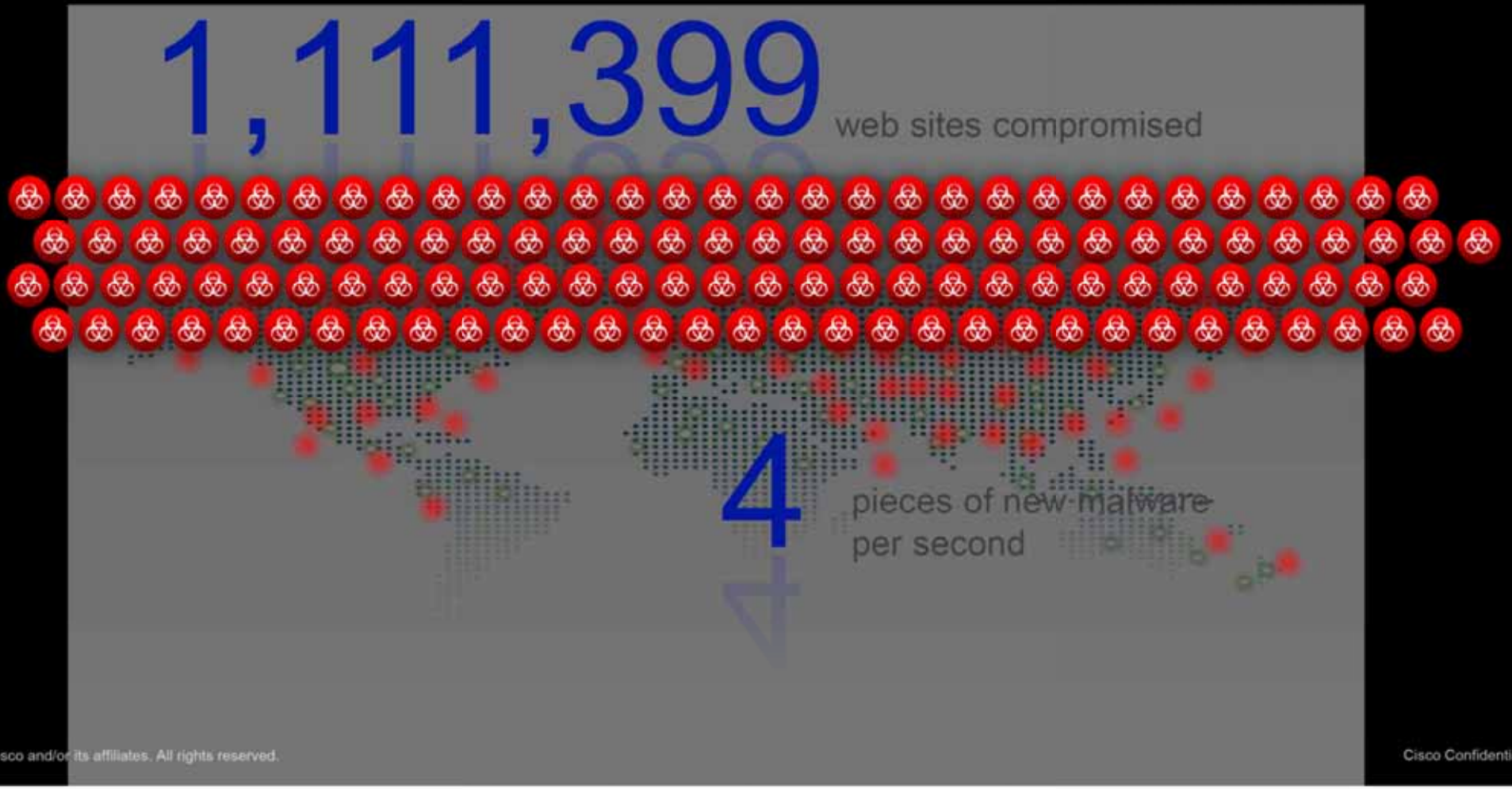
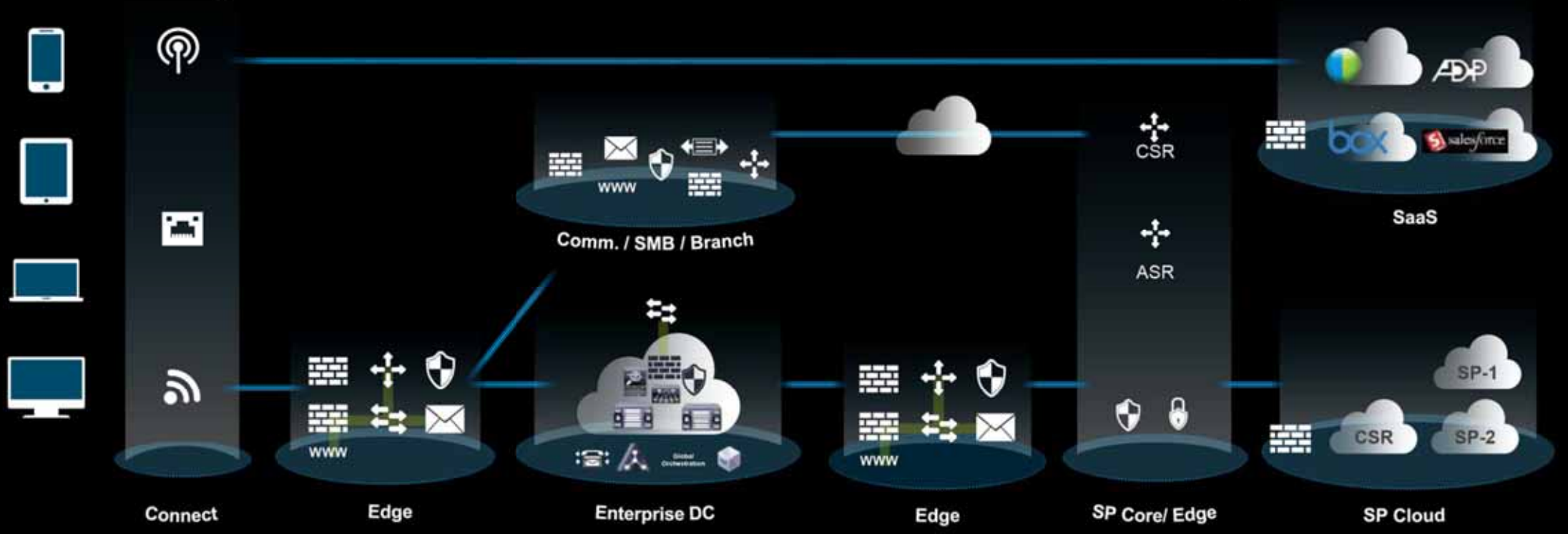

ATEC
How to protect against the evolving threats of today's Internet
Nikos Mourtzinos,
CCIE#9763
PSS Cisco Security
Greece, Cyprus, Malta, Israel, Portugal

Changing Threat Landscape

- Cyber attacks are one of the unfortunate realities of doing business today.



Today's Security is Complex and Fragmented



Multiple Management Paradigms

Multiple Identity Stores

Isolated Threat Intelligence

Inconsistent Enforcement


Any Device to Any Cloud
salesforce.com
box
Google
SkyDrive
Apps
PUBLIC CLOUD
HYBRID CLOUD
PRIVATE CLOUD

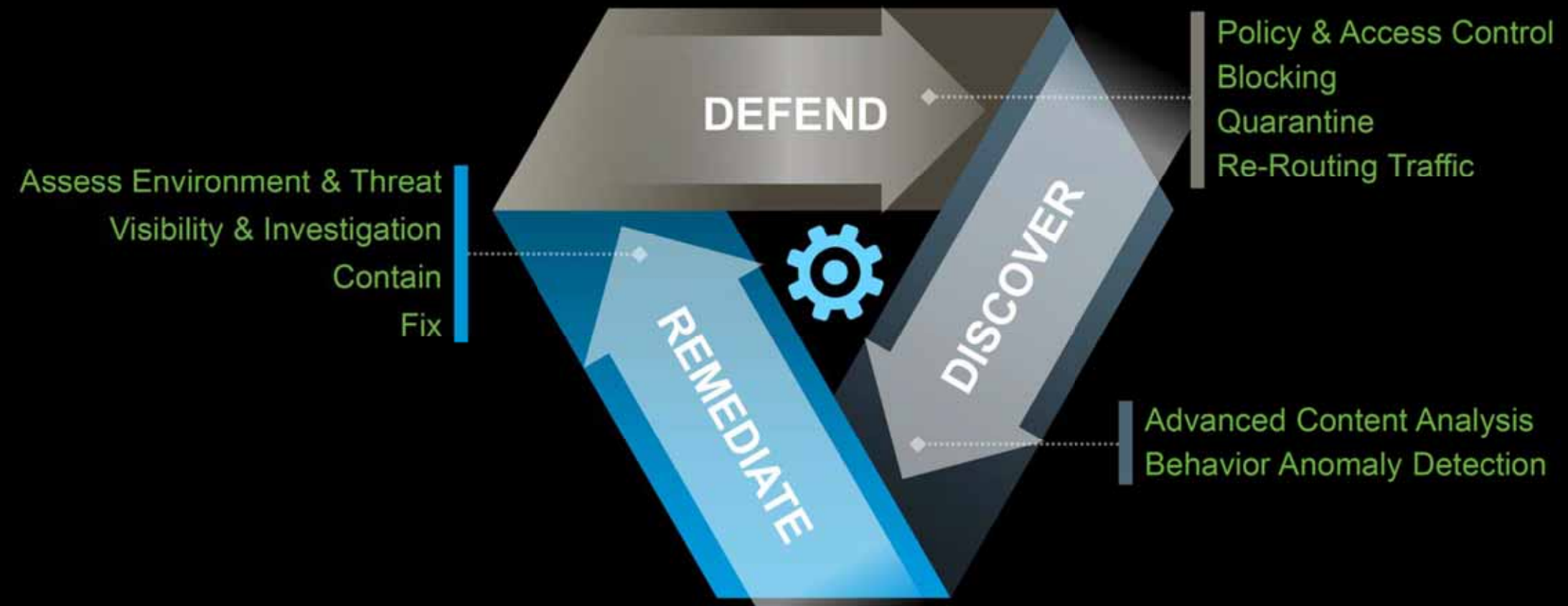
Your Biggest Security Challenges

Maintain Security and Compliance as business models change (Agility)

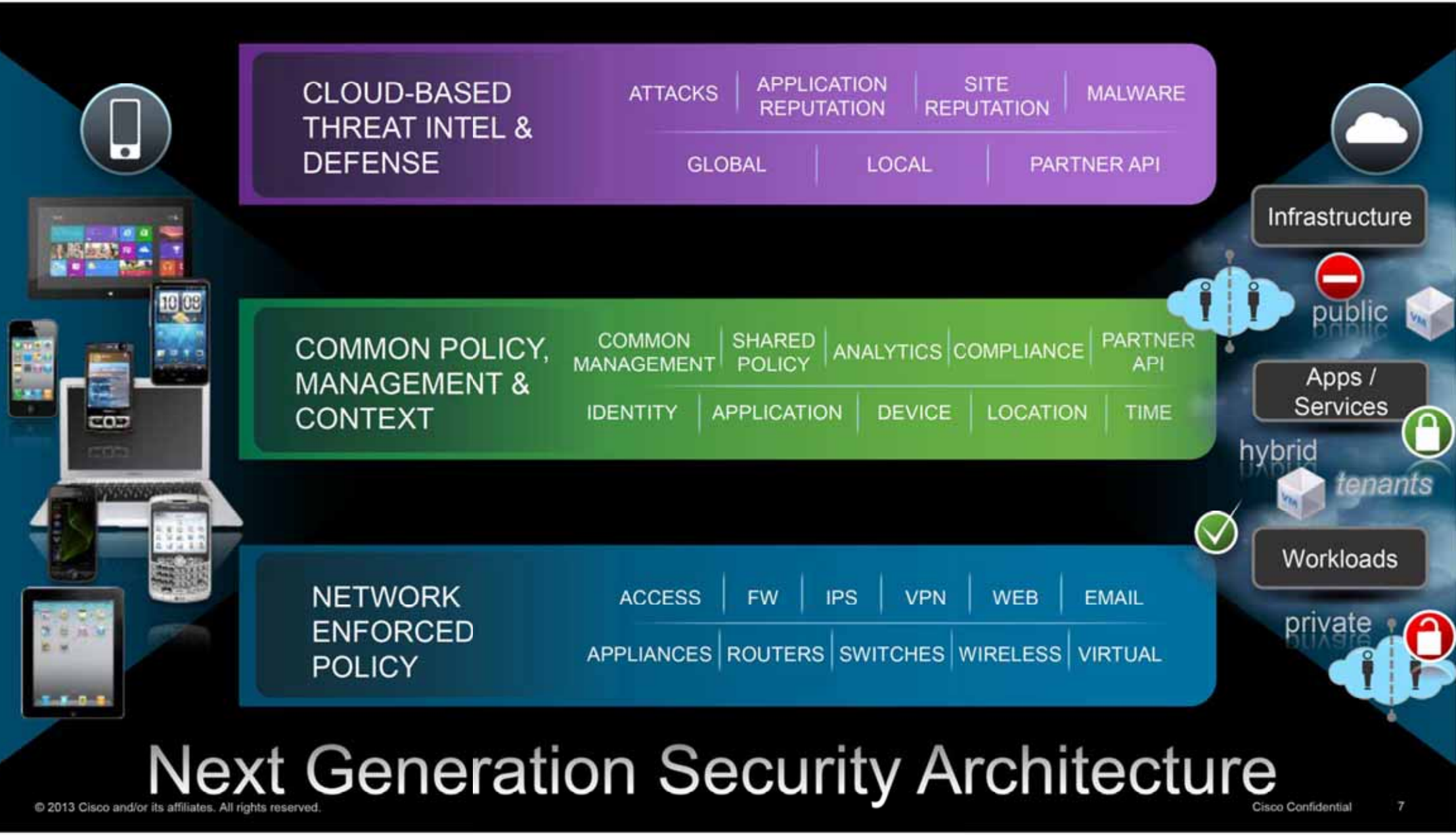
Stay ahead of the threat landscape

Reduce complexity and fragmentation of security solutions

Re-Think Security Process and Technology



Advanced Targeted Attacks Inside the Network



Next Generation Security Architecture

Cisco Security Intelligence Operations

Outstanding Cloud-based Global Threat Intelligence

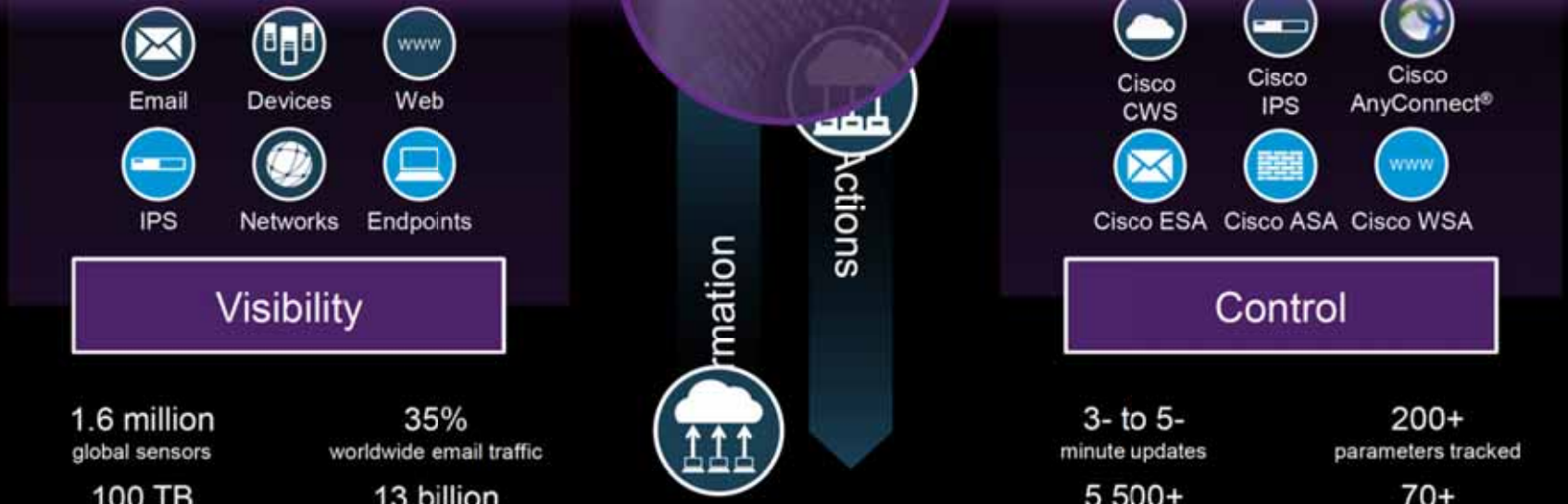
24x7x365 operations

40+ languages

More than US$100 million
spent on dynamic research and development

600+
engineers, technicians, and researchers

80+
PH.D., CCIE, CISSP, AND MSCE users



1.6 million
global sensors

100 TB
of data received per day

150 million+
deployed endpoints

35%
worldwide email traffic

13 billion
web requests

3- to 5-
minute updates

5,500+
IPS signatures produced

8 million+
rules per day

200+
parameters tracked

70+
publications produced

COMMON POLICY, MANAGEMENT & CONTEXT

Who/What is currently connected on the Network ?

How Do I Control
Who and What Access the Network/Resources?

How to Quarantine a User ?

Cisco Identity Services Engine (ISE)

Next Generation Network Access Control

Identity Context

- AAA
- Profiling
- Posturing
- Guest Management

Who | What | Where | When | How

Security Policy Attributes

Cisco® ISE

Business-Relevant Policies

Wired | Wireless | VPN

Virtual machine client, IP device, guest, employee, and remote user

Next Generation Firewall Services

FW

Stateful Inspection FW

VPN

User Secure Access Any Device

IPS

Intrusion Prevention

AVC

Application Visibility & Cotrol

WSE

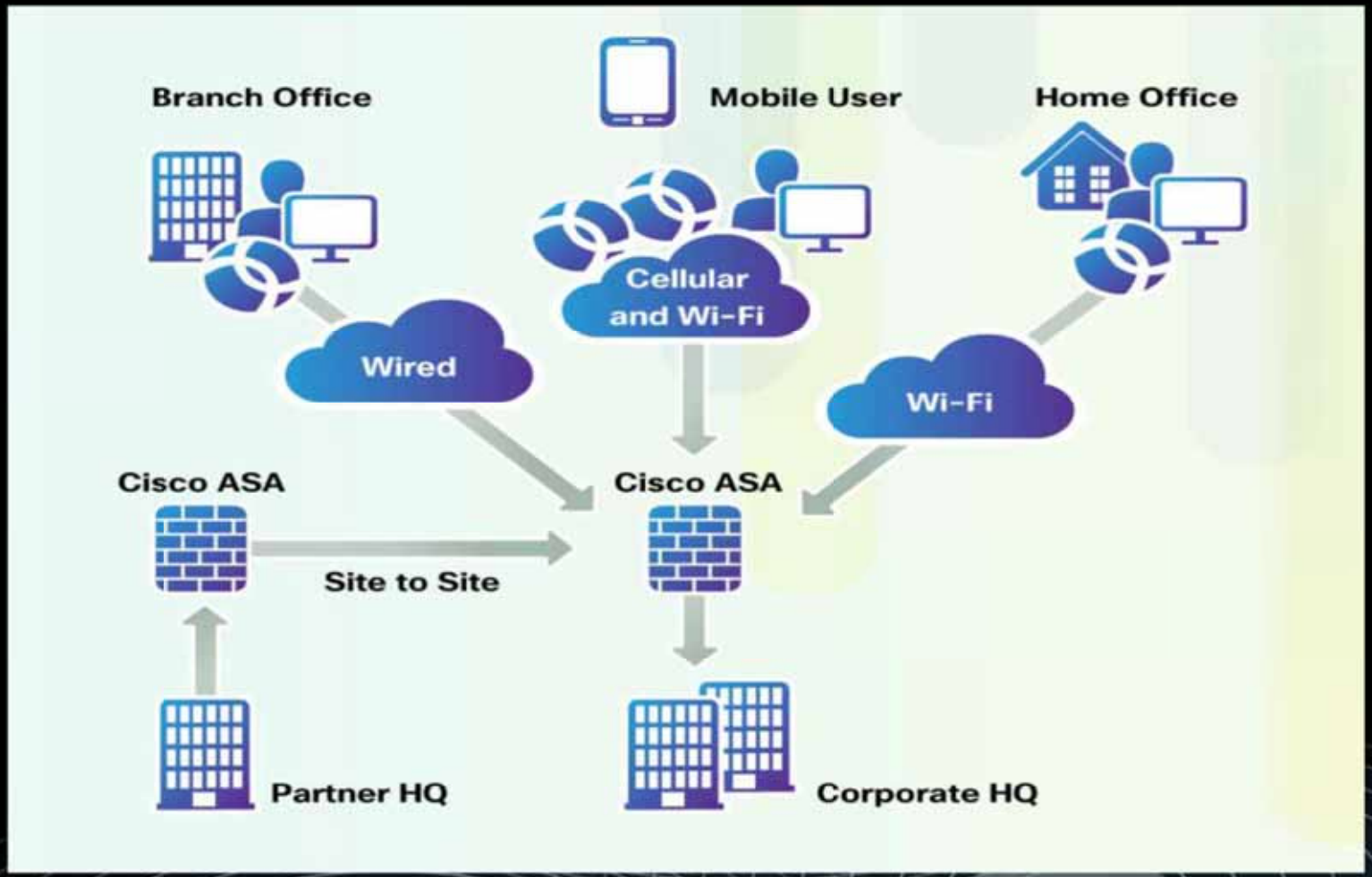
Web Security

Botnet

Identify & Prevent Botnets

ASA NGFW

- FW
- VPN



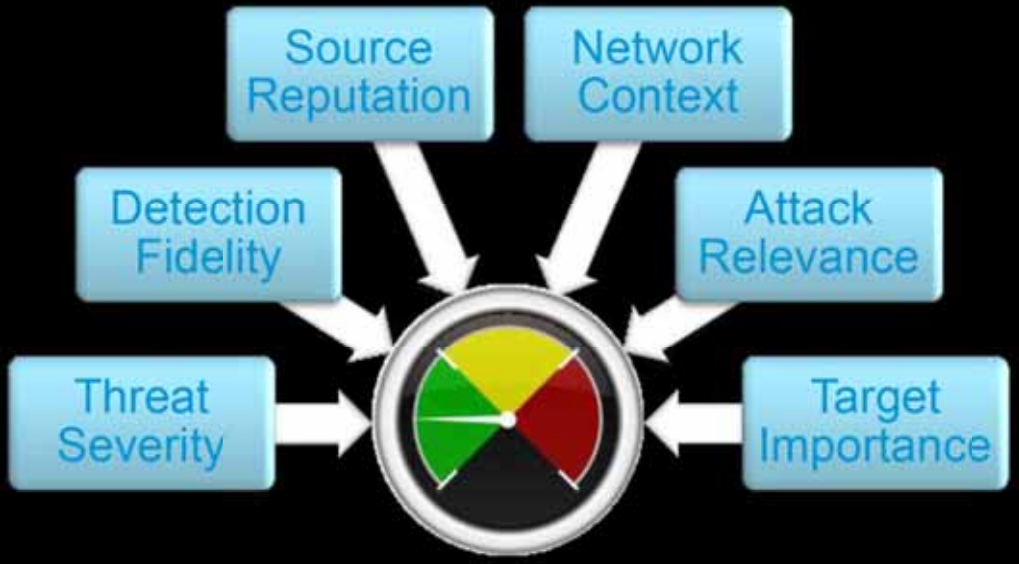
IPS

Intrusion Prevention

What is the Attack?

Who is the Attacker?

What is the Target?



Risk Rating Engine

Business Class URL Filtering & Application Visibility & Contol

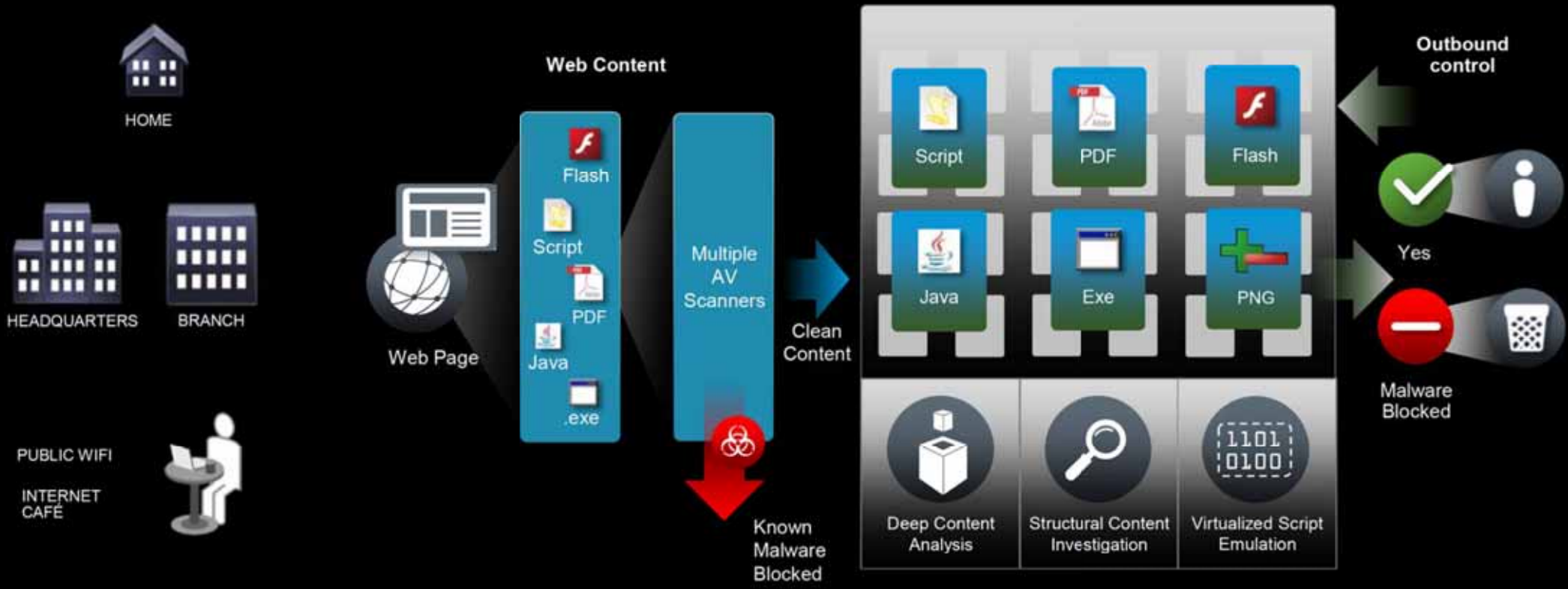
URL Filtering

- Constantly updated URL database covering over 50 million sites worldwide
- 60 languages, 200 countries, 98% coverage
- Real-time dynamic categorization for unknown URLs

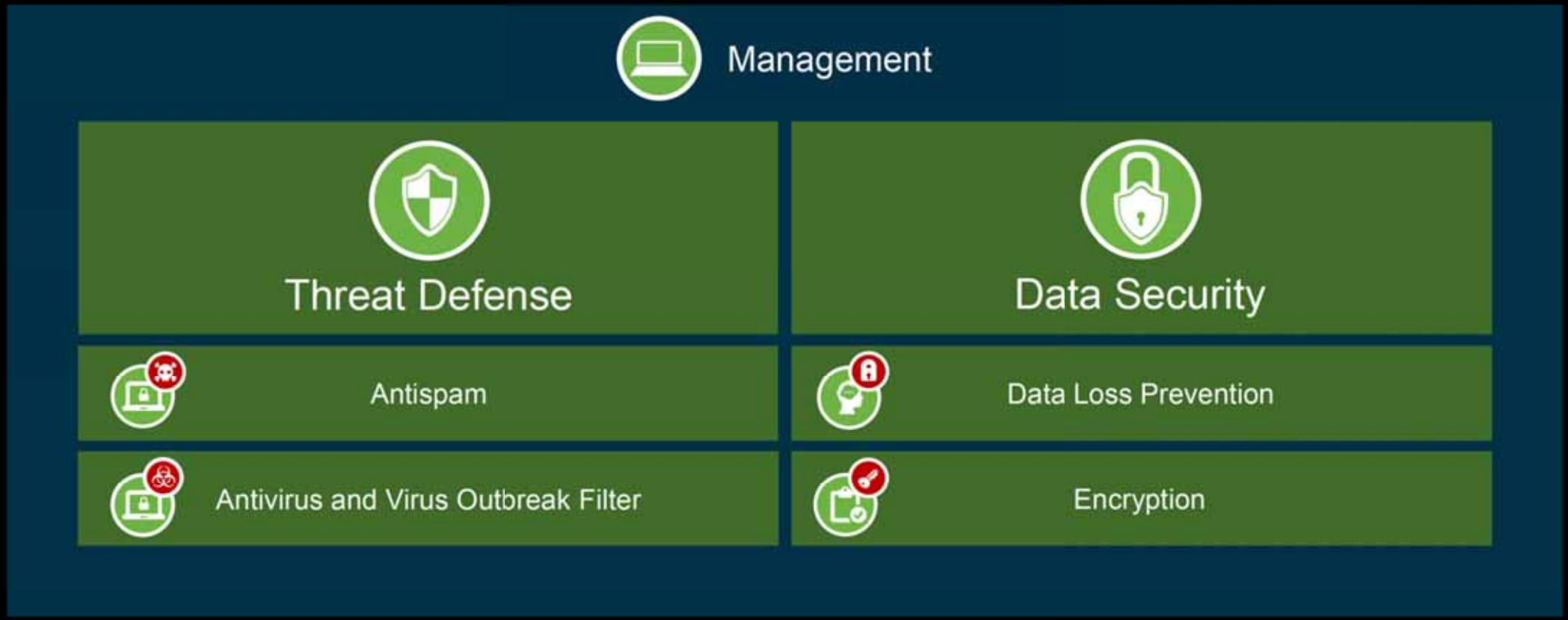
Application Visibility and Control (AVC)

- Broad Classification of Apps
- Granular enforcement of behaviors within applications
- Control user interaction with the application

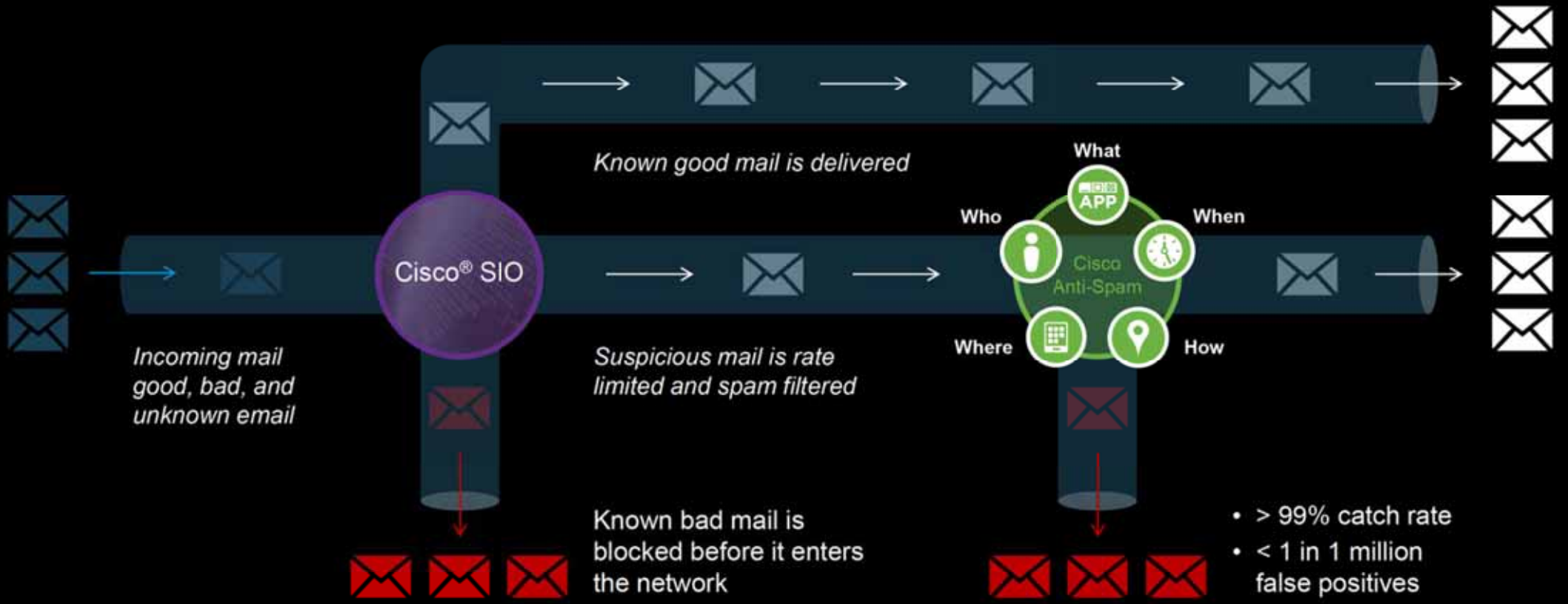
Cisco Cloud Web Security



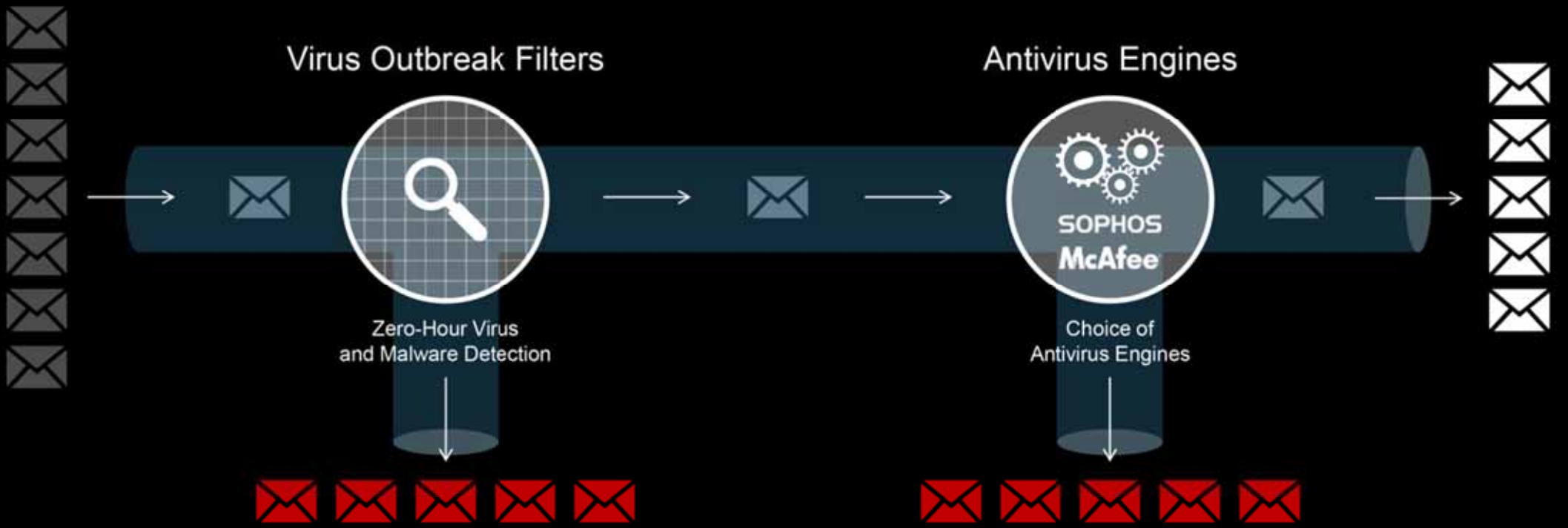
Cisco Email Security Architecture



Antispam Defense in Depth



Antivirus Defense in Depth



DLP and Compliance

Built-in Comprehensive DLP Solution with RSA: Accurate, Easy, and Extensible

- Fast setup
- Low administrative overhead
- Comprehensive policy creation and modification
- Exceptional accuracy
- Direct integration for enterprisewide DLP deployments

Cisco Encrypted Email Is Integrated into the Network

Traditional Email Has Limitations

Anyone
can read message

No guaranteed
message recall

No control
over forwarding

Confidential
Email

Read
Receipt

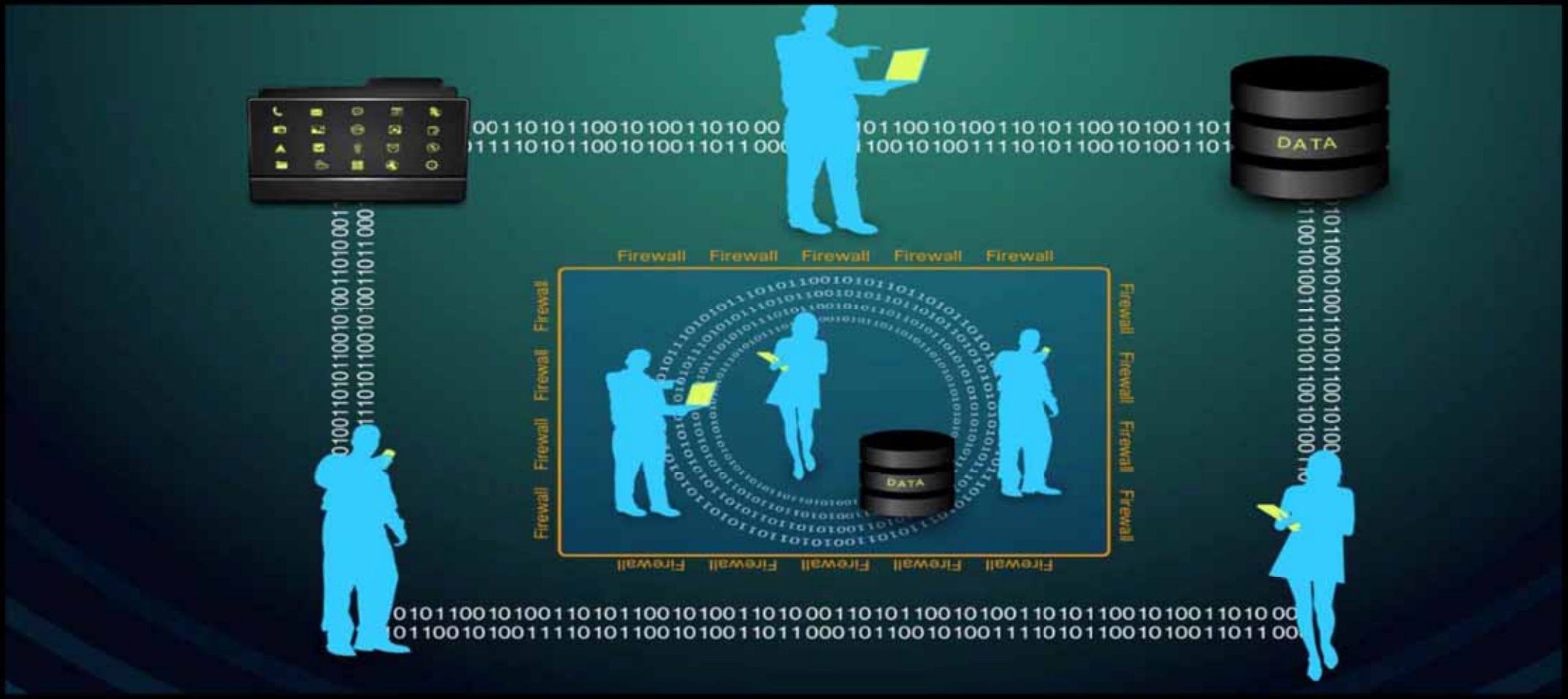
Guaranteed
Recall

Secure
Reply and forward

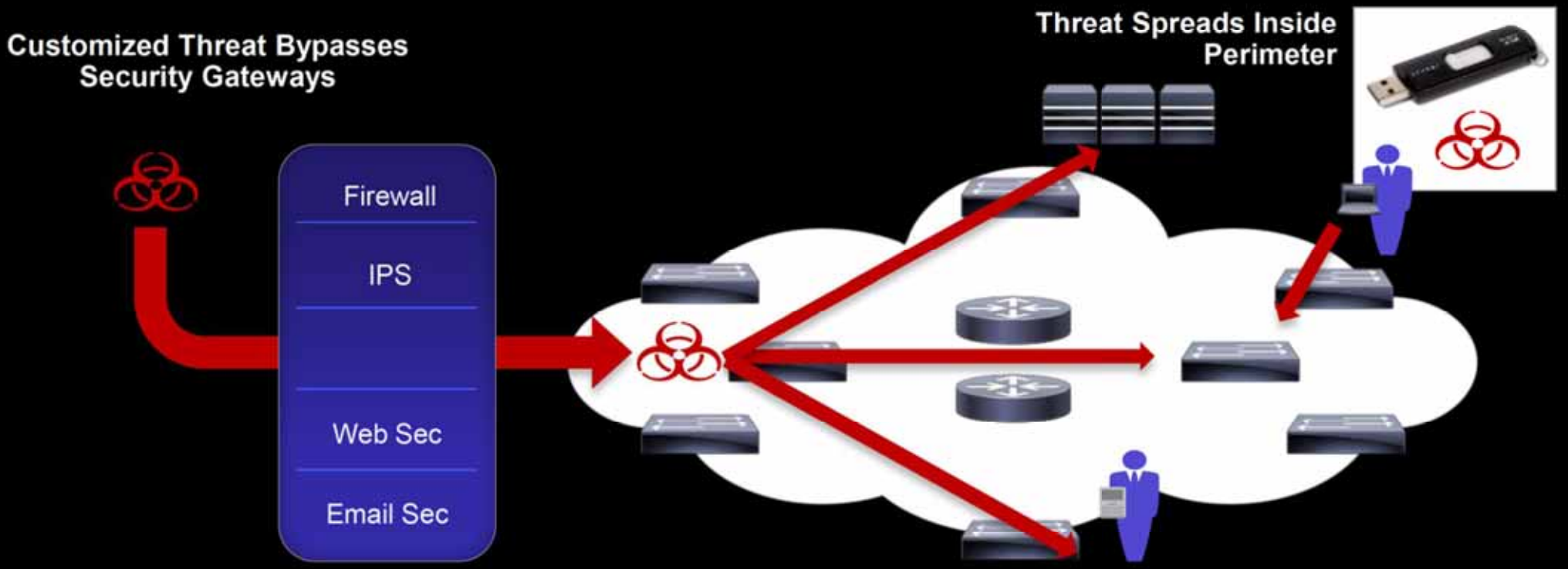
Perimeter Security

Any to Any

Perimeter Security is not working



Cisco Cyber Threat Defense: The Need



Customized Cyber Threats Evade Existing Security Constructs

Fingerprints of Threat are Found Only in Network Fabric

The Importance of Detection and Classification

- Ability to detect undesirable network traffic and to classify it appropriately
- We cannot contain/mitigate what we cannot detect
- To detect the abnormal, and possibly malicious, we have to know what's normal—we must establish a baseline of network activity, traffic patterns, etc.

A complete picture of everything happening on the network.

Uncover the root cause of security threats

Key Concept — NetFlow

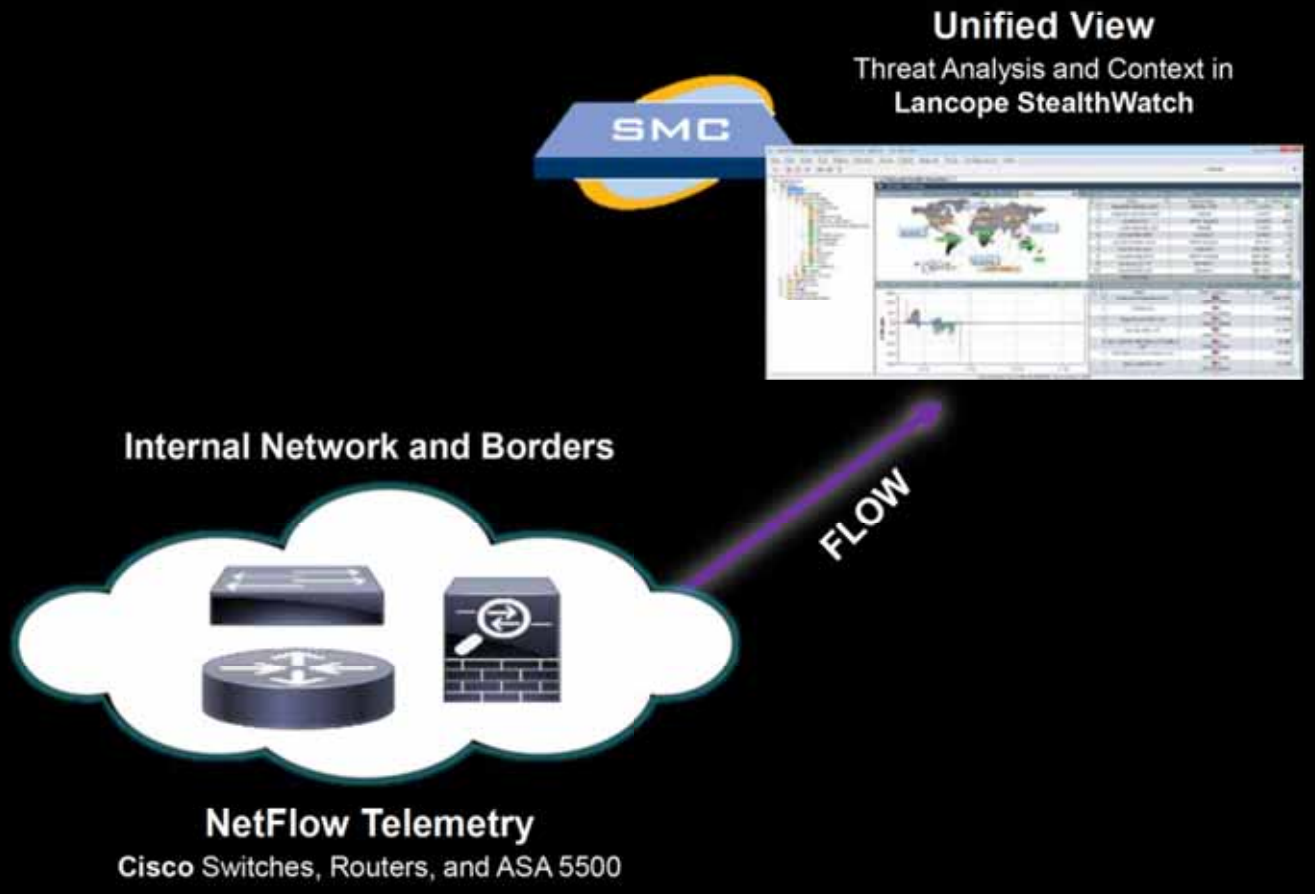
- NetFlow is like a phone bill

NetFlow provides detailed data such as:

- What is talking to what
- Direction of traffic
- over what protocols and ports
- for how long, at what speed
- for what duration
- Volume of traffic
- What nations traffic is going to
- Protocol sequence anomalies

Next Generation Cyber Threat Defense

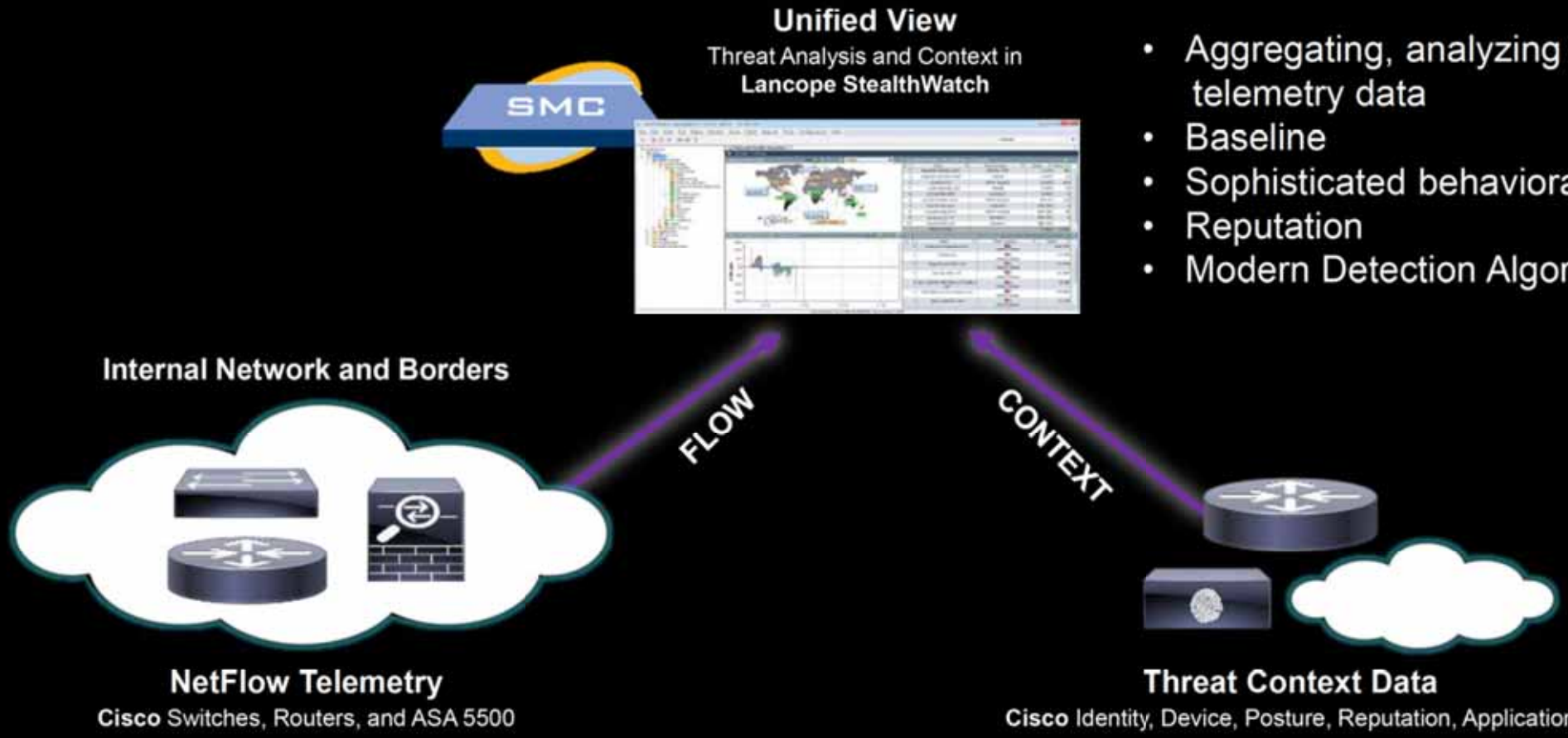
Visibility, Identity, Reputation, faster Mean Time To Know



- Aggregating, analyzing NetFlow telemetry data
- Baseline
- Sophisticated behavioral analysis
- Reputation
- Modern Detection Algorithms

Next Generation Cyber Threat Defense

Visibility, Identity, Reputation, faster Mean Time To Know



- Aggregating, analyzing NetFlow telemetry data
- Baseline
- Sophisticated behavioral analysis
- Reputation
- Modern Detection Algorithms

Cisco Threat Defense Use Cases





- Detecting Sophisticated and Persistent Threats
- Identifying BotNet Command & Control Activity
- Uncovering Network Reconnaissance
- Finding Internally Spread Malware
- DDoS attacks
- Revealing Data Loss

Security Information Event Management

SIEM

Log collection

Correlation

Reporting

IBM LogRhythm TIBCO splunk>

Cisco ISE SIEM/Threat Defense Ecosystem

CISCO ISE PROVIDES CONTEXT

Identity, Device Type, Posture,
Authorization Level, Location
Make policy changes on the network

SIEM/TD TAKE ACTION

Logs, Correlation, Reporting

Network quarantine users & devices via ISE

Discover Defend Remediate

IBM Lancope LogRhythm TIBCO splunk>

- Gain Visibility and Take Action
- Make security events actionable in the network
- Decreased time to detect, assess and respond to security events

Cisco in 60 Seconds

16 billion NetFlows / day

2.5 billion DNS records / day

2 billion events / day collected in Splunk

6 million transactions / day handled by WSAs

Malware for 1.2% of all transactions automatically blocked by WSAs

1500 Labs globally

More than 200 Business Support and Development Partners

More than 25,000 Channel Partners

12 Critical Enterprise Production DCs

Over 100 Application Service Providers

124,000 employees worldwide

68,000 FTEs

56,000 vendors

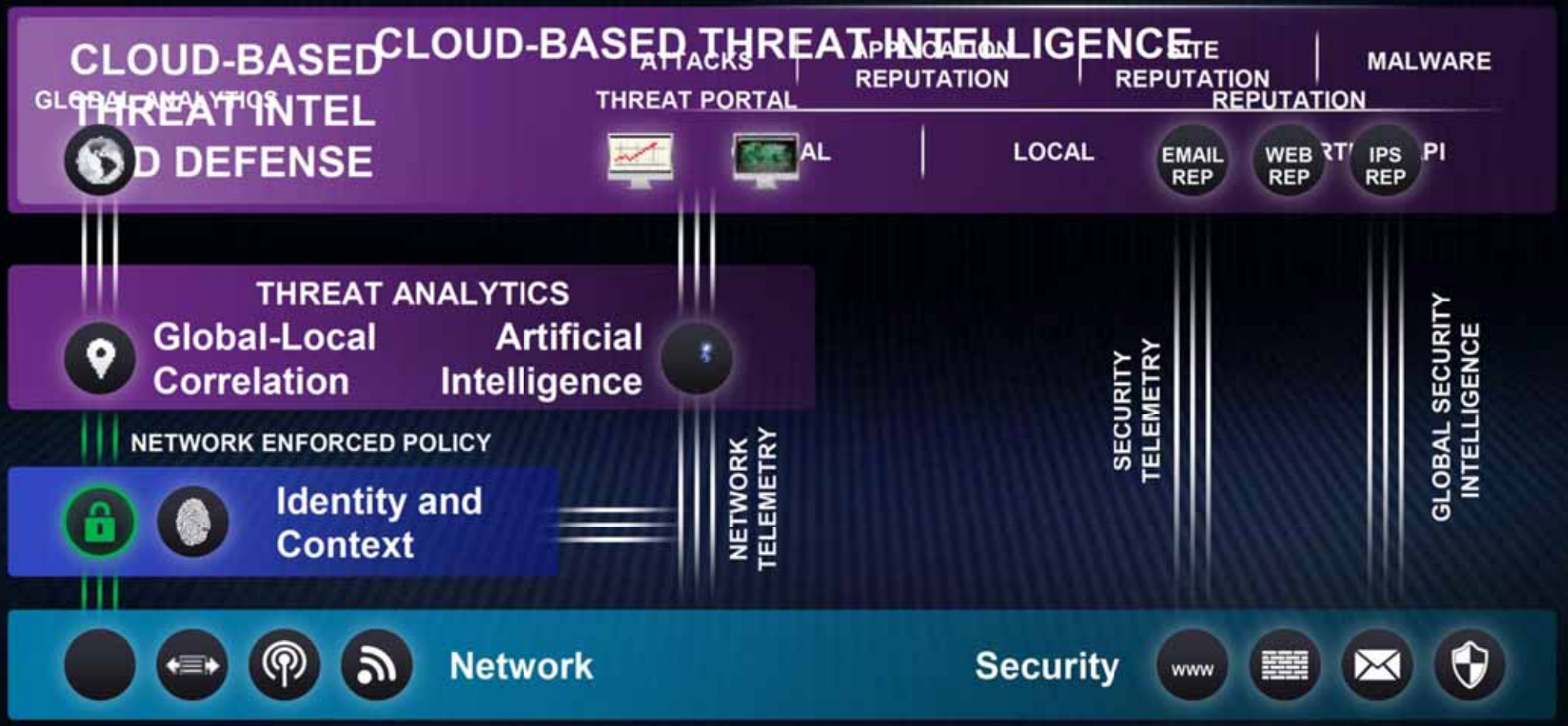
120,000 Windows hosts

40,000 routers on Cisco's network

27TB of traffic inspected / day

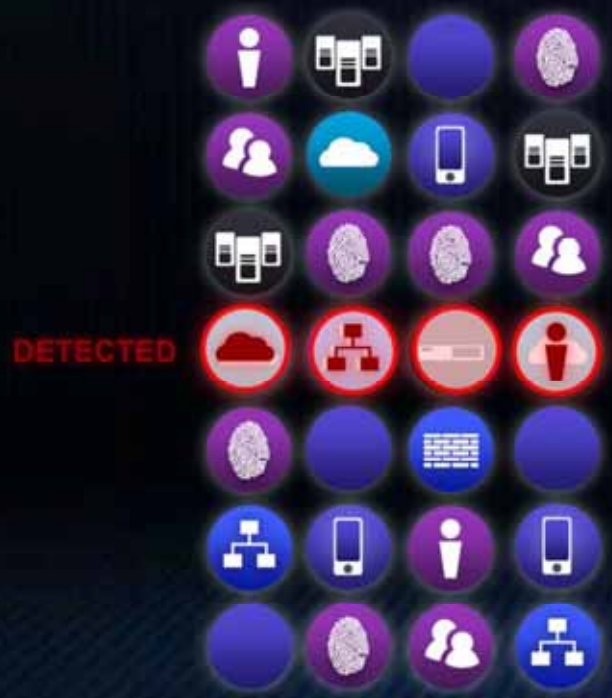
750GB of system logs collected / day

Threat Defense **and** Intelligence



Cisco Acquires Sourcefire

Advanced Threat Protection



IDENTIFY ADVANCED CYBER THREATS

Behavioral Analysis Artificial Intelligence

THREAT BEHAVIOR ANALYSIS

Leveraging Network, Web, and Identity Context

MODERN DETECTION ALGORITHMS

Behavioral Analysis Artificial Intelligence

SELF-LEARNING AND EVASION RESISTANCE

Game Theoretic Self Optimization

Cisco Acquires
COGNITIVE SECURITY

Why Cisco Security?

1. **Architecture** Can Solve the Security Challenges of Today and Tomorrow
2. Unique **Context Awareness**, Policy, Visibility, and Control Capabilities
3. Most Prolific **Security Intelligence Operations** in the Industry
4. Cisco Security: **Investment**
5. **Innovations & Leadership**


ATEC
CISCO
TM