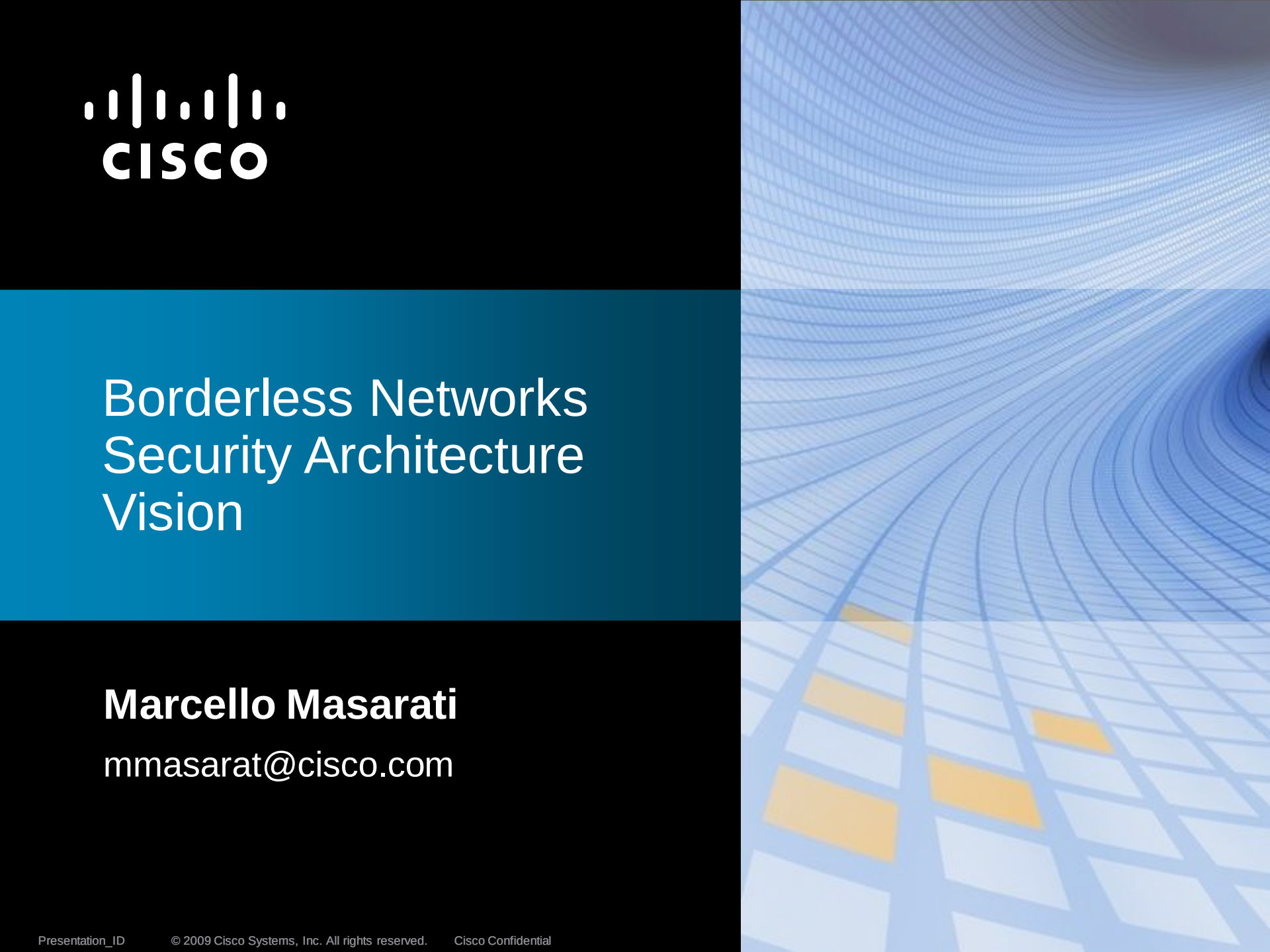
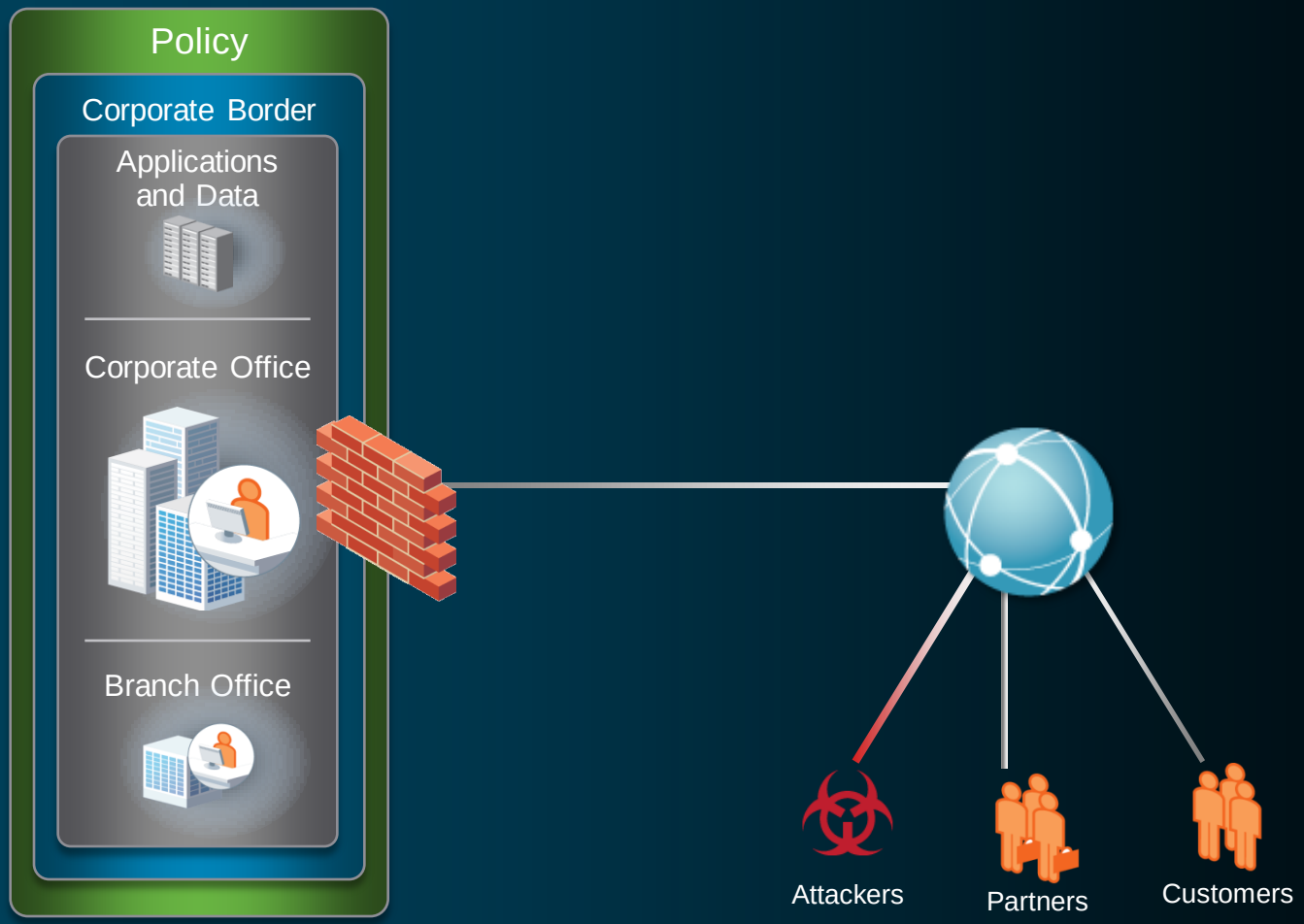


Borderless Networks Security Architecture Vision

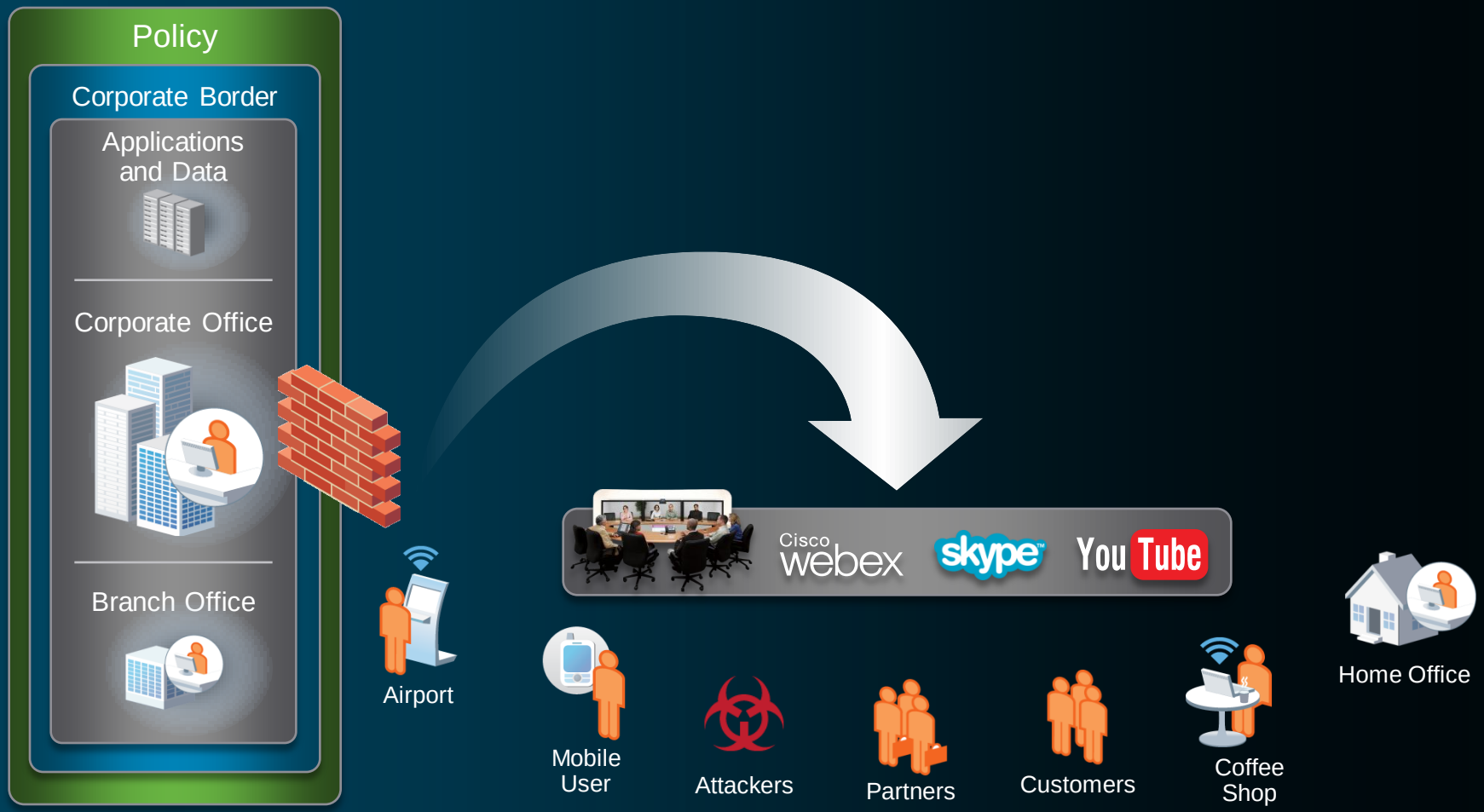
Marcello Masarati

mmasarat@cisco.com

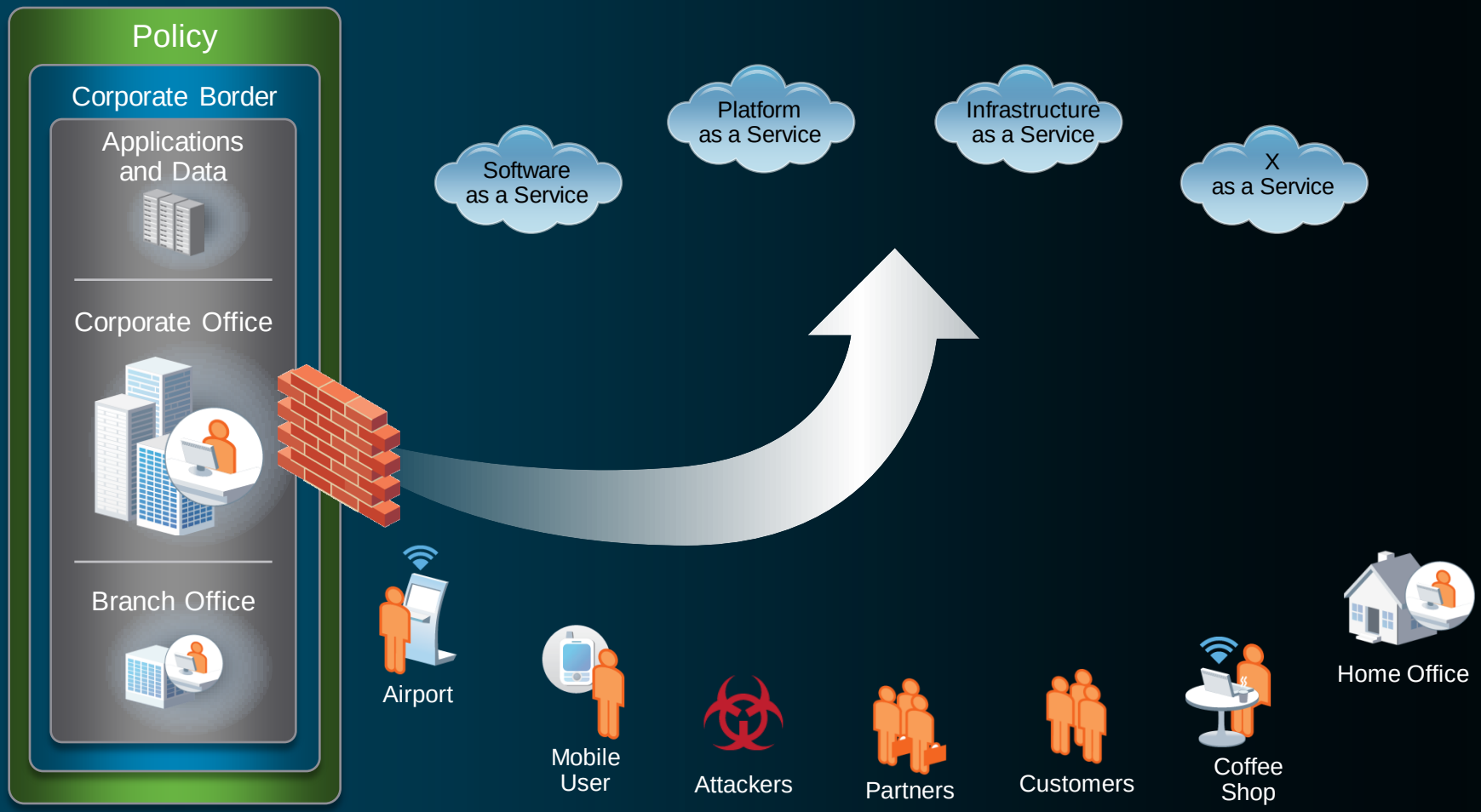
Traditional Corporate Border



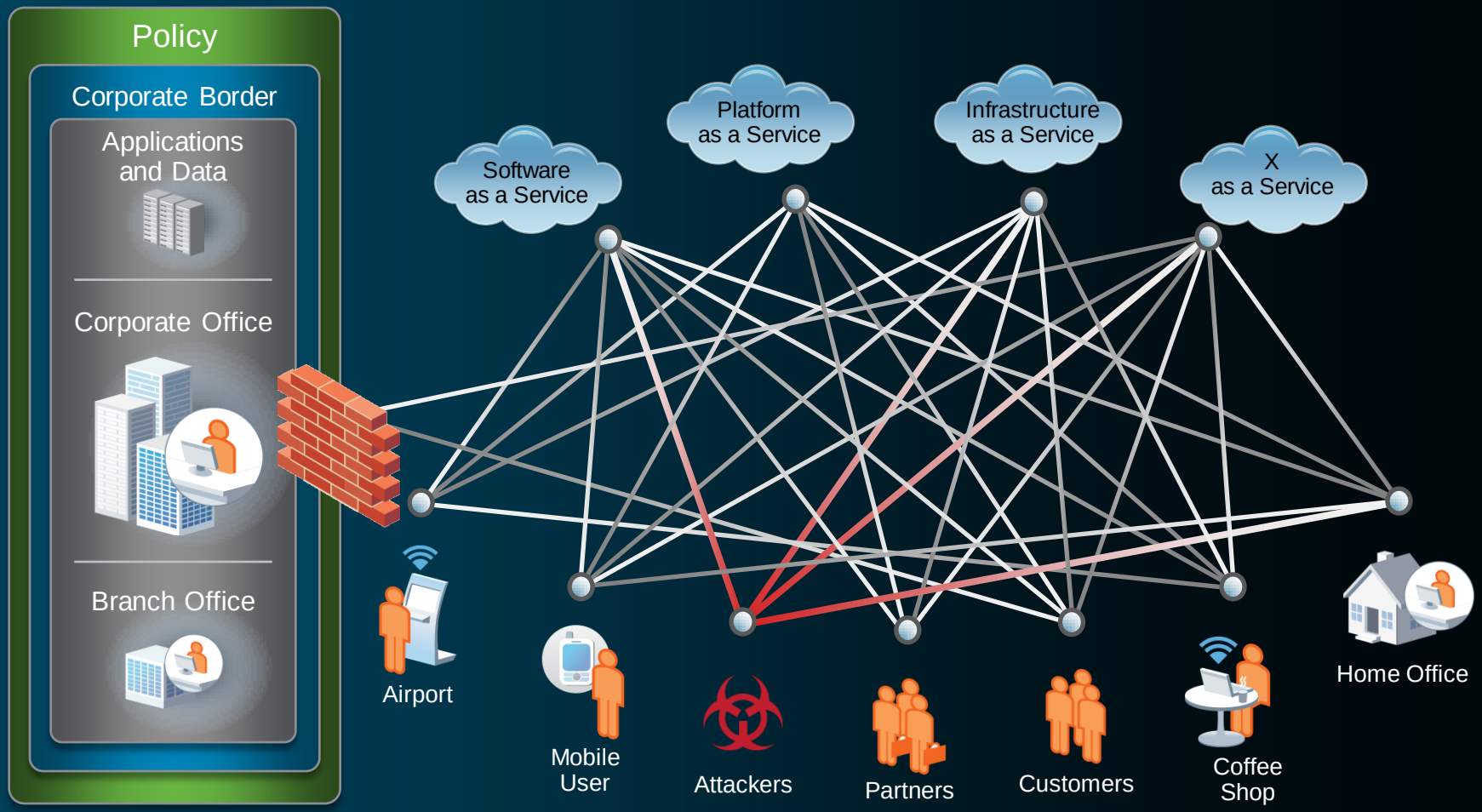
Mobility and Collaboration Is Dissolving the Internet Border



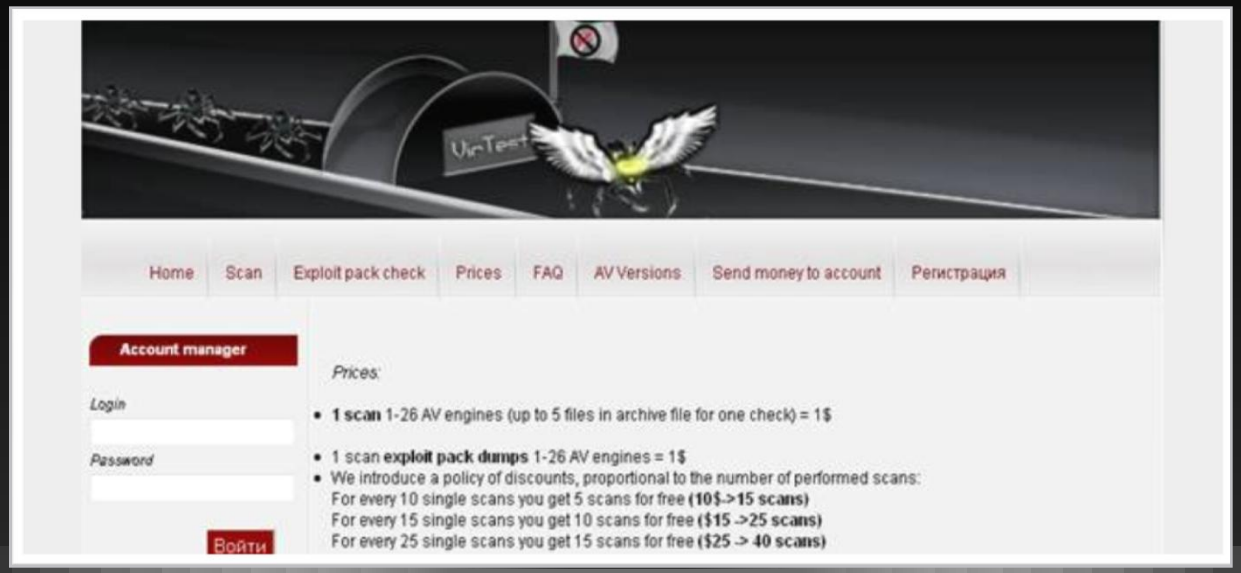
Cloud Computing Is Dissolving the Data Center Border



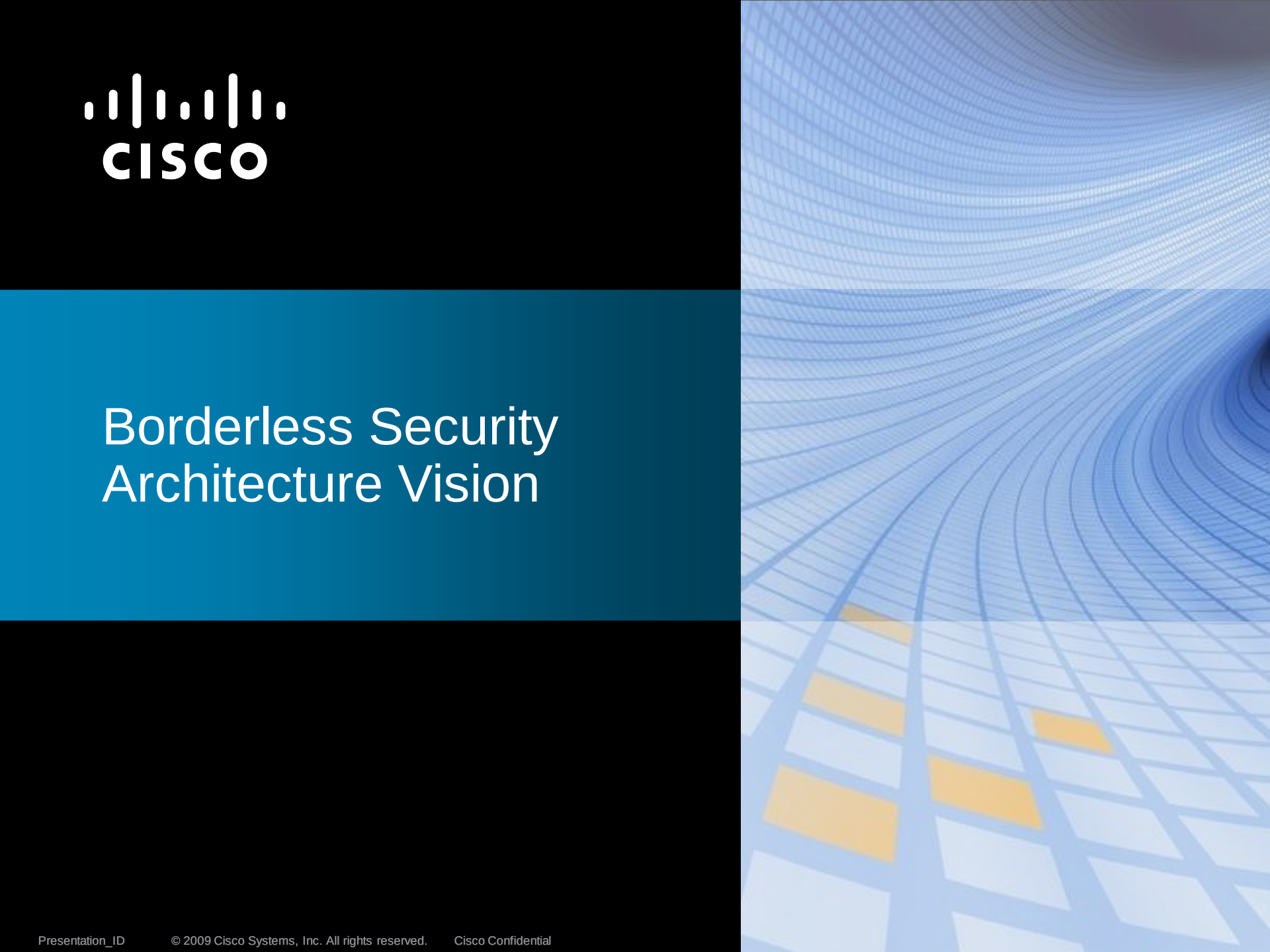
Customers Want Business Without Borders



Criminal SaaS Offerings Expand

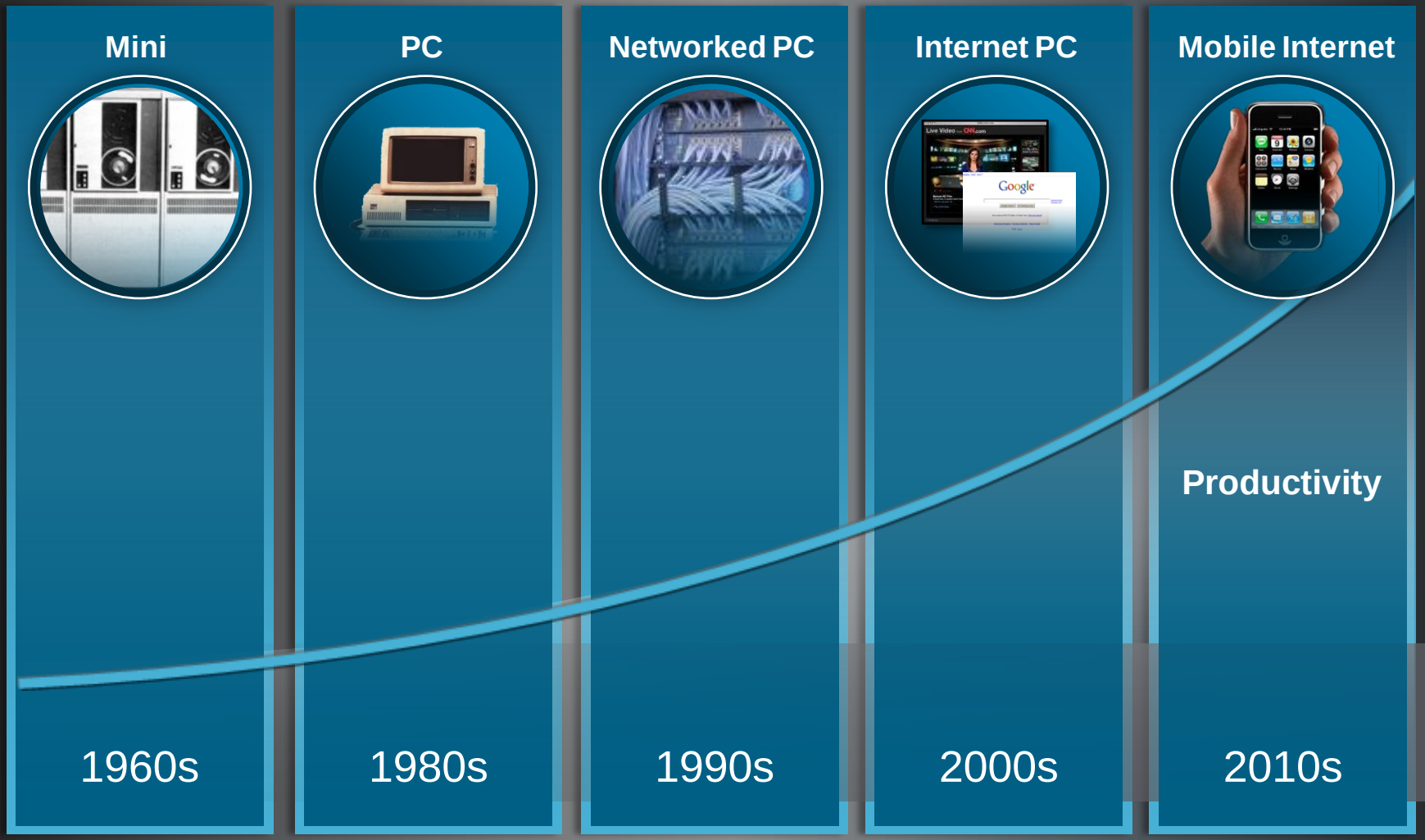


Service dedicated to checking if a malware executable is detectable by AV engines



Borderless Security Architecture Vision

Mobility: The Next Computing Cycle



Borderless Experiences

Always Connected—Wired/Wireless Access Anytime, Anywhere from Any Device

New Video-based Experiences

Context-Based Services: Equipment Tracking, Trigger Digital Signage or Voice Services

Optimized Energy Use, Automated Office Control

The New Borderless Organization

Anyone

Employee, Partner,
Customer Communities

Person to Person,
Person to Device,
Device to Device

Anything

Anywhere

Work,
Home, On the Go…

Securely, Reliably and Seamlessly

Always Works,
Instant Access,
Instant Response

Anytime

Borderless Networks

Architecture for Agile Delivery of the Borderless Experience

Borderless Management and Policy

Borderless End-Point/User Services

Mobility | **Workplace Experience** | **Video**

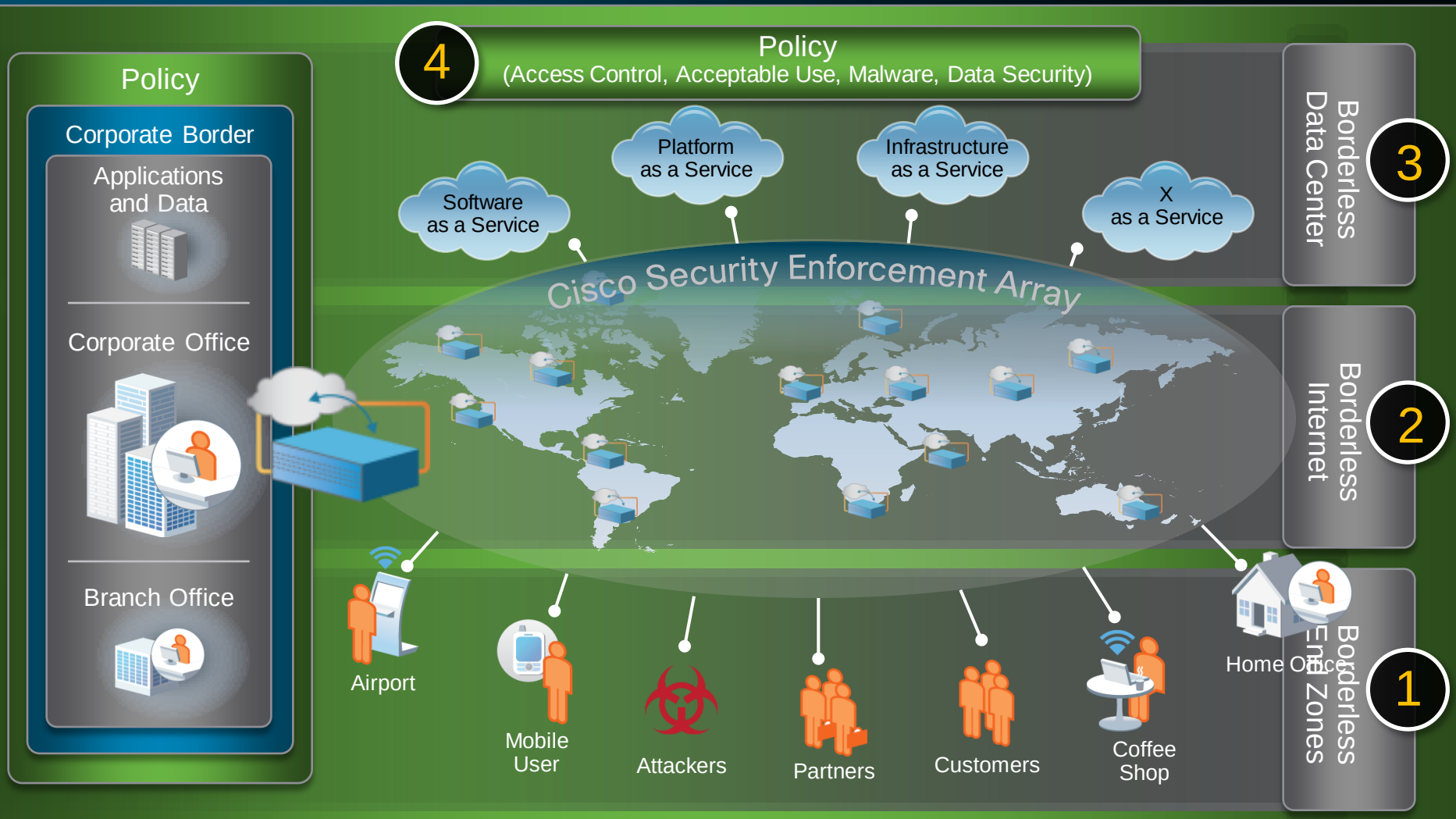
AnyConnect

Borderless Network Services

Video: Medianet | **Green:** EnergyWise | **Security:** TrustSec | **Performance** | **Mobility**

Infrastructure

Cisco's Architecture for Borderless Network Security



Pillar 1: Borderless End Zone

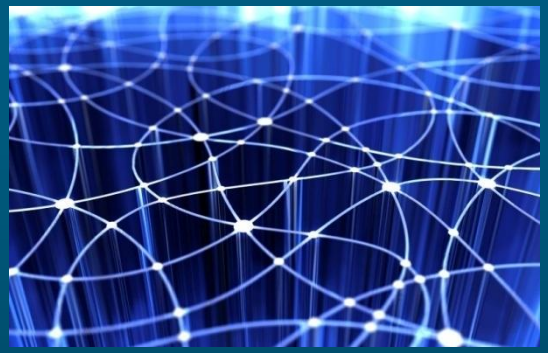
Intelligent End Point Traffic Routing

Broadest Coverage

Most OS's and Protocols

Windows Mobile

Apple iPhone



Persistent Connectivity

Always On, Location Aware

Auto Head-end Discovery

IPsec , SSL VPN, DTLS

Advanced Security

Strong Authentication

Fast, Accurate Protection

Consistent Enforcement

Cisco AnyConnect Secure Mobility

Choice

Diverse Endpoint Support for Greater Flexibility

Data Loss Prevention

Threat Prevention

Acceptable Use

Access Control

Security

Rich, Granular Security Integrated Into the network

Access Granted

skype

YouTube

Intranet

salesforce.com

Corporate File Sharing

Experience

Always-on Intelligent Connection for Seamless Experience and Performance

AnyConnect Secure Mobility

NEW

1 Cisco AnyConnect

Next Generation Remote Access

"It just works"

Broad device support

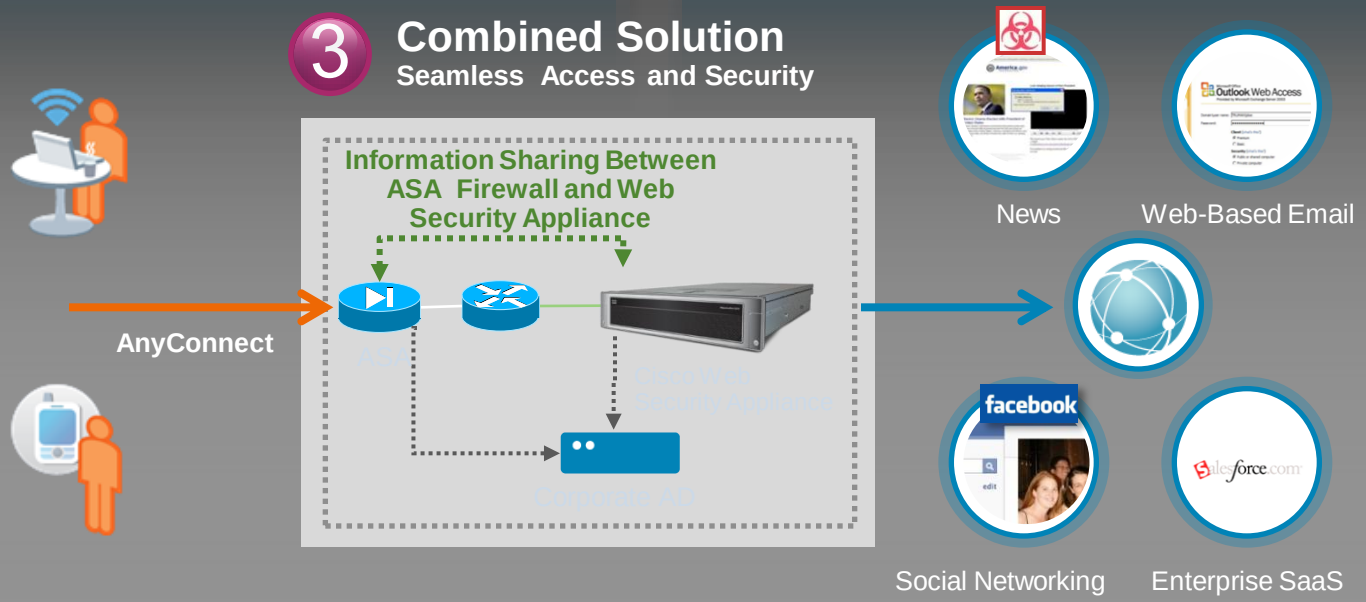
2 Cisco IronPort Web Security Appliance

Complete Web Security

Malware, Acceptable Use, Access Control, and Data Security

3 Combined Solution

Seamless Access and Security



Cisco TrustSec: Guest Access Made Easy

Consultant for
a Project

Do I Have a Consistent Access Policy Architecture
Across My Network for all Users and Devices?

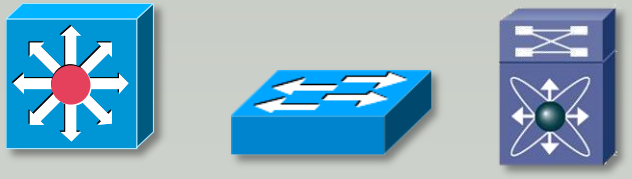
Announcing: Cisco TrustSec

Identity-aware Networking

Policy-based Access Control

Data Integrity and Confidentiality

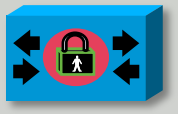
Infrastructure Components



Cisco® Catalyst® and Nexus® Switches

NEW

Policy and Security Components



Access Control System

NAC Manager, Server, Profiler, Guest Server

Endpoint Components

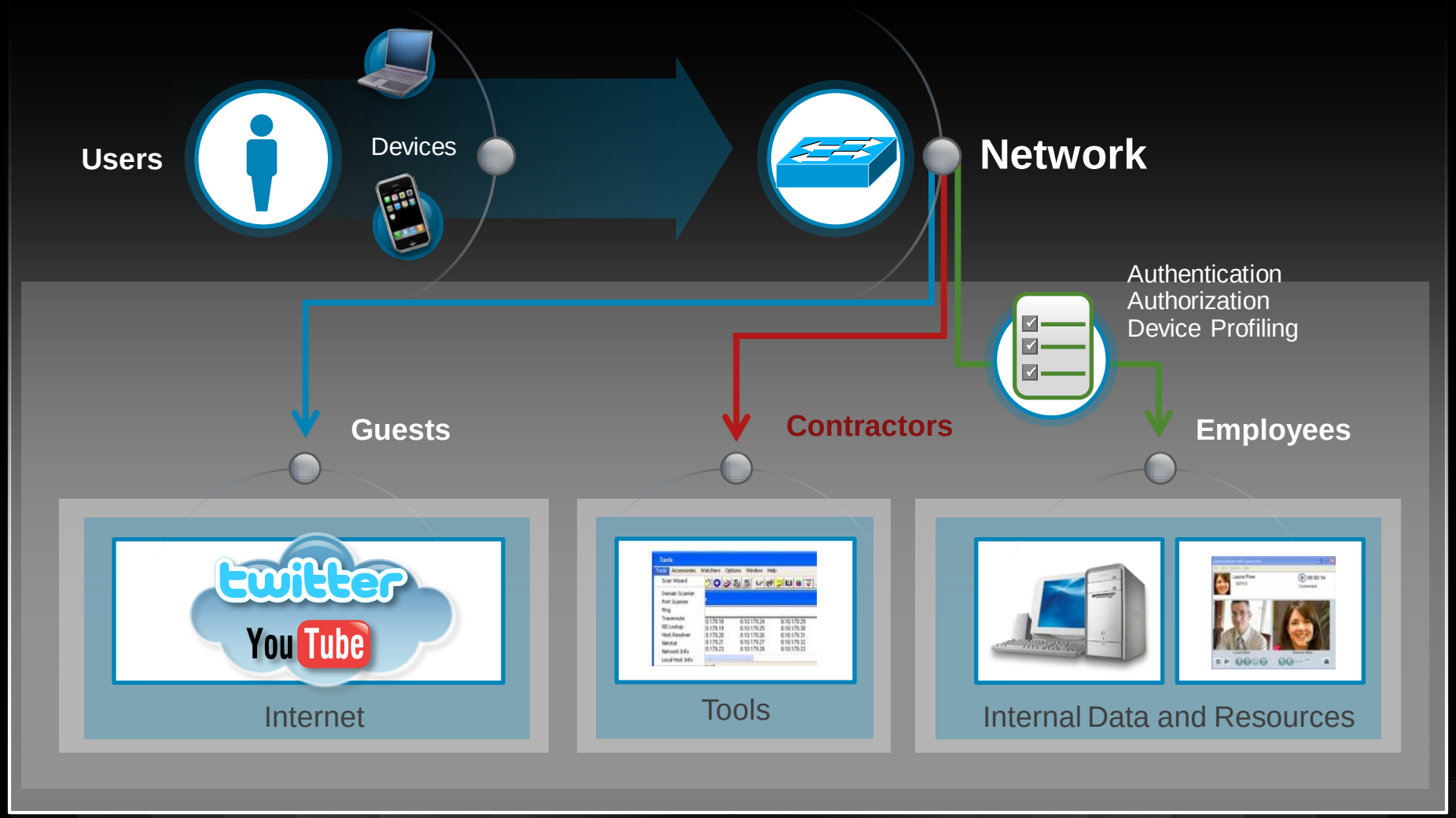
802.1X Supplicant

NAC Client

AnyConnect

Future

Use Case: TrustSec in a Conference Room



Pillar 2: Borderless Security Array

Advanced Scanning and Enforcement Capabilities

Cisco Adaptive Security Appliance

Cisco Integrated Services Routers

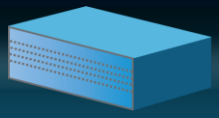
Cisco IronPort Web Security Appliance

Cisco IronPort Email Security Appliance

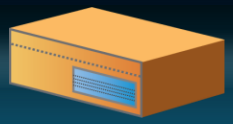
Access Control | Acceptable Use | Data Security |Threat Protection

Integrated into the Fabric of the Network

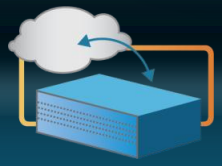
VM Software



Appliance



Security Module



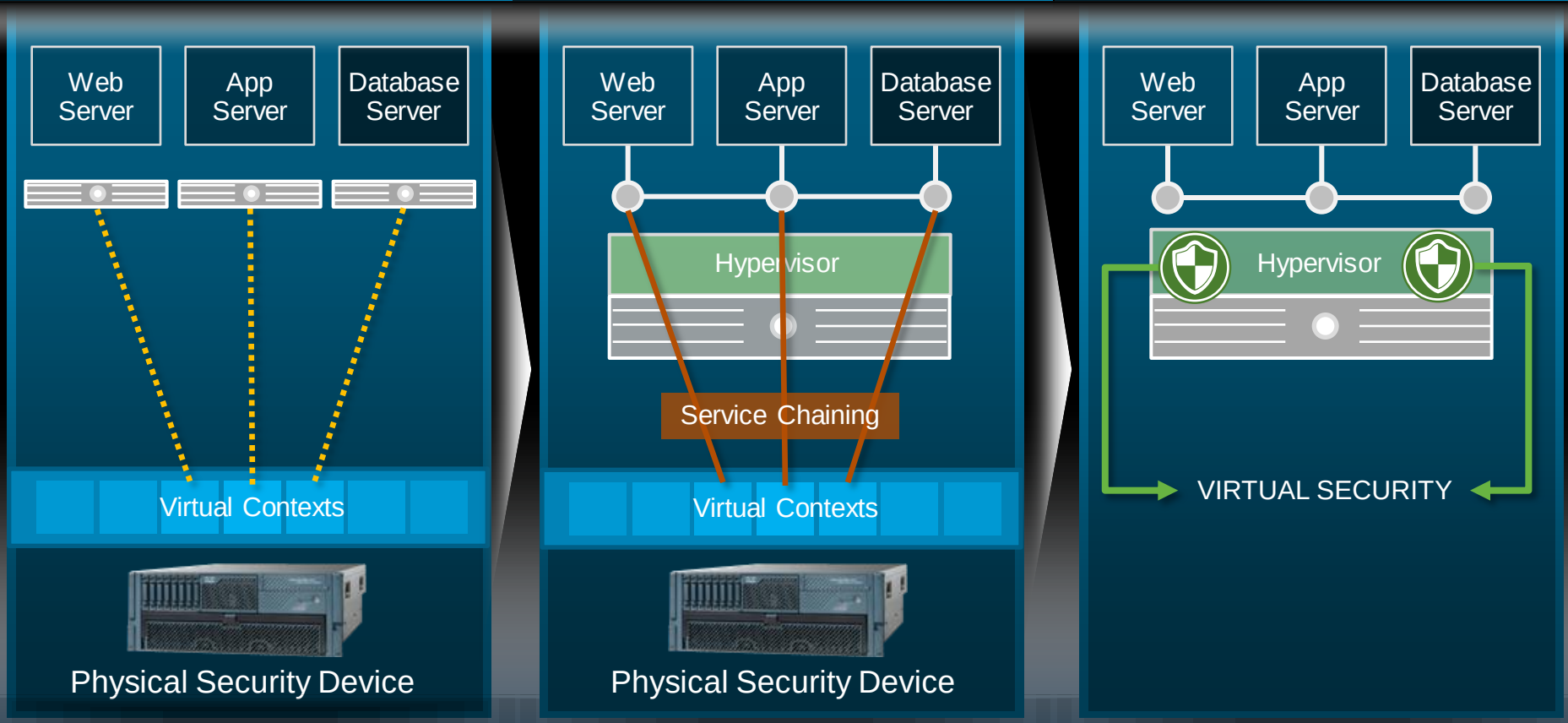
Hybrid Hosted

Pillar 3: Secure Virtualized Data Center

1 Secure Physical Infrastructure

2 Connect Physical Security to Virtual Machines with Cisco's SIA

3 Embed Security in the Virtual Switch



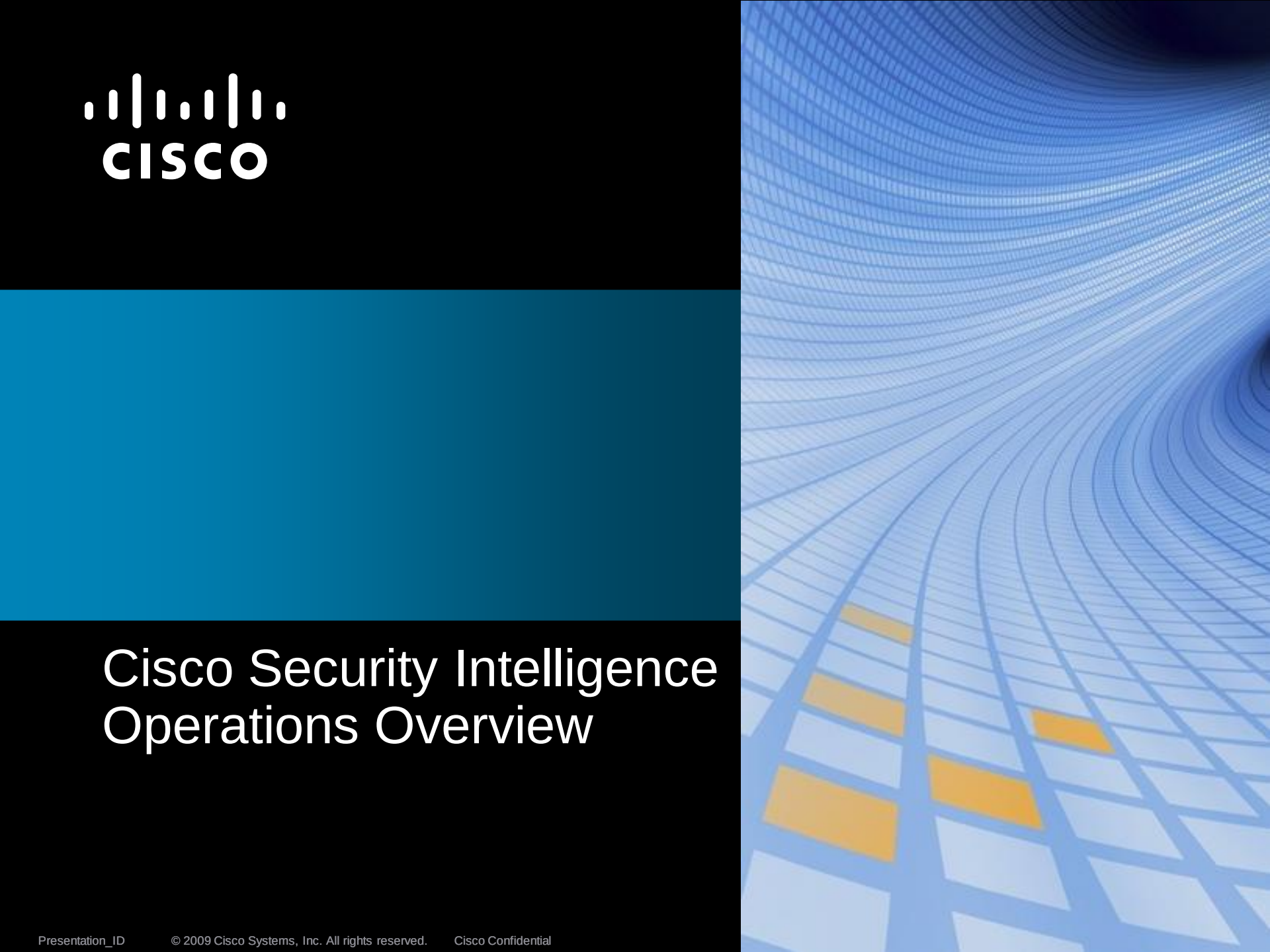
Pillar 4: Rich Policy Enables "Ubiquitous", Consistent Control

1 Access Policy

Who? What? When? Where? How?

2 Dynamic Containment Policy

3 Policy On and Off Premise



Cisco Security Intelligence Operations Overview

Cisco Security Intelligence Operations

- Watchlist
- Manage Profiles
- Sources Monitoring
- Sources Report
- Filenames Grouping
- Profiles Grouping
- Rules
  - Rule Status
  - Create Rule
  - Create Rule (V2)
- Public Notes
  - Edit/Create—Notes
  - Edit/Create—Reasons
- Map

Botnet Activity

Botnet	Time	Nodes Detected
Srizbi	2009-11-18 11:36:25	313,593
Bobax	2009-11-18 11:49:33	180,793
Rustock	2009-11-18 11:46:27	145,856

Calculating:

Email Traffic Alert

IP Address	Vol.	Rep.
222.76.214.57	5.5	Poor
189.143.8.15	4.5	Poor
189.72.170.115	2.9	Poor
208.84.101.165	2.6	Poor
193.252.22.29	0.3	Good
212.214.213.238	0.3	Poor
76.162.254.116	6.9	Neutral

Threat Correlation

Threat URLs

Web Server	IP Address	Rep.
www.Adware-Download.com	70.86.182.194	Poor
www.brothersoft.com	68.26.180.23	Poor
www.rocketdownload.com	38.102.33.137	Neutral
chennaiplus.net	208.113.167.238	Neutral
aeroflighttraining.com	66.96.130.122	Neutral
tizybwtyaj.prv.pl	194.94.24.158	Poor

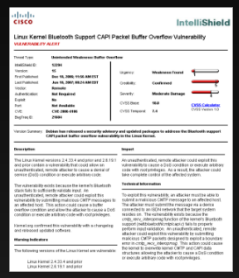
Threat Rule Publication

Rule	Time	Platform
URL (view/.exe)	2009-11-18 12:05:06	☐ All ☑ Email ☐ Web ☐ IPS
URL (insidevideo/exe$/)	2009-11-18 12:05:13	☐ All ☐ Email ☑ Web ☐ IPS
CON (ch/gallery/$$$/exe)	2009-11-18 12:05:16	☐ All ☑ Email ☐ Web ☐ IPS
URL (insidevideo/exe$/)	2009-11-18 12:05:22	☐ All ☑ Email ☐ Web ☐ IPS
URL (video/php$)	2009-11-18 12:05:29	☑ All ☐ Email ☐ Web ☐ IPS
MES (out/phon$$$/bin)	2009-11-18 12:05:33	☑ All ☐ Email ☐ Web ☐ IPS

Dashboard | SensorBase | Threat Operations Center | Advanced Protection

Cisco Security Intelligence Operations

Three Defense Pillars



SensorBase

Comprehensive Threat Intelligence

Threat Operations Center

Researchers and Automated Analysis

Dynamic Updates

Real-Time Updates and Best Practices

SensorBase

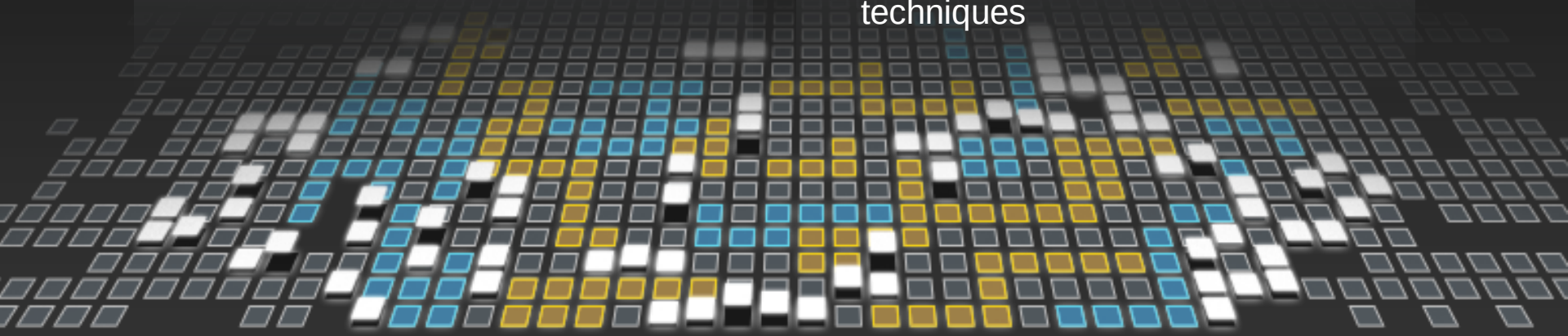
Depth of Coverage

Threat Intelligence

- 700,000+ global sensors
- Historical library of 40,000 threats
- 30% of global email and web traffic
- 500 third-party feeds, 100 news feeds, open source and vendor partnerships

Benefits

- 360 degree dynamic threat visibility
- Understanding of vulnerabilities and exploit technologies
- Visibility into highest threat vehicles
- Latest attack trends and techniques



Over 1000 servers process over 500GB of threat data per day

Threat Operations Center

Security Expertise

Researchers and Analysts

- 500 analysts and White Hat engineers
- 80+ PhDs, CCIEs, CISSPs, MSCEs
- Human-aided rule creation and QC
- Penetration testing, botnet infiltration, malware reverse engineering, vulnerability research
- 24 x 7 x 365 operations in five centers
- 95% of Internet languages covered

Benefits

- Network security best practices and mitigation techniques
- Insight into threat trends and future outlook
- Quality assurance, reduced false positives
- Around-the-clock global coverage

Dynamic Updates

Automated Defense

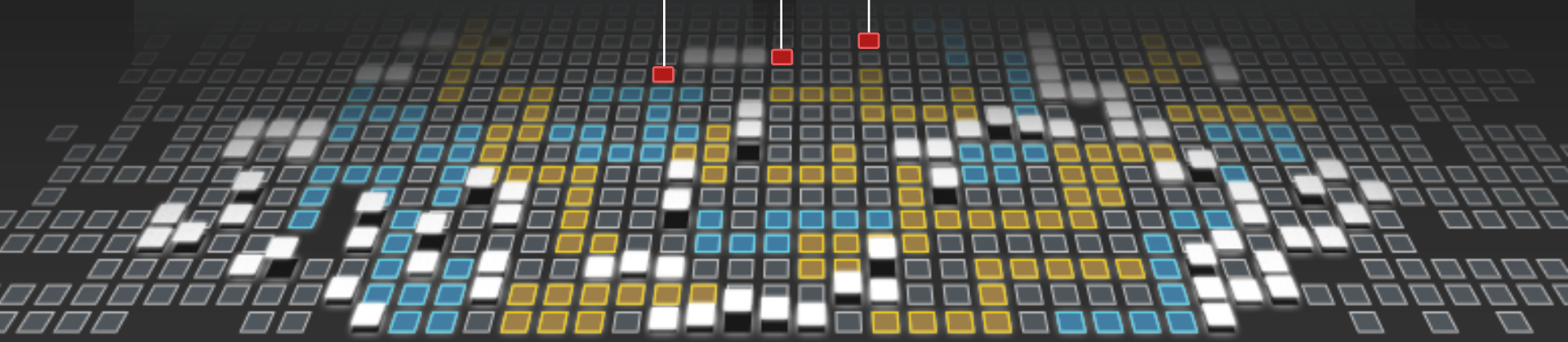
Updates

- Automated updates delivered to Cisco security devices every 3–5 minutes
- Reputation updates for real-time protection

Cisco Security Intelligence Operations

Benefits

- Reduces exposure window
- Minimizes security management overhead



Advanced, Proactive Threat Protection

Cisco Security Intelligence Operations

Higher Threat Coverage, Greater Accuracy, Proactive Protection

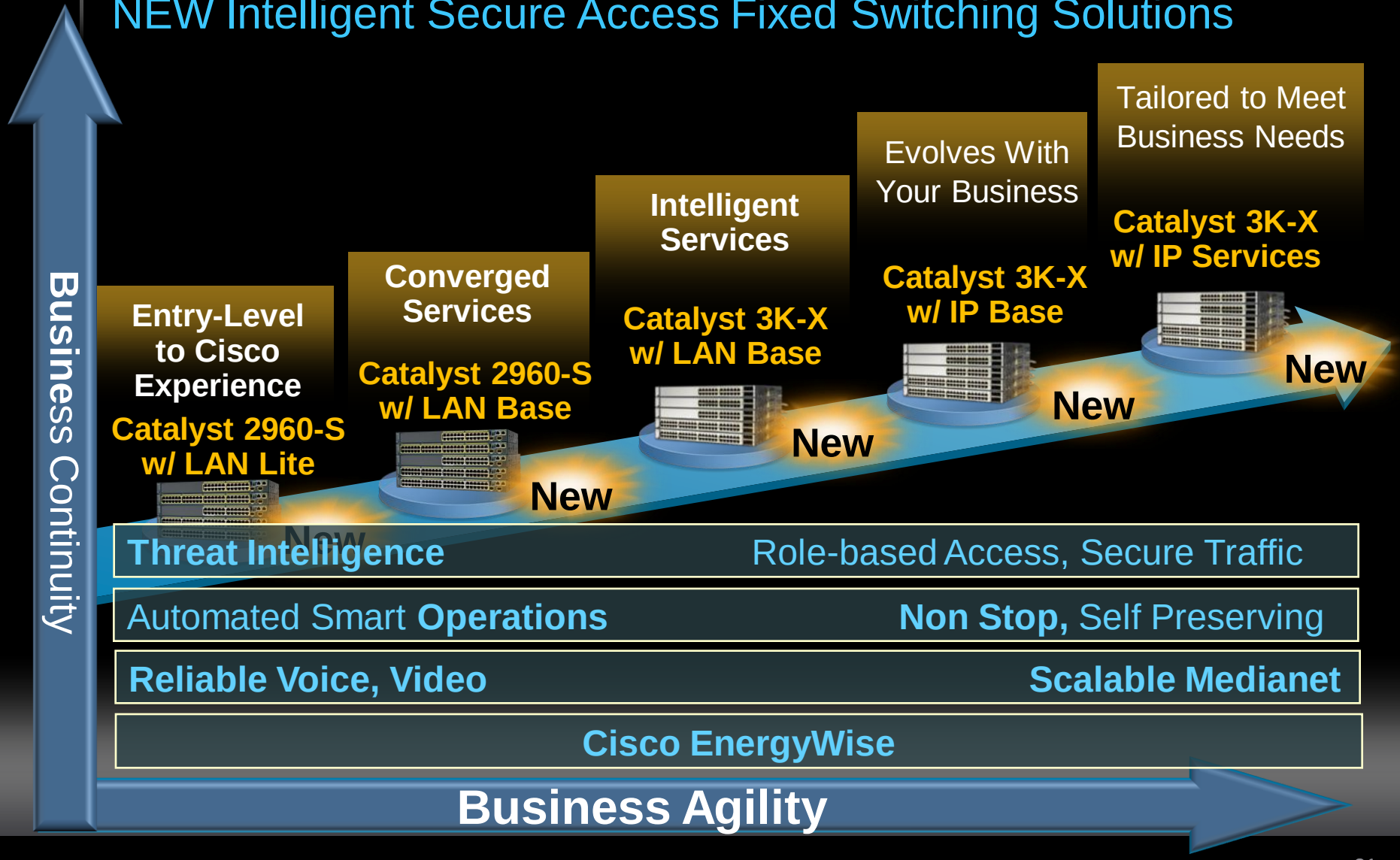
Products and Services

Latest Announcements

Introducing: Cisco Integrated Services Router Generation 2

Addressing Business Transformation

NEW Intelligent Secure Access Fixed Switching Solutions



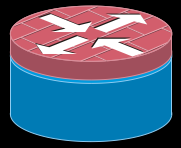
Borderless Security: Building the System

Enforcement Points

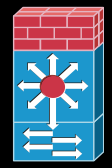
Adaptive Security Appliance

IPS with Global Correlation

Email Security Gateway



Secure Router



Switch Security

Web Security Gateway

Security as a Service

Hybrid Hosted Email Security

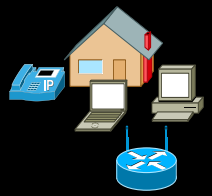
Cisco Security Intelligence Operations

Coming Soon: Hosted Web Security

End Zone

AnyConnect

NAC



CVO