# Business Resiliency Through Superior Threat Defense

Firepower 2100 Series/ Cisco Identity Services Engine

Andre Lambertsen, Consulting Systems Engineer
ala@cisco.com

# Cisco Firepower NGFW

## Fully Integrated

- FW / applications / IPS
- Cisco® AMP – network / endpoint
- Analysis and remediation
- Cisco security solutions
- Application-aware DDoS

## Threat Focused

- Networkwide visibility
- Industry-best threat protection
- Known and unknown threats
- Track / contain / recover

## Unified Management

- Across attack continuum
- Manage, control, and investigate
- Automatically prioritize
- Automatically protect

# Firepower 2100

High performance without sacrificing state of the art security

# Business resiliency through superior threat defense – introducing the Firepower 2100 NGFW

**Superior threat defense**
Industry best protection and
rapid breach detection

**Sustained performance**
Threat inspection with
minimal throughput impact

**Simpler management**
Easier management,
lower operating costs

# Choose from four powerful new appliances with industry-best price-performance

## Models 2110 & 2120

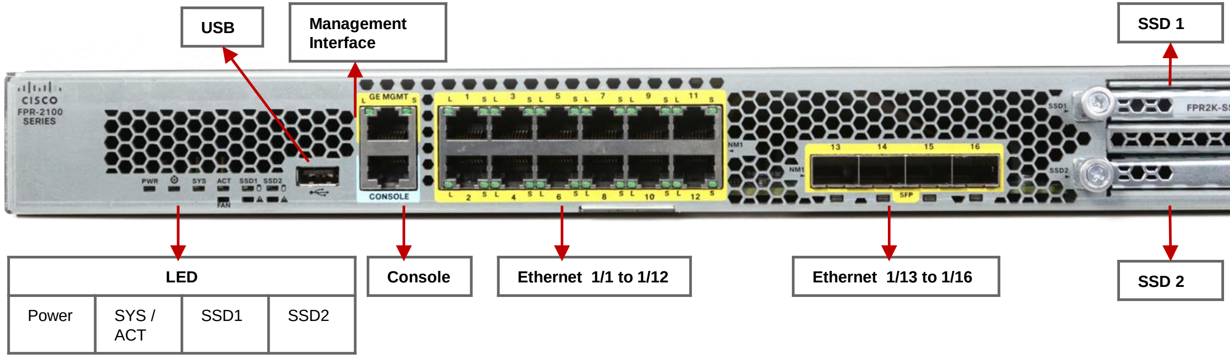
Low-cost, high–performance
1 RU NGFW, Fixed 16-port
1GbE connectivity

## Models 2130 & 2140

High–performance 1 RU NGFW
Network modularity, up to 24-port 1GbE
and up to 12 10GbE connectivity

**Up to 8.5 Gbps FW+AVC+IPS throughput**

# Firepower 2110/2120 Front and Rear View



USB

Management Interface

SSD 1

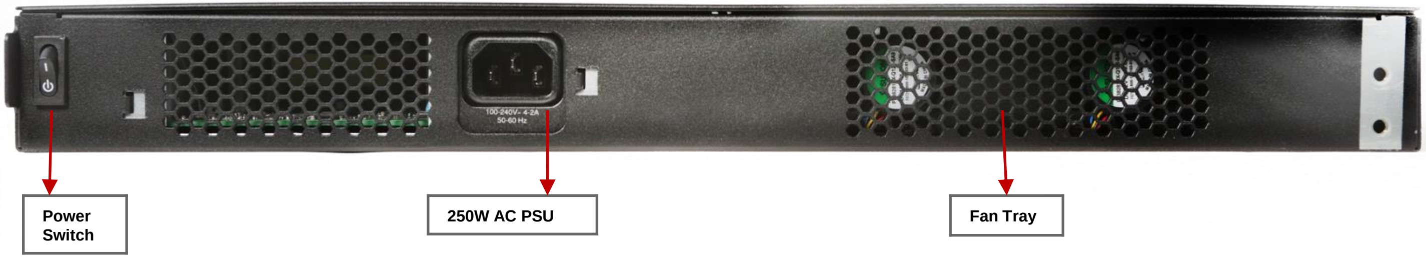
Console

Ethernet 1/1 to 1/12

Ethernet 1/13 to 1/16

SSD 2

| LED | | | |
|---|---|---|---|
| Power | SYS / ACT | SSD1 | SSD2 |

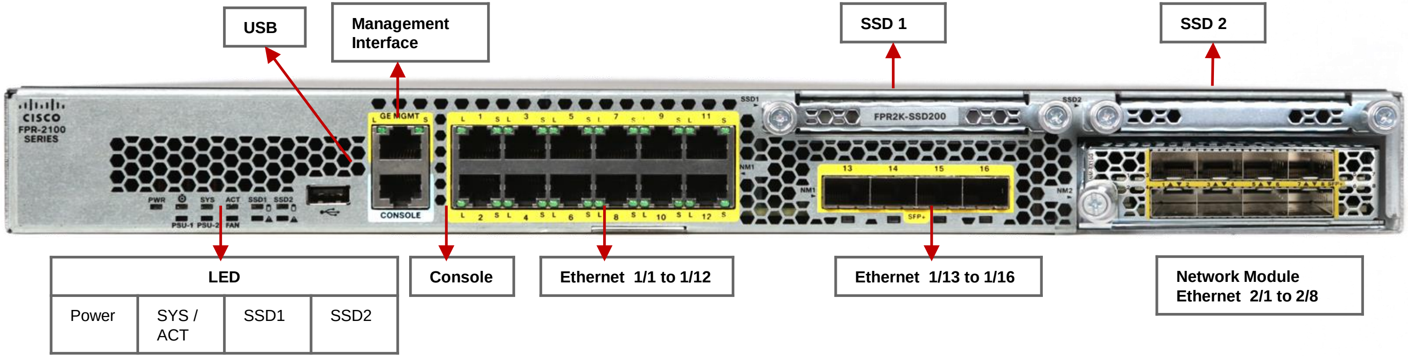


Power Switch

250W AC PSU

Fan Tray

# Firepower 2130/2140 Front and Rear View



USB

Management Interface

SSD 1

SSD 2

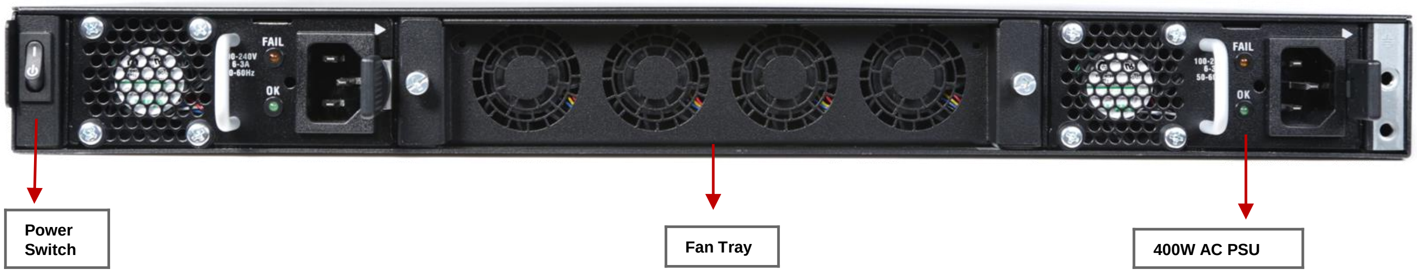
| LED | | | |
|---|---|---|---|
| Power | SYS / ACT | SSD1 | SSD2 |

Console

Ethernet 1/1 to 1/12

Ethernet 1/13 to 1/16

Network Module Ethernet 2/1 to 2/8



Power Switch

Fan Tray

400W AC PSU

# Get leading security effectiveness

## Superior threat defense

## Firepower 2100 series NGFWs deliver:

### Advanced threat detection

Exclusive integration of Firepower NGIPS and AMP

Ranked #1 in breach detection by NSS Labs in  2016

Superior time to detection of advanced threats

### Optimized architecture

Unique dual multi-core CPUs sustains threat inspection performance as services are added

Future-proofs your investment

### Superior price-performance

Less than 50% of the cost per-protected Mbps vs. competitors

200% greater throughput vs. competitors when IPS is enabled

# Firepower 2100 Series Models

| Description | FPR 2110 | FPR 2120 | FPR 2130 | FPR 2140 |
|---|---|---|---|---|
| Chassis & I/O | 1RU<br>12 Fixed RJ-45 (1G)<br>4 x SFP (1G) | 1RU<br>12 Fixed RJ-45 (1G)<br>4 x SFP (1G) | 1RU<br>12 Fixed RJ-45 (1G)<br>4 x SFP+ (10G)<br>1 x NM Slot | 1RU,<br>12 Fixed RJ-45 (1G)<br>4 x SFP+ (10G)<br>1 x NM Slot |
| CPU x86 | 4-Core | 6-Core | 8-Core | 16-Core |
| CPU DDR4 DRAM | 16GB | 16GB | 32GB | 64GB |
| NPU Octeon | 6-Core | 8-Core | 12-Core | 16-Core |
| NPU DDR4 DRAM | 8 GB | 8 GB | 16 GB | 16 GB |
| SSD | 1 x 100GB Default<br>2nd Optional SSD for MSP 800GB | | 1 x 200GB Default<br>2nd Optional SSD for MSP 800GB | |
| PSU – Default/Options | 1x 250W Fixed AC PSU | 1x 250W Fixed AC PSU | 1x 400W AC default<br>2x AC, 1x or 2x DC options | 2x 400W AC default<br>2x 350W DC options |

# Firepower 2100 Series Performance

| | FPR 2110 | FPR 2120 | FPR 2130 | FPR 2140 |
|---|---|---|---|---|
| Throughput FW + AVC | 1.9 Gbps | 3 Gbps | 4.75 Gbps | 8.5 Gbps |
| Throughput FW + AVC + NGIPS | 1.9 Gbps | 3 Gbps | 4.75 Gbps | 8.5 Gbps |
| Maximum concurrent sessions, with AVC | 1 M | 1.2 M | 2 M | 3.5 M |
| Maximum new connections per second, with AVC | 12000 | 16000 | 24000 | 40000 |

# Firepower 2100, 4100, 9300 Snapshot

| Features | FPR 2100 | FPR 4100 | FPR 9300 |
|---|---|---|---|
| Throughput range Firewall + AVC | 2 to 8 Gbps | 12 to 30 Gbps | 30 to 54 Gbps |
| Throughput range Firewall + AVC+IPS | 2 to 8 Gbps | 10 to 24 Gbps | 24 to 53 Gbps |
| Interface Speed | 1/10 Gbps | 1/10/40 Gbps | 1/10/ 40/100 Gbps |
| Rack Unit size | 1 RU | 1 RU | 3 RU |
| Clustering | Roadmap | Yes (6.2) | Yes (6.2) |
| Other Apps | No | Yes (Radware DDoS) | Yes (Radware DDoS) |
| Chassis Manager | Unified With FMC / FDM | Yes | Yes |

# Enable threat defense without compromising throughput

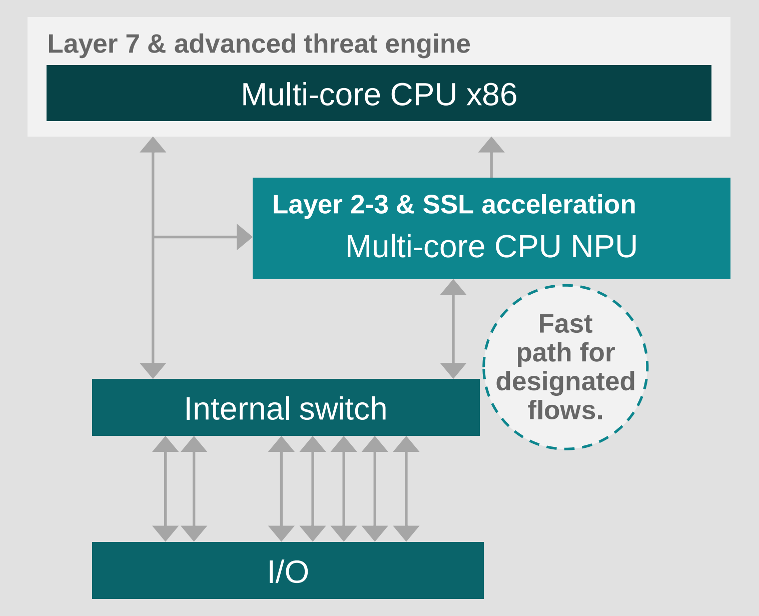
## Dual Multi-Core CPU architecture enables:

**Sustained throughput performance** when threat functions are enabled vs. competing designs

**Flexibility and future-proofing** vs. ASIC-based designs that degrade as new defenses and functions are added

**Prefix filtering with fast path** verifies flows that do not require threat inspection, further enhancing performance

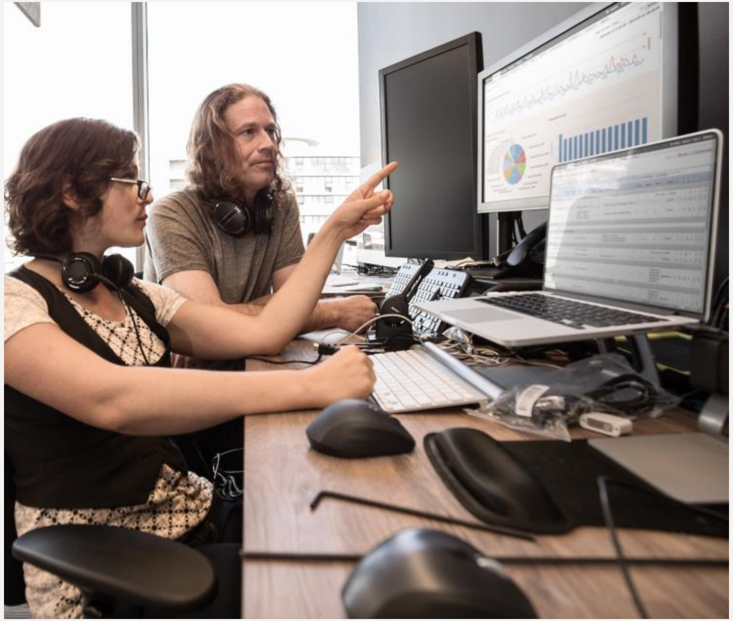
## Sustained performance



Layer 7 & advanced threat engine
Multi-core CPU x86
Layer 2-3 & SSL acceleration
Multi-core CPU NPU
Fast path for designated flows.
Internal switch
I/O

# Improve IT efficiency with streamlined management

## Simpler management



## Firepower 2100 series NGFWs deliver:

### Scalable design

50% increased management capacity (FMC)

Expanded file storage

Network modularity

### Easy setup

Quick setup wizard (FDM)

Low-touch provisioning

Templates for multi-site provisioning

### Faster time-to-value

Cloud-based policy delivery (CDO)

Automated executive summary

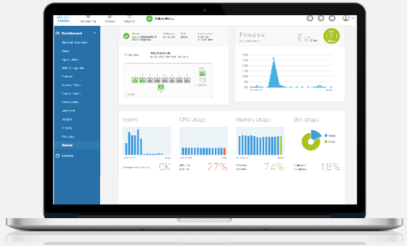
Demonstrate value more easily

# Management Options

# Cisco offers management designed for the user

## On-box, web-based management

### Firepower Device Manager



Consolidated management

Enhanced control

Easy set-up

## Centralized management for multiple devices

### Firepower Management Center

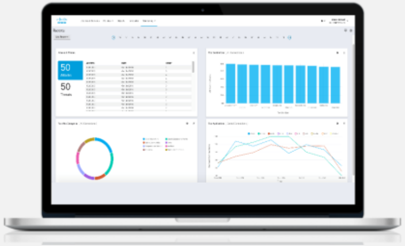
Unified insight

Scalable management

Intelligent automation

## Cloud-based policy orchestration for multiple sites

### Cisco Defense Orchestrator



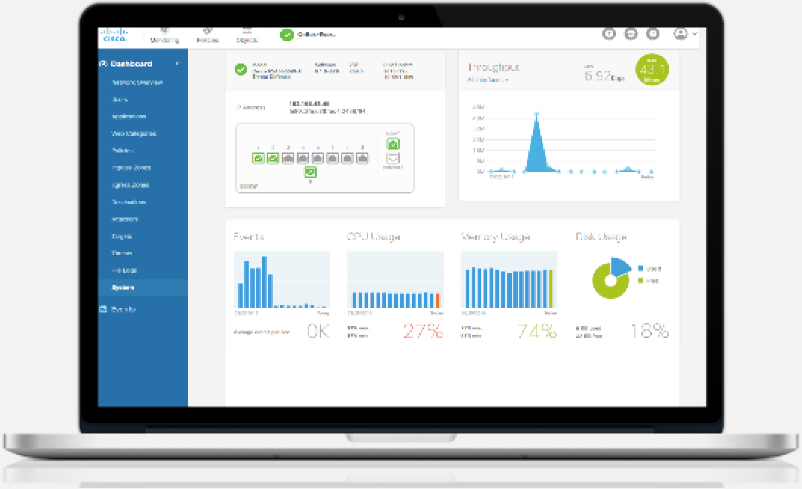
Simple interface

Efficient management

Streamlined user experience

# Enable easy on-box management of common security and policy tasks

## Firepower Device Manager



## Improved functionality

### Consolidated management

Manage basic firewall capabilities and Firepower solutions such as NGIPS, AMP, and more with a unified interface

### Enhanced control

Investigate incidents, prioritize responses, and establish role-based access control to increase your network security

### Easy set-up

Easily set up security, control access and set policies, and more with a simple on-box interface

# Centralize security administration and automation of multi-device deployments

## Firepower Management Center

## Same trusted functionality

**Unified insight**

Gain network to endpoint visibility, with deep insight into the network firewall, applications, and threats – all in one place

**Scalable management**

Utilize policy inheritance and centralized role-based management to easily expand

**Intelligent automation**

Leverage intelligent rule recommendations, remediation APIs, and impact assessments to minimize management burden

## New integration features

Threat Grid

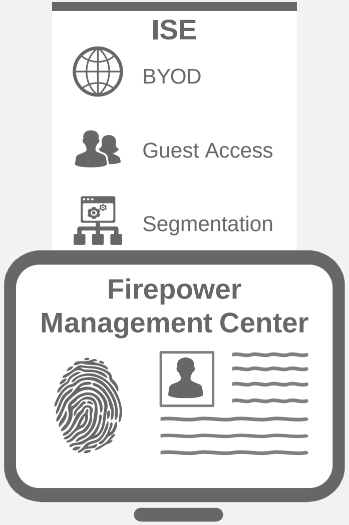
ISE

AMP for Endpoints

# Integrations

# Ensure compliance before granting access

## Identity Services Engine (ISE)



**ISE**

BYOD

Guest Access

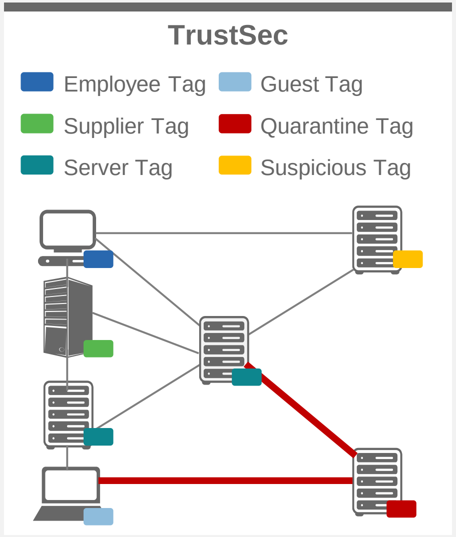
Segmentation

**Firepower Management Center**

**pxGrid**

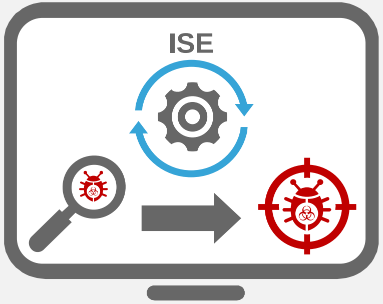
**Propagate**

- User Context
- Device context
- Access policies



**TrustSec**

🟦 Employee Tag
🟦 Guest Tag
🟩 Supplier Tag
🟥 Quarantine Tag
🟦 Server Tag
🟨 Suspicious Tag



**ISE**

**Policy automation**

Set access control policies

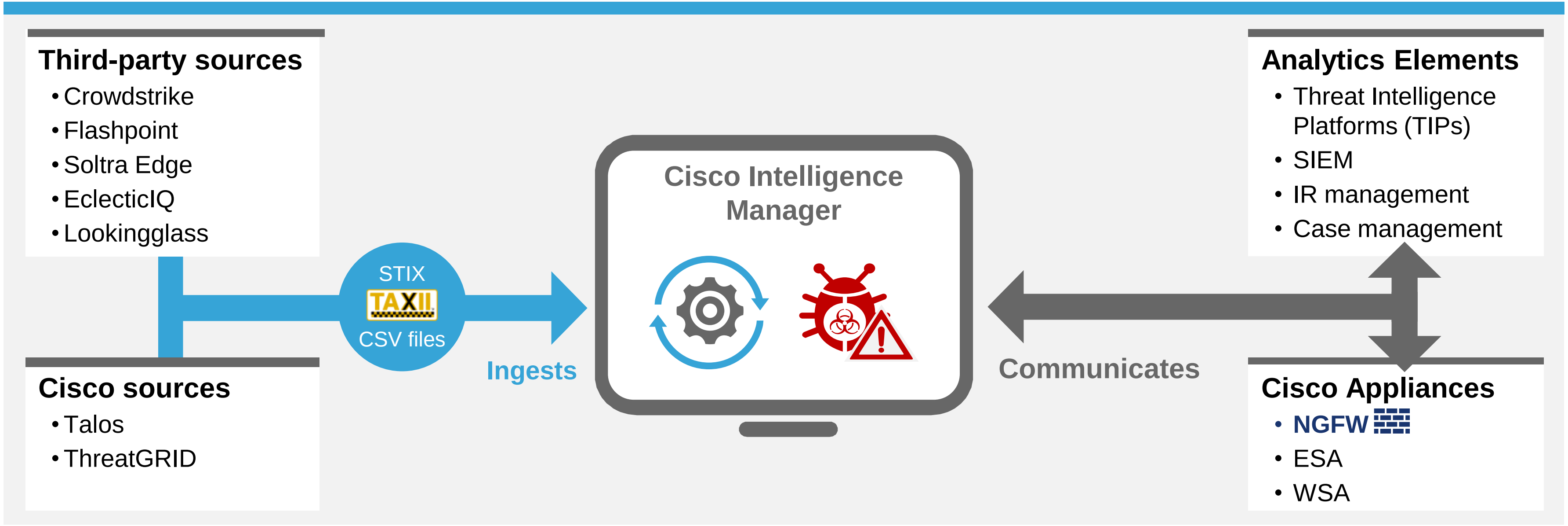
Propagate rules and context

Establish a secure network

Remediate breaches automatically

# Integrate third-party security intelligence

## Cisco Intelligence Manager



### Third-party sources

- Crowdstrike
- Flashpoint
- Soltra Edge
- EclecticIQ
- Lookingglass

### Cisco sources

- Talos
- ThreatGRID

### Cisco Intelligence Manager

### Analytics Elements

- Threat Intelligence Platforms (TIPs)
- SIEM
- IR management
- Case management

### Cisco Appliances

- **NGFW**
- ESA
- WSA

Analyze security intelligence

Correlate observations

Generate rich incident reports

Refine security posture

# Pricing

# Pricing

| | FPR 2110 | FPR 2120 | FPR 2130 | FPR2140 |
|---|---|---|---|---|
| HW List Price | $10,995 | $19,995 | $29,995 | $64,995 |
| TMC 3Y List Price | $13,460 | $24,475 | $36,715 | $79,555 |
| T/M/C 3Y List Price | $5,280 | $9,600 | $14,400 | $31,200 |

*Note that our 3Y pricing is approximately 2.4 times 1 year price.

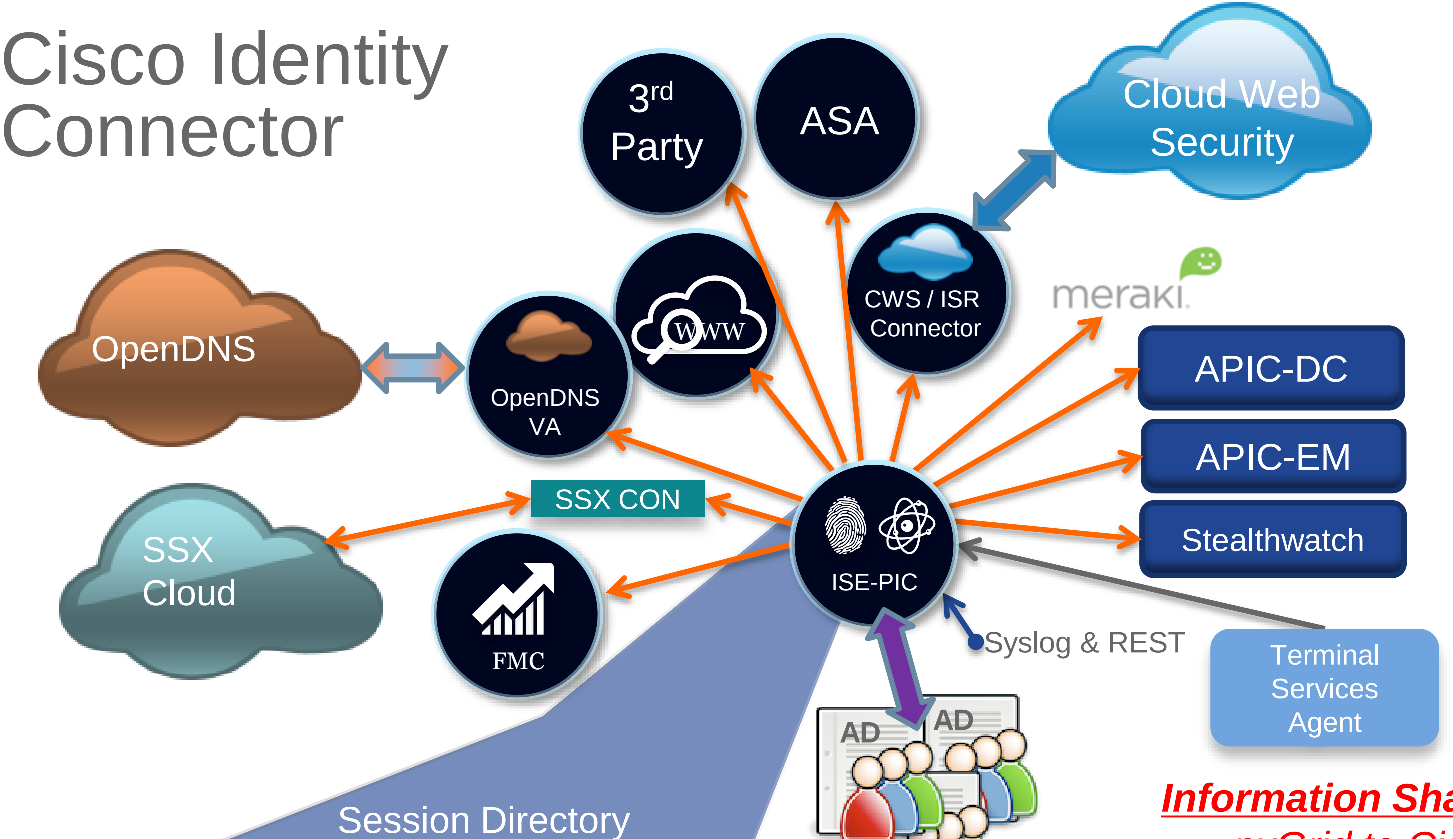
# Identity Services Engine 2.2

# ISE 2.2 at a glance

- ISE - Passive Identity Connector
- Next Generation Posture Phase 1
- Threat Centric NAC Phase 2
- ACS Migration Phase 3
- Enhanced Visibility

- Anomalous Behavior Detection
- Easy Wireless Setup (Project “Xenia”)
- Guest Backwards Compatibility Features
- Multiple TrustSec Matrices
- TrustSec-ACI Integration Phase 2

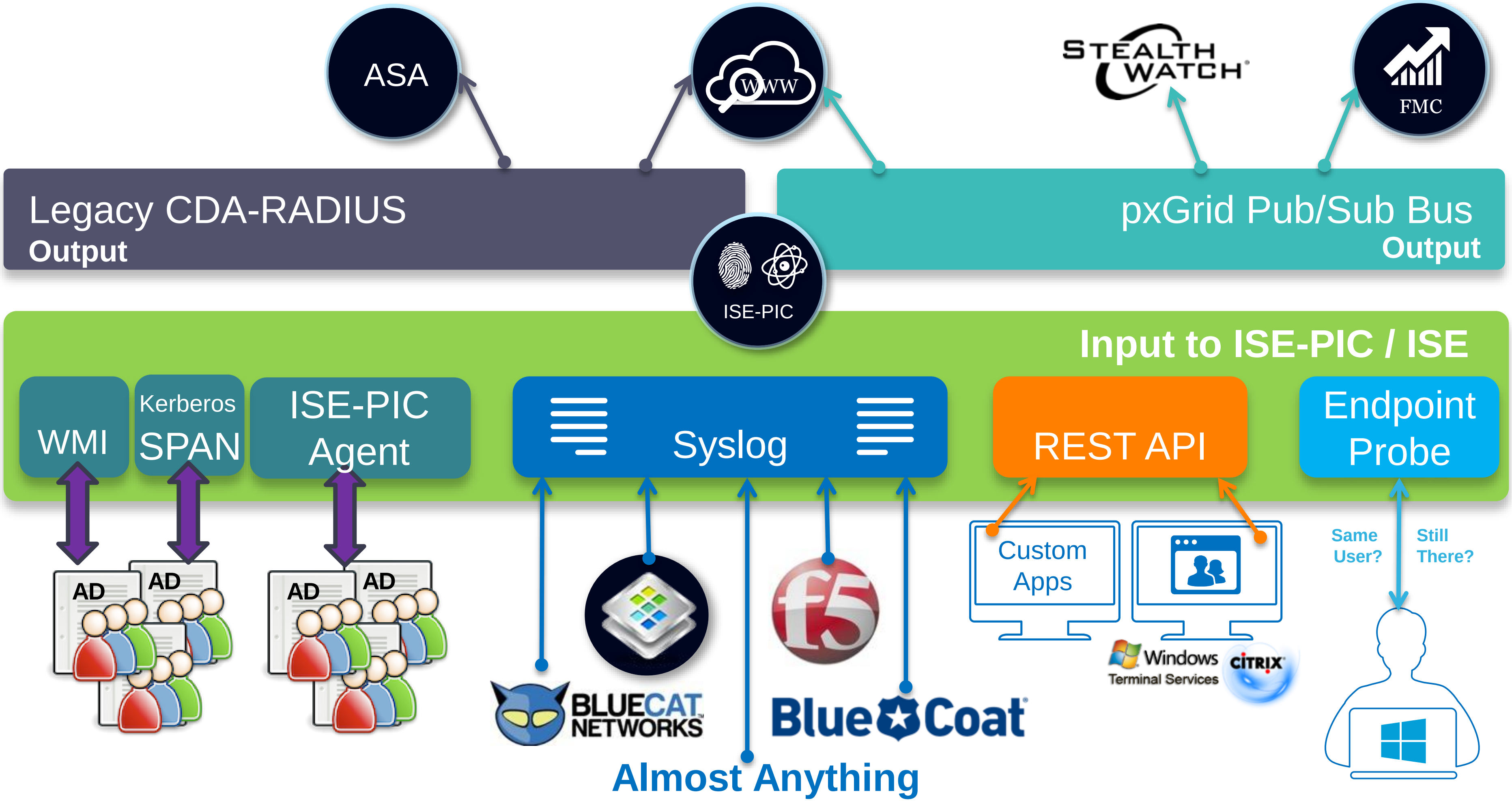
# Cisco Identity Connector



| Context Attributes Needed | | |
|---|---|---|
| Username | AD Group Membership (?) | MSE Location |
| AD Domain Name | Endpoint Profile | NDG Location |
| Assigned SGT | ISE ID Groups (User / Endpoint) | Express Raw EPG? |
| Users' DN | AD Attributes | NSX Group Scraping? |
| Certificate Attribs & Template ID (may have to allow SmartSearch Editing) | | MDM Management Info (Which MDM & State) |

***Information Sharing:***

- *pxGrid to Cisco only*
- *RADIUS for CDA compatibility*
- *No NAD communication*



Legacy CDA-RADIUS
**Output**

pxGrid Pub/Sub Bus
**Output**

ISE-PIC

**Input to ISE-PIC / ISE**

WMI

Kerberos
SPAN

ISE-PIC
Agent

Syslog

REST API

Endpoint
Probe

Custom
Apps

Same
User?

Still
There?

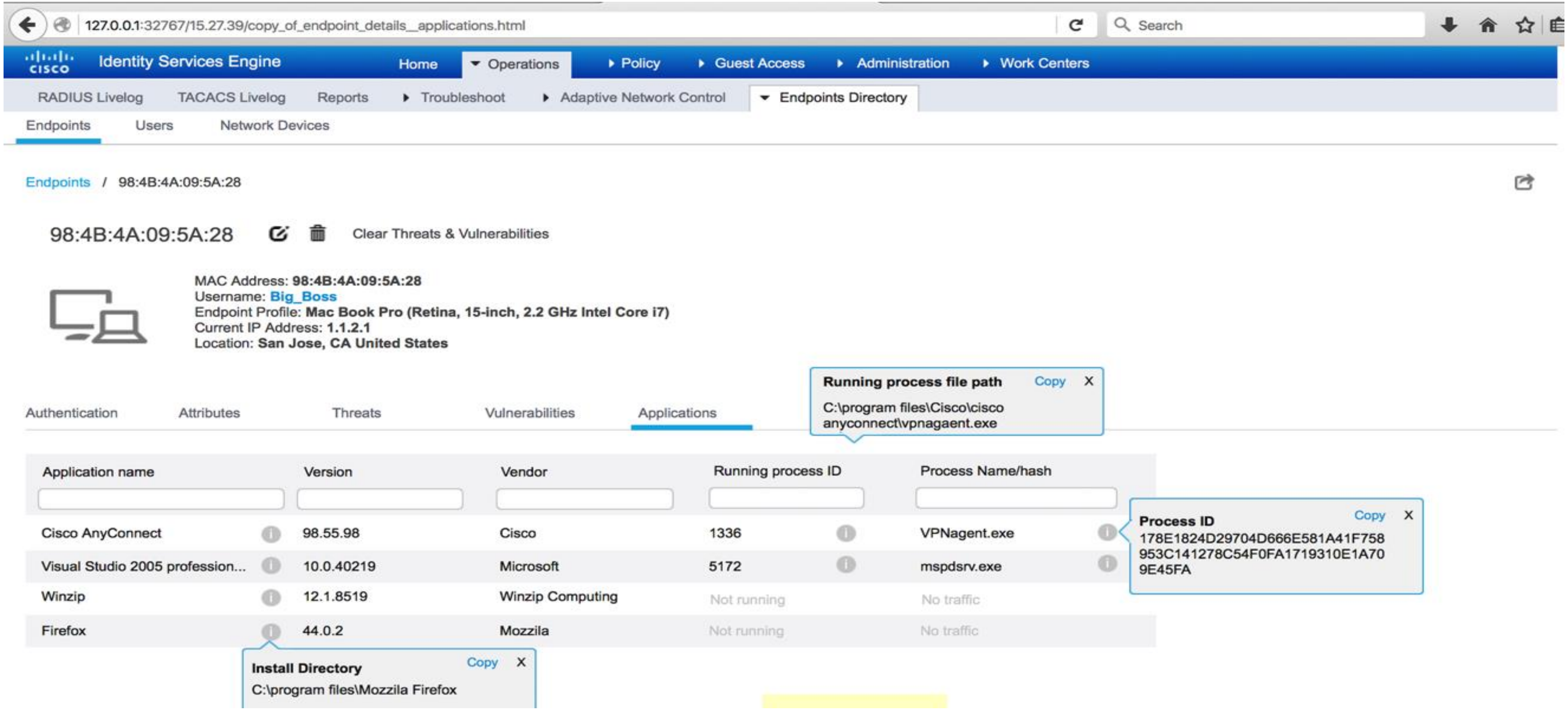
**Almost Anything**

# ISE PIC at a Glance

- Single ID Solution for ALL Cisco Security Portfolio
  - Best of All Existing Solutions
  - True Single Source of ID
    - No Longer Need Separate Connection to AD, LDAP, etc.
- Very Low Cost
- Passive Identity Only
  - No Authorization. No Policies.

- New Features & Sources
  - Agents, WMI, Syslog, REST
  - Remotely Check with Endpoints
    - Is Endpoint Still on Network?
    - Is User Still Logged In?
- Simple to Install and Use
- Scale to 100’s of DC’s

# App Inventory



98:4B:4A:09:5A:28

MAC Address: **98:4B:4A:09:5A:28**
Username: **Big_Boss**
Endpoint Profile: **Mac Book Pro (Retina, 15-inch, 2.2 GHz Intel Core i7)**
Current IP Address: **1.1.2.1**
Location: **San Jose, CA United States**

**Running process file path**
C:\program files\Cisco\cisco anyconnect\vpnagent.exe

| Application name | Version | Vendor | Running process ID | Process Name/hash |
|---|---|---|---|---|
| Cisco AnyConnect | 98.55.98 | Cisco | 1336 | VPNagent.exe |
| Visual Studio 2005 profession... | 10.0.40219 | Microsoft | 5172 | mspdsrv.exe |
| Winzip | 12.1.8519 | Winzip Computing | Not running | No traffic |
| Firefox | 44.0.2 | Mozzila | Not running | No traffic |

**Process ID**
178E1824D29704D666E581A41F758953C141278C54F0FA1719310E1A709E45FA

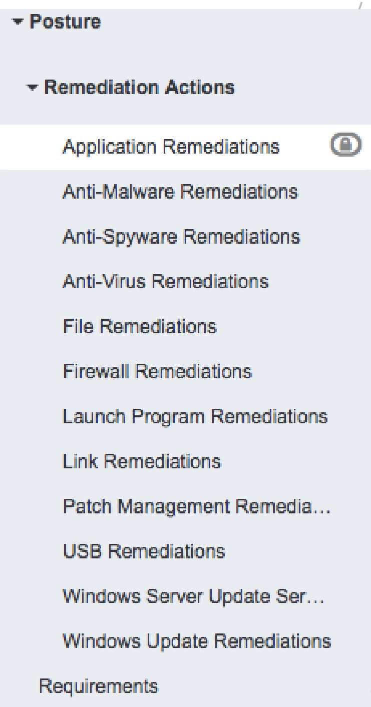
**Install Directory**
C:\program files\Mozzila Firefox

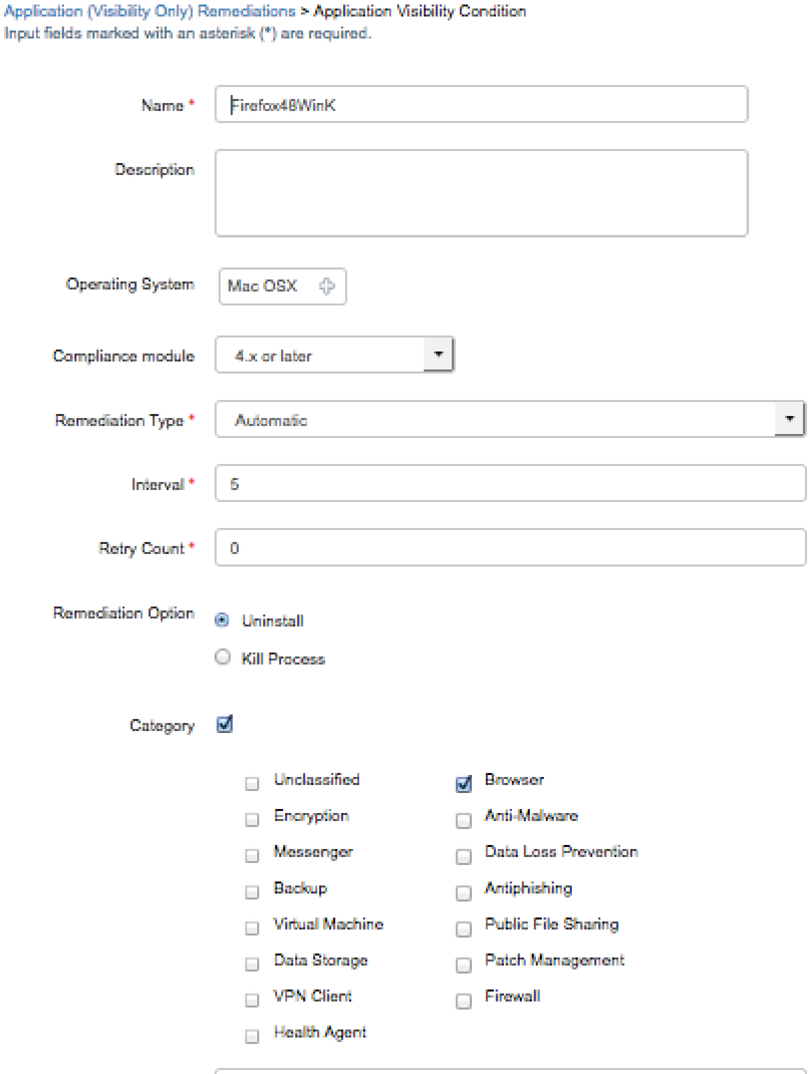
# Application Enforcement

If an Admin can create a requirement that if a malicious app is installed/running, then uninstall/terminate all processes of application A

The enforcement is at

- Initial posture
- PRA time





Application (Visibility Only) Remediations > Application Visibility Condition

Input fields marked with an asterisk (*) are required.

Name * Firefox48WinK

Description

Operating System Mac OSX

Compliance module 4.x or later

Remediation Type * Automatic

Interval * 5

Retry Count * 0

Remediation Option
● Uninstall
○ Kill Process

Category ☑

☐ Unclassified
☐ Encryption
☐ Messenger
☐ Backup
☐ Virtual Machine
☐ Data Storage
☐ VPN Client
☐ Health Agent

☑ Browser
☐ Anti-Malware
☐ Data Loss Prevention
☐ Antiphishing
☐ Public File Sharing
☐ Patch Management
☐ Firewall

# Threat Centric NAC

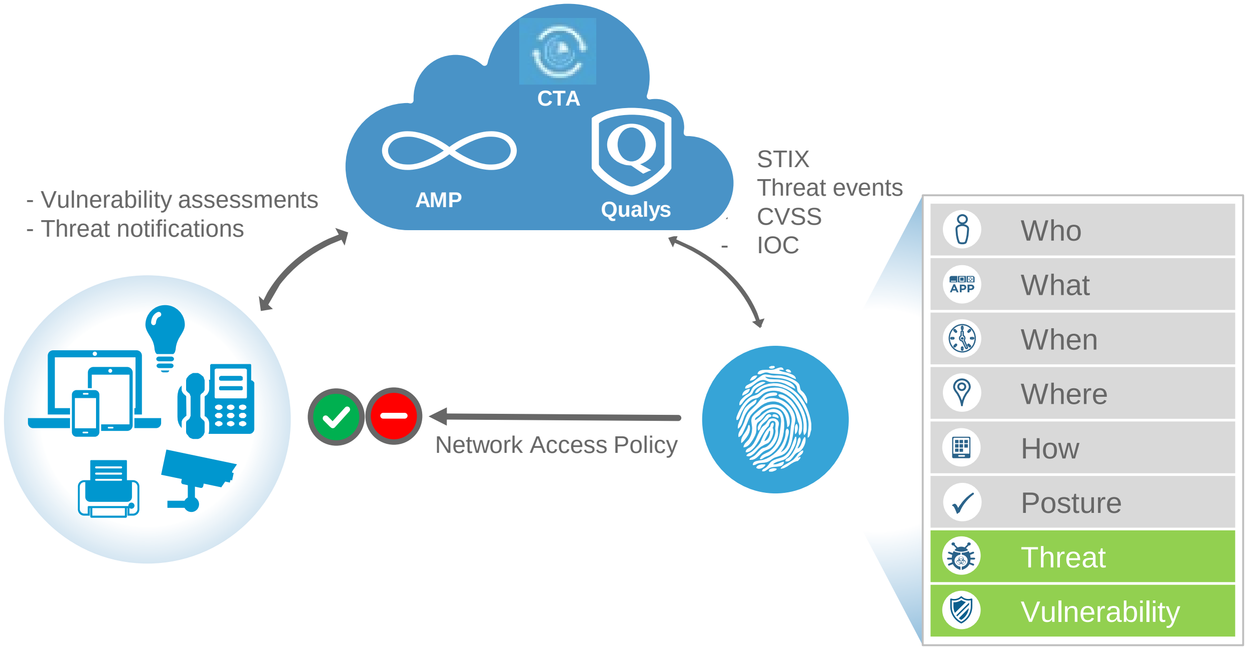
Cisco ISE protects your network from data breaches by segmenting compromised and vulnerable endpoints for remediation.

**Compliments Posture**
Vulnerability data tells endpoint's posture from the outside

**Expanded control**
driven by threat intelligence and vulnerability assessment data

**Faster response**
with automated, real-time policy updates based on vulnerability data and threat metrics

## Create ISE authorization policies based on the threat and vulnerability attributes



CTA

AMP

Qualys

- Vulnerability assessments
- Threat notifications

STIX
Threat events
CVSS
- IOC

Network Access Policy

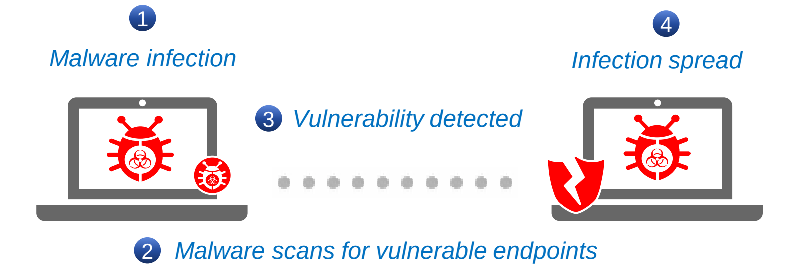
| |
|---|
| Who |
| What |
| When |
| Where |
| How |
| Posture |
| Threat |
| Vulnerability |

STIX over TAXII | Common Vulnerability Scoring System (CVSS) | Indicators of Compromise (IOC)

# Threat Centric NAC explained

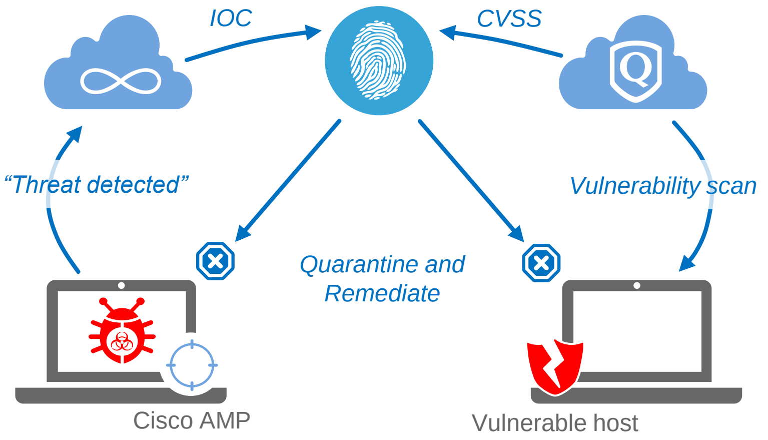
## Reduce vulnerabilities, contain threats

### Problem



Compromised endpoints spread malware by exploiting known vulnerabilities in the network

### Solution

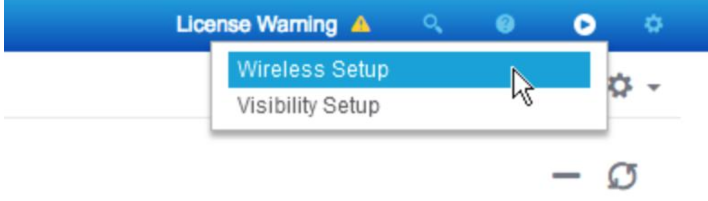


Flag compromised and vulnerable hosts and limit access to remediation Segment

Most endpoint AMP deployed in 'visibility only' mode

Common Vulnerability Scoring System (CVSS) | Indicators of Compromise (IOC) | Advanced Malware Protection (AMP)

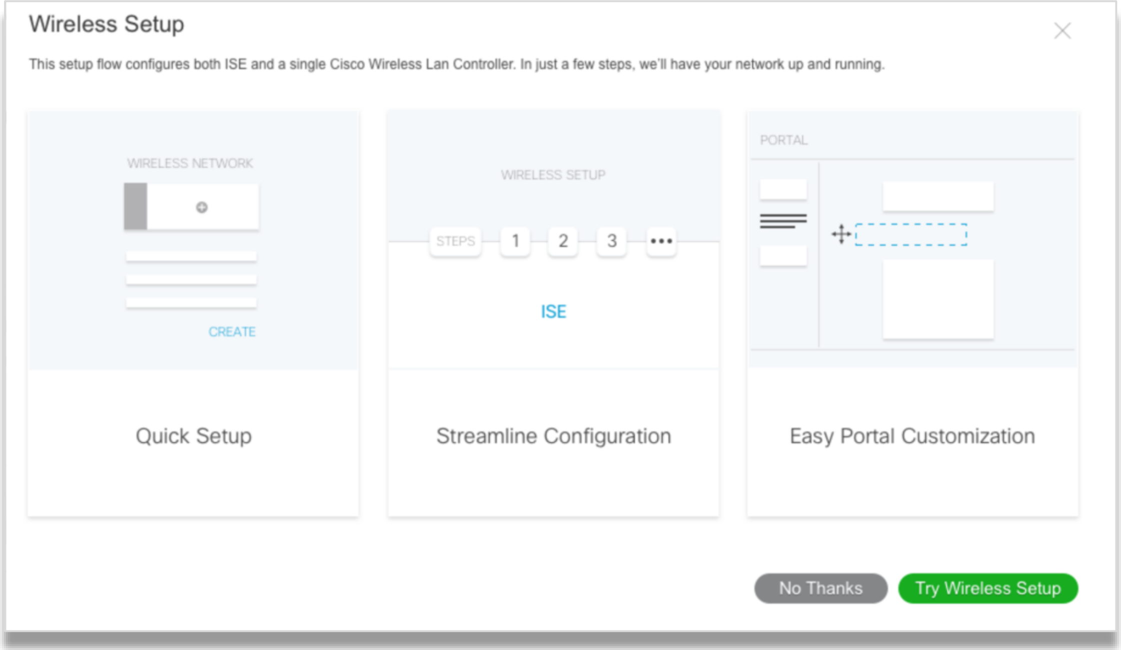
# Easy Wireless Setup
## Flow Wizard



Simple unified management for wireless networks

Enterprise (802.1X), Guest and BYOD Use cases

Easy portal creation and customization


Wireless Setup

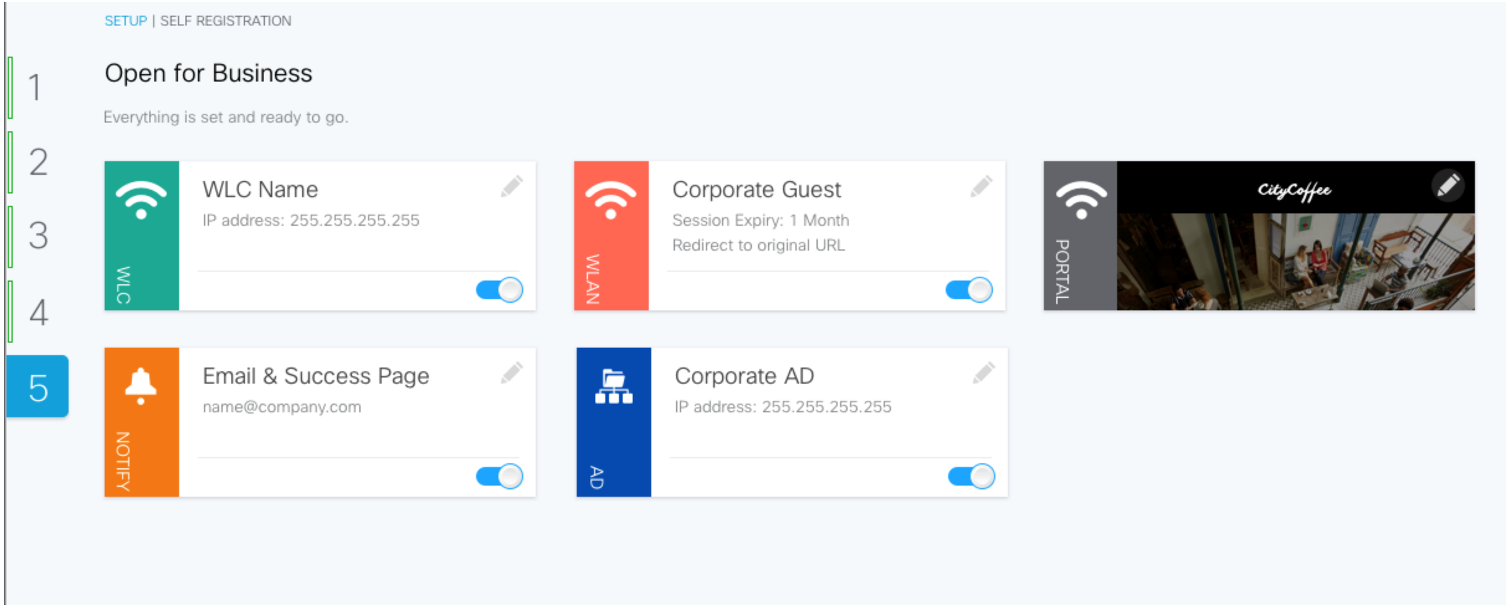
This setup flow configures both ISE and a single Cisco Wireless Lan Controller. In just a few steps, we'll have your network up and running.

Quick Setup

Streamline Configuration

Easy Portal Customization

# Configure ISE & WLC in a Single Stroke



SETUP | SELF REGISTRATION

Open for Business

Everything is set and ready to go.

WLC Name
IP address: 255.255.255.255

Corporate Guest
Session Expiry: 1 Month
Redirect to original URL

Email & Success Page
name@company.com

Corporate AD
IP address: 255.255.255.255

# Summary

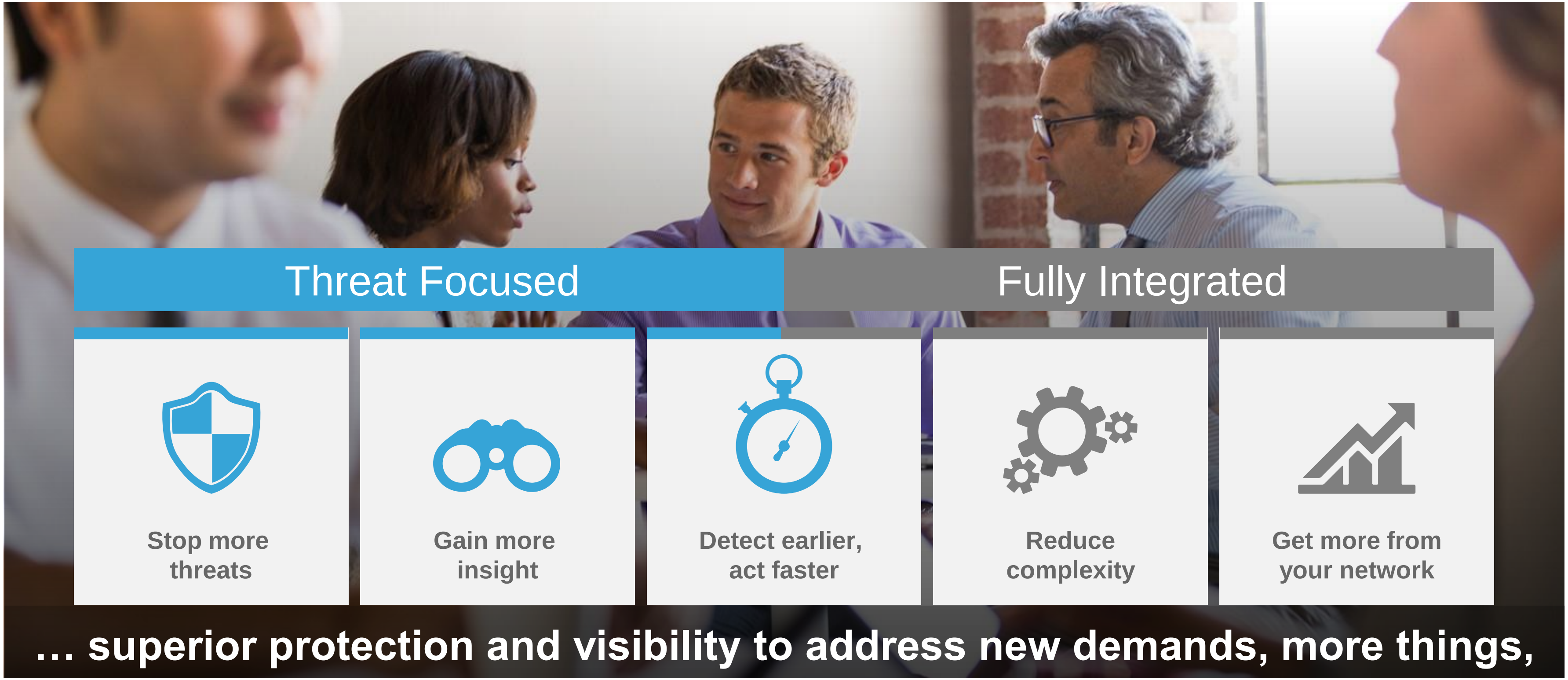
# Firepower 2100

- 1RU Mid-Range Security Platform
  - High Performance
  - High Port Density
  - 10G Support
- Purpose-Built Hardware for Cisco NGFW
- Versatile Deployment
- Management options
  - On-box
  - Off-Box
  - Cloud

# ISE 2.2

- ISE - Passive Identity Connector
  - Single source for Identity
- New and enhanced Posture features
  - Application visibility and enforcement
- Threat Centric NAC
- Easy Wireless Setup
- Enhanced Visibility

# Only Cisco delivers…



Threat Focused

Fully Integrated

Stop more threats

Gain more insight

Detect earlier, act faster

Reduce complexity

Get more from your network

… superior protection and visibility to address new demands, more things,