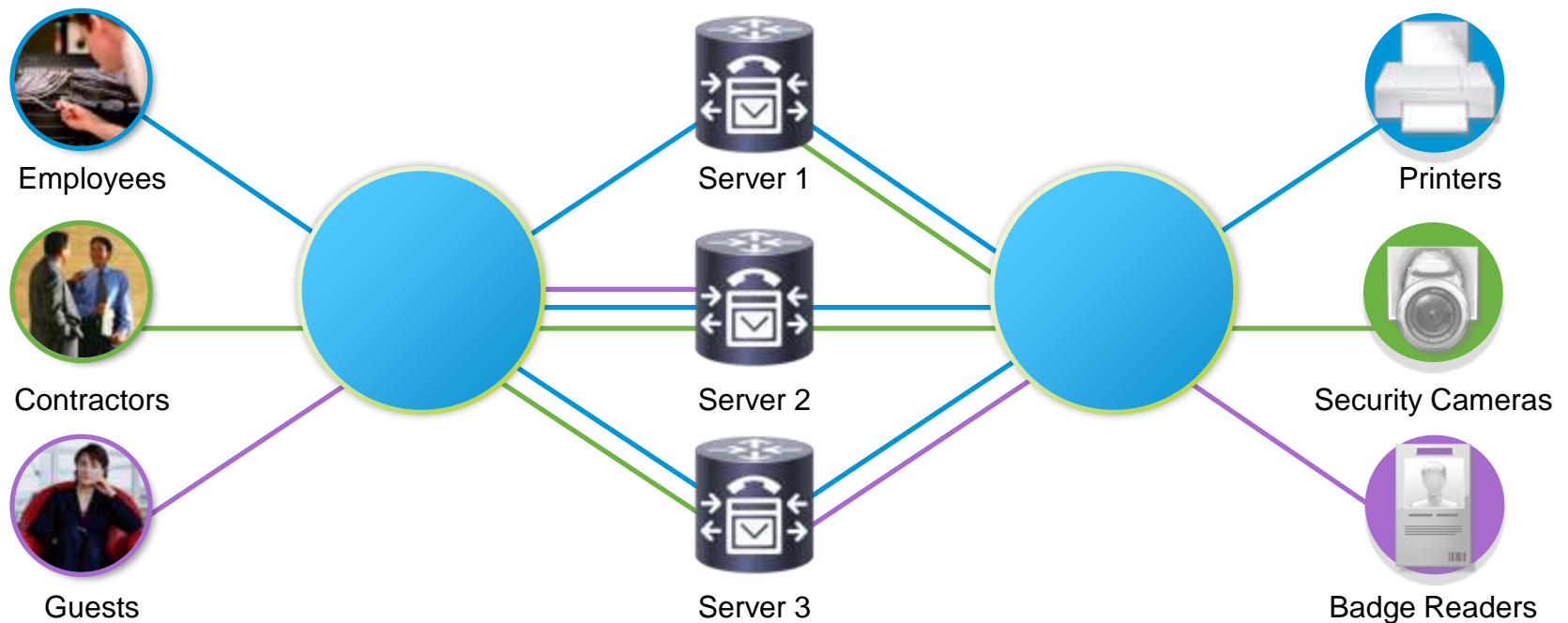
- 
- Provide unified access policy for wired, wireless, and VPN connections
  - Provide role-based access for any user or group
  - Provide self-service guest access
  - Ensure switch-to-switch data security using MACsec encryption

- 
- Enforce device health through posture assessment
  - Secure communications between endpoints and the network

- 
- Tag data and enforce policy using Secure Group Access
  - Secure access to and between Data Center resources (static and virtual)

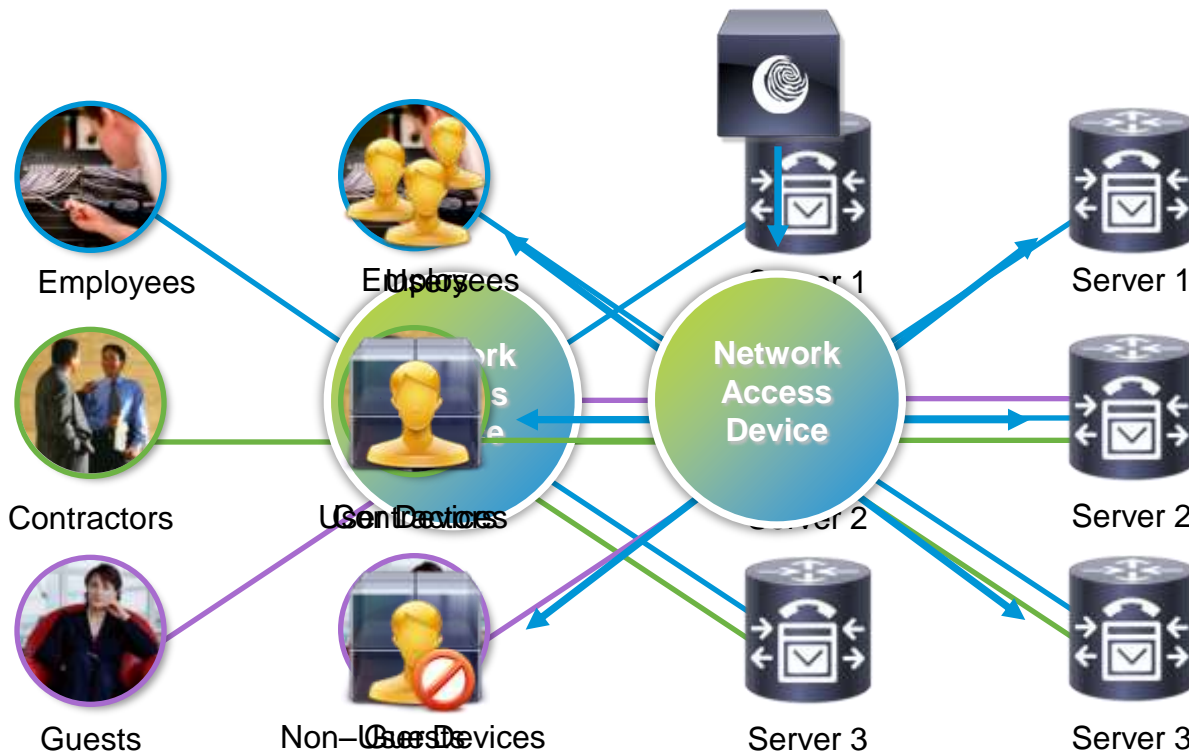
# 802.1X Use Case—Access Control

- Guests, users, devices
- Authenticating users and devices
- Role-based access policy



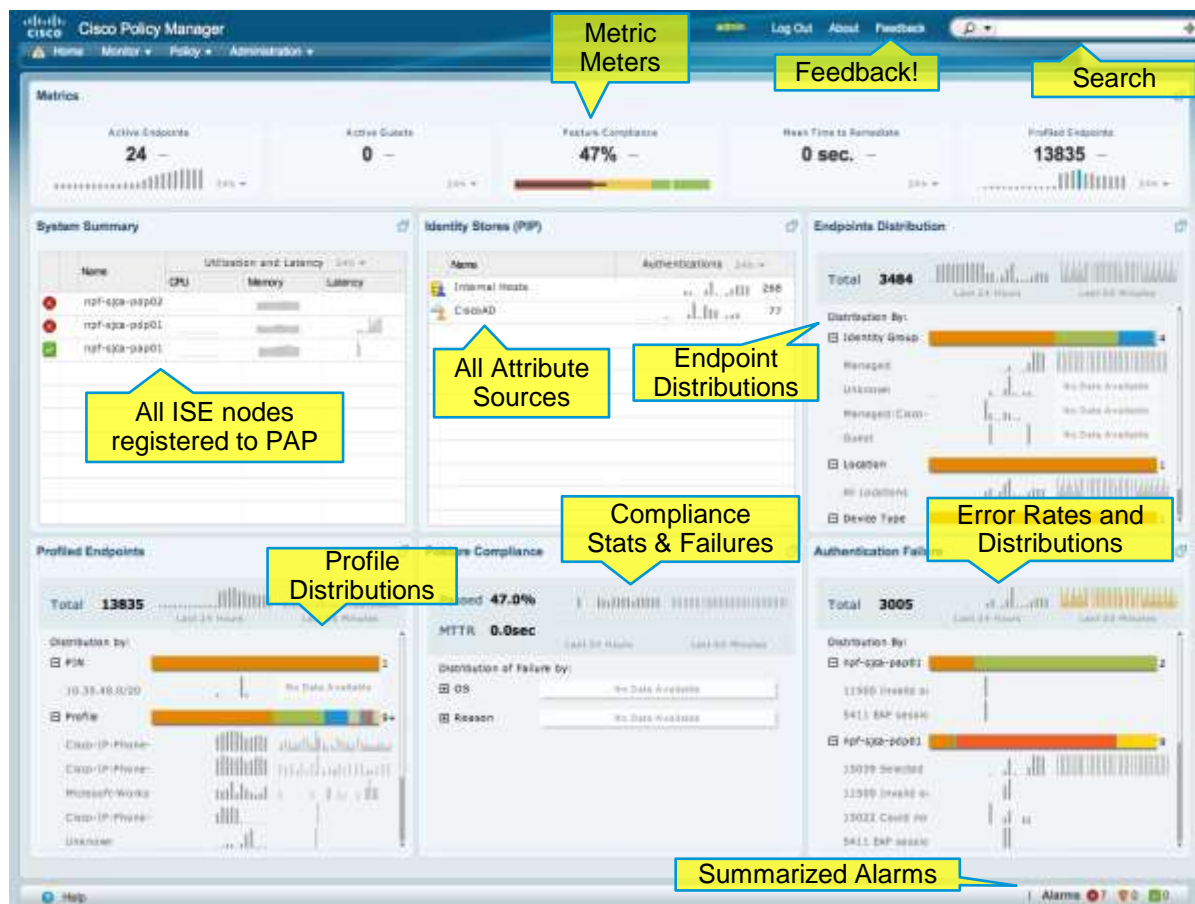
# 802.1X Use Case—Consistent Policy

- Inconsistent policy deployment and enforcement creates opportunities for threats



# 802.1X Use Case – Management

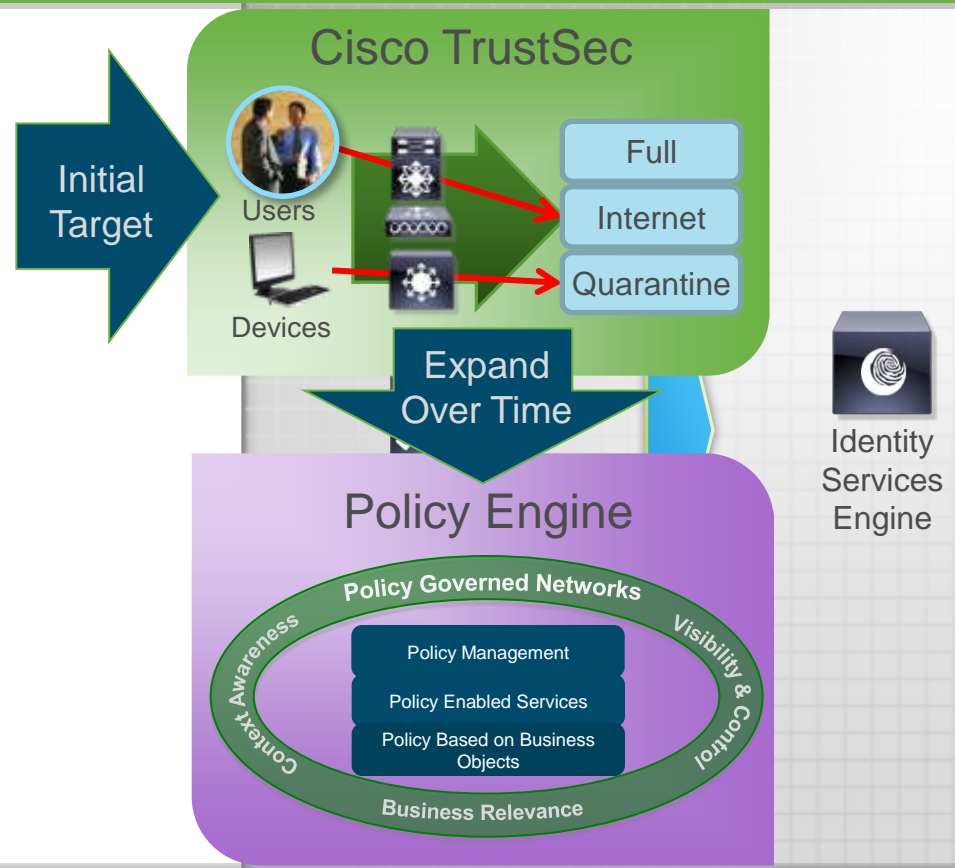
- ISE management, troubleshooting, monitoring, and reporting



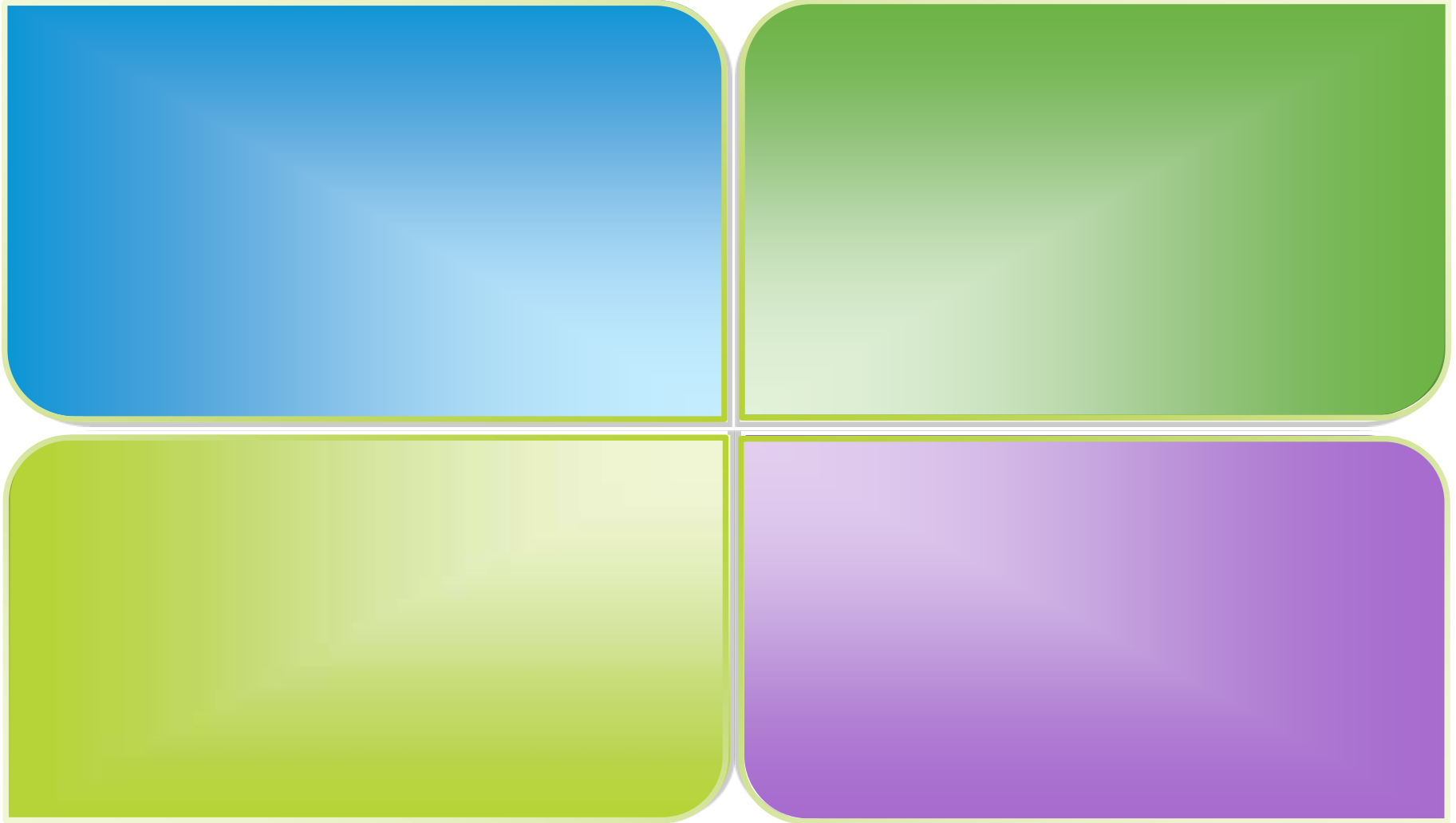
# TrustSec 2.0 – What's New?

## Introducing the Cisco Identity Services Engine

- Policy Creation and Governance
- AAA Services
- Posture Assessment
- Guest Access Services
- Device Profiling
- Monitoring
- Troubleshooting
- Reporting



# TrustSec 2.0 – What's New?



# Getting From Here To There

## What is it?

- Readiness assessment
- User and device discovery and access
- MACsec data encryption

## How do we do it?

- User: 802.1X enables access – monitor mode, limited access, differentiated access
- Guest: Web Auth
- Device: MACAuth Bypass with Profiling
- Encryption: MACsec

## What is it?

- Simplified access: limited and normal
- Posture assessment of devices

## How do we do it?

- Limited network access permitted by default
- Normal access granted based authorization
- Posture Assessment for user-based devices

## What is it?

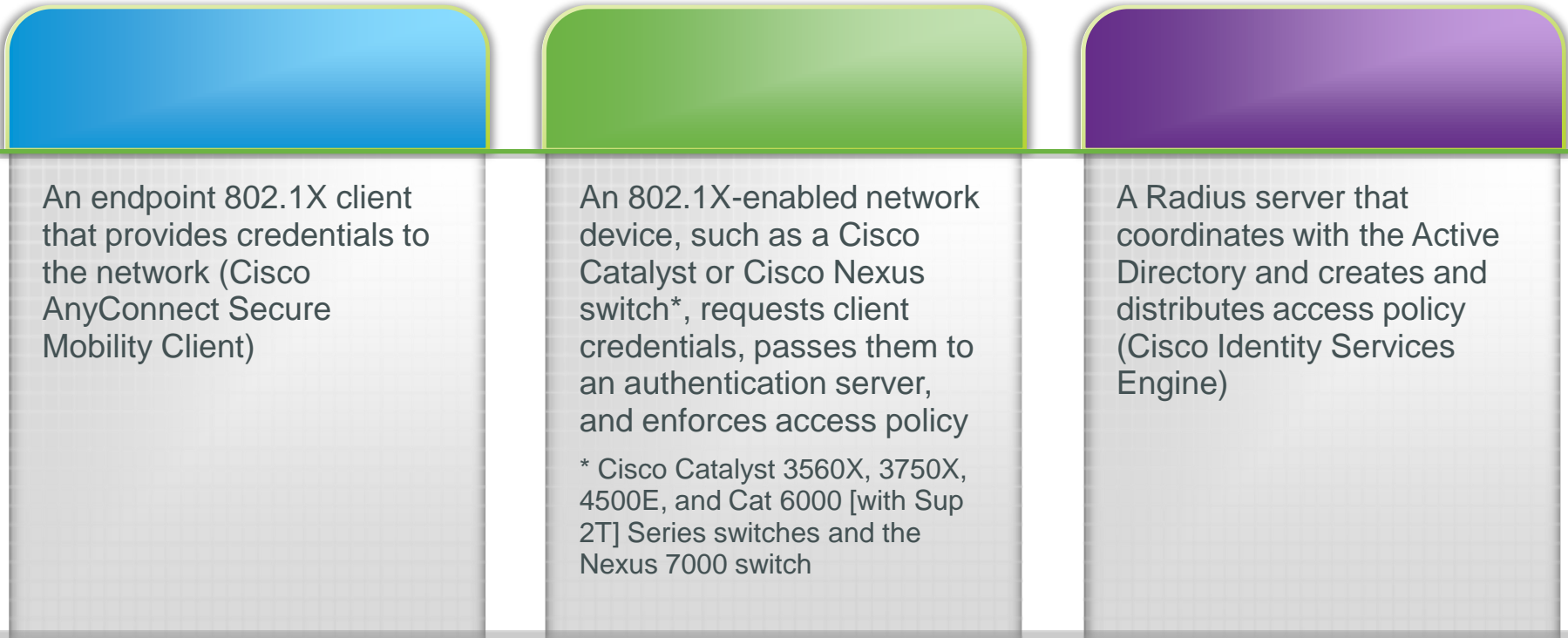
- Differentiated access control based on user and device group membership
- User to DC topology-independent access
- DC Server segmentation

## How do we do it?

- Advanced infrastructure access control using Secure Group Access
- Data Center physical and virtual resources enforcement (VDI)

# Getting from Here to There

- Secure the Access Layer—Deploy 802.1X to identify and authenticate devices at the access switch
- 802.1X requires three components:



An endpoint 802.1X client that provides credentials to the network (Cisco AnyConnect Secure Mobility Client)

An 802.1X-enabled network device, such as a Cisco Catalyst or Cisco Nexus switch\*, requests client credentials, passes them to an authentication server, and enforces access policy

\* Cisco Catalyst 3560X, 3750X, 4500E, and Cat 6000 [with Sup 2T] Series switches and the Nexus 7000 switch

A Radius server that coordinates with the Active Directory and creates and distributes access policy (Cisco Identity Services Engine)

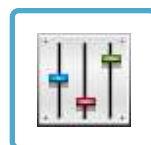


# Getting From Here To There

- Secure the Access Layer – Enable WebAuth for web-based, self-service Guest authentication, restricted network access, and monitoring



**Provision:** Guest accounts via sponsor portal



**Manage:** Sponsor privileges, guest accounts and policies, guest portal



**Notify:** Guests of account details by print, email, or SMS



**Report:** On all aspects of guest accounts

# Getting From Here To There

- Secure the Access Layer – Enable MACAuth Bypass and the TrustSec Device Profiler

## Device Identification

Determines device type

Centralizes device discovery and inventory

Uses network device tables and analyzes endpoint traffic

## Control and Audit

Authorize based on device role

Monitor and audit to prevent spoofing

Many endpoint devices are undocumented and cannot authenticate to the network



IP Cameras



Alarm Systems



Fax Machines



Turnstiles



Cash Registers



HVAC Systems



Video Conference

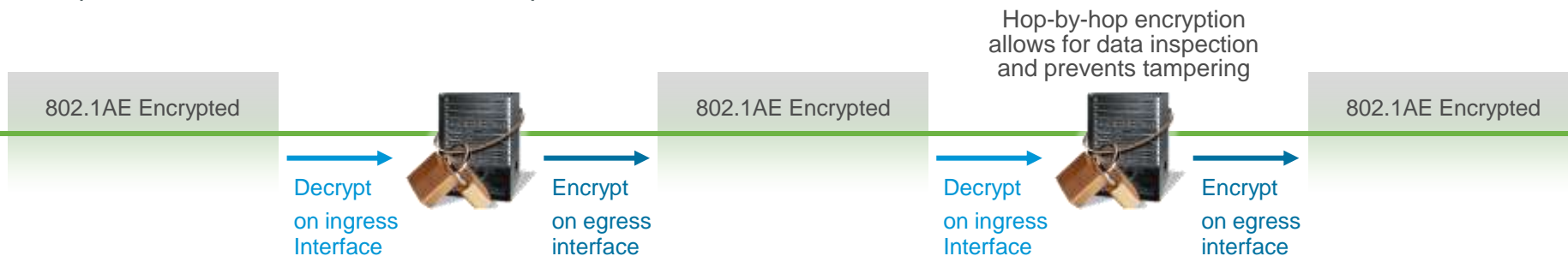


Printers

# Getting from Here to There

- Phase One—Enable MACsec on your wired access infrastructure

Ensures a consistent security profile across all access technologies (wired, wireless and VPN)



- Encryption mitigates packet eavesdropping, tampering, and injection
- Supports standards-based strong encryption technology
  - 128-bit AES-GCM, NIST-approved, 10Gb line-rate encryption
- Hop-by-hop encryption supports data and packet inspection
- Works in shared media environments (IP Phones, Desktops)

# Getting from Here to There

- Secure the Access Layer—Cisco 802.1X and MACsec-enabled solutions:

Cisco AnyConnect Secure Mobility Client 3.0

Cisco Catalyst 3750-X and 3560-X Series switches (requires service module)

Cisco Catalyst 4500E Series switches

Cisco Catalyst 4712 Series switch line cards

(WS-X4712-SFP+E, WS-X4748-RJ45V+E)

Cisco Catalyst 6000 Series switches (Sup 2T)

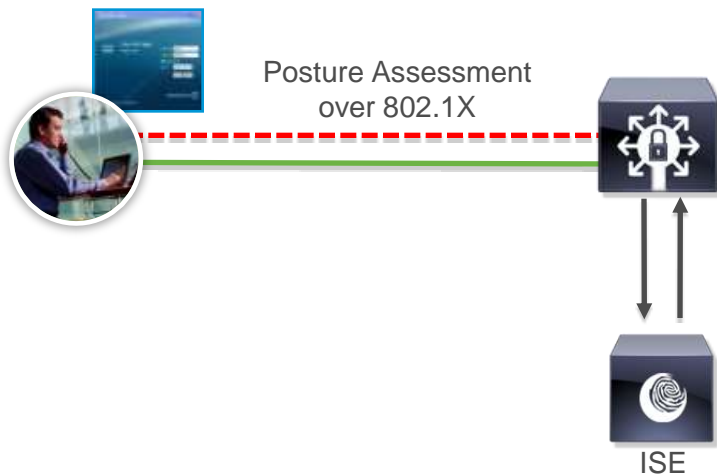
Cisco Nexus 7000 Series switches



Cisco Catalyst 3750-X

# Getting From Here To There

- Secure Endpoints – Enable Posture Assessment to ensure endpoints meet security policy:



- Scans endpoints for malware
- Checks for presence of required security applications
- Quarantines and remediates non-compliant devices
- Enforces OS patch levels
- Updates installed security solutions from 350+ security vendors

# Getting From Here to There

- Secure Endpoints – Secure network connection and communication from endpoint devices

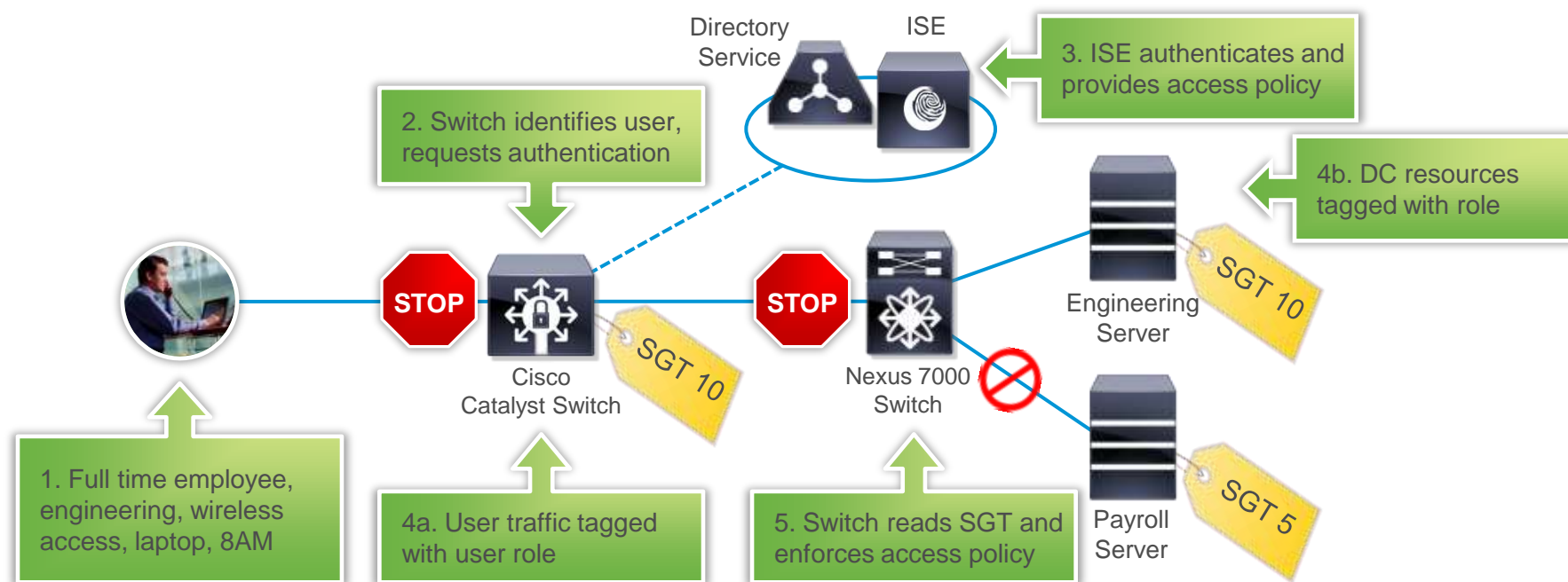
## Deploy AnyConnect Secure Mobility Client 3.0

- Unified access interface for SSL-VPN, IPSec & 802.1X for LAN/WLAN
- MACsec / MKA data encryption in software
- MACsec capable hardware (network interface) enhances performance



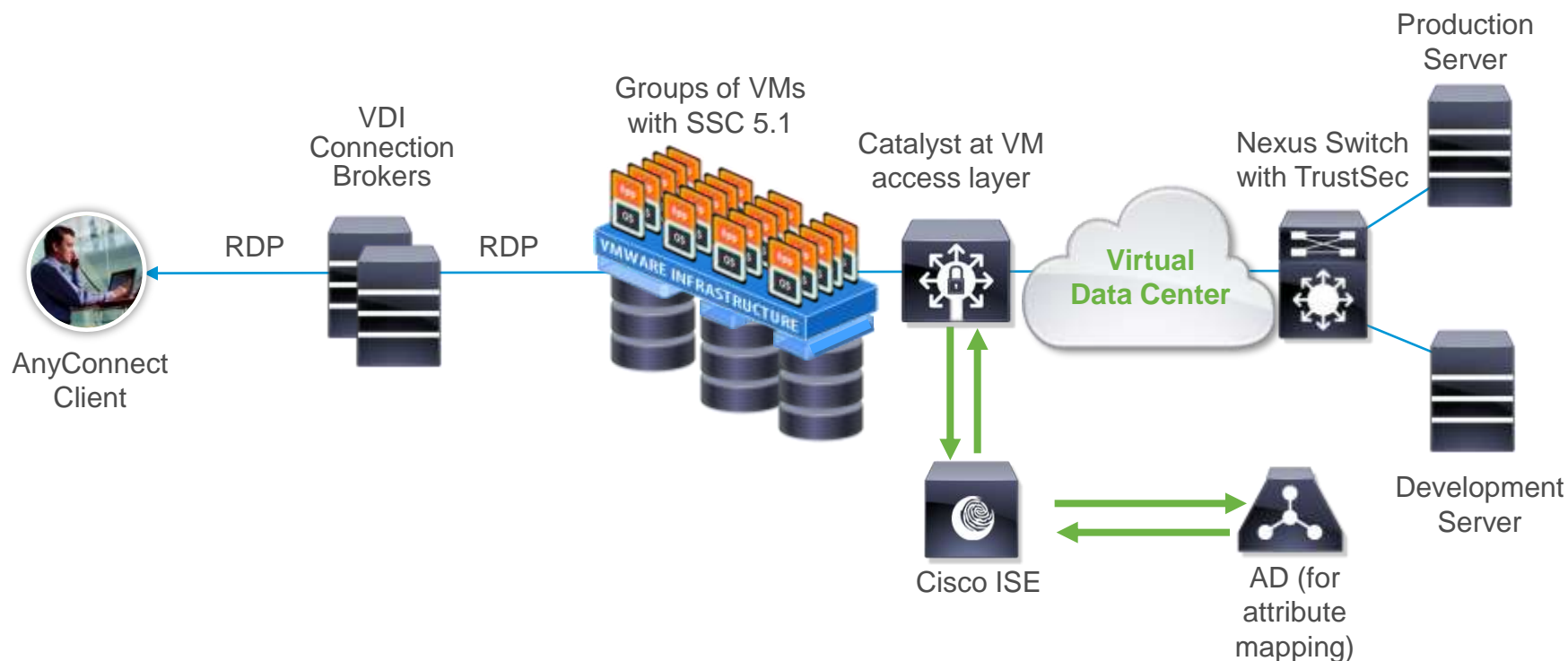
# Getting From Here To There

- Secure Resources– Secure Group Access (SGA)
  - TrustSec restricts user access using Security Group Access feature
  - Access policy is inserted as Security Groups Tags (SGTs) into devices
  - SGA reads and enforces policy tags on TrustSec-enabled Cisco switches along data path using Security Group ACLs (SGACLs)



# Getting From Here To There

- Secure Resources– Enable Virtualized Data Center security

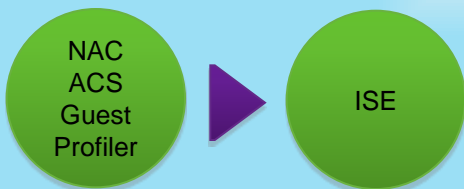


VM Connection Broker maps the user to any VM  
and SGT is assigned via 802.1X authentication



# Where Are We Going? Two Year View

## Converged Policy Platform



- AAA, 802.1X, guest, profiler, posture
- System monitoring and diagnostics
- ISE: next gen ACS + NAC

## Unified Agent



- AnyConnect: on & off premises security
- Extends 802.1x & VPN client + NAC
- Extends management to Positron

## Identity-Based Firewalls



- User, group, device based policy
- ASA & Positron platforms

## Simplified Device Profiling



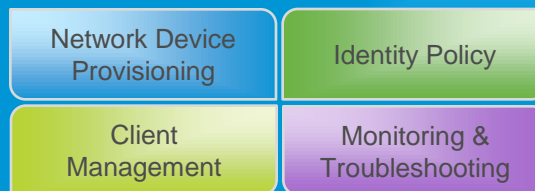
- Cisco delivered device template feed
- Switches collect & forward device fingerprint, no traffic re-engineering

## Network Infection Containment



- Streamline the locate, contain, & remediation process
- Leverage reputation & NIPS feeds

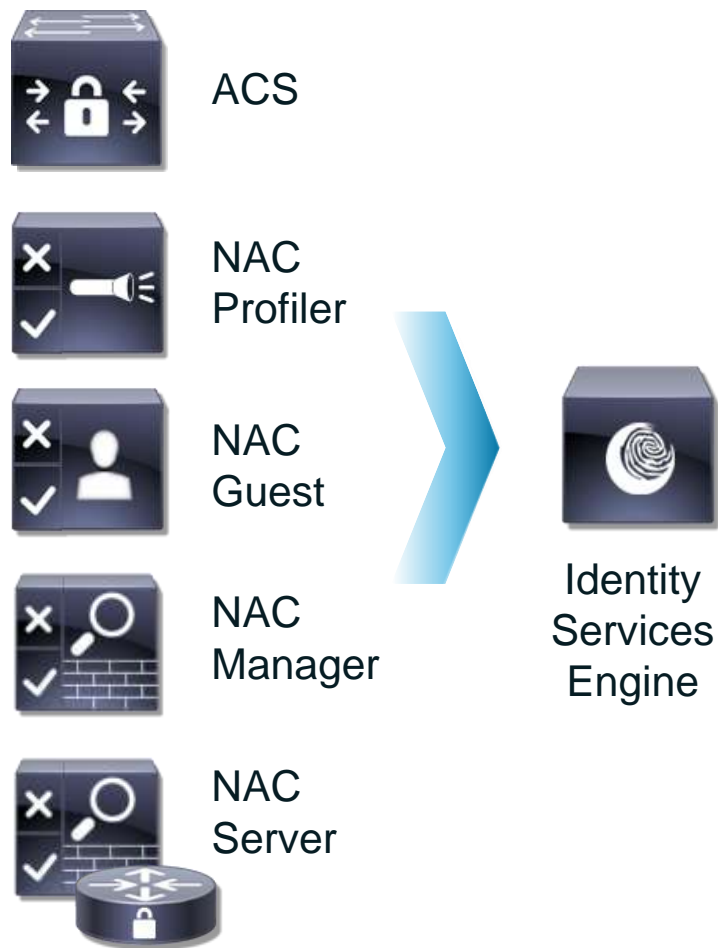
## Consolidated Network and Service Management



- Single admin pane-of-glass
- Wired & wireless infrastructure

# Cisco TrustSec-ISE

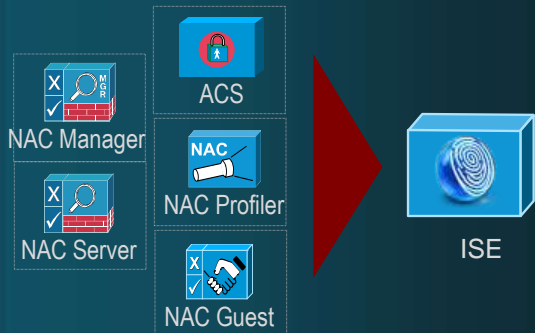
# Identity Services Engine



Centralized Policy  
Distributed Enforcement  
AAA Services  
Posture Assessment  
Guest Access Services  
Device Profiling  
Monitoring  
Troubleshooting  
Reporting

# Identity Services Engine Advantages

## Consolidated Services, SW Packages



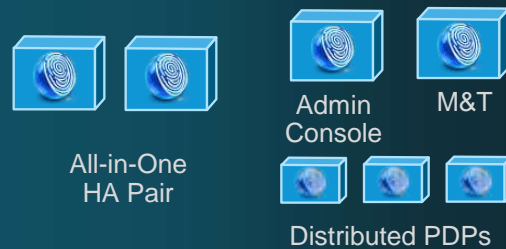
## Simplify Deployment & Admin

# Session Directory



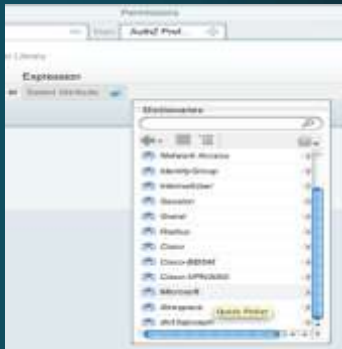
## Tracks Active Users & Devices

# Flexible Service Deployment



## Optimize Where Services Run

# Policy Extensibility



## Link in Policy Information Points

## Manage Security Group Access

SGT	Public	Private
Staff	Permit	Permit
Guest	Permit	Deny

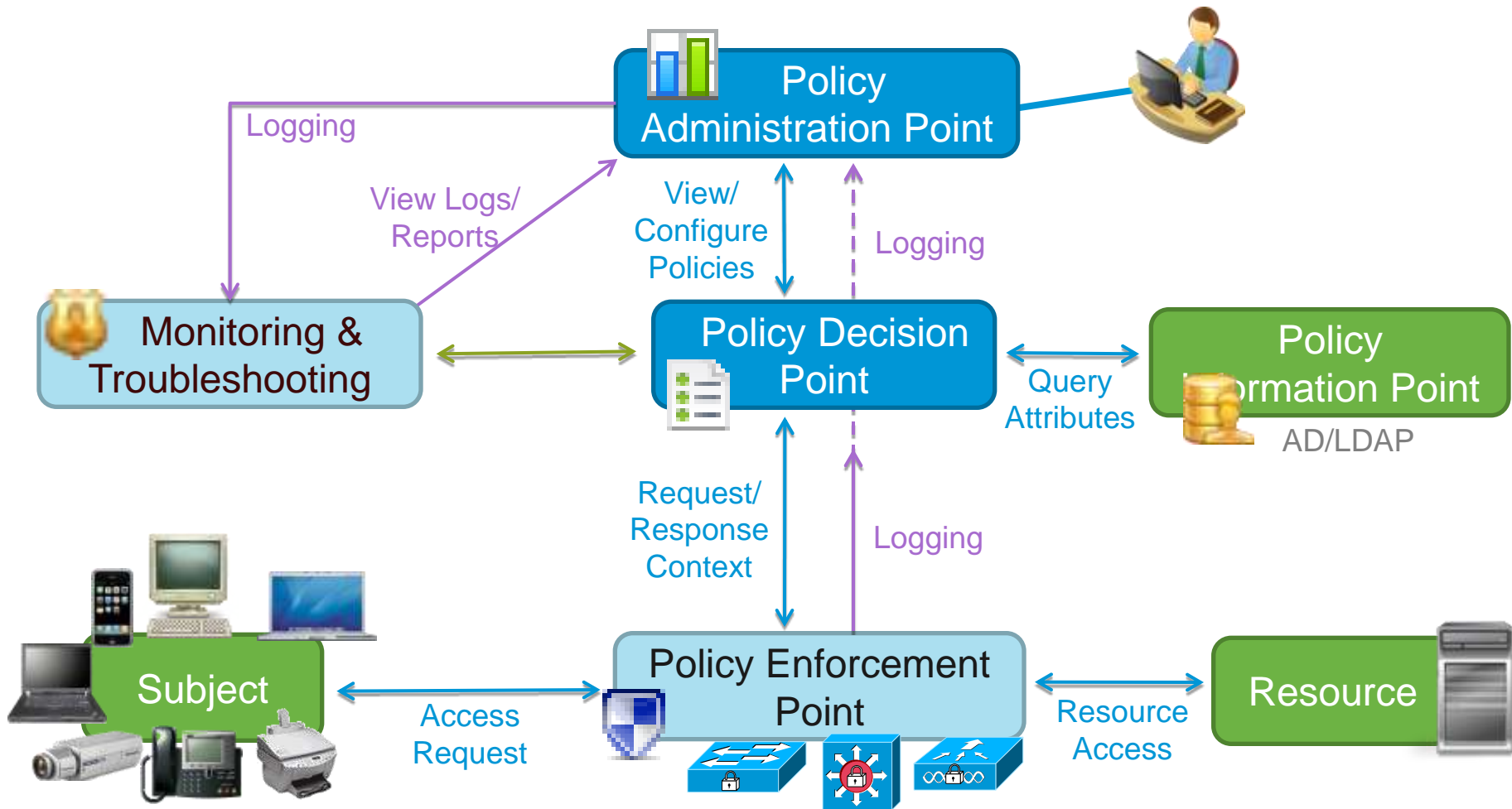
## Keep Existing Logical Design

## System-Wide Monitoring & Troubleshooting

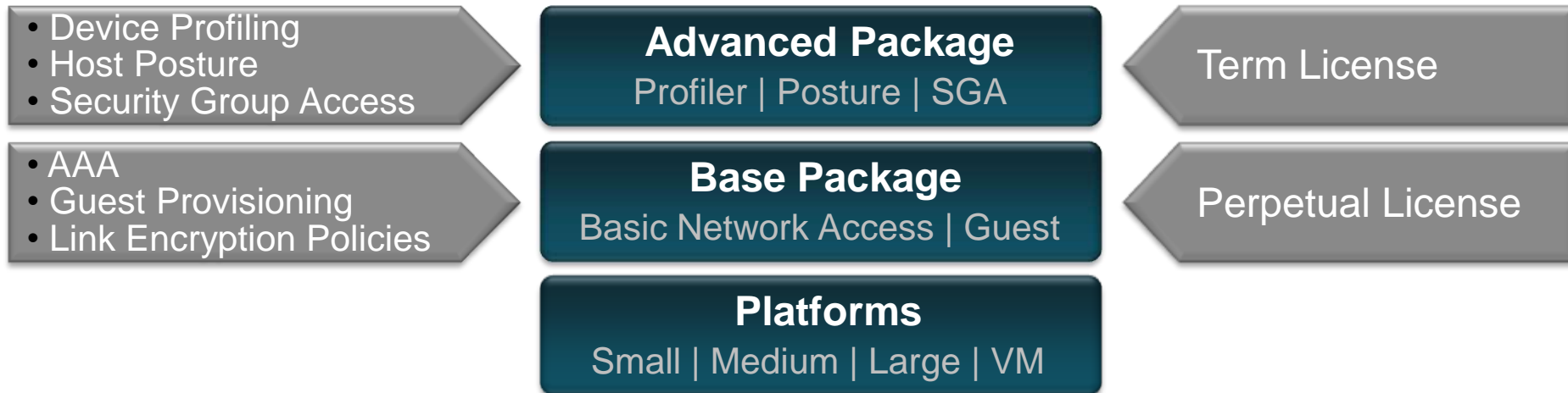


## Consolidate Data, 3 Click Drill-In

# ISE Architecture



# ISE Packaging & Licensing



## 3 Different Hardware Appliances or VMware-Based Solution

- Small = 3315/1121 appliances
- Medium = 3355 appliances
- Large = 3395 appliances
- ESX v4.x, ESXi v4.x and Server 2.0

## Software License Model

- Licenses based on concurrent # endpoints counted centrally (not tied to HW)
- Floating (active) device/user based pricing

# Conclusion

# Let Us Help – Cisco Professional Services

- Security Policy Review
- Design Strategy Development
- Controlled Deployment
- Full Deployment
- Training and Knowledge Transfer

Professional Services from Cisco, or one of our Services Partners, is an Important Component of Any Successful Rollout

- Security policy review
- Match compliance to infrastructure
- Custom design for authentication and access objectives
- Customized solution for existing network
- Experienced rollout services
- Expertise decreases deployment time
- Training for operation, maintenance, management, and tuning



# Cisco – A Leader In Access Control

- The Network Provides Comprehensive Visibility and Control



## A single vendor for:

- Technology and solution leadership:
  - Identity across the network
  - Posture assessment
  - Guest access
  - Device profiling
  - Data encryption with MACsec
  - TrustSec SGA
  - Data Center virtualization
- Deployment experience with the most experienced direct and partner-led professional service teams to address PDIO complexities

<sup>1</sup>Infonetics, June 2008

<sup>2</sup>Gartner Magic Quadrant March 2009, Frost & Sullivan April 2008, Forrester September 2008, IDC Dec 2007, Infonetics June 2008

<sup>3</sup>[http://searchsecurity.techtarget.com/productsOfTheYearCategory/0,294802,sid14\\_tax310405\\_ayr2008,00.html3](http://searchsecurity.techtarget.com/productsOfTheYearCategory/0,294802,sid14_tax310405_ayr2008,00.html3)

# TrustSec Solves Business Problems

Business Problem	TrustSec 2.0
I'd like to simplify my role-based access control deployment	Integrated policy manager & client: <ul style="list-style-type: none"><li>• Identity Services Engine with integrated profiling, guest, posture</li><li>• AnyConnect with 802.1X supplicant, MACsec, etc.</li></ul>
I need to ensure my endpoints don't bring malware into my network	802.1X with Posture Assessment
I need to identify the wireless devices in my network (like iPads)	Device Profiler with Wireless (Authorization supported only with 802.1X)
I am worried about data confidentiality in my LAN	MACsec switch to switch encryption (Cat 3K/4K/6K)
I'd like to have scalable role-based access control in my network	SGT/SGACL enforcement on the Cat 6K SUP 2T
I need my scalable role-based access control method to work in virtualized environment	SGA tested and validated in a VDI environment

# Summary

- Cisco TrustSec provides comprehensive identity and access control solutions for any organization. These include:

Context-based network access

Endpoint posture assessment

Non-user device authentication

Self-service guest access

MACsec data encryption with inspection

Phased deployment options

Security Group Access

Centralized, unified access policy and enforcement

# TrustSec Resources

- For more information on TrustSec and related products and services, please go to:

[www.cisco.com/go/trustsec](http://www.cisco.com/go/trustsec)

[www.cisco.com/go/nac](http://www.cisco.com/go/nac)

[www.cisco.com/go/ise](http://www.cisco.com/go/ise)

[www.cisco.com/go/security](http://www.cisco.com/go/security)

Thank you.

