

ALGO SYSTEMS
THE PATH FORWARD



How to Control Who Gets Onto Your Network

A Large Systemic Bank's Security Case Study

Nikos Mourtzinis, CCIE #9763
Cyber Security Sales Specialist, Cisco
nmourtzi@cisco.com

Algosystems, 4/2018

Christos Stefanekou, CCIE #43578
ICT Architect, Algosystems
xstefan@algosystems.gr

Digital transformation is demanding change at an unprecedented pace



Mobility

Wireless and mobile device traffic will be 66% of total IP traffic by 2020



IoT

26 billion networked devices and connections will exist by 2020



BYOD

95% of global enterprises will have both a CYOD and a formal BYOD plan in place by 2019



Cloud

Annual global cloud IP traffic will reach 14.1 ZB by the end of 2020

[2017 Cisco Security report](#)
[Cisco Complete VNI Forecast](#)
[Gartner](#)
[Cisco Global Cloud Index Whitepaper](#)

It's Harder Than Ever to See Who Is on Your Network and What They Are Doing



90% of surveyed organizations are not “fully aware” of the devices accessing their network

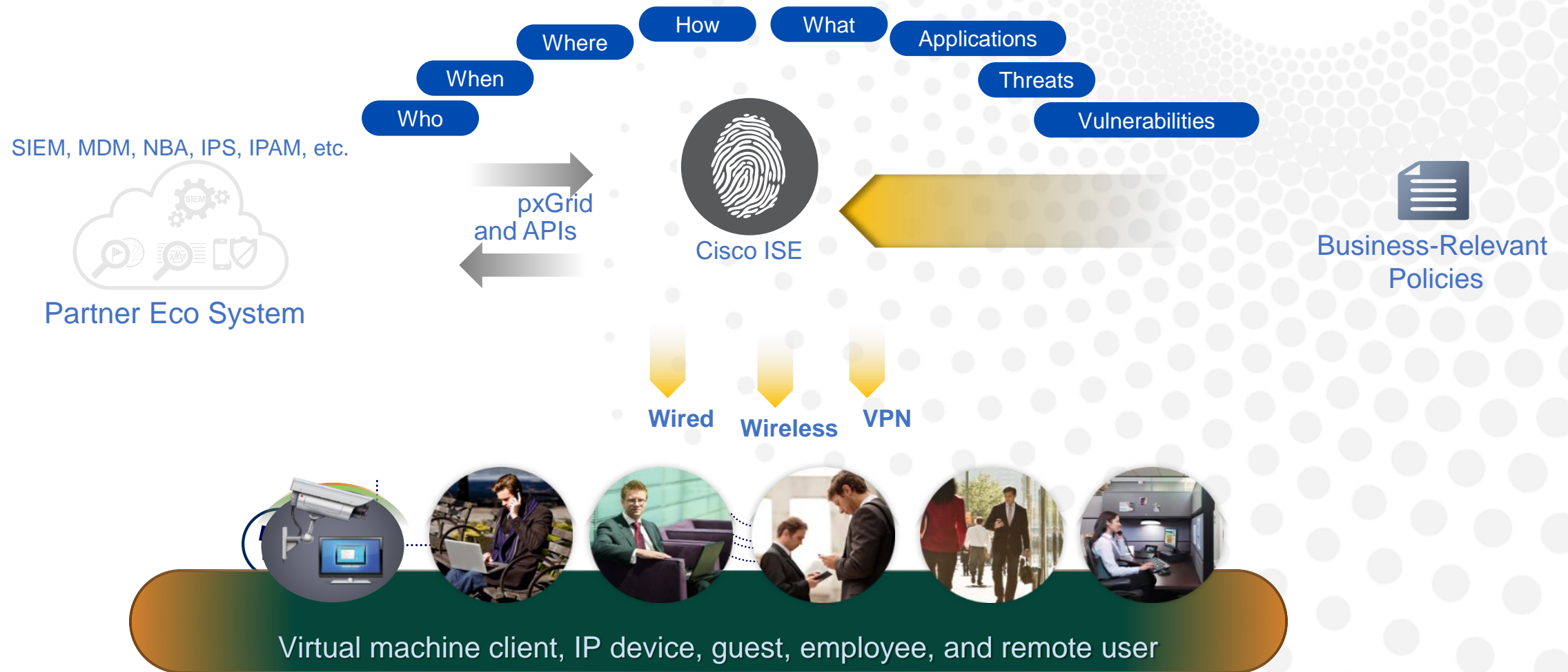
75% of companies say their mobile devices were targeted by malware in the last 12 months

Cisco Identity Services Engine (ISE)

Who/What is currently connected on the Network ?

- **How Do I Control Who and What Access the Network/Resources?**
 - ✓ **Compliance**
 - ✓ **Insider Threat**
 - ✓ **Once inside, threats can spread quickly**
- **How to Quarantine a User or an Endpoint ?**

Cisco Identity Services Engine



Authentication, Authorization, Accounting AAA



Corporate User



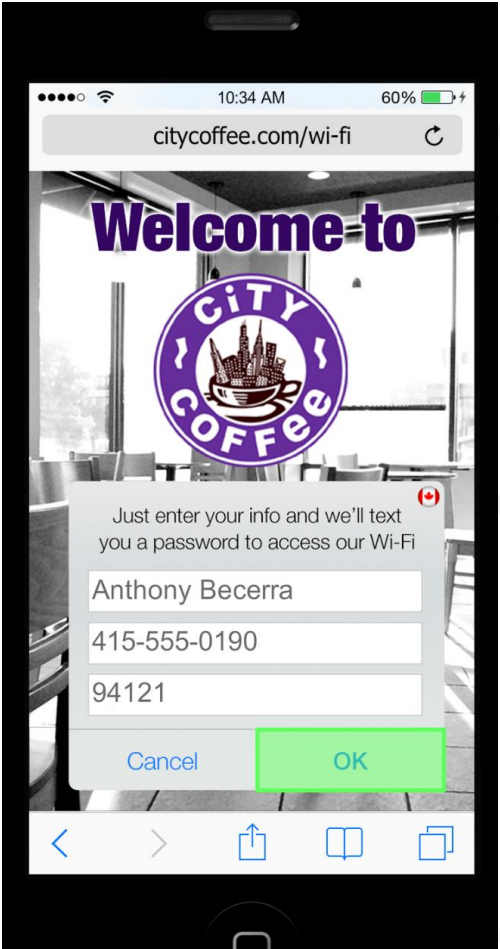
Company Asset



Guest
Registration Required

IEEE 802.1x, Easy Connect
MAC-Authentication Bypass (MAB)
Web Authentication

Guest Management

A web interface for Corporate Guest Management. The header has a 'CITY COFFEE' logo and a 'CORPORATE' label. Below the header is a navigation bar with 'Create account', 'Manage accounts', and 'Approve accounts (1)'. The main content area is a form for creating a new account. It has a 'Guest type' dropdown set to 'Daily' with a note '- 3 Device limit. Valid from 9 AM to 5 PM on weekdays'. Below this is a section 'Enter guest information for:' with two tabs: 'Known guests' (selected) and 'Random guests'. The 'Known guests' tab has input fields for 'First Name *' (Anthony), 'Last Name *' (Becerra), 'Email *' (abecerra@finebeans.com), 'Company' (Fine Beans), and 'Phone' (415-555-0190). There is an 'Import names' button and an 'Add another guest' link. To the right is a section 'Access valid for:' with a 'Days (30 maximum)' dropdown set to '1'. Below this are input fields for 'From *' (11/20/2014 10:30 AM), 'To *' (11/21/2014 10:30 AM), 'Location *' (San Jose, CA), 'SSID *' (Guestnet), and 'Group tag'. At the bottom right are 'Cancel' and 'Create' buttons. A footnote at the bottom left says '* Required fields'.

Device Profiling



Company Asset



Non-User Device



Personal Asset

Active Probes
Netflow DHCP DNS HTTP RADIUS NMAP SNMP

Device Sensor
CDP LLDP DHCP HTTP H323 SIP MDNS

1.5 Million

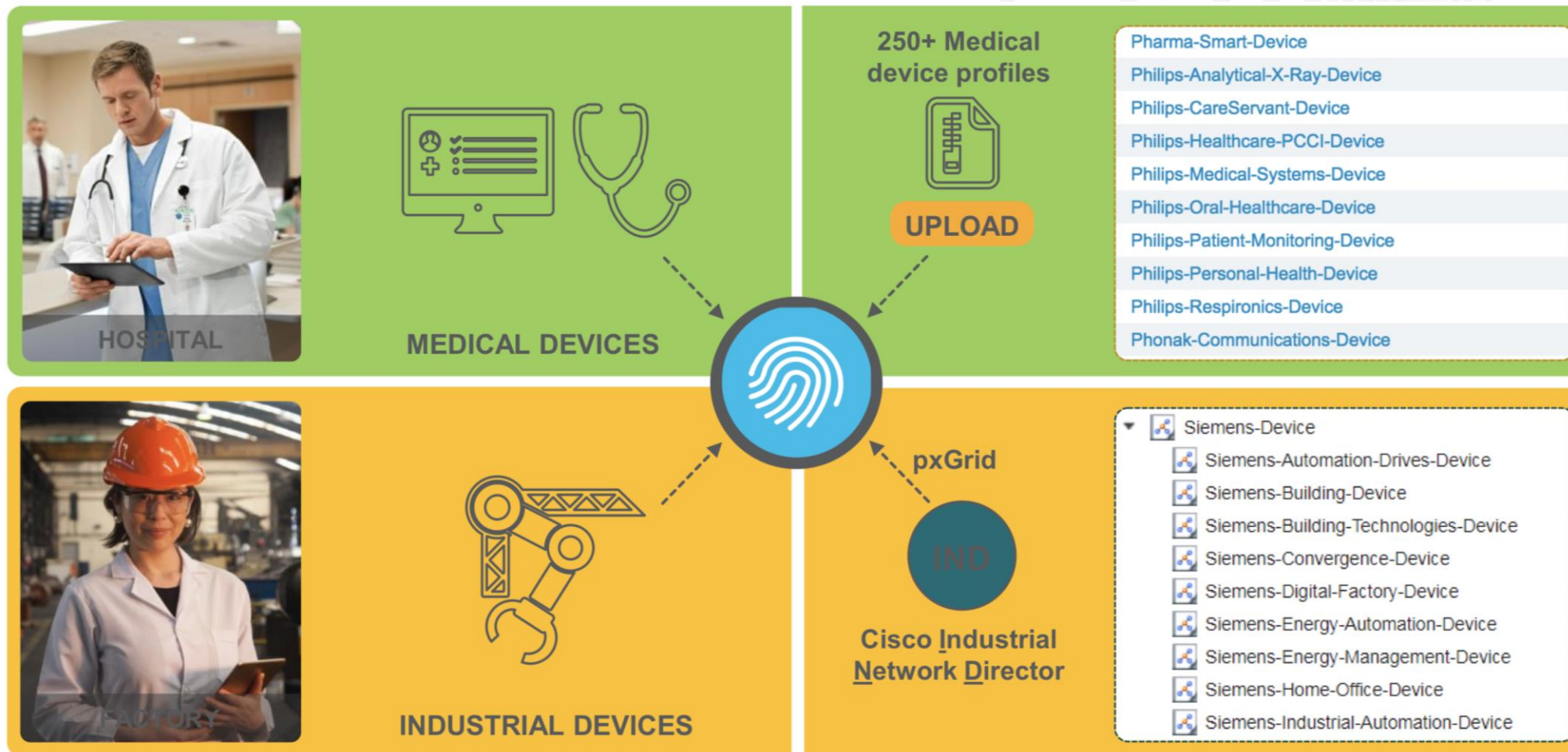
Devices with '50' attributes each can be stored

550+

High-level canned profiles. +Periodic feeds

<input type="checkbox"/>	MAC Address	IPv4 Address	Username	Hostname	Endpoint Profile
×	<input type="text" value="MAC Address"/>	<input type="text" value="IPv4 Address"/>	<input type="text" value="Username"/>	<input type="text" value="Hostname"/>	<input type="text" value="Endpoint Profile"/>
<input type="checkbox"/>	E8:B1:FC:F5:18:65	10.35.70.248	CISCO\lagollabi	AGOLLABI-BV...	Windows7-Workstation
<input type="checkbox"/>	AC:BC:32:A9:FD:81	10.33.249.93	ccarty	CCARTY-M-H2...	Apple-iDevice
<input type="checkbox"/>	AC:5F:3E:D0:71:75	10.56.129.19	ac5f3ed07175	android-c7f130...	Android-Samsung
<input type="checkbox"/>	28:CF:E9:1B:A7:B7	10.33.249.192	loverbey	LOVERBEY-M...	OS_X_El_Capitan-Work...
<input type="checkbox"/>	18:5E:0F:71:4D:1E	10.32.2.23	CISCO\lamshah	ARNSHAH-J36..	Microsoft-Workstation
<input type="checkbox"/>	10:4A:7D:D5:8D:4C	10.35.68.51	CISCO\bychan	BYCHAN-WS03	Microsoft-Workstation

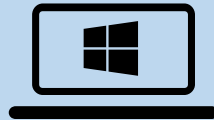
Medical NAC and Internet of Things



Posture Assessment



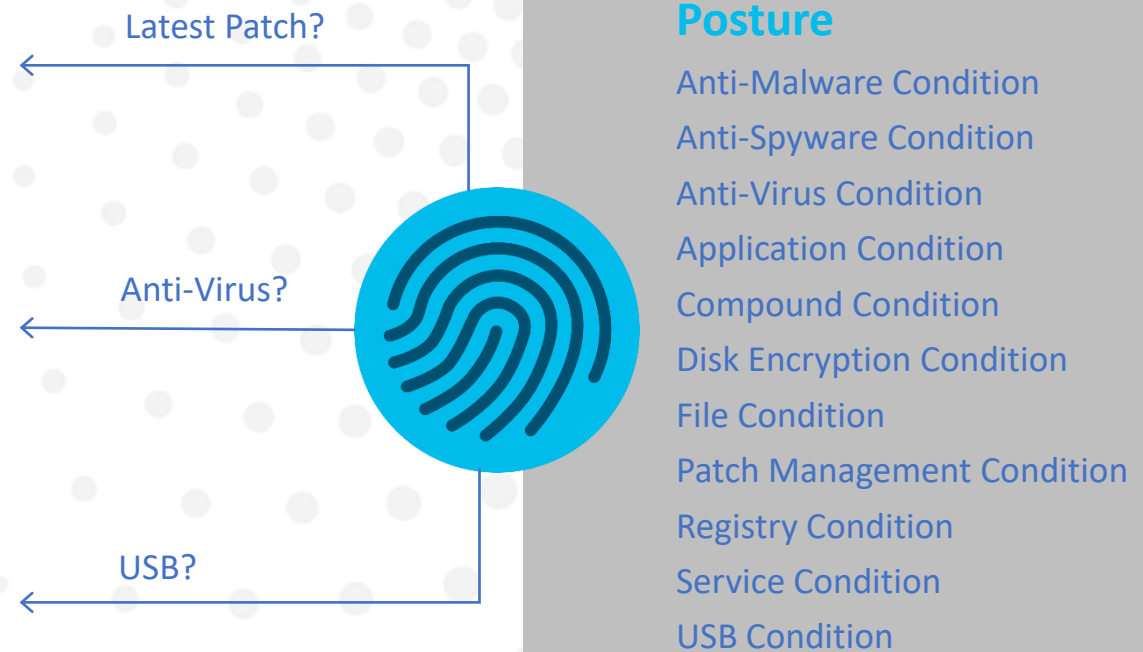
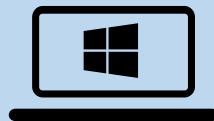
Posture defines the state of compliance with the company's security policy



- Is the system running the current Windows patches?
- Do you have anti-virus software installed? Is it up to date?
- Do you have anti-spyware software installed? Is it up to date?



Non-compliance, such as MDM or vulnerability can be automatically enforced with a change in access policy




Application Visibility

Continuous Data Monitoring on APP's

ISE will report a complete list of running applications and installed applications.

Endpoints > 48:D7:05:E3:E4:93

48:D7:05:E3:E4:93



MAC Address: 48:D7:05:E3:E4:93

Username: test

Endpoint Profile: Apple-Device

Current IP Address: 192.10.10.229

Location: Location → All Locations

Applications

Attributes

Authentication

Threats

Vulnerabilities

Refresh

Policy Actions

Filter

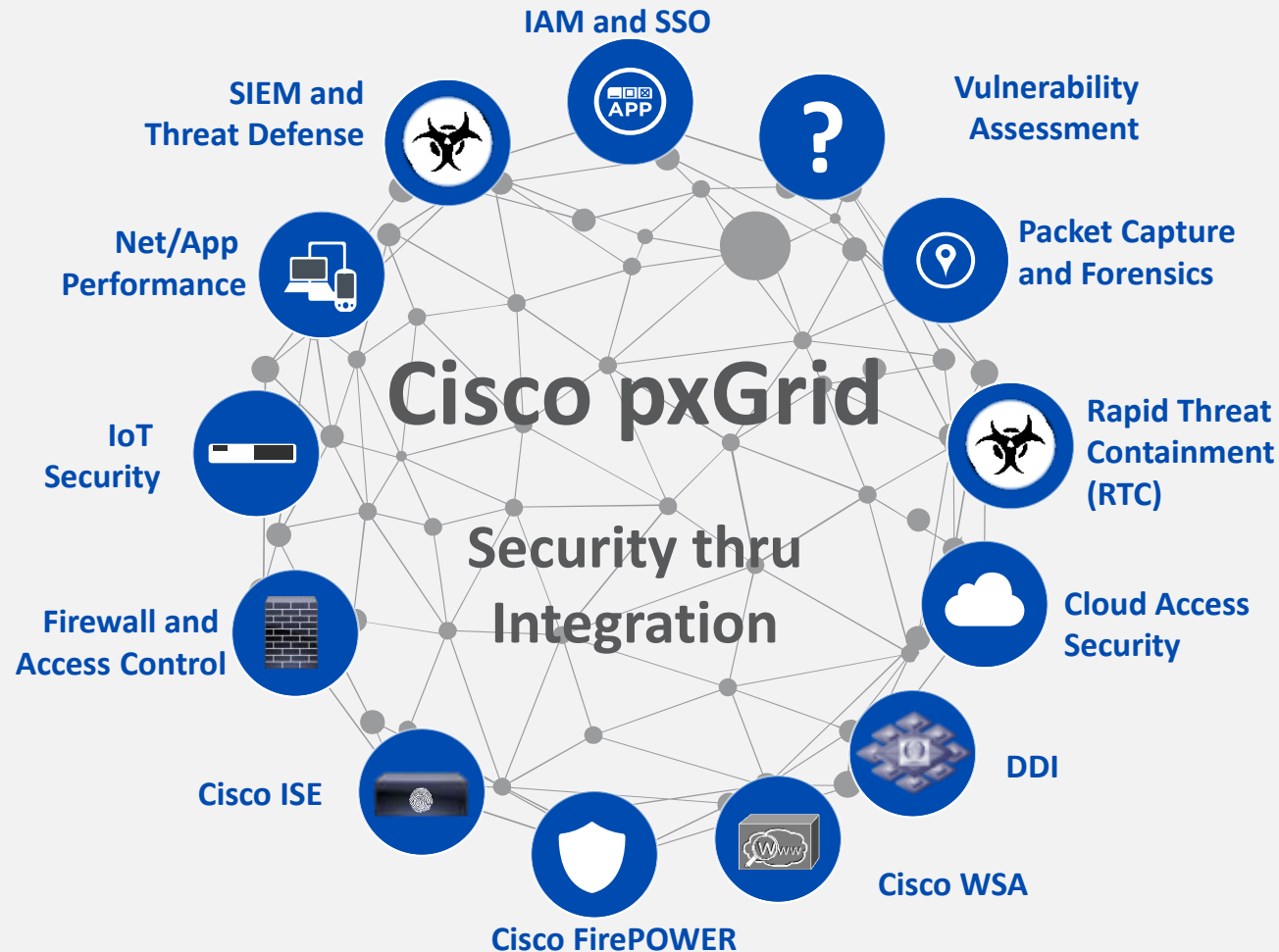
<input type="checkbox"/>	Application Name	Version	Vendor	Running process	Category	Install Path
<input type="checkbox"/>	Dashboard	1.8	Apple Inc.		Unclassified	/Applications/Dashboar...
<input type="checkbox"/>	Network Utility	1.8	Apple Inc.		Unclassified	/System/Library/CoreS...
<input type="checkbox"/>	Digital Color Meter	5.10	Apple Inc.		Unclassified	/Applications/Utilities/D...
<input type="checkbox"/>	Safari	8.0	Apple Inc.	1	AntiPhishing,Browser	/Applications/Safari.app

Process Name	Hash	Process ID
/Applications/Safari.app/Contents/MacOS/Safari	4F2F2AEA2274E52F7BD736EE91756F5A36ADBA9D948CC3B578634AA6210AA8BD	4372

<input type="checkbox"/>	Cisco AnyConnect Secure Mobil...	4.4.00154	Cisco Systems, Inc.	1	VPNClient	/Applications/Cisco/Cis...
<input type="checkbox"/>	FileVault	10.10.1	Apple Inc.		DiskEncryption	/System/Library/Prefer...

PxGrid – Industry Adoption Critical Mass

40+ Partner Product Integrations and 12 Technology Areas



pxGrid-Enabled ISE Partners:

- **RTC:** Cisco FirePower, Bayshore, E8, Elastica, Hawk, Huntsman, Infoblox, Invincea, Lancope, LogRhythm, NetIQ, Rapid7, SAINT, Splunk, Tenable
- **Firewall:** Check Point, Infoblox, Bayshore
- **DDI:** Infoblox
- **Cloud:** Elastica, SkyHigh Networks
- **Net/App:** Savvius
- **SIEM/TD:** Splunk, Lancope, NetIQ, LogRhythm, FortScale, Rapid7
- **IAM:** Ping, NetIQ, SecureAuth
- **Vulnerability:** Rapid7, Tenable, SAINT
- **IoT Security:** Bayshore Networks
- **P-Cap/Forensics:** Emulex
- **Cisco:** WSA, Firesight, Firepower, ISE

Other ISE Partners:

- **SIEM/TD:** ArcSight, IBM QRadar, Tibco LogLogic, Symantec
- **MDM/EMM:** Cisco Meraki, MobileIron, AirWatch, JAMF, SOTI, Symantec, Citrix, IBM, Good, SAP, Tangoe, Globo, Absolute

So you can leverage your network to improve security without sacrificing performance

Network. Intuitive.



Network Visibility

360° visibility

Real-time analysis of data and traffic to provide visibility and intelligence across the network



Network Segmentation

Dynamic control

Software-defined segmentation for effective and consistent policy application

Comprehensive automation

Integrated solutions that augment your capabilities and reduce manual processes

Transform your network for the digital era and detect threats faster

According to an independent total economic impact study conducted by Forrester

80%

Lower IT operational costs

by avoiding set-up and maintenance costs of traditional bolt-on solutions

98%

Improve network agility

by reducing the time to implement network changes

According to the 2017 Cisco Annual Cybersecurity Report

hours.

Boost threat detection

by leveraging industry-leading time-to-detection capabilities

ISE is a market leader

F R O S T
&
S U L L I V A N

FORRESTER®

Gartner®

SC
MAGAZINE

Frost & Sullivan 2016
Best in Class

80% operations savings
with ISE & TrustSec*

Gartner MQ Leader
3 Years
Included in 3 of Gartner
Top 10 Information
Technologies

SC Magazine 2016 &
2017 Best NAC Award



A Large Systemic Bank's Case Study

Strengthening Network Access Control in a Large Banking Environment

GOALS

Secure Wired & Wireless Network Access

For **thousands** endpoints covering HQs & remote buildings

Ensure Endpoint Compliance

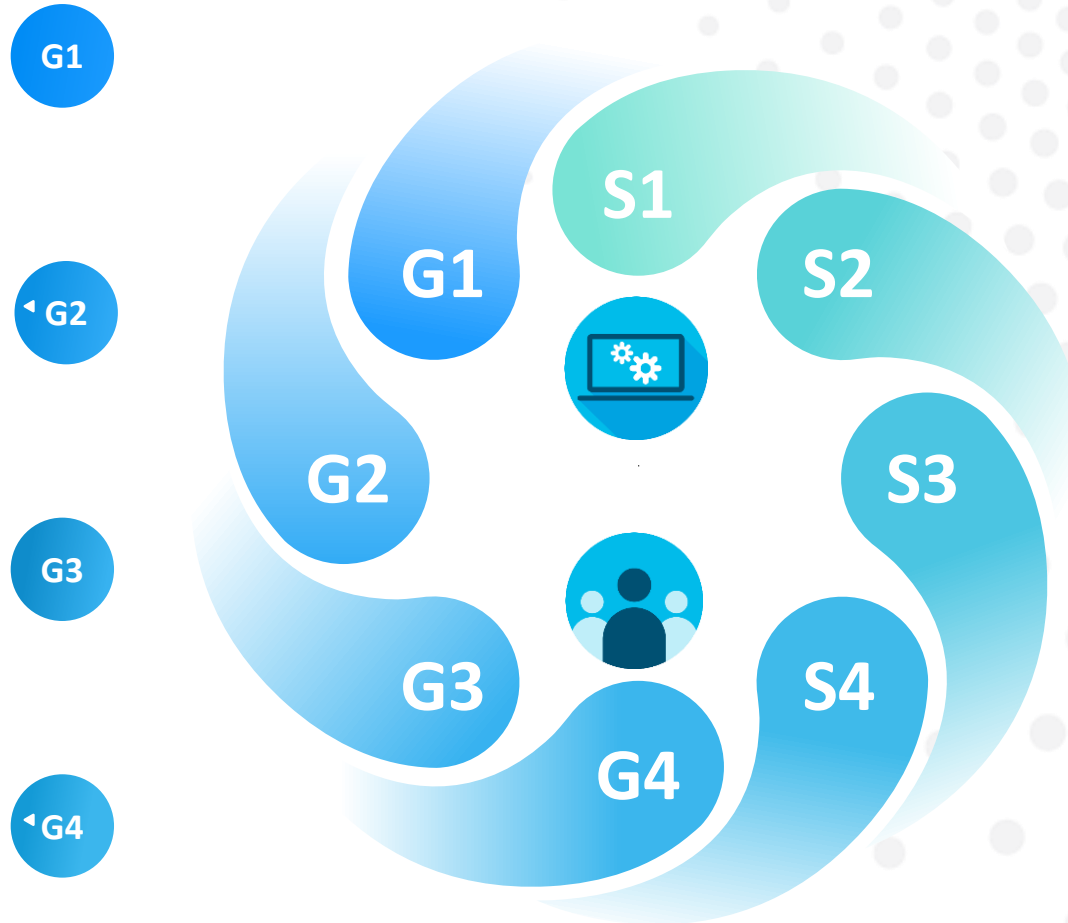
For all Bank's employees, Partners & Guests

Achieve Centralized Device Administration

For **thousands** of Network Devices (routers, firewalls, etc) for all Bank's points of presence in Greece.

Ensure Context Visibility

See and share user and device details



SOLUTION

S1

802.1X, MAB, Web Authentication, Profiling

S2

Posture Assessment, Cisco AnyConnect & Web Agent

S3

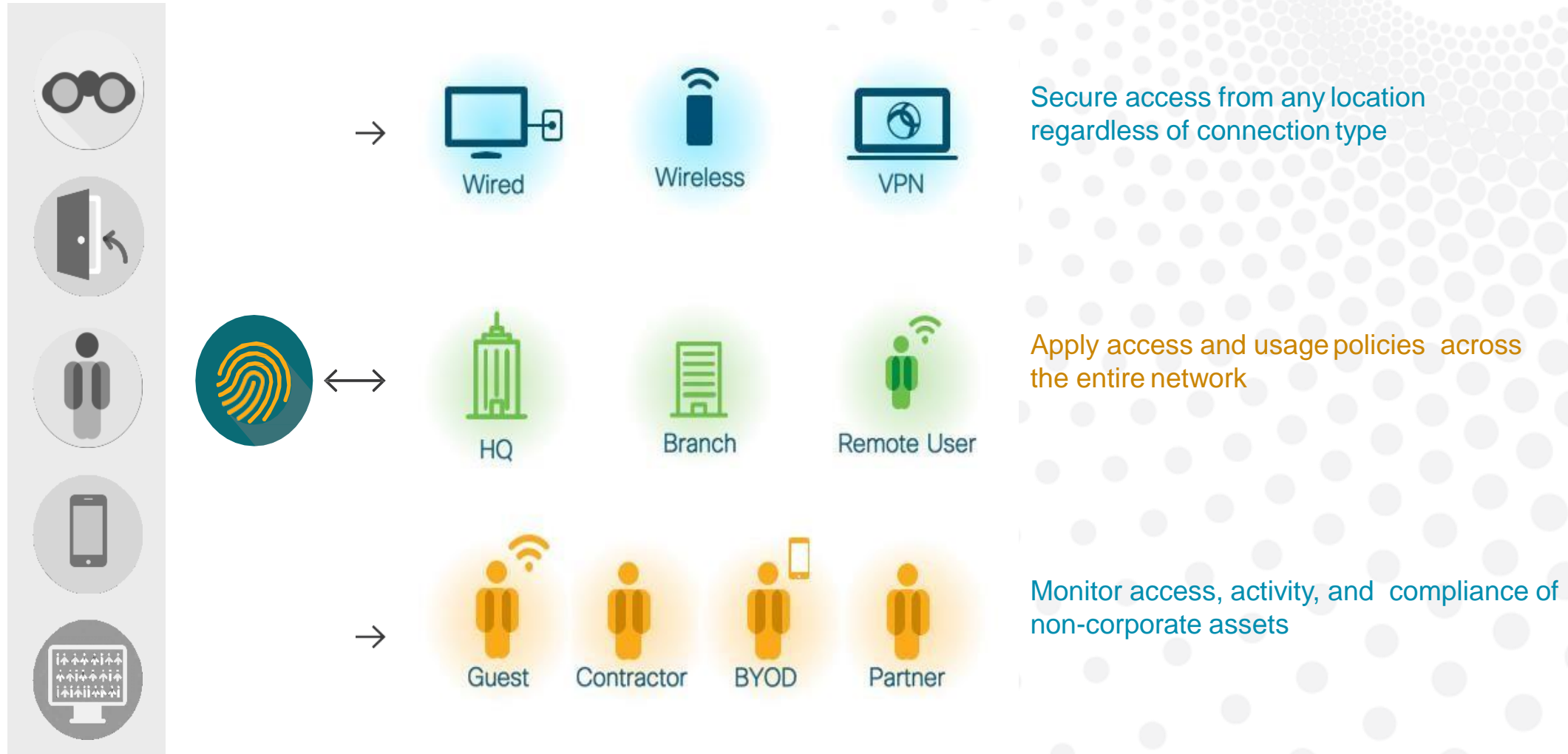
Tacacs+

S4

Profiling, Reporting

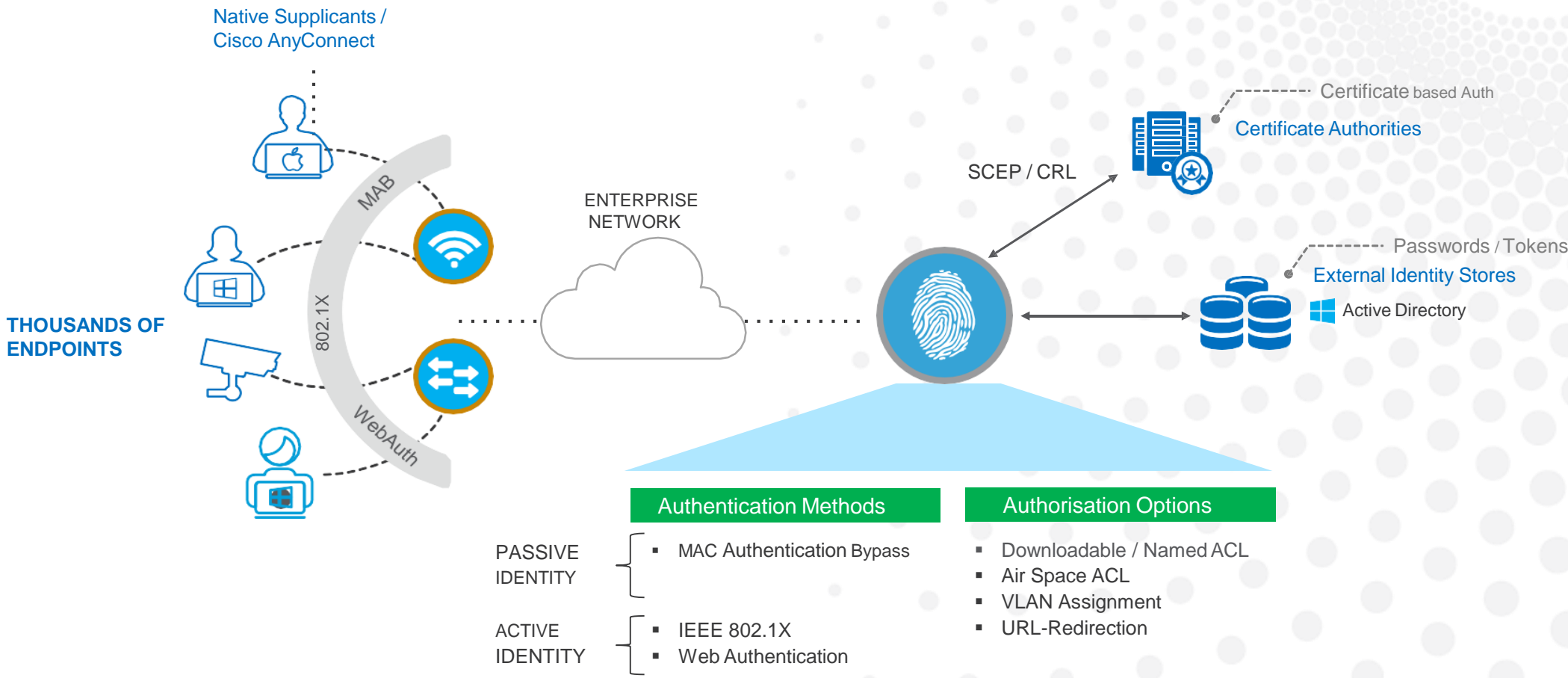
NAC Case Goal 1: Secure Wired and Wireless Network Access

Solution: 802.1X, MAB, Web Authentication, Profiling



NAC Case Goal 1: Secure Bank's Wired and Wireless Network Access

Solution: 802.1X, MAB, Web Authentication, Profiling








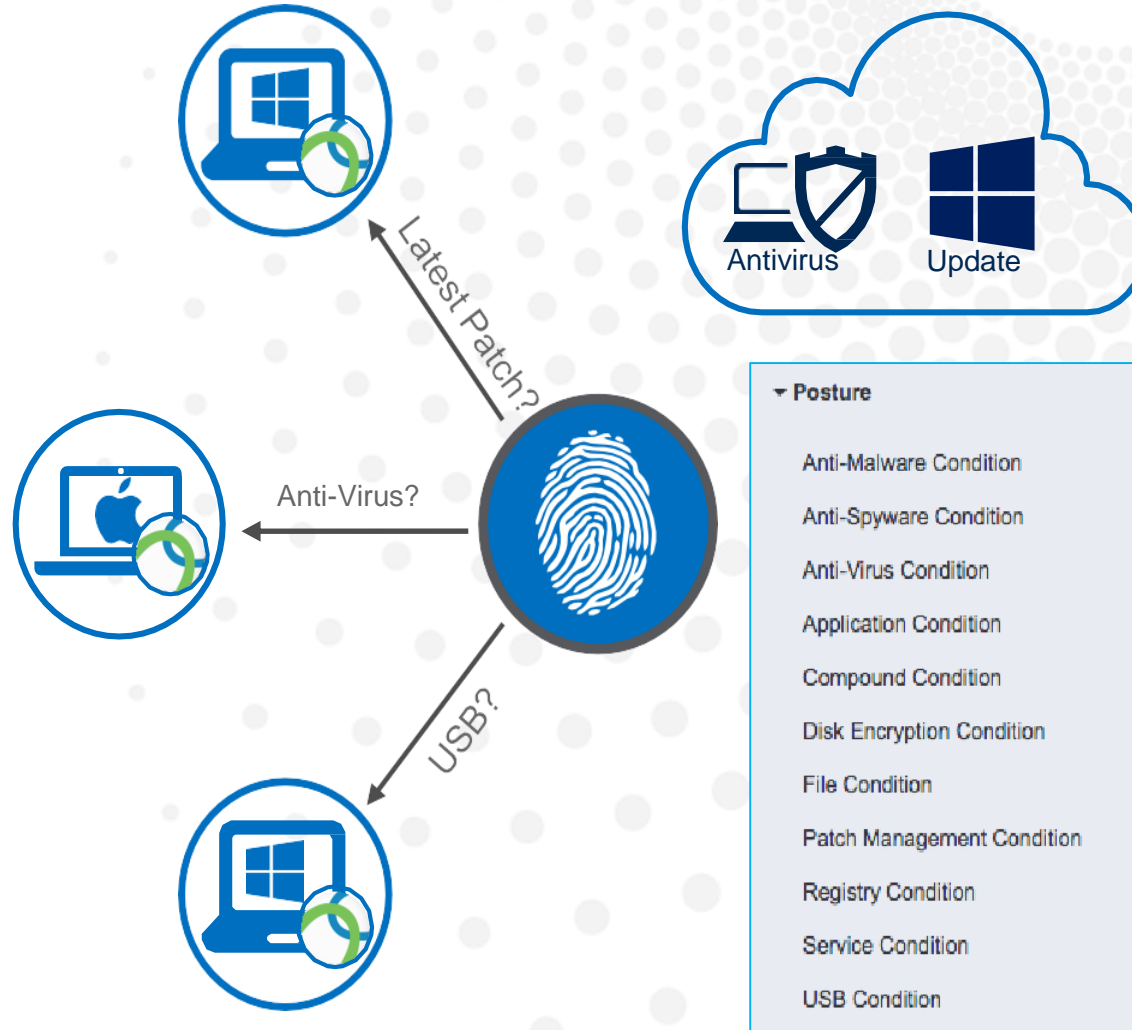
NAC Case Goal 2: Ensure Endpoint Compliance

Solution: Posture Assessment, Cisco Any Connect & Web Agent

Posture defines the state of compliance with the company's security policy

Posture Flow

-  **AUTHENTICATE USER/DEVICE**
Posture: Unknown / Non-Compliant ?
-  **QUARANTINE**
Limited Access: VLAN / dACL / SGTs
-  **POSTURE ASSESMENT**
Check Hotfix, AV, Pin lock, USB Device, etc.
-  **REMEDiation**
WSUS, Launch App, Scripts, MDM, etc.
-  **AUTHORISATION CHANGE**
Full Access – VLAN / dACL / SGTs.



NAC Case Goal 3: Achieve Centralized Device Administration

Solution: TACACS+

THOUSANDS OF NETWORK DEVICES

Benefits



Simplified, centralized device administration

Increase security, compliancy, auditing for a full range of administration use cases



Flexible, granular control

Control and audit the configuration of network devices



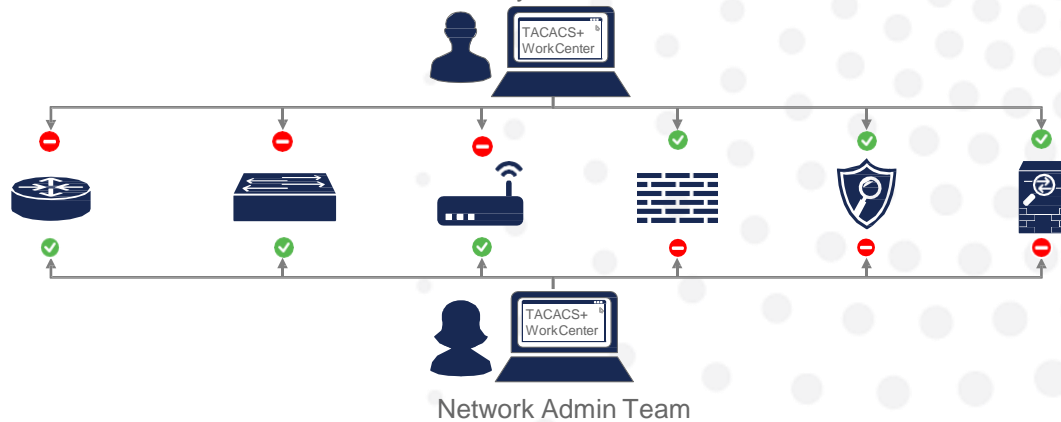
Holistic, centralized visibility

Get a comprehensive view of TACACS+ configurations with the TACACS+ administrator work center

TACACS+ Device Administration

Role-based access control

Security Admin Team





Capabilities


- Role-based access control
- Flow-based user experience
- Command level authorization with detailed logs for auditing
- Dedicated TACACS+ workcenter for network administrators
- Support for core ACS5 features


NAC Case Goal 4: Ensure Context Visibility


Solution: Profiling, Reporting, Posturing









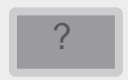











UNKNOWN

Without ISE

Poor context awareness	Rich context awareness	
IP ADDRESS: 192.168.2.101	WHO	Yiannis (Employee)
Unknown	WHAT	Apple iPad/iOS/11.0.1
Unknown	WHEN	10:30 AM PST
Unknown	WHERE	Building XYZ
Unknown	HOW	Wireless
Unknown	APPS	Firefox, MS Word, AnyConnect
Unknown	SPEC	Serial number, CPU, memory
Access to any device/user	RESULT	Authorised network access
<div></div>	<div></div>	

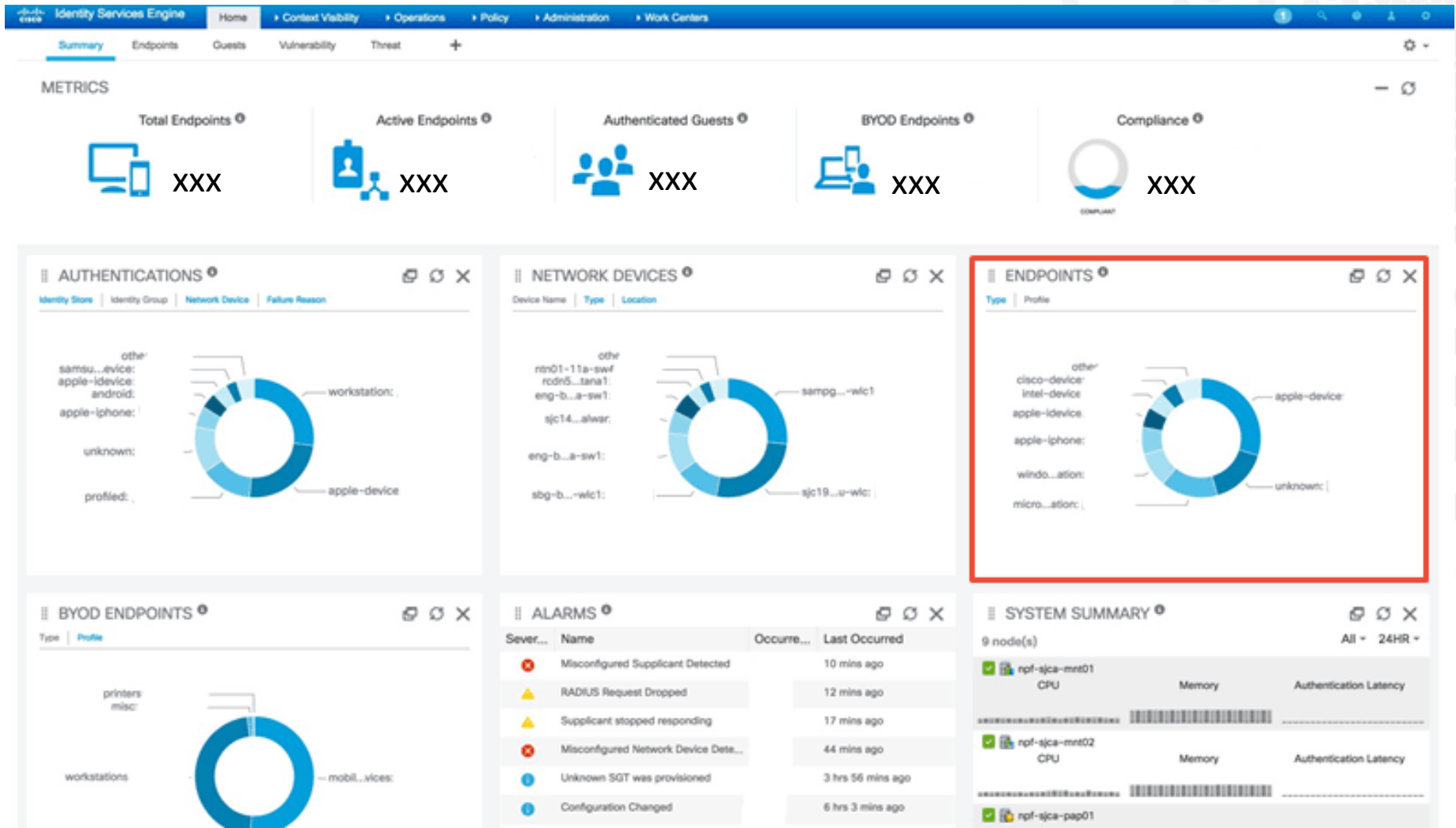


KNOWN

With ISE

NAC Case Goal 4: Ensure Context Visibility

Solution: Profiling, Reporting



NAC Banking Case: Business Benefits



Asset Visibility

See and share user and device details and consolidate security solutions with pxGrid



Access Control

Streamline enterprise network access policy over wired wireless & VPN access



Guest Access

Easily provide visitors secure guest internet access



BYOD & enterprise mobility

Seamlessly classify and securely onboard non-corporate devices



Segmentation

Segment network without VLAN and IP subnet. Simplify role-based access control

About Algosystems

31 Years of solid presence in Greece. Active in **Greece, Europe, Africa** and the **Middle East**



Offices in **Athens**, Greece & **Doha**, Qatar



97 highly specialized, certified and motivated professionals. Dedicated **Project Management Team**, PMP certified



Active in **ICT& Business Software, Industrial Automation & Control, IoT and Metrology** solutions



Strong and dedicated 24*7 customer support NOC/SOC Team



Valuable Gold Partnerships



Gold
Microsoft Partner



Flexible, trustworthy, quick and reliable problem-solvers!



Thank You!



ALGOSYSTEMS
THE PATH FORWARD

Algosystems S.A., 206 Sygrou Avenue, 176 72 Kallithea (Athens)

Tel. (+30) 210 9548000 / E-mail info@algosystems.gr / www.algosystems.gr