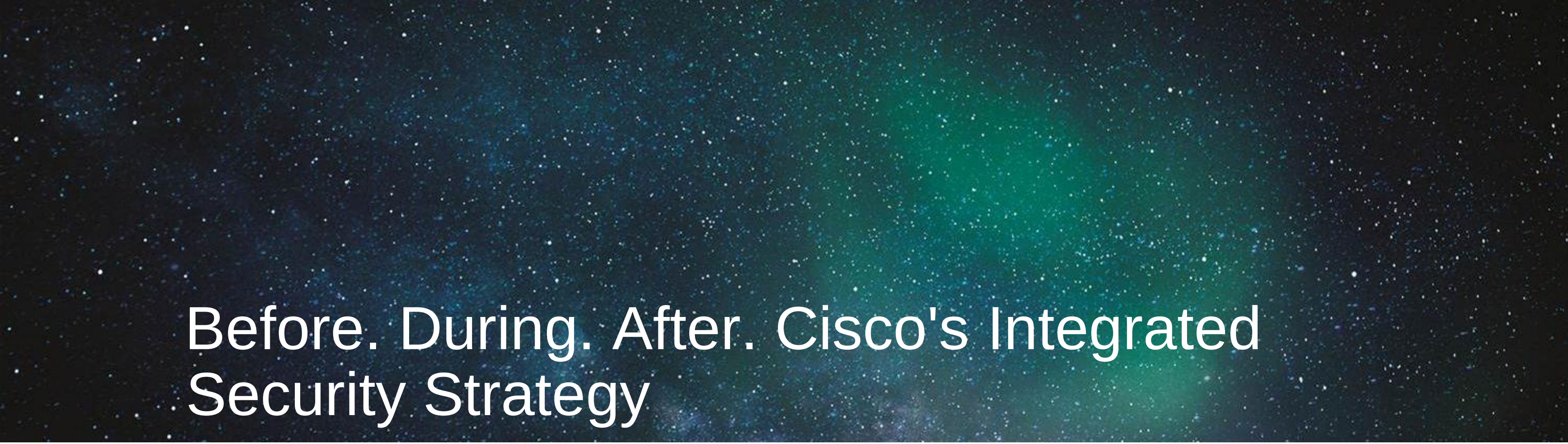
TOMORROW starts here.

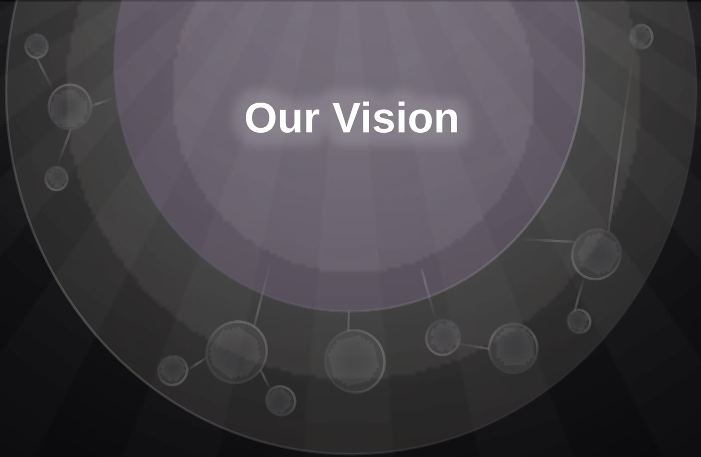


Before. During. After. Cisco's Integrated Security Strategy

BRKSEC-2663

Andy Burke
SE Manager Enterprise and Security

Our Vision



intelligent cybersecurity

for the real world

New security model primed for toughest customer challenges

Supreme talent & innovative portfolio elements

We are set to drive growth!

Strategic Imperatives

Visibility-Driven

Network-Integrated, Broad Sensor Base, Context and Automation

Threat-Focused

Continuous Advanced Threat Protection, Cloud-Based Security Intelligence

Platform-Based

Agile and Open Platforms, Built for Scale, Consistent Control, Management

Network

Endpoint

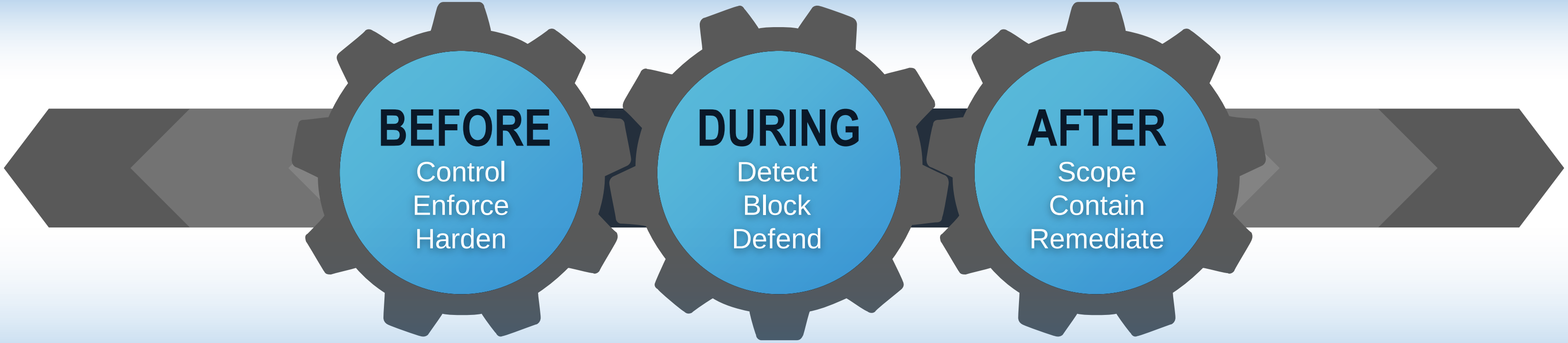
Mobile

Virtual

Cloud

The New Security Model

Attack Continuum



BEFORE
Control
Enforce
Harden

DURING
Detect
Block
Defend

AFTER
Scope
Contain
Remediate

Network

Endpoint

Mobile

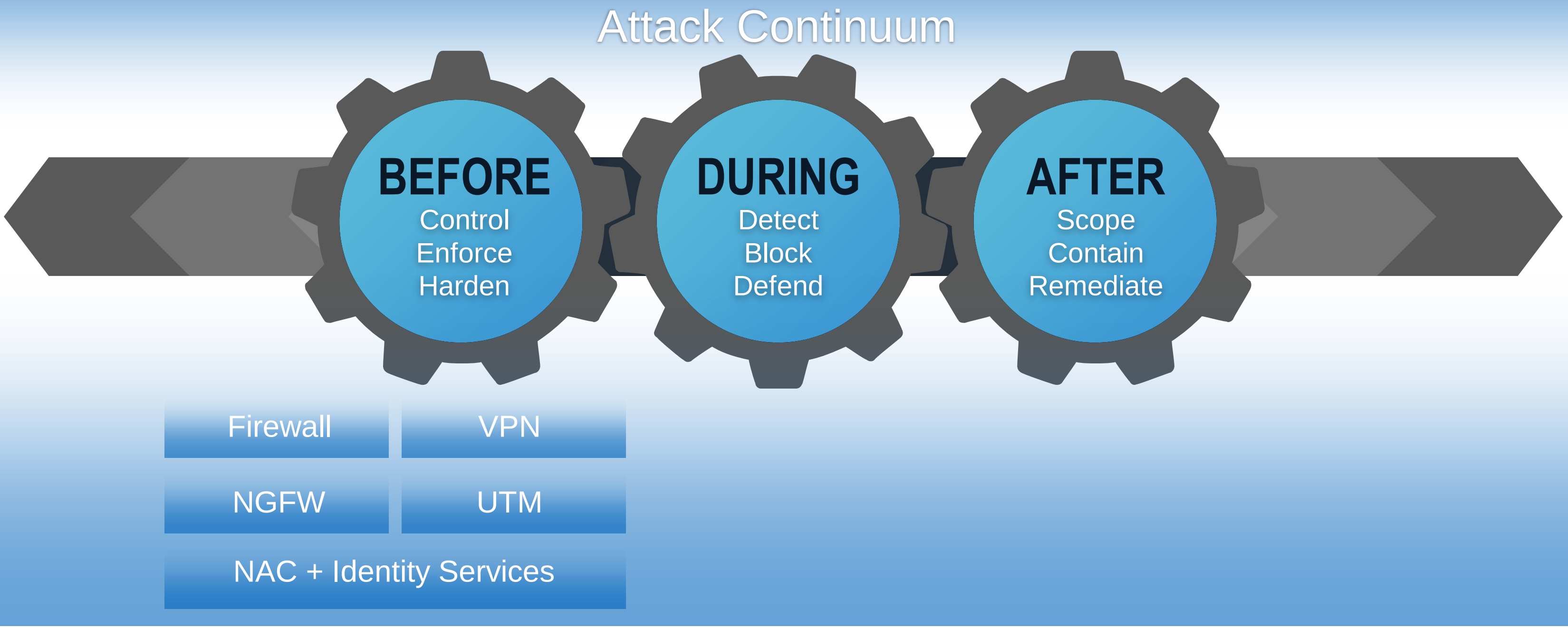
Virtual

Cloud

Point in time

Continuous

Cisco and Sourcefire - Better Together

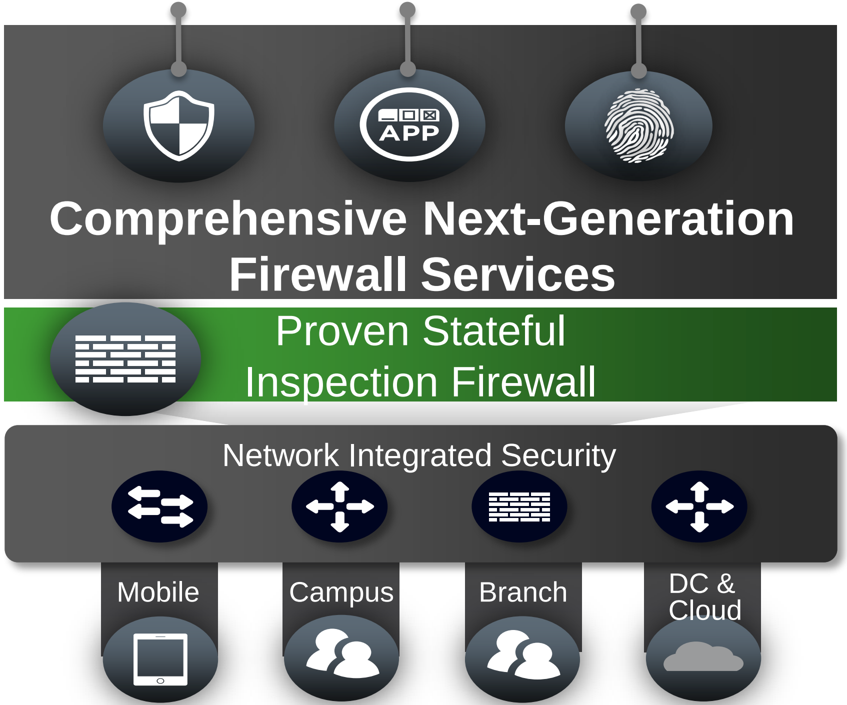


Visibility and Context

Next Generation FireWall

The ASA-X Next-Generation Firewall

Security Without Compromise


Comprehensive Next-Generation Firewall Services
Proven Stateful Inspection Firewall
Network Integrated Security
Mobile
Campus
Branch
DC & Cloud

The industry’s most widely deployed firewall

Largest global security footprint delivers the most comprehensive threat protection

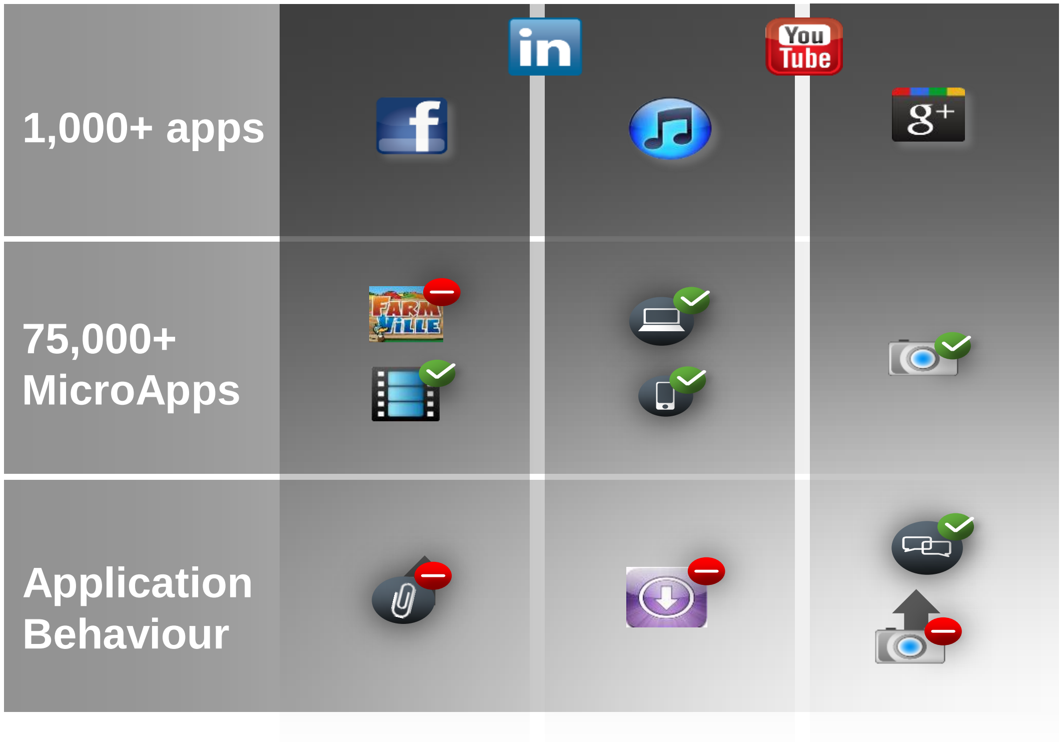
Leading-class VPN

Leading-class Web Security

#1 market share in IPS

Application Visibility and Control

Enforcing acceptable usage



1,000+ apps

75,000+ MicroApps

Application Behaviour

- Greatest control and visibility over mobile, collaborative, and web 2.0 applications
- Ensures security of (and from) port-hopping applications, such as Skype and BitTorrent

OpenAppID Overview

What is OpenAppID?

An open source application-focused detection language that enables users to create, share and implement custom application detection.

Key Advantages

- New simple language to detect apps
- Reduces dependency on vendor release cycles
- Build custom detections for new or specific (ex. Geo-based) app-based threats
- Easily engage and strengthen detector solutions
- Application-specific detail with security events

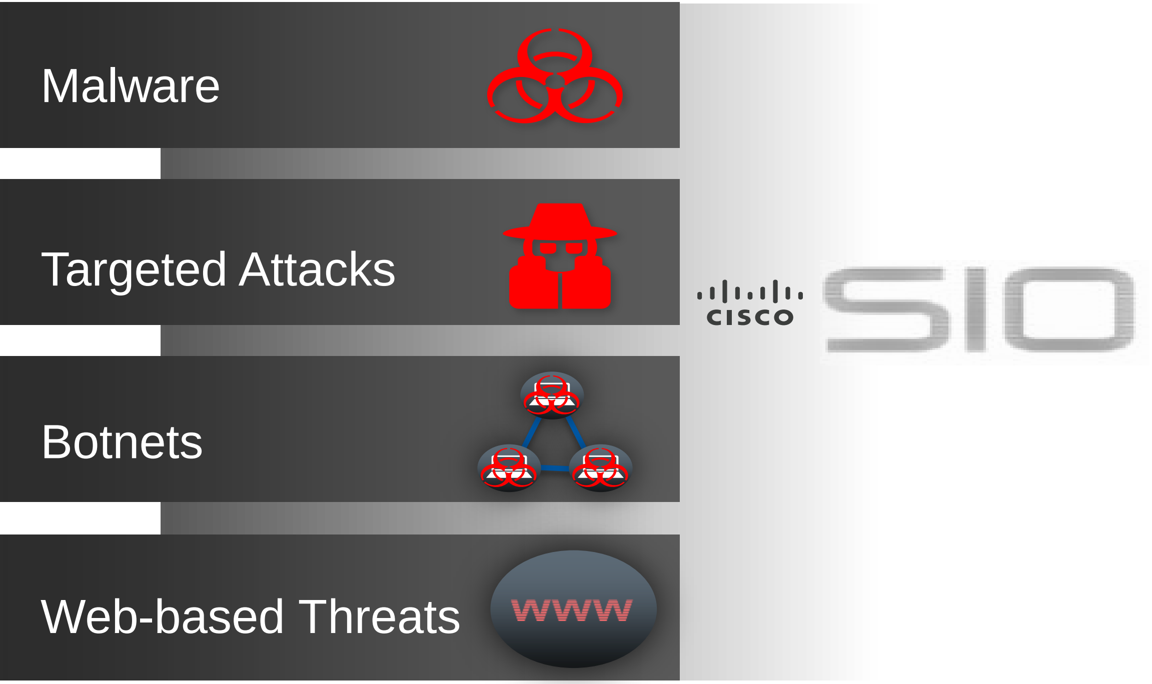
OpenAppID Deliverables at Launch

- OpenAppID Language Documentation
- A special Snort release engine with the OpenAppID preprocessor
  - Detect apps on network
  - Report usage stats
  - Block apps by policy
  - Snort rule language extensions to enable app specification
  - Include ‘App Context’ to IPS events
- Library of OpenAppID Detectors
  - > 1000 detectors contributed by Cisco
  - Extendable sample detectors

Available to community at Snort.org

Comprehensive Threat Protection

Stopping Threats Everywhere with ASA-X Next Generation Firewall

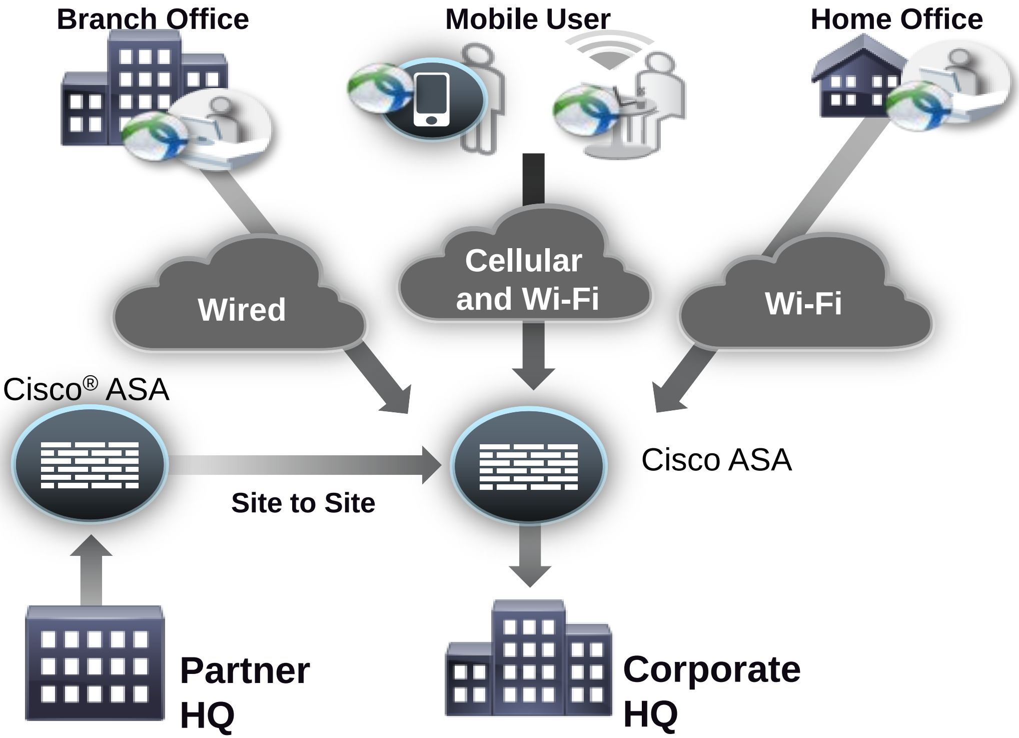


Reputation-based protection days before competition

- Only NGFW vendor with 3 dimensions of reputation protection
- Software-expandable security
  - Targeted attacks with IPS
  - Botnet filter
  - Cloud-based anti-malware

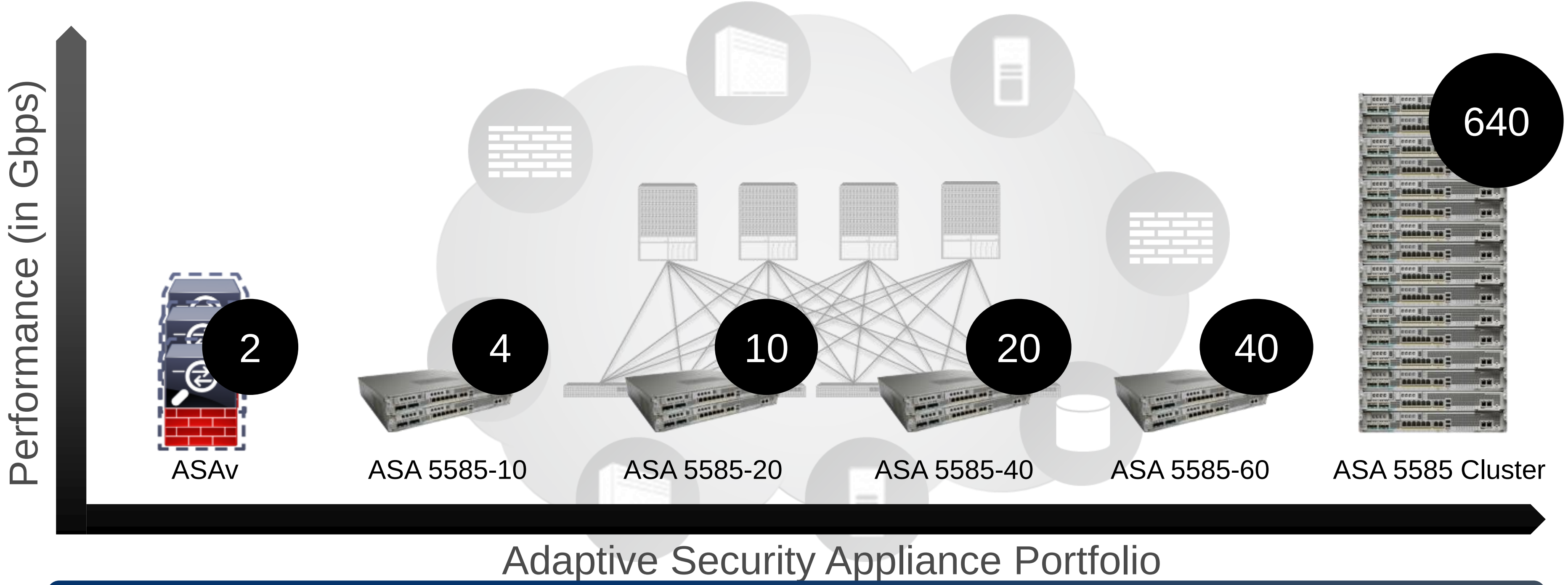
Secure VPN Connectivity

Solution Overview



- Simplified connectivity
- Supports the widest range of mobile devices in the industry
- Deployed on 150 million endpoints around the world

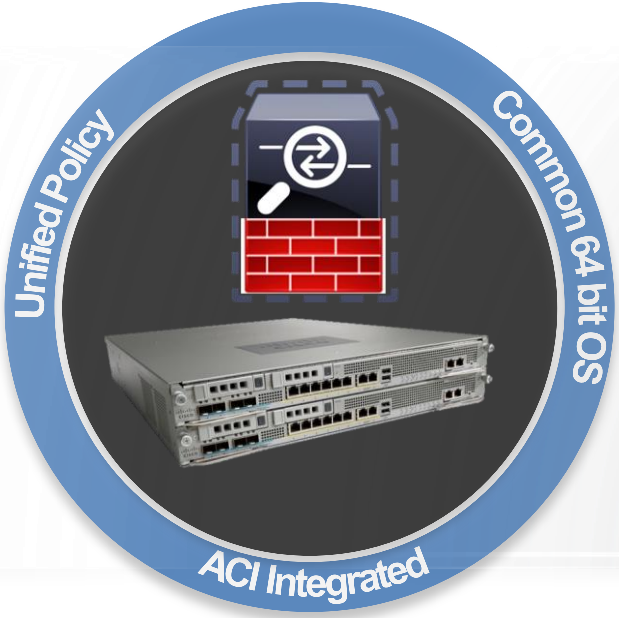
Cisco Adaptive Security Appliance in a Data Centre



Purpose-Built for Agility, Scale, Programmability, and Application Awareness

Cisco ONE Security Starts with the ASA

ASA



Virtual

vmware KVM

Xen Microsoft Hyper-V

ASAv

Full ASA Feature Set
Hypervisor Independent
Virtual Switch Agnostic
Dynamic Scalability

Physical

ASA 5585-X

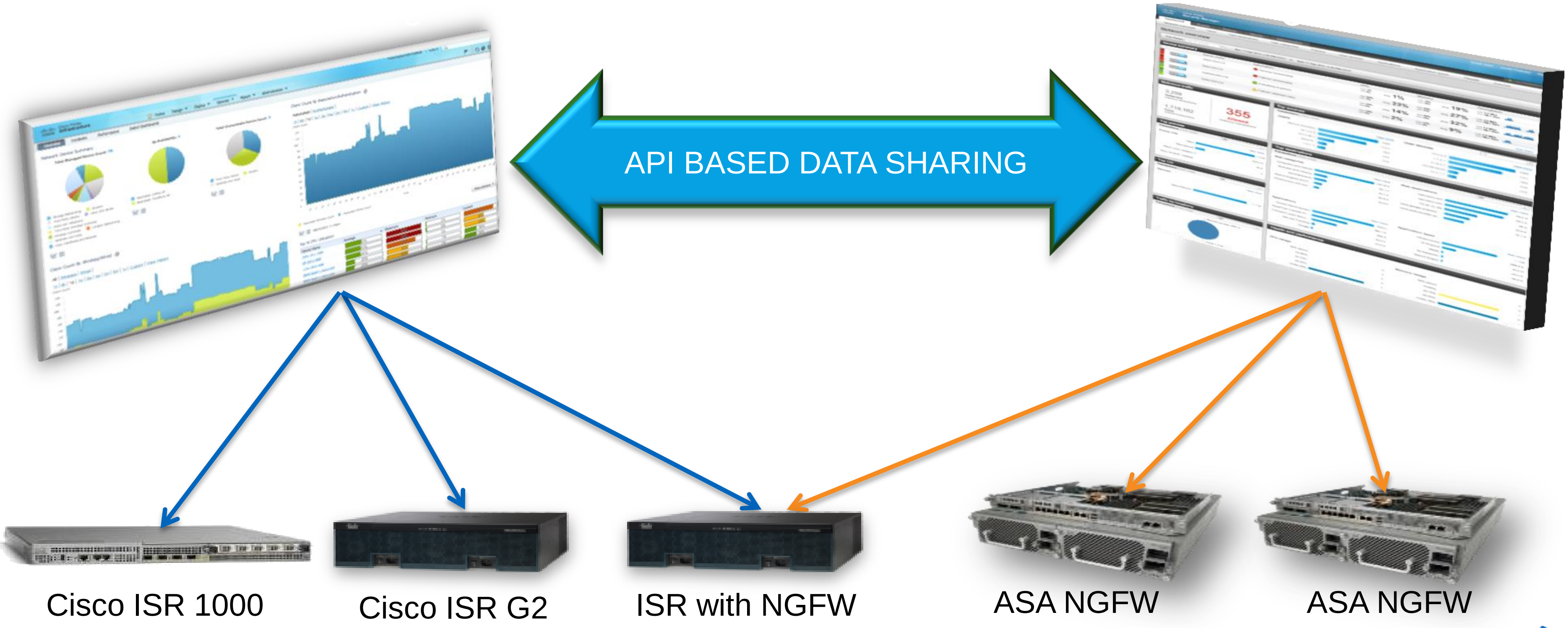
16 Way Clustering with
State Synchronisation
Scalable to **640Gbps**

Available in 1HCY14

Management Options

Product Offering (Cisco & SourceFire)	Management Option
ASA FW + FirePOWER (NGFW/NGIPS)	CSM + Defence Centre
ASA 5500-X + NGFW	PRSM or (CSM + PRSM)
ASA 5585 FW w/ Integrated IPS	CSM
ASA FW + FirePOWER (virtual and physical)	CSM + Defence Centre

Integration Strategy with Prime Infrastructure



API BASED DATA SHARING

Cisco ISR 1000

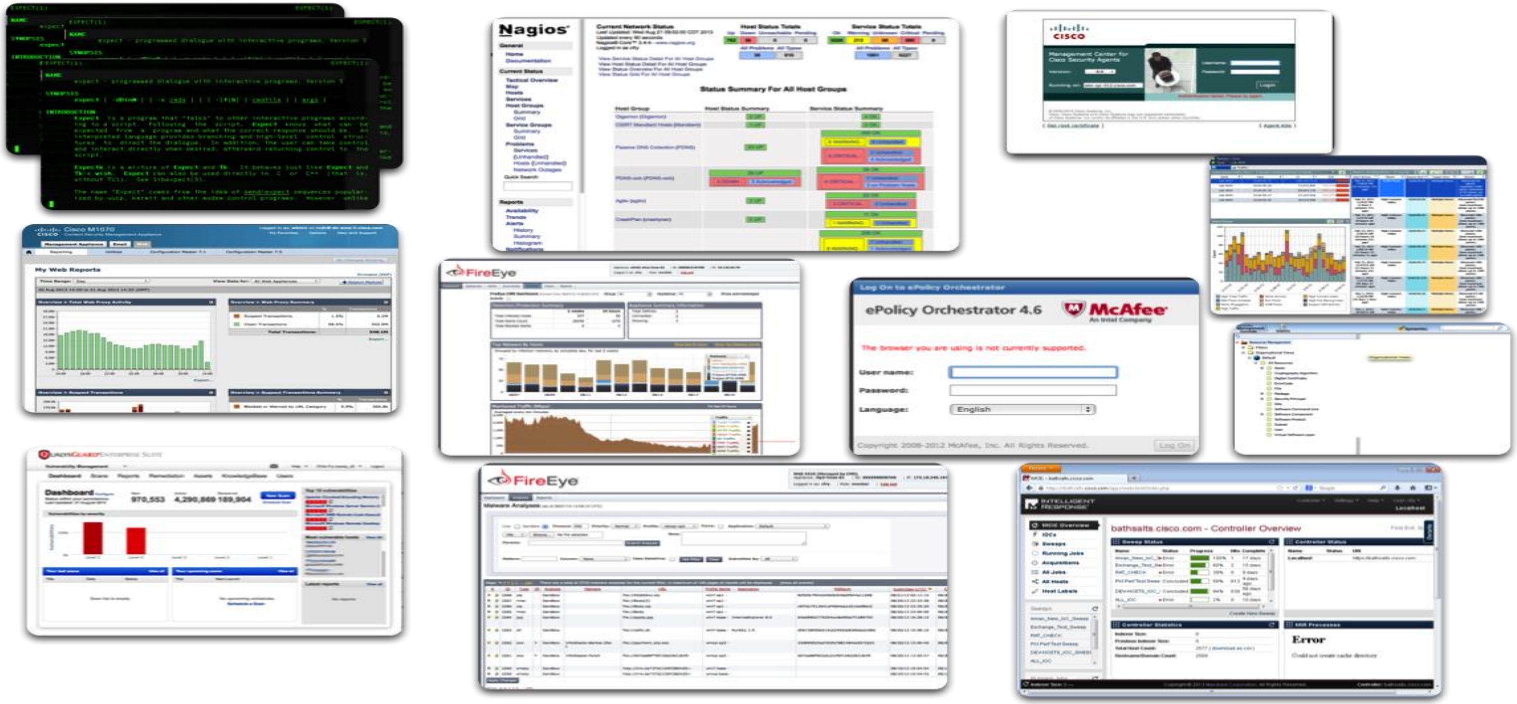
Cisco ISR G2

ISR with NGFW

ASA NGFW

ASA NGFW

Device and Policy Management: Today


Nagios
Status Summary For All Host Groups
Cisco M1070
My Web Reports
FireEye
Malware Analysis
Log On to ePolicy Orchestrator
ePolicy Orchestrator 4.6
McAfee
An Intel Company
User name:
Password:
Language:
English
Log On
Management Center for Cisco Security Agents
QualysGuard Enterprise Suite
Dashboard
Intelligent Response
bathsalts.cisco.com - Controller Overview

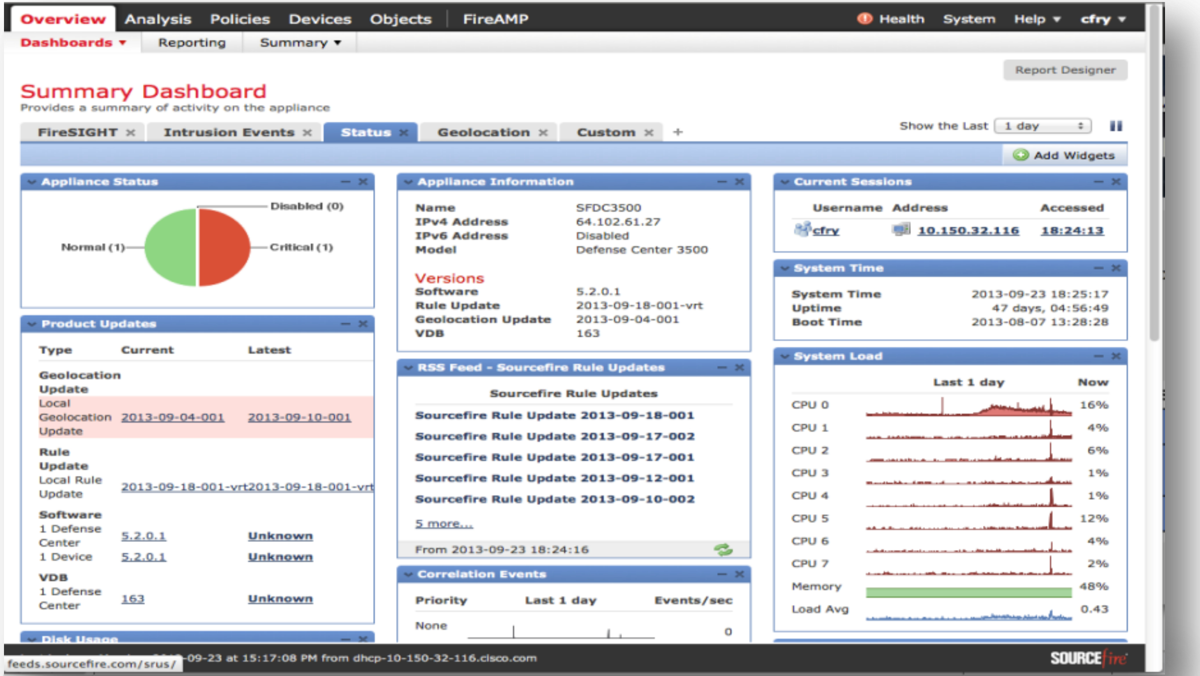
The browser you are using is not currently supported.

Copyright 2008-2012 McAfee, Inc. All Rights Reserved.

Error

Could not create cache directory

Device and Policy Management: Future



Summary Dashboard

Provides a summary of activity on the appliance

Appliance Status

Product Updates

Type	Current	Latest
Geolocation Update		
Local Geolocation Update	2013-09-04-001	2013-09-10-001
Rule Update		
Local Rule Update	2013-09-18-001-vrt	2013-09-18-001-vrt
Software		
1 Defense Center	5.2.0.1	Unknown
1 Device	5.2.0.1	Unknown
VDB		
1 Defense Center	163	Unknown

Disk Usage

Appliance Information

Name	SFDC3500
IPv4 Address	64.102.61.27
IPv6 Address	Disabled
Model	Defense Center 3500

Versions

Software	5.2.0.1
Rule Update	2013-09-18-001-vrt
Geolocation Update	2013-09-04-001
VDB	163

RSS Feed - Sourcefire Rule Updates

Sourcefire Rule Updates

- Sourcefire Rule Update 2013-09-18-001
- Sourcefire Rule Update 2013-09-17-002
- Sourcefire Rule Update 2013-09-17-001
- Sourcefire Rule Update 2013-09-12-001
- Sourcefire Rule Update 2013-09-10-002

5 more...

From 2013-09-23 18:24:16

Correlation Events

Priority	Last 1 day	Events/sec
None		0

Current Sessions

Username	Address	Accessed
cfry	10.150.32.116	18:24:13

System Time

System Time	2013-09-23 18:25:17
Uptime	47 days, 04:56:49
Boot Time	2013-08-07 13:28:28

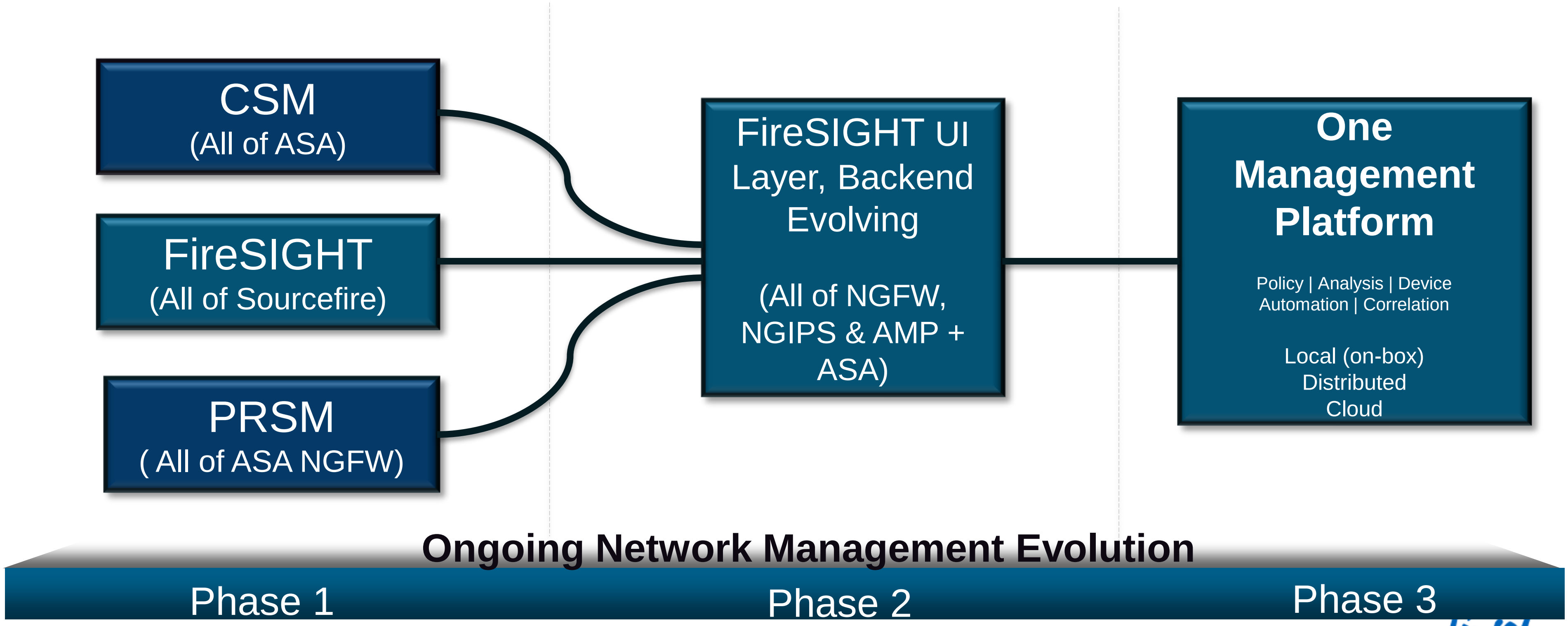
System Load

	Last 1 day	Now
CPU 0		16%
CPU 1		4%
CPU 2		6%
CPU 3		1%
CPU 4		1%
CPU 5		12%
CPU 6		4%
CPU 7		2%
Memory		48%
Load Avg		0.43

feeds.sourcefire.com/srus/ -09-23 at 15:17:08 PM from dhcp-10-150-32-116.cisco.com

Converging the Management

Unifying “the best of“ three management systems into one over time



CSM
(All of ASA)

FireSIGHT
(All of Sourcefire)

PRSM
(All of ASA NGFW)

FireSIGHT UI Layer, Backend Evolving

(All of NGFW, NGIPS & AMP + ASA)

One Management Platform

Policy | Analysis | Device Automation | Correlation

Local (on-box)
Distributed
Cloud

Ongoing Network Management Evolution

Phase 1

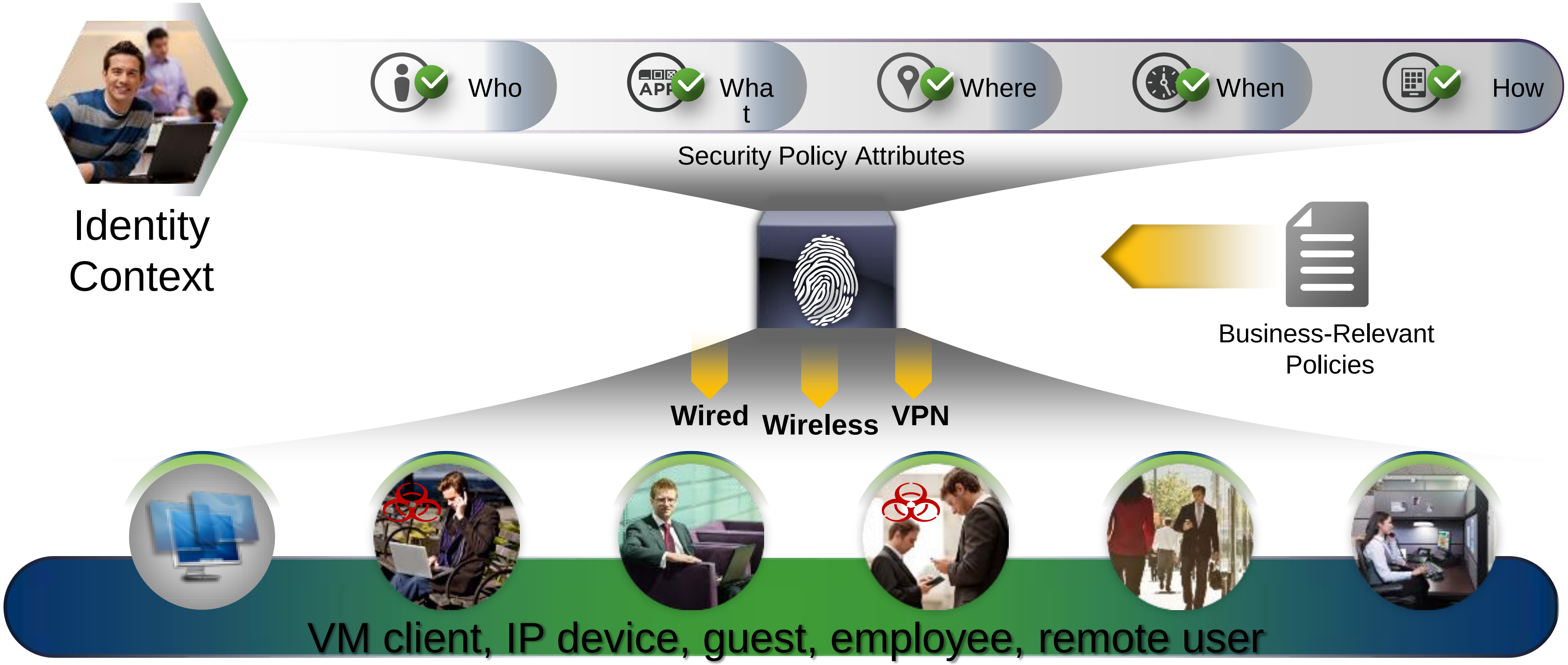
Phase 2

Phase 3

ISE ISE ISE BABY

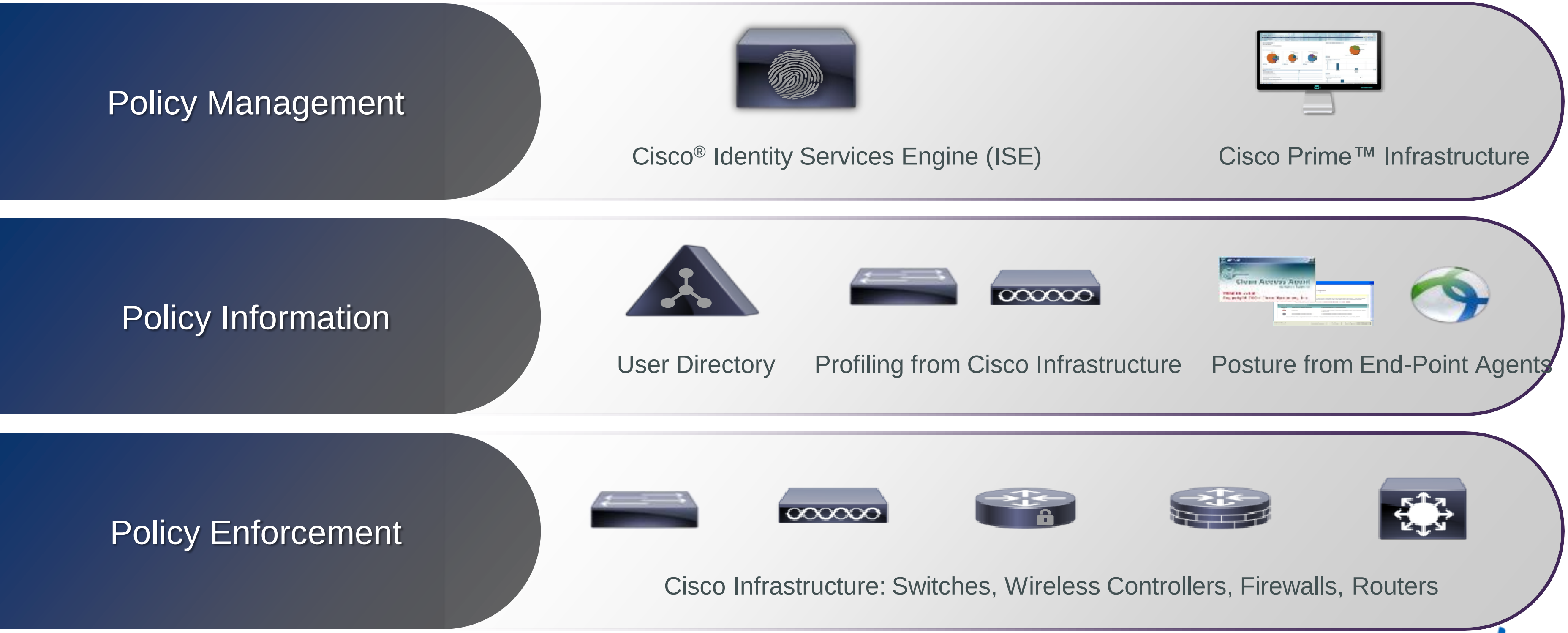
Cisco Identity Services Engine (ISE)

All-in-One Enterprise Policy Control


Who
APP
Wha t
Where
When
How
Security Policy Attributes
Identity Context
Business-Relevant Policies
Wired
Wireless
VPN
VM client, IP device, guest, employee, remote user

Replaces AAA & RADIUS, NAC, guest mgmt & device identity servers

Secure Access Enabled by Cisco ISE



Policy Management

Cisco® Identity Services Engine (ISE)

Cisco Prime™ Infrastructure

Policy Information

User Directory

Profiling from Cisco Infrastructure

Posture from End-Point Agents

Policy Enforcement

Cisco Infrastructure: Switches, Wireless Controllers, Firewalls, Routers

How Cisco ISE is Used Today

BYOD

Users connect safely to the Internet quickly
and easily

GUEST ACCESS

It's easy to provide
guests limited time and resource access

SECURE ACCESS ON WIRED, WIRELESS, AND VPN

Control with one policy across wired, wireless, and remote infrastructure

CISCO TRUSTSEC NETWORK POLICY

Rules written in business terms control access

Introducing Cisco TrustSec

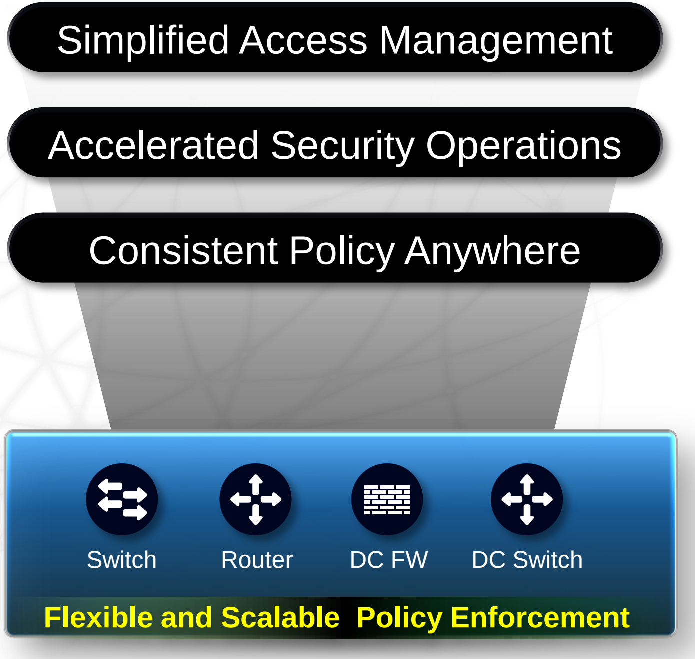
Policy-Defined Segmentation based on business policy

Desired Policy

- Who can talk to whom
- Who can access protected assets
- How systems can talk to other systems

Protected Assets

Source	Production Servers	Development Servers	Internet Access
Employee (managed asset)	PERMIT	DENY	PERMIT
Employee (Registered BYOD)	PERMIT	DENY	PERMIT
Employee (Unknown BYOD)	DENY	DENY	PERMIT
ENG VDI System	DENY	PERMIT	PERMIT



Simplified Access Management

Accelerated Security Operations

Consistent Policy Anywhere

Flexible and Scalable Policy Enforcement

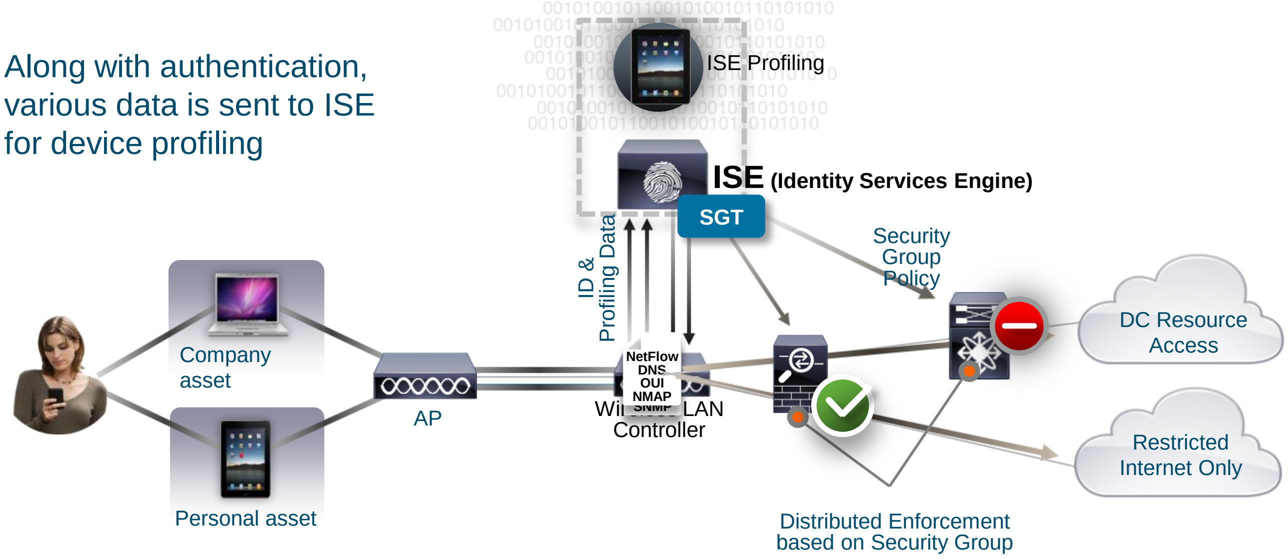
TrustSec in Action

Device Type: Apple iPAD
User: Mary
Group: Employee
Corporate Asset: No

Classification Result:

Personal Asset SGT

Along with authentication, various data is sent to ISE for device profiling



Classify Propagate Enforce

TrustSec: Taking Complexity out of Network Security

Simplified Access Management

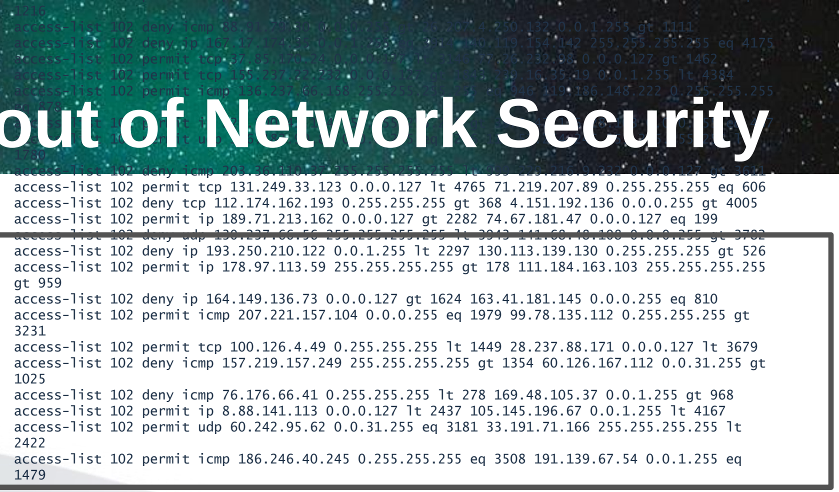
- Manages policies using plain language
- Control access to critical assets by business role
- Maintain policy compliance

Accelerated Security Operations

- Quickly onboard servers
- Speed-up adds, moves and changes, eliminate many
- Automate FW & ACL administration

Consistent Policy Anywhere

- Segments networks using central policy management
- Enforces policy on wired, wireless & VPN
- Scales to remote, branch, campus & data centre



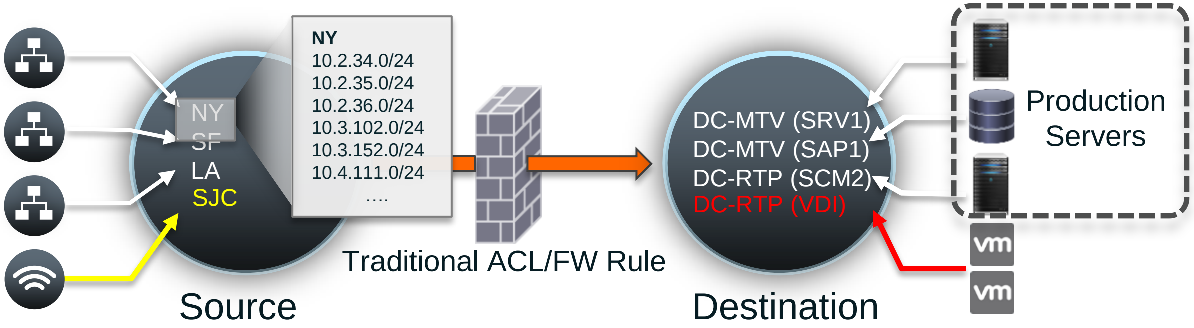
```
1216
access-list 102 deny icmp 88.91.[illegible] 207.4.250.132 0.0.1.255 gt 1111
access-list 102 deny ip 167.17.174.35 0.0.1.255 [illegible] 140.119.154.142 255.255.255.255 eq 4175
access-list 102 permit tcp 37.85.170.24 0.0.0.127 [illegible] 77.26.232.98 0.0.0.127 gt 1462
access-list 102 permit tcp 155.237.22.232 0.0.0.127 gt [illegible] 239.16.35.19 0.0.1.255 lt 4384
access-list 102 permit icmp 136.237.66.158 255.255.255.255 eq 946 119.186.148.222 0.255.255.255
eq 878
access-list 102 permit [illegible]
access-list 102 permit udp [illegible]
1780
access-list 102 deny icmp 203.36.110.37 255.255.255.255 lt 999 229.216.9.232 0.0.0.127 gt 3611
access-list 102 permit tcp 131.249.33.123 0.0.0.127 lt 4765 71.219.207.89 0.255.255.255 eq 606
access-list 102 deny tcp 112.174.162.193 0.255.255.255 gt 368 4.151.192.136 0.0.0.255 gt 4005
access-list 102 permit ip 189.71.213.162 0.0.0.127 gt 2282 74.67.181.47 0.0.0.127 eq 199
access-list 102 deny udp 130.237.66.56 255.255.255.255 lt 3943 141.68.48.108 0.0.0.255 gt 3782
access-list 102 deny ip 193.250.210.122 0.0.1.255 lt 2297 130.113.139.130 0.255.255.255 gt 526
access-list 102 permit ip 178.97.113.59 255.255.255.255 gt 178 111.184.163.103 255.255.255.255
gt 959
access-list 102 deny ip 164.149.136.73 0.0.0.127 gt 1624 163.41.181.145 0.0.0.255 eq 810
access-list 102 permit icmp 207.221.157.104 0.0.0.255 eq 1979 99.78.135.112 0.255.255.255 gt
3231
access-list 102 permit tcp 100.126.4.49 0.255.255.255 lt 1449 28.237.88.171 0.0.0.127 lt 3679
access-list 102 deny icmp 157.219.157.249 255.255.255.255 gt 1354 60.126.167.112 0.0.31.255 gt
1025
access-list 102 deny icmp 76.176.66.41 0.255.255.255 lt 278 169.48.105.37 0.0.1.255 gt 968
access-list 102 permit ip 8.88.141.113 0.0.0.127 lt 2437 105.145.196.67 0.0.1.255 lt 4167
access-list 102 permit udp 60.242.95.62 0.0.31.255 eq 3181 33.191.71.166 255.255.255.255 lt
2422
access-list 102 permit icmp 186.246.40.245 0.255.255.255 eq 3508 191.139.67.54 0.0.1.255 eq
1479
```

Traditional Security Policy

Protected Assets

Source	Production Servers	Development Servers	Internet Access
Employee (managed asset)	PERMIT	DENY	PERMIT
Employee (Registered BYOD)	PERMIT	DENY	PERMIT
Employee (Unknown BYOD)	DENY	DENY	PERMIT
ENG VDI System	DENY	PERMIT	PERMIT

Traditional Security Administration



```
permit NY  to SRV1 for HTTPS
deny   NY  to SAP2 for SQL
deny   NY  to SCM2 for SSH
permit SF  to SRV1 for HTTPS
deny   SF  to SAP1 for SQL
deny   SF  to SCM2 for SSH
permit LA  to SRV1 for HTTPS
deny   LA  to SAP1 for SQL
deny   LA  to SAP  for SSH
```

ACL for 3 source objects & 3 destination objects

A Global Bank dedicated 24 global resources to manage Firewall rules currently

```
Permit SJC to SRV1 for HTTPS
deny   SJC to SAP1 for SQL
deny   SJC to SCM2 for SSH
```

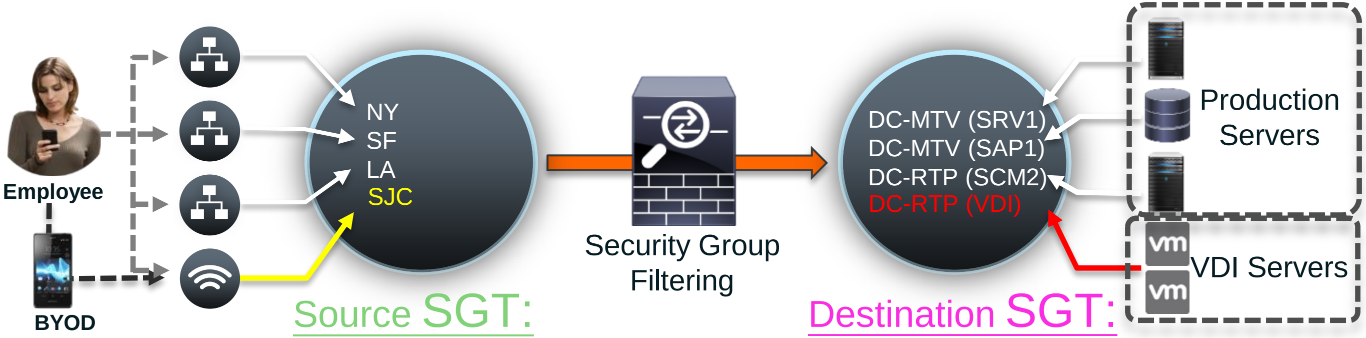
Adding source Object

```
permit NY  to VDI  for RDP
deny   SF  to VDI  for RDP
deny   LA  to VDI  for RDP
deny   SJC to VDI  for RDP
```

Adding destination Object

Complex Task and High OPEX continues

Security Administration with TrustSec



Source SGT:

Employee (10)

BYOD (200)

Destination SGT:

Production_Servers (50)

VDI (201)

DC Access Control & Segmentation

Policy enforced from end user device to data centre resources

“Visibility and Control”

“BYOD–
Bring Your
Own Device”

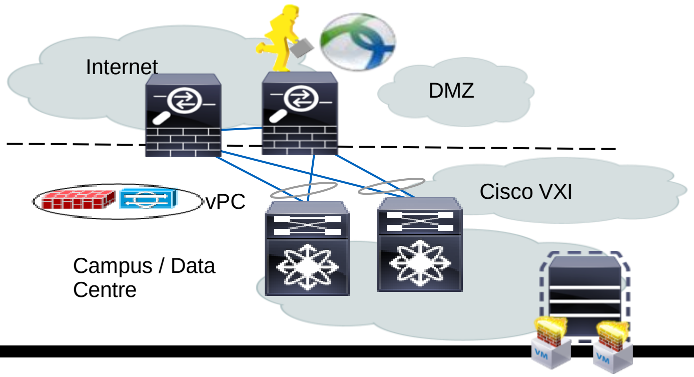
“Data Centre”

Cisco TrustSec – Policy Control for any user, with any device, anywhere

Secure DC: Traditional Use Cases

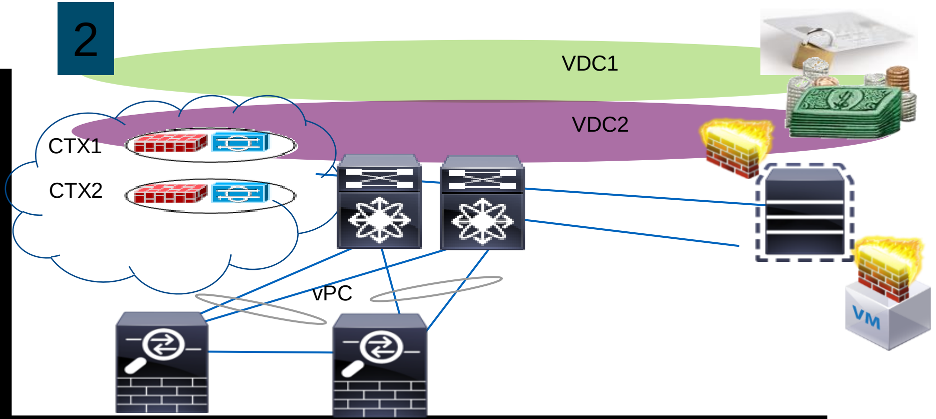
1

Secure Internal Zone From External Zone



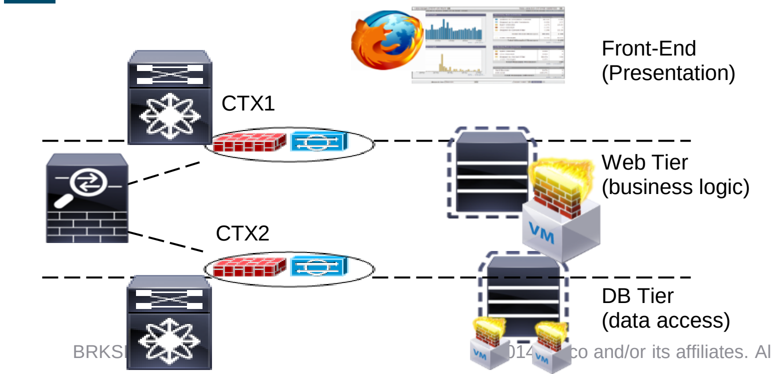
2

Secure Data in a Compliance Scenario [PCI, FISMA, HIPAA, etc.]



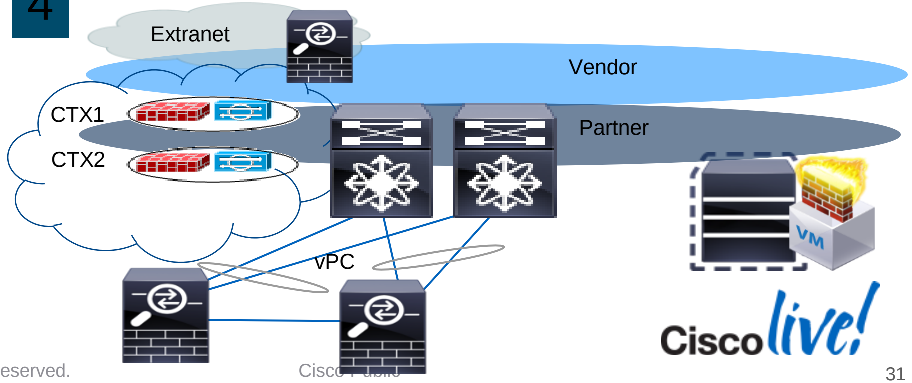
3

Secure Application Tiers

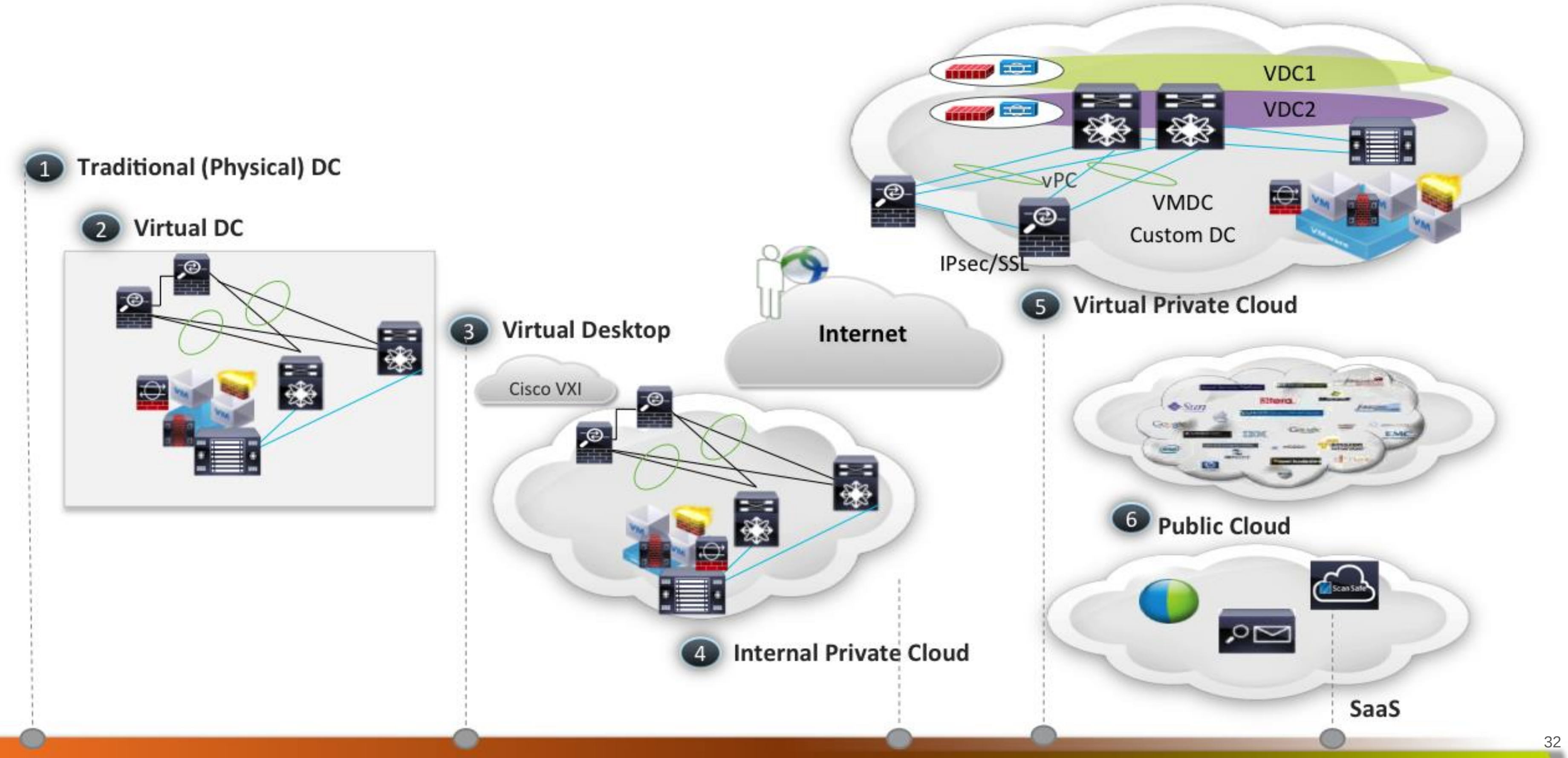


4

Secure Multi-Tenancy



Secure DC : Evolving Deployment Use Cases



The Evolving Data Centre Architecture

Aggregation Layer

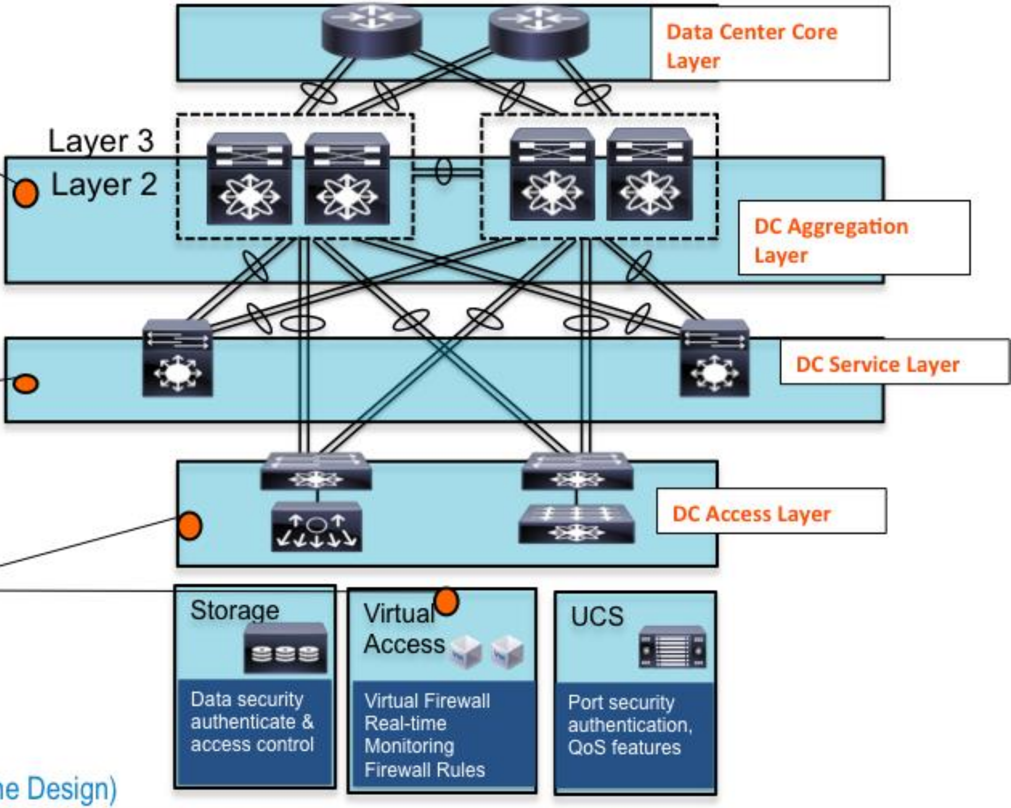
- Workload is localized to the Aggregation Block
- Centralized point for ingress and egress data center flows
- Can be demarcation point for L2 and L3
- Services can be scaled as data center grows

Services Layer (option)

- Additional services location for server farm specific protection / optimization
- Services localized to the applications running on the servers connected to the physical pod – SLB, Monitors, etc.
- Offloads port utilization from Aggregation Layer

Virtual Network & Access

- Physical and virtual form factor for server connectivity
- Top of rack provides port density for server connections
- Merging point between physical and virtual networks



Data Center Core Layer
Layer 3
Layer 2
DC Aggregation Layer
DC Service Layer
DC Access Layer
Storage
Data security authenticate & access control
Virtual Access
Virtual Firewall Real-time Monitoring Firewall Rules
UCS
Port security authentication, QoS features

- **Goal #1:** Understand the current approach (De-Couple the Elements of the Design)
- **Goal #2:** Understand the options we have to build a more efficient architecture (Re-assemble the elements into a more flexible design)

The Evolving Data Centre Architecture

Adding Layered Security Services

Data Center Edge

- Physical Delineation for all ingress and egress into the 'CORE' of the DC – Traditional Security Models apply to North-South Protection

Aggregation Layer

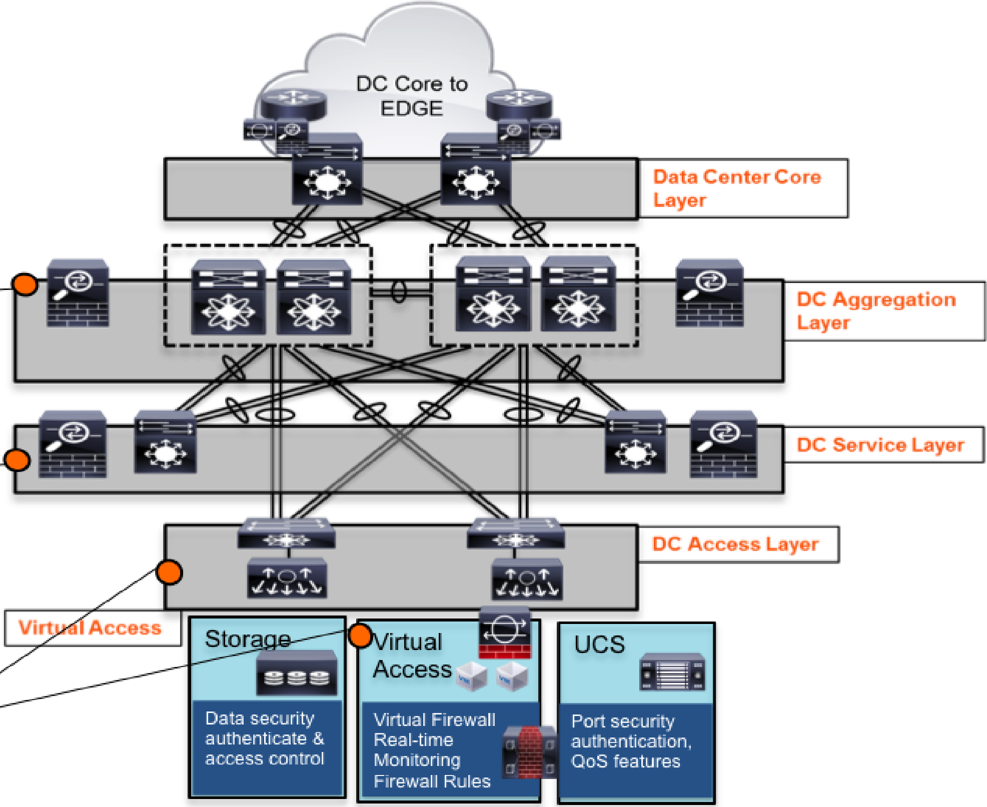
- Initial filter for all ingress and egress to DC services & compute - "North-South" protection
- Stateful filtering and logging for all ingress and egress traffic flows
- Physical appliances can be virtualized and applied to server enclaves

Services Layer (option)

- Additional services location for server farm specific protection and other potential zones

Virtual Network & Access

- Virtual firewall, zone/enclave based filtering
- IP-Based Access Control Lists
- VM attribute-based policies – Should Follow VM


DC Core to EDGE
Data Center Core Layer
DC Aggregation Layer
DC Service Layer
DC Access Layer
Virtual Access
Storage
Data security authenticate & access control
Virtual Access
Virtual Firewall Real-time Monitoring Firewall Rules
UCS
Port security authentication, QoS features

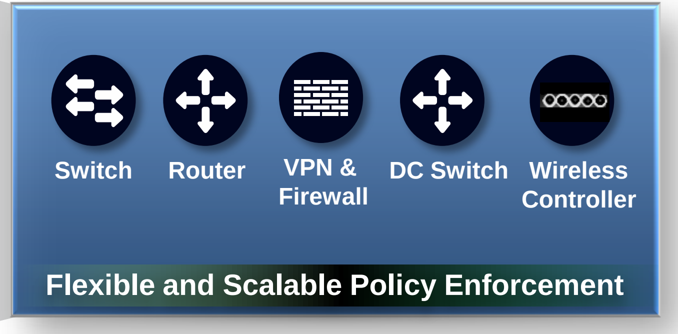
Announcing Cisco TrustSec 4.0

Open Specification for Secure Access and Network Segmentation

Business Asset Mapped to Access Policy

Source/Destination	Employee	Email	Finance	Inte
Employee	Malware ACL	Permit	Deny	Permit
Executive	Malware ACL	Permit	Permit	Permit
BYOD	Deny	Permit	Deny	Permit
Guest	Deny	Deny	Deny	Permit

Policy Enforced Across Network

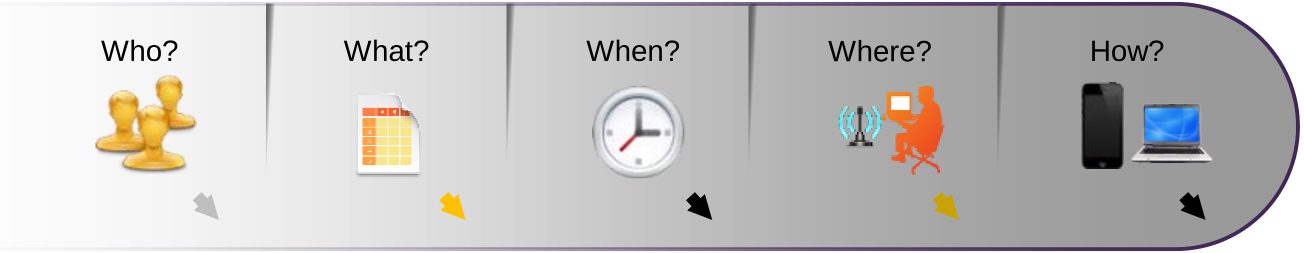


TrustSec 4.0 supports End-to-End Data Centre, Campus and Branch Deployments

Secure Access

Role-Based, Dynamic Provisioning

1 Context-Aware Classification

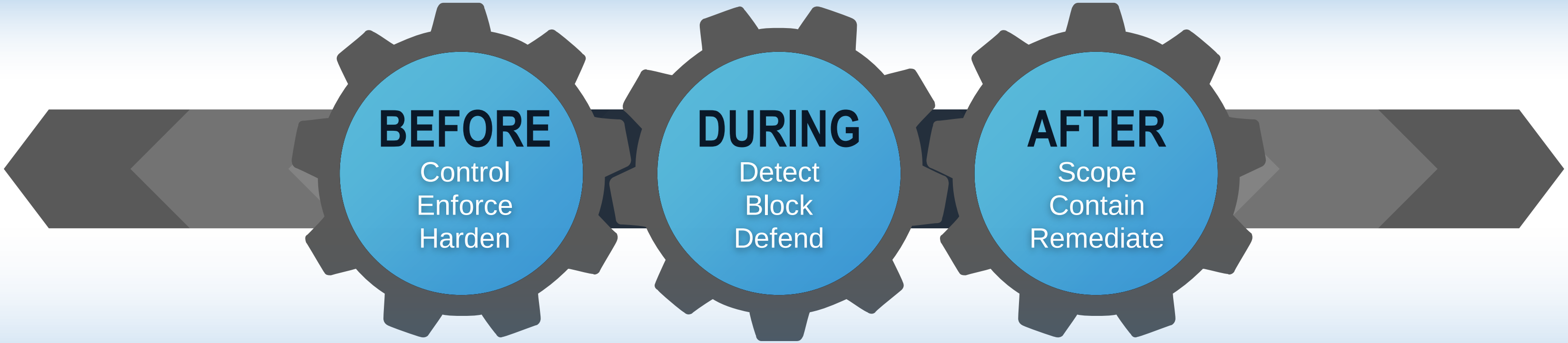


2 Context-Aware Policy

3 Enforcement

Cisco and Sourcefire - Better Together

Attack Continuum



BEFORE
Control
Enforce
Harden

DURING
Detect
Block
Defend

AFTER
Scope
Contain
Remediate

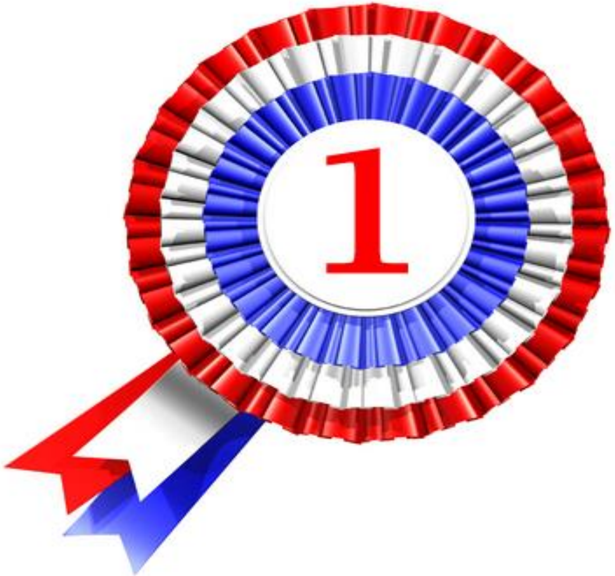
Firewall	VPN	NGIPS
NGFW	UTM	Web Security
NAC + Identity Services		Email Security

Visibility and Context

Next Generation IPS

What Makes Sourcefire NGIPS Unique?

- Context
- Speed
- Accuracy
- Flexibility
- Value



Context is Everything

Event + network & user context

Event:	Attempted Privilege Gain
Target:	96.16.242.135 (vulnerable)
Host OS:	Blackberry
Apps:	Mail, Browswer, Twitter
Location:	Kirrabilli, AUS
User ID:	tabbot
Full Name:	Tony Abbot
Department:	Executive Office

Event + network context

Event:	Attempted Privilege Gain
Target:	96.16.242.135 (vulnerable)
Host OS:	Blackberry
Apps:	Mail, Browser, Twitter
Location:	Whitehouse, US

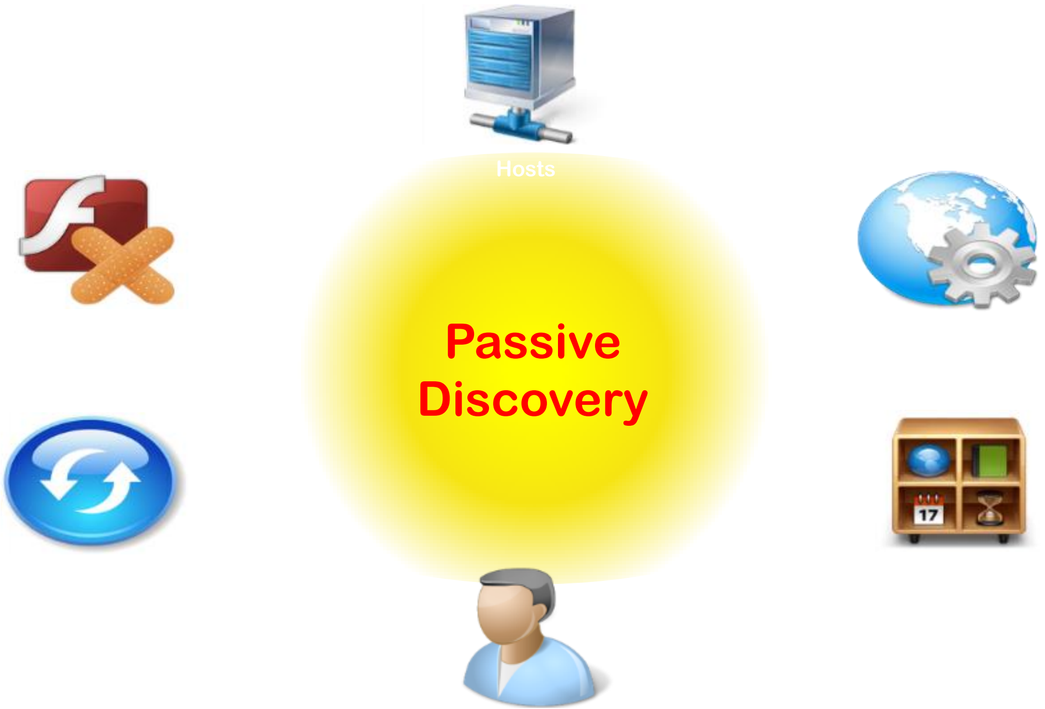
Event

Event:	Attempted Privilege Gain
Target:	96.16.242.135

Context has the capability of *fundamentally changing* the interpretation of your event data.

First, you must know your estate

You cannot protect what you do not know!

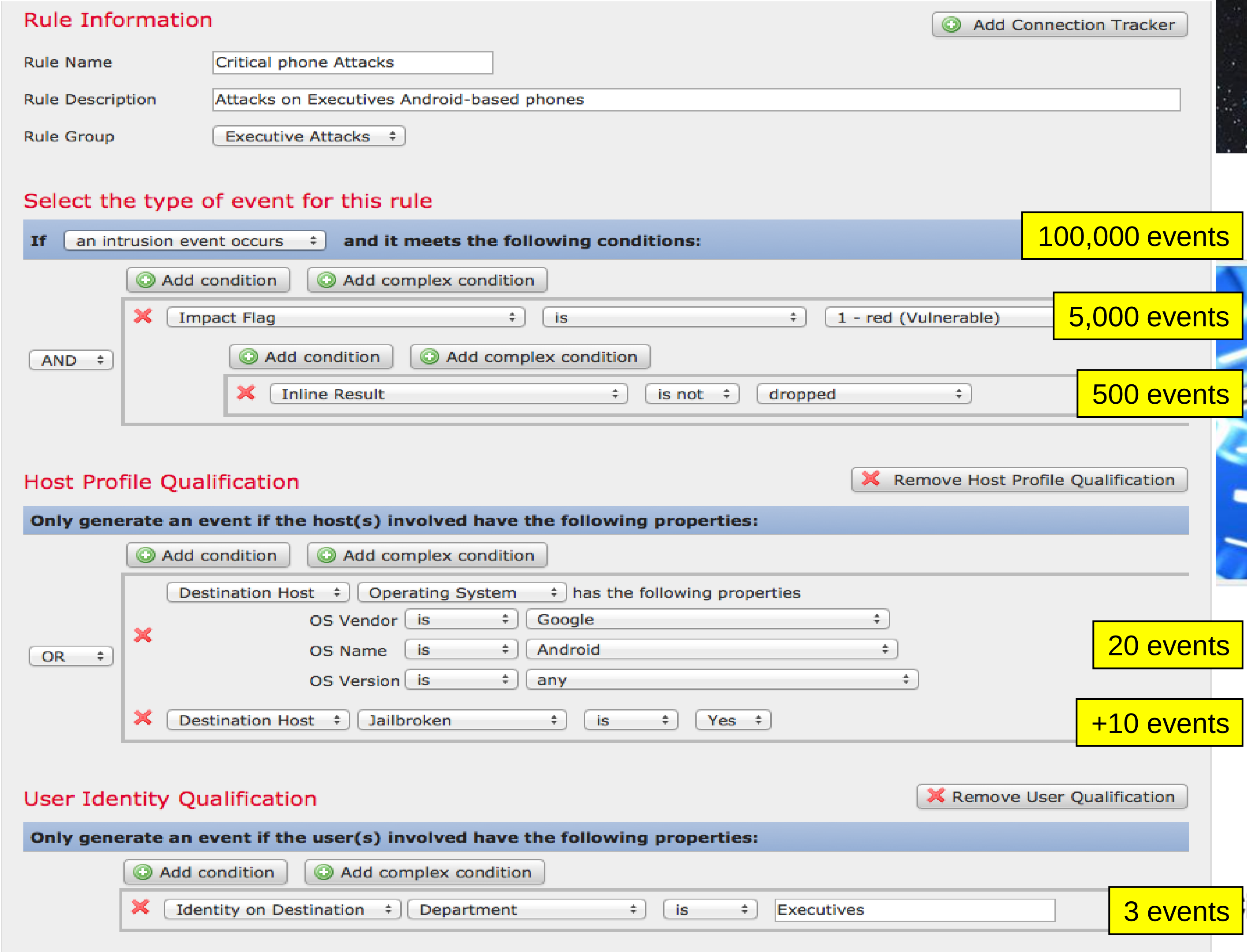


fireSIGHT™

All the time
In real-time

Spee

- Sens
  - →
  - →
  - →
- Anal
  - →
  - →
  - →
  - →
- Rem



Rule Information

Add Connection Tracker

Rule Name	Critical phone Attacks
Rule Description	Attacks on Executives Android-based phones
Rule Group	Executive Attacks

Select the type of event for this rule

If an intrusion event occurs **and it meets the following conditions:**

Add condition | Add complex condition

AND
- Impact Flag is 1 - red (Vulnerable)
- Add condition | Add complex condition
  - Inline Result is not dropped

Host Profile Qualification

Remove Host Profile Qualification

Only generate an event if the host(s) involved have the following properties:

Add condition | Add complex condition

OR
- Destination Host Operating System has the following properties
  - OS Vendor is Google
  - OS Name is Android
  - OS Version is any
- Destination Host Jailbroken is Yes

User Identity Qualification

Remove User Qualification

Only generate an event if the user(s) involved have the following properties:

Add condition | Add complex condition

- Identity on Destination Department is Executives

100,000 events

5,000 events

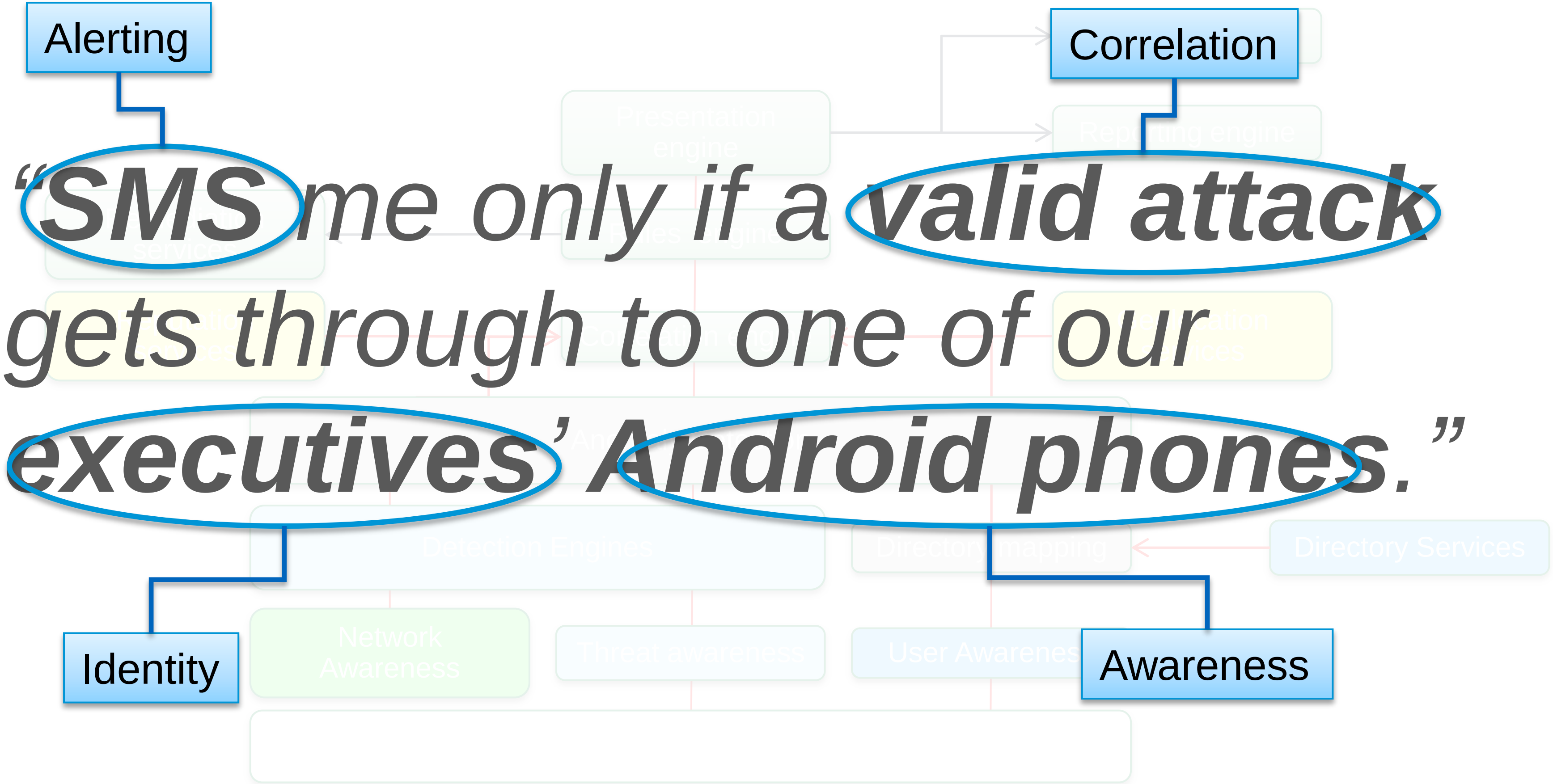
500 events

20 events

+10 events

3 events

ciscolive!



*“**SMS** me only if a **valid attack** gets through to one of our **executives’ Android phones**.”*

Alerting

Correlation

Identity

Awareness

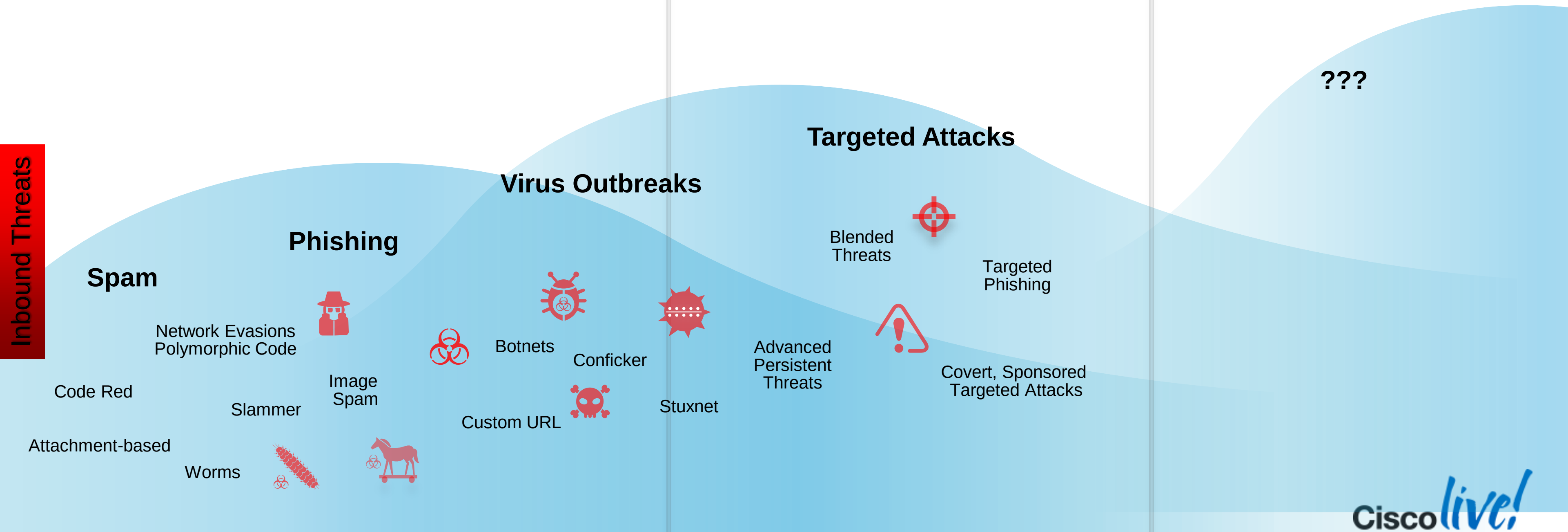
Email and Content Security

Email Threat Landscape Evolution: Inbound

HIGH VOLUME
LOW $ VALUE
Past

LOW VOLUME
HIGH $ VALUE
Today

?
Tomorrow



Email Threat Landscape Evolution: Outbound

Outbound

Usage

LOW VOLUME
LOW $ IMPACT
Past

Customer asset loss

Compliance

HIPAA

State regulations

PCI

Credit card numbers

Brand

Social security numbers

Access email only
from behind
corporate firewall

HIGH VOLUME
HIGH $ IMPACT
Today

Intellectual property

Trade secrets

Data breaches

Corporate espionage

Legal documents

Product-planning documents

Access email
anywhere, anytime

?

Tomorrow

Changing legislation

European Union laws

State laws

Federal laws

Province laws

By 2015, access
from over 7B
mobile devices

Tackle the Most Advanced Threats with Cisco Email Security Solutions

Solutions

Threat Defence

Data Security

Strengths

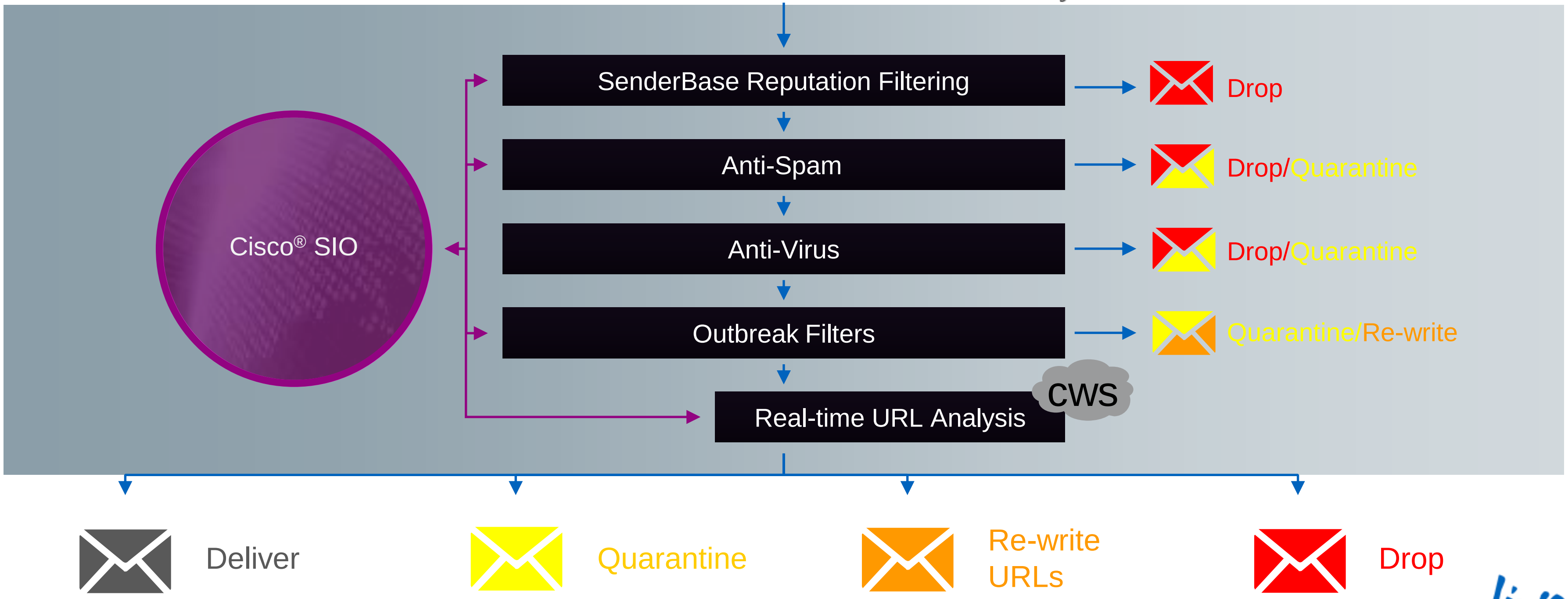
Best performance

Lowest TCO

Future focus

Cisco Email Security Threat Defence

Complete Inbound Protection



Cisco® SIO

SenderBase Reputation Filtering → Drop

Anti-Spam → Drop/Quarantine

Anti-Virus → Drop/Quarantine

Outbreak Filters → Quarantine/Re-write

Real-time URL Analysis

CWS

Deliver

Quarantine

Re-write URLs

Drop

Cisco Security Intelligence Operations (SIO)

Outstanding cloud-based global threat intelligence

24x7x365
operations

40+
languages

Email

Devices

Web

IPS

Networks

Endpoints

Visibility

1.6 million
global sensors

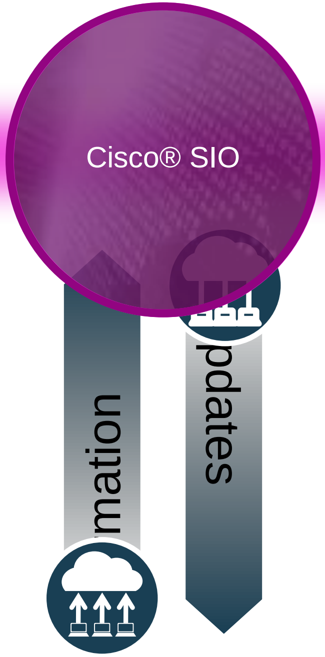
35%
worldwide email traffic

100 TB
of data received per day

13 billion
web requests

150 million+
deployed endpoints

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



600+
engineers, technicians, and researchers

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

Cisco CWS

Cisco IPS

Cisco AnyConnect®

Cisco ESA

Cisco ASA

Cisco WSA

Control

3- to 5-
minute updates

200+
parameters tracked

5,500+
IPS signatures produced

70+
publications produced

8 million+
rules per day

Cisco SenderBase: Email Reputation Database

Threat Intelligence

- Over 1.6M global devices
- Historical library of 40,000 threats
- 35% of global email traffic seen per day
- 13B+ Worldwide web requests seen per day
- 200+ parameters tracked
- Multi-vector visibility

Benefits

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

Spam Traps

Complaint Reports

IP Blacklists and Whitelists

Message Composition Data

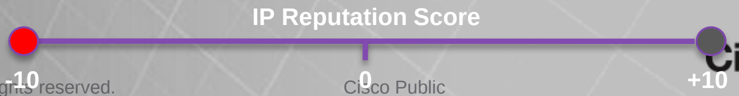
Compromised Host Lists

Website Composition Data

Global Volume Data

Domain Blacklist and Safelists

Other Data



Threat Operations Centre

Security Expertise

AMP and Sourcefire security intelligence
VRT Powered: Feeds all our systems

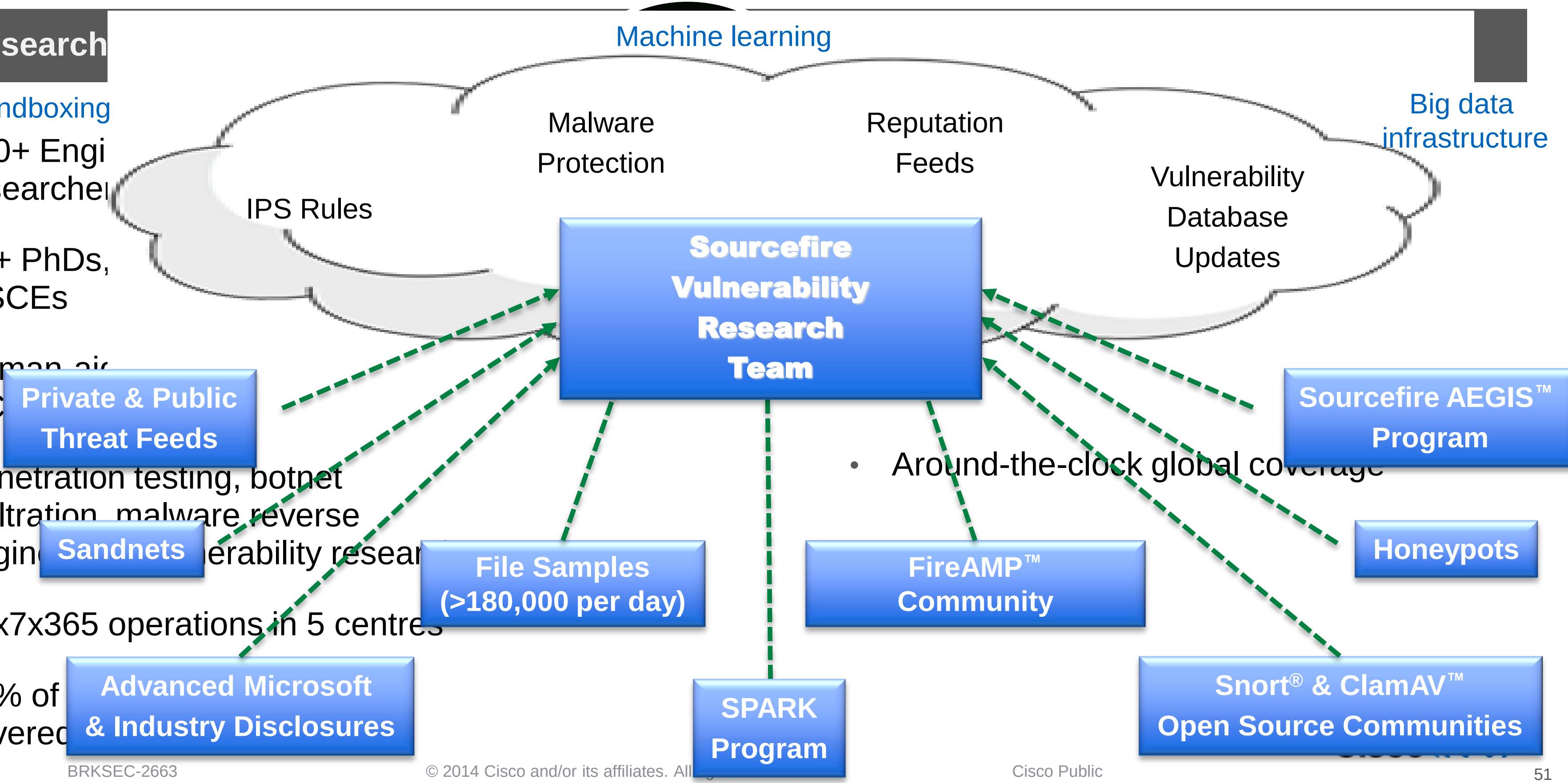
Research

Sandboxing

- 600+ Engi researche
- 80+ PhDs, MSCEs
- Human aic QC
- Penetration testing, botnet infiltration, malware reverse engin erability resear
- 24x7x365 operations in 5 centres
- 95% of covered
- Around-the-clock global coverage

Machine learning

Big data infrastructure


IPS Rules
Malware Protection
Reputation Feeds
Vulnerability Database Updates
Sourcefire Vulnerability Research Team
Private & Public Threat Feeds
Sandnets
File Samples (>180,000 per day)
Advanced Microsoft & Industry Disclosures
SPARK Program
FireAMP™ Community
Snort® & ClamAV™ Open Source Communities
Honeypots
Sourcefire AEGIS™ Program

Dynamic Updates

Automated Defence

Updates

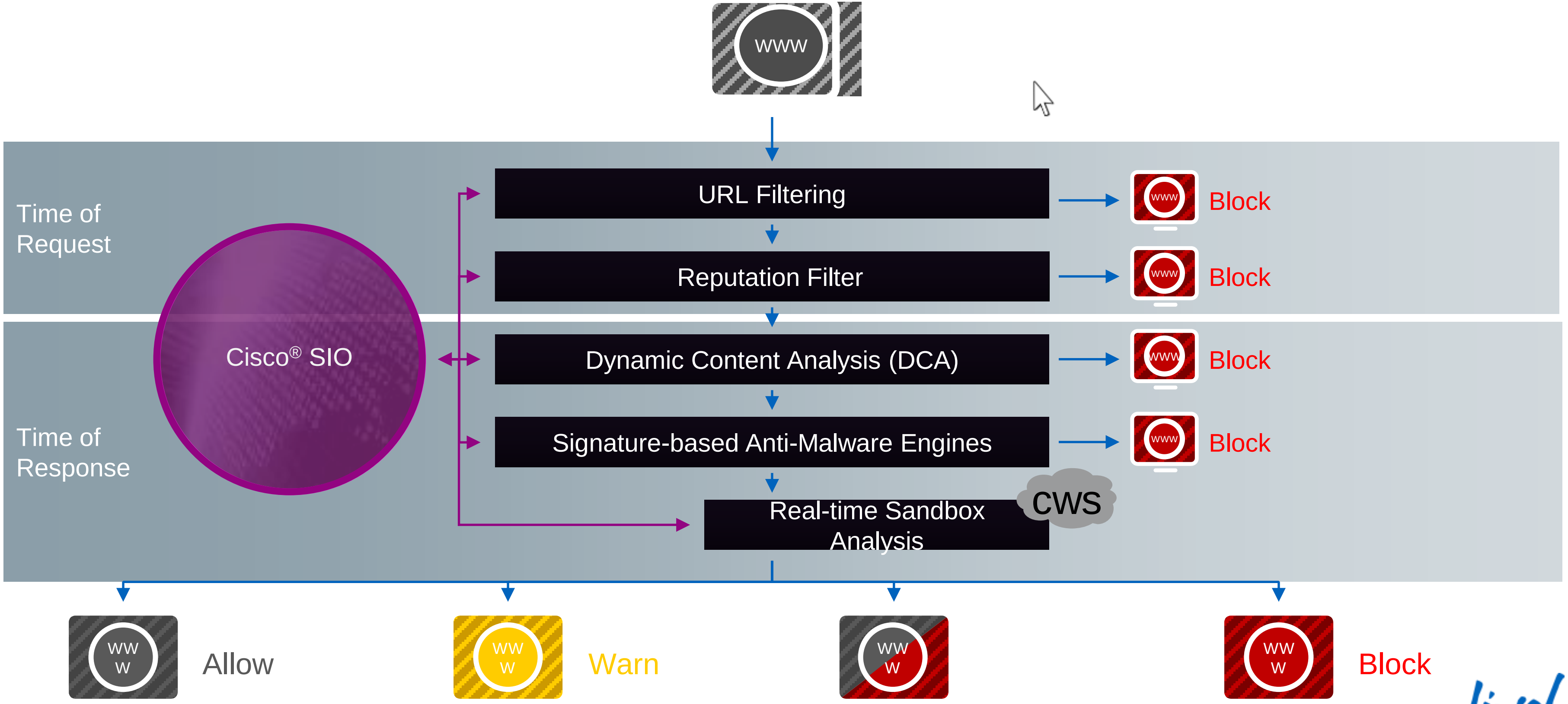
- Automated updates for AS/AV and Outbreak filter engines for Cisco security devices every 3–5 minutes
- 8M+ Rules per day
- Reputation updates for real-time protection against known bad senders

Cisco® SIO

Benefits

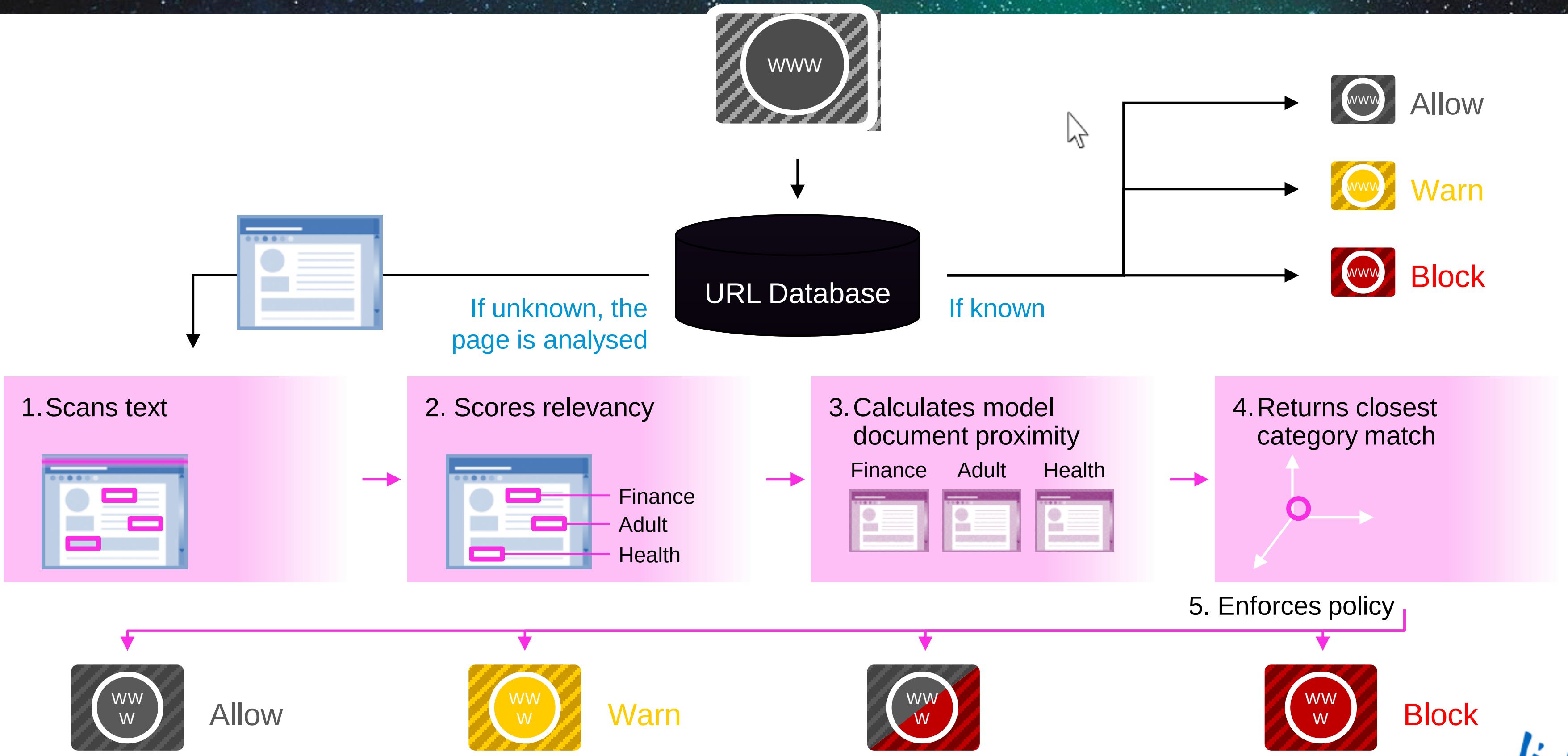
- Reduces exposure window
- Eliminates processing of most spam messages
- Minimises security management overhead

Cisco Web Security Provides Strong Protection



Cisco Web Usage Controls

URL Filtering and Dynamic Content Analysis



URL Database

If known

Allow

Warn

Block

If unknown, the page is analysed

1. Scans text

2. Scores relevancy

Finance
Adult
Health

3. Calculates model document proximity

Finance Adult Health

4. Returns closest category match

5. Enforces policy

Allow

Warn

Block

Cisco and Source Fire – Better Together
AMP Integration

Key Features of AMP on Content Security

File Reputation

Preventative blocking of suspicious files

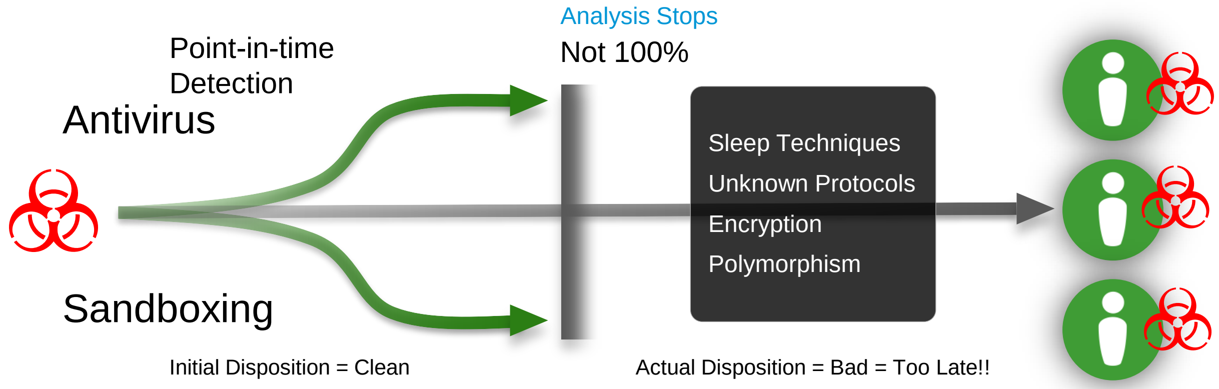
File Sandboxing

Behavioural analysis of unknown files

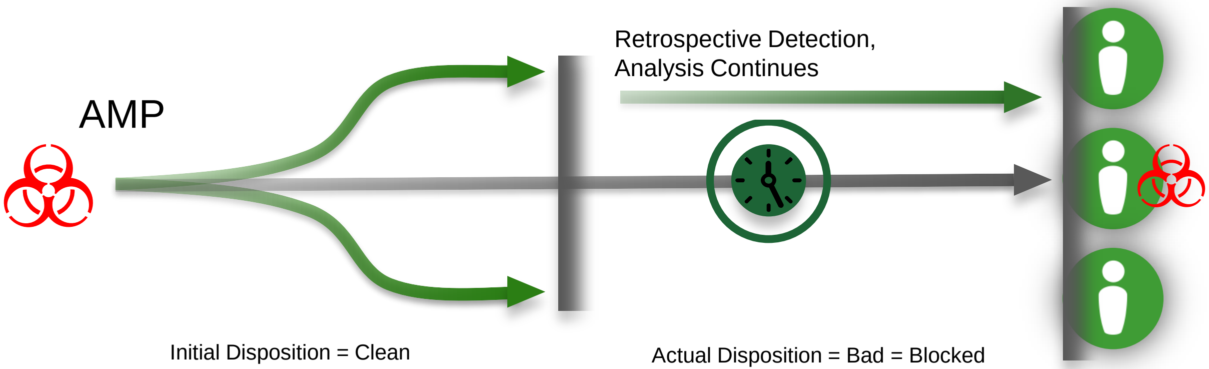
File Retrospection

Retrospective alerting after an attack

Beyond the Event Horizon



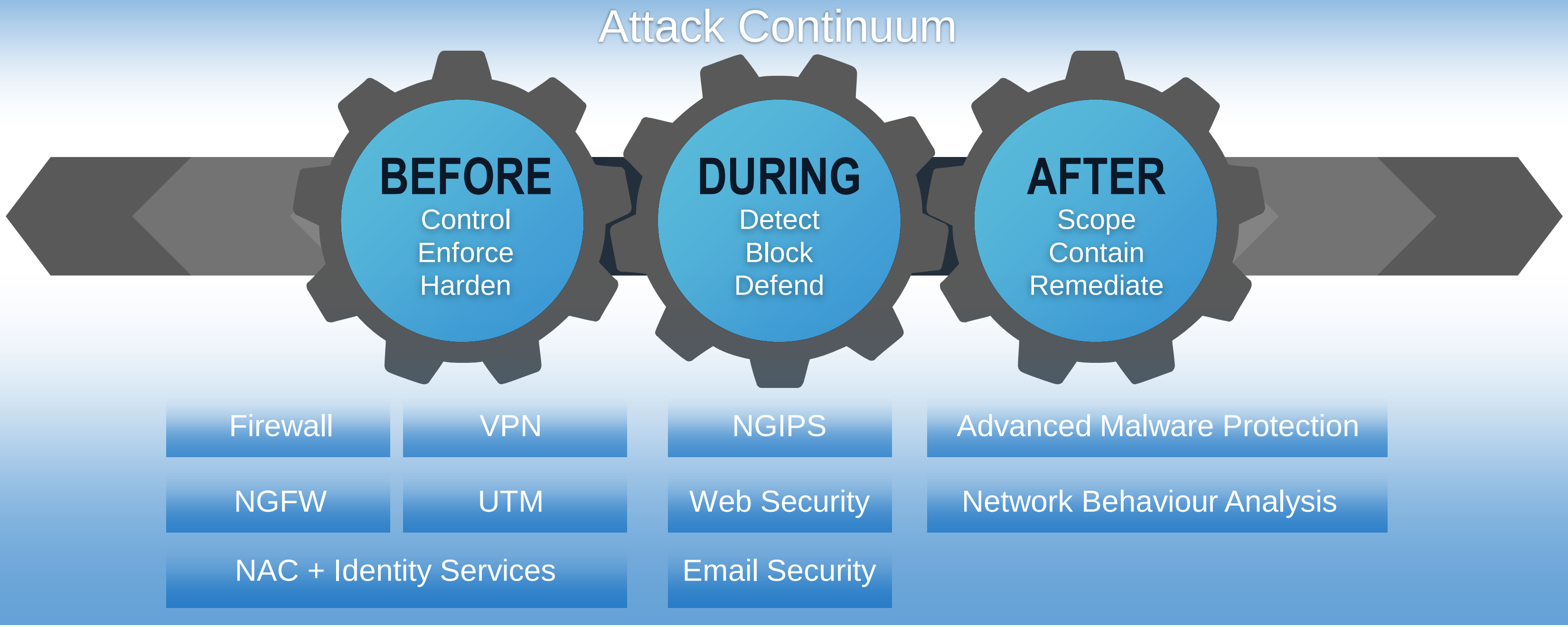
Blind to scope of compromise


Retrospective Detection,
Analysis Continues
AMP
Initial Disposition = Clean
Actual Disposition = Bad = Blocked

Turns back time

Visibility and Control are Key

Cisco and Sourcefire—Better Together



Before		During	After
Firewall	VPN	NGIPS	Advanced Malware Protection
NGFW	UTM	Web Security	Network Behaviour Analysis
NAC + Identity Services		Email Security	

Visibility and Context

Advanced Malware Protection AMP

AV as a Malware Countermeasure

- It's limited:
  - –Can only use 2-5% of your available CPU.
  - –Limited in rule set
  - –Limited in scope
  - –Operates as immediate point in time.
- **Why trust your entire corporate IP to a 386?**

To your AV, this …

… looks like this.

What if your malware counter-measure could be resourced like this?

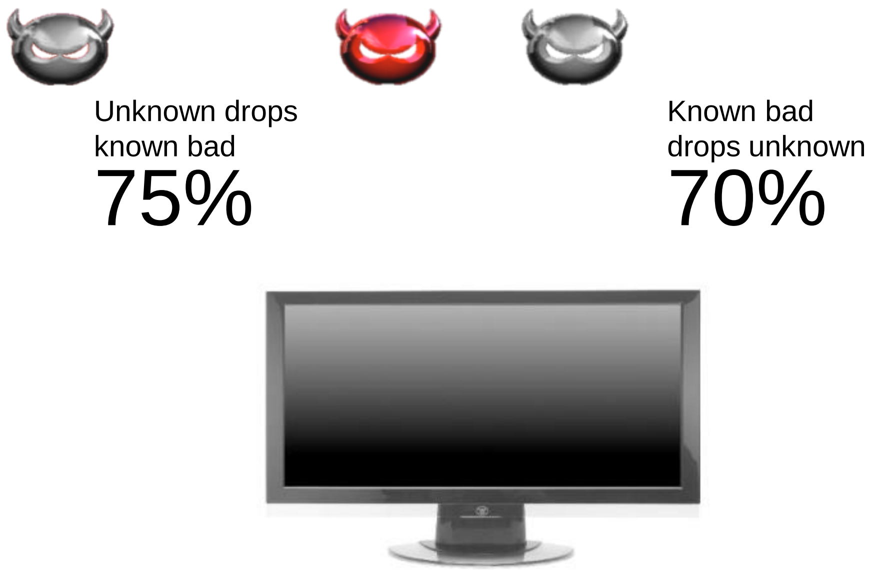
- Petaflop processing
- Petabyte storage
- Big data analytics
- Continuous analysis
- State-of-the-art AI algorithms for continuous malware targeting

“Now, *that’s* what I’m talkin’ about!”

Malware detection is by no means a sure thing ….

- Don’t view instances in isolation.
- Think ***malware ecosystem*****,** look for underlying context and find the hidden actors
- Track **malware trajectory** to patient 0, else chance of re-infection will be high

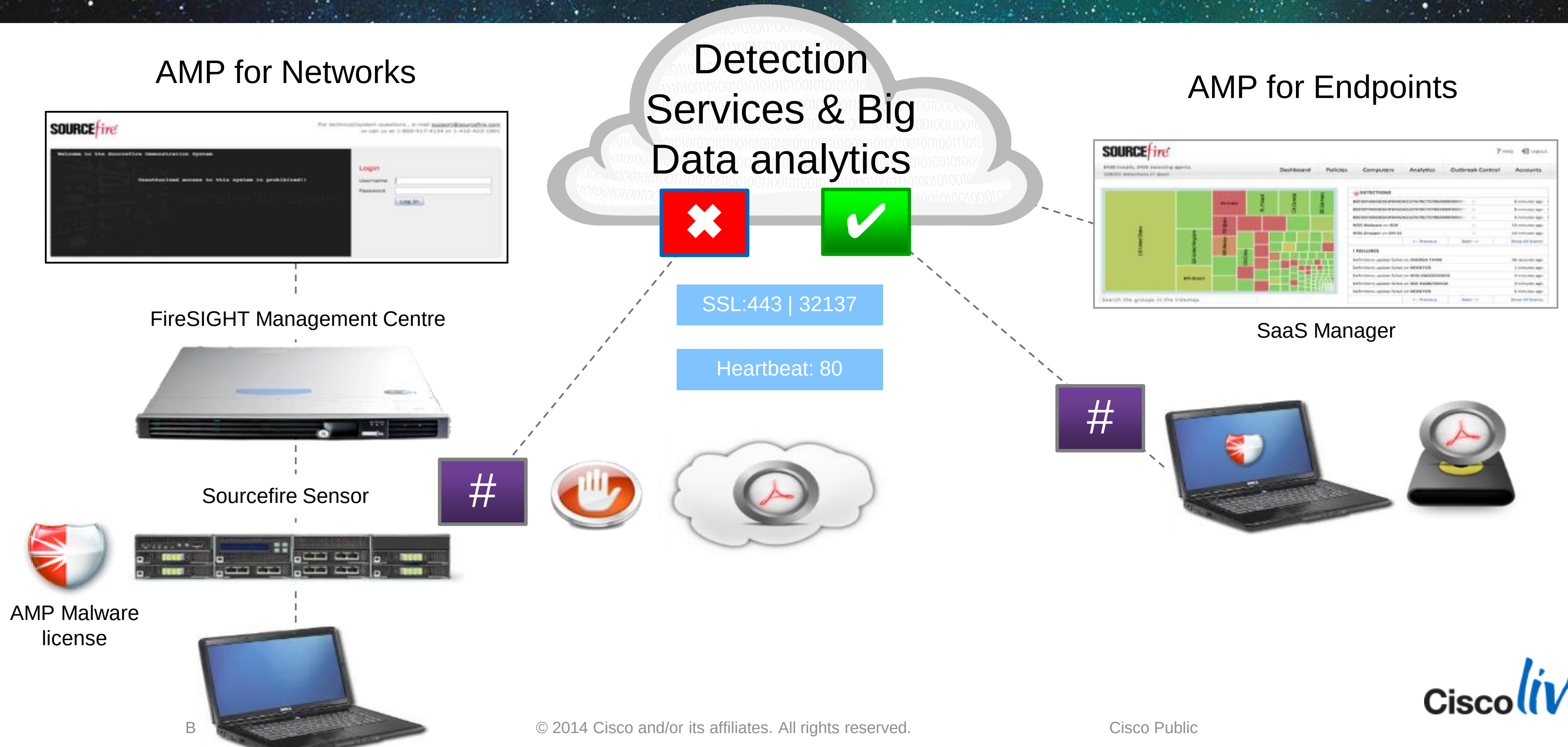
File disposition:
🟥 Known bad
🟩 Known good
⬛ Unknown



Unknown drops known bad
75%

Known bad drops unknown
70%

Our Approach to Advanced Malware Protection



AMP for Networks

FireSIGHT Management Centre

Sourcefire Sensor

AMP Malware license

Detection Services & Big Data analytics

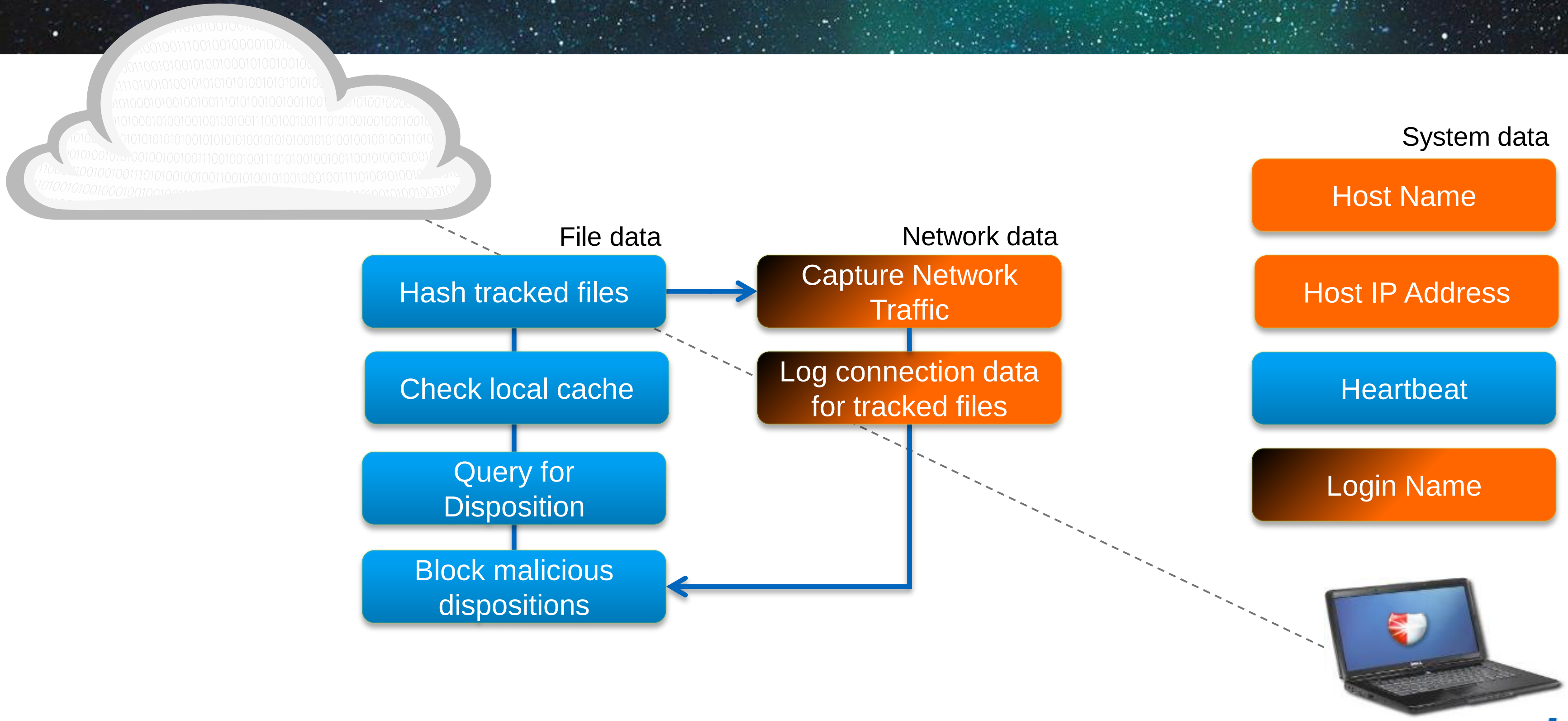
SSL:443 | 32137

Heartbeat: 80

AMP for Endpoints

SaaS Manager

Endpoint Operational Architecture



File data

Hash tracked files

Check local cache

Query for Disposition

Block malicious dispositions

Network data

Capture Network Traffic

Log connection data for tracked files

System data

Host Name

Host IP Address

Heartbeat

Login Name

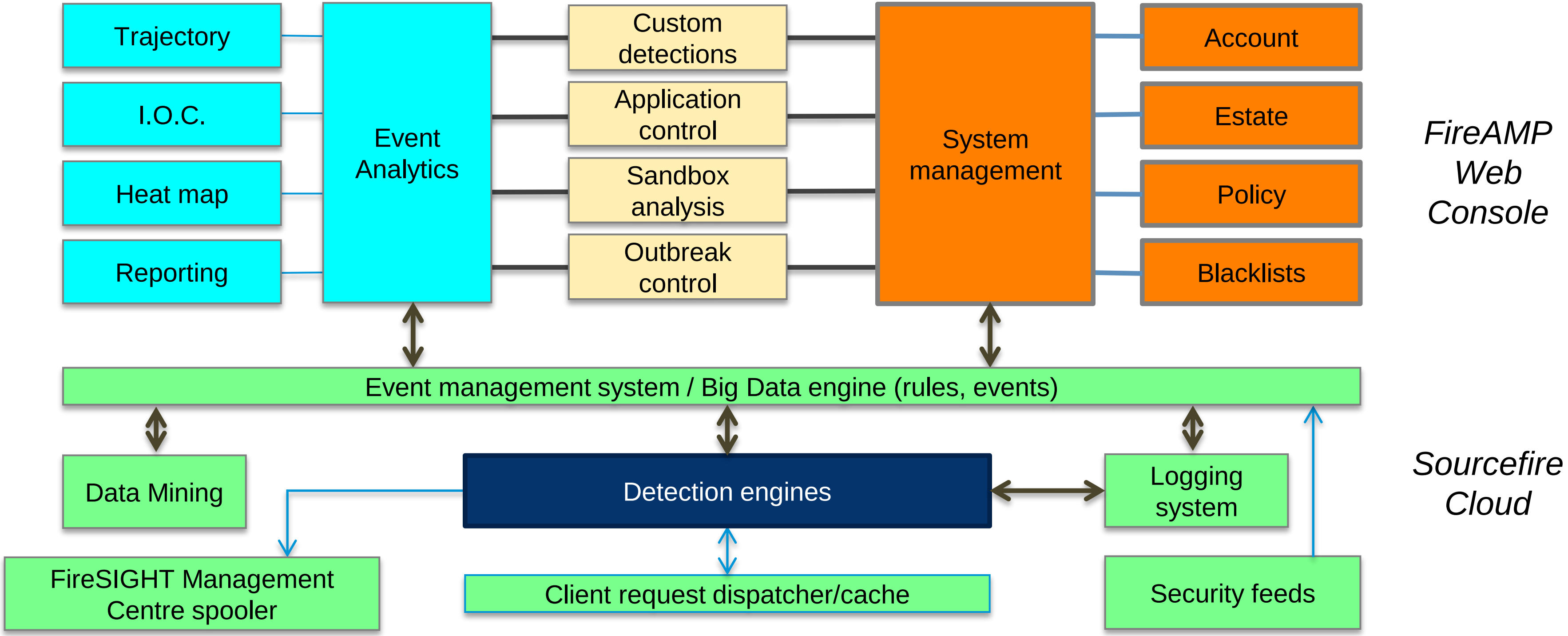
Legend

No Personally Identifiable Information (PII)

Optional PII

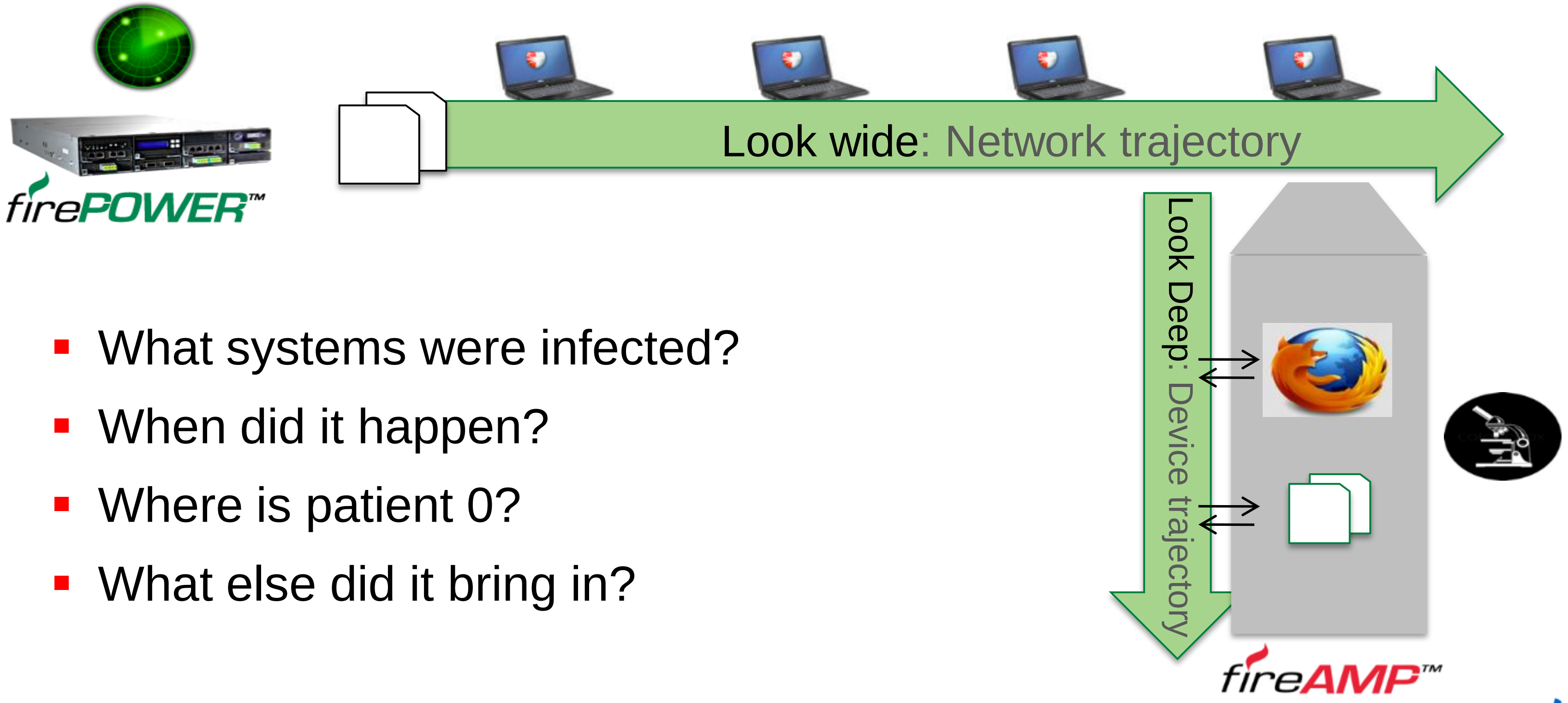
PII

The “Smarts” are in the Back-end



Finding Patient 0: Trajectory Analysis

Look wide (AMP for Networks), look deep (AMP for Endpoints)



- What systems were infected?
- When did it happen?
- Where is patient 0?
- What else did it bring in?

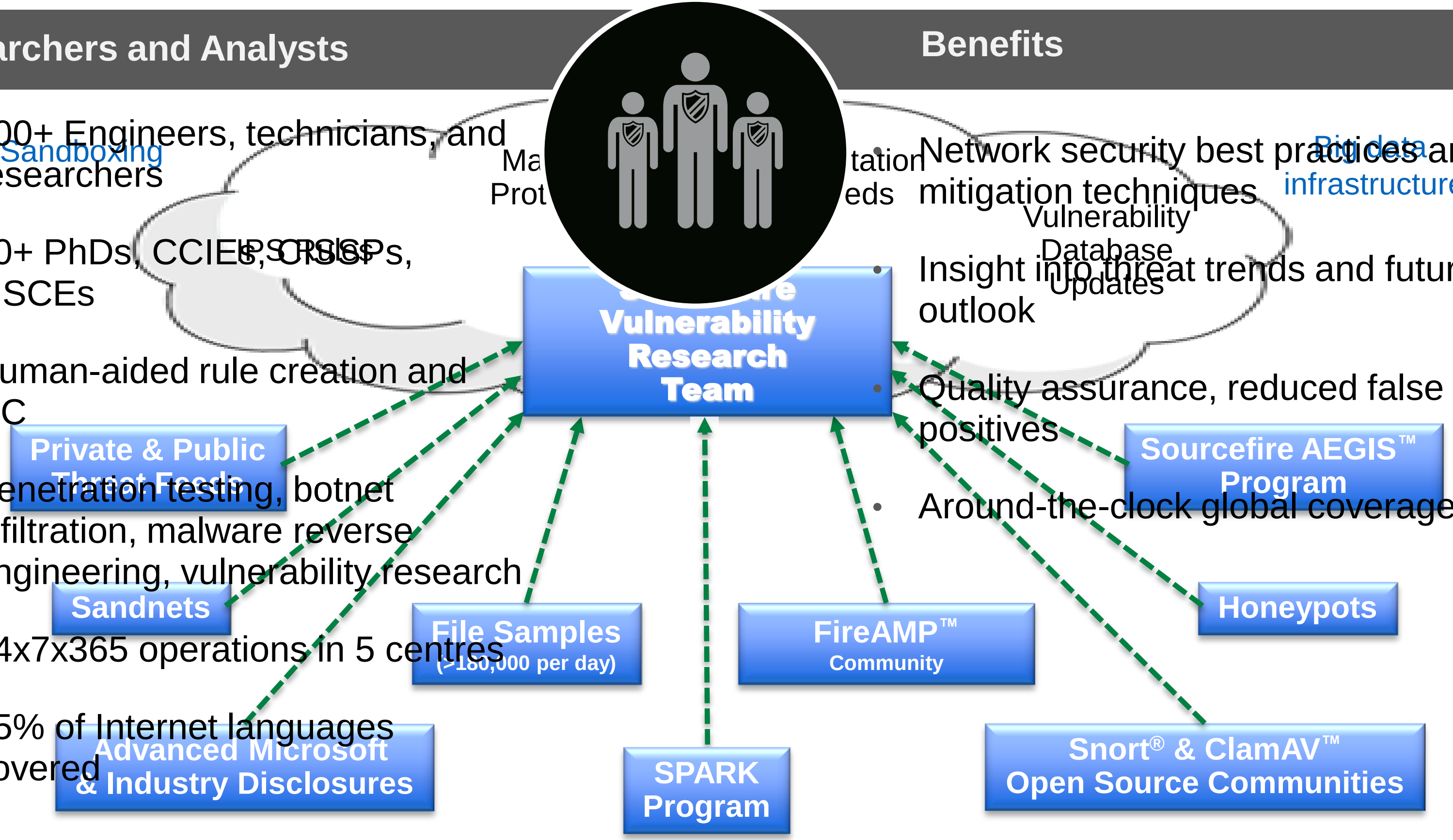
Threat Operations Centre Security Expertise

Researchers and Analysts

- 600+ Engineers, technicians, and researchers
- 80+ PhDs, CCIEs, CISSPs, MSCEs
- Human-aided rule creation and QC
- Penetration testing, botnet infiltration, malware reverse engineering, vulnerability research
- 24x7x365 operations in 5 centres
- 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

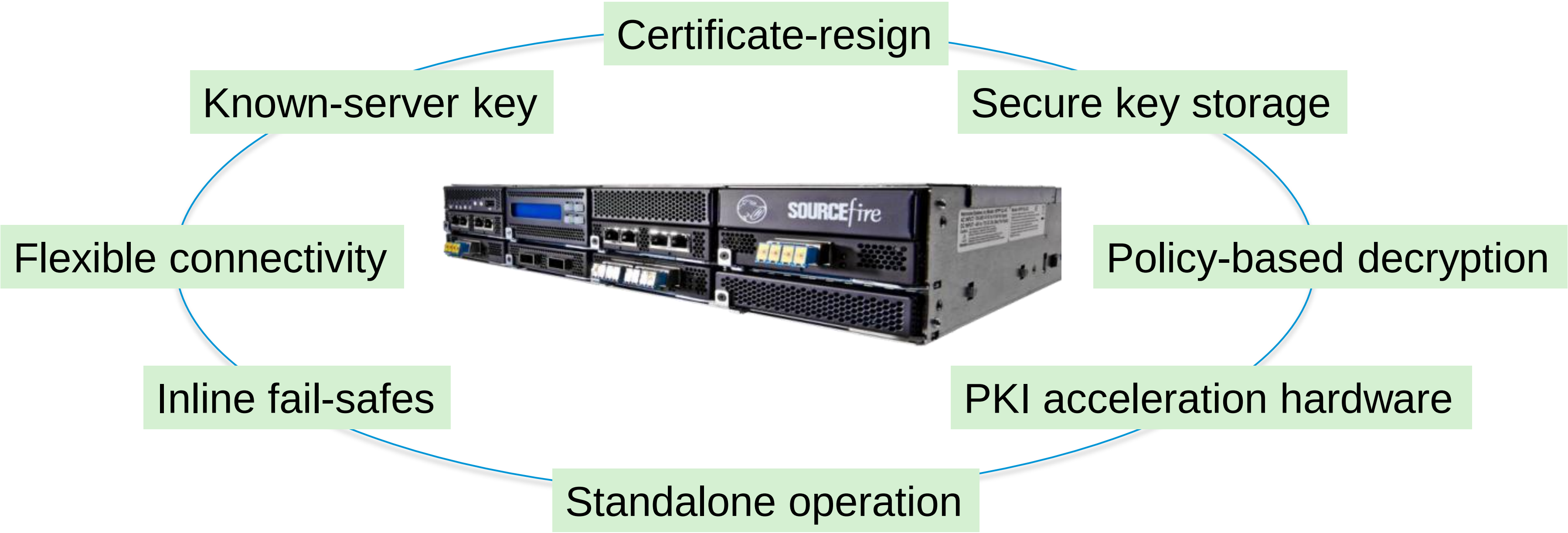


Sandboxing
IPS Rules
Ma
Prot
tation
eds
Big data infrastructure
Vulnerability Database Updates
re Vulnerability Research Team
Private & Public Threat Feeds
Sandnets
File Samples (>180,000 per day)
Advanced Microsoft & Industry Disclosures
SPARK Program
FireAMP™ Community
Snort® & ClamAV™ Open Source Communities
Honeypots
Sourcefire AEGIS™ Program

But what if my traffic is encrypted?

Sourcefire SSL Appliance

Based on Sourcefire Sensor hardware



Certificate-resign

Known-server key

Secure key storage

Flexible connectivity

Policy-based decryption

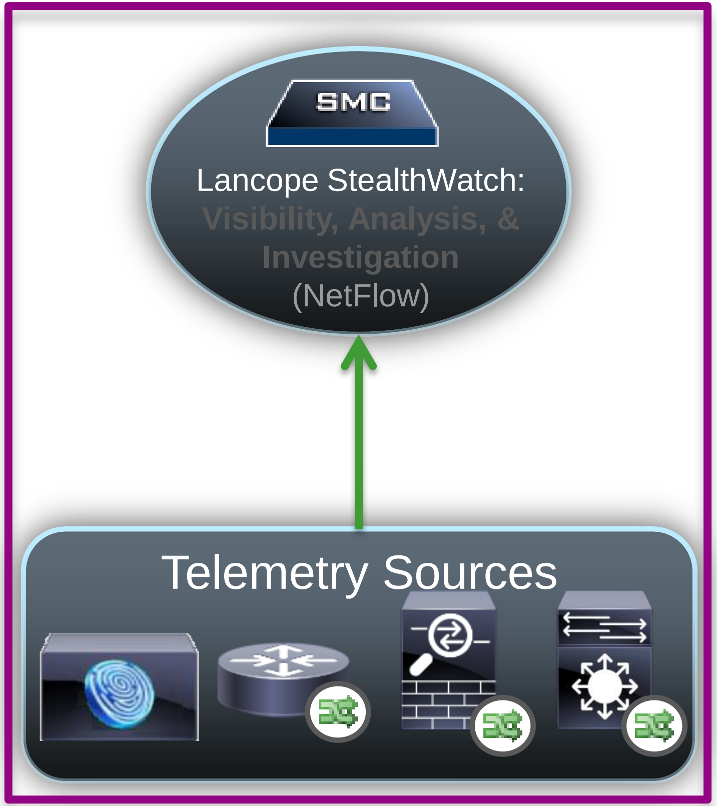
Inline fail-safes

PKI acceleration hardware

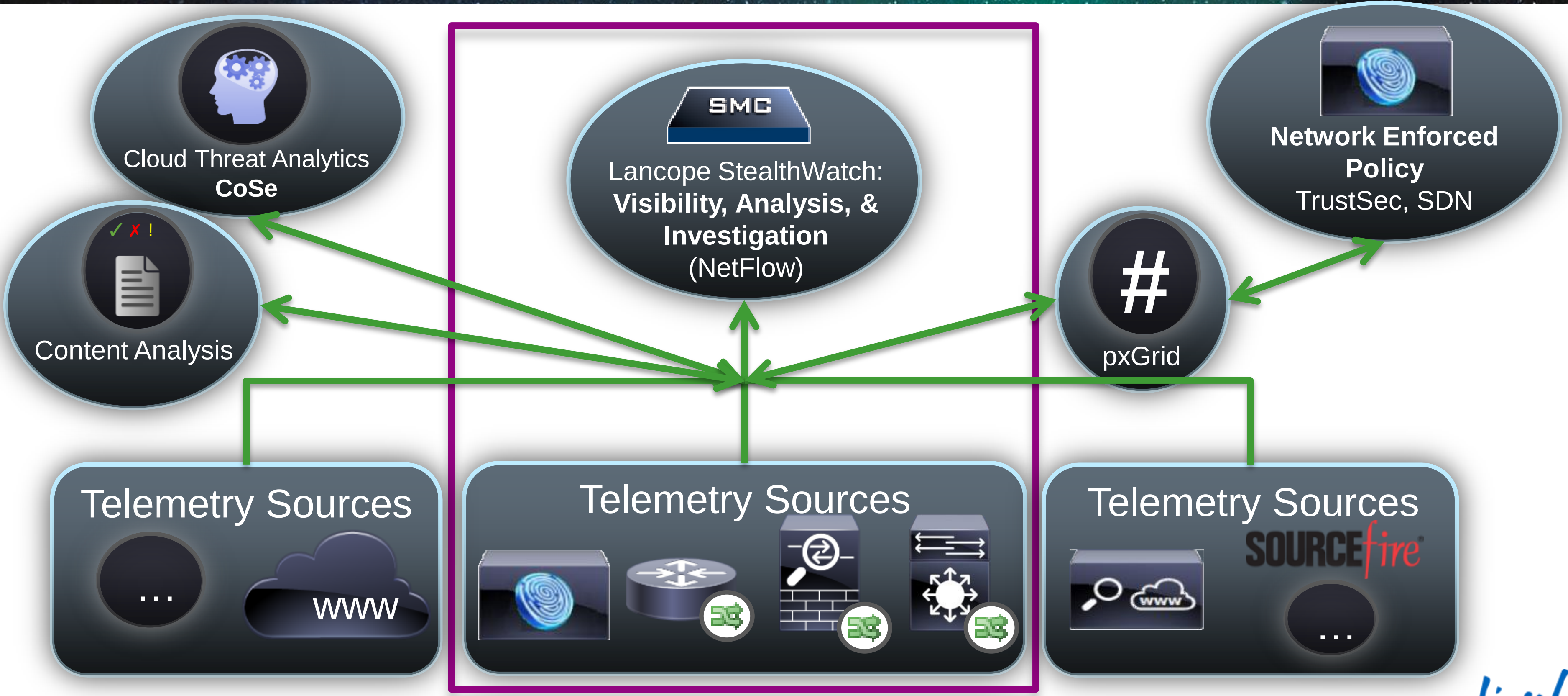
Standalone operation

Threat Detection

Cyber Threat Defence



Cyber Threat Defence is a Solution



Cloud Threat Analytics
CoSe

Content Analysis

Lancope StealthWatch:
Visibility, Analysis, & Investigation
(NetFlow)

Network Enforced Policy
TrustSec, SDN

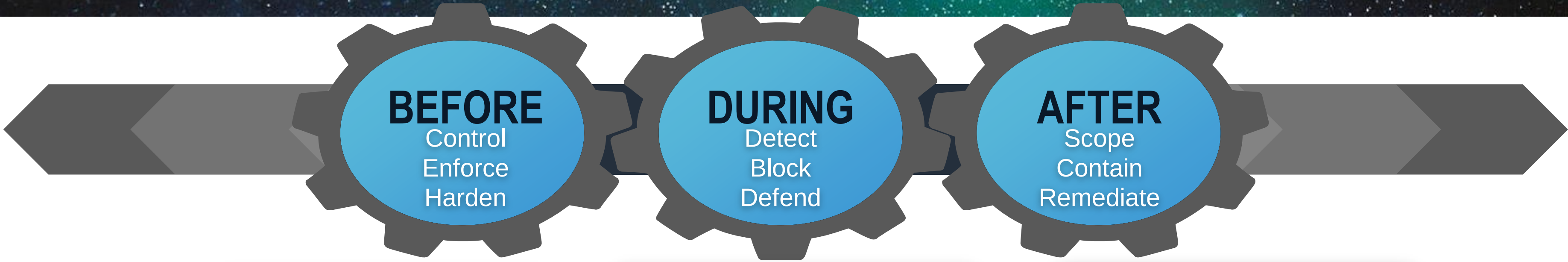
pxGrid

Telemetry Sources

Telemetry Sources

Telemetry Sources

Cisco and SourceFire: Comprehensive Security Portfolio



BEFORE
Control
Enforce
Harden

DURING
Detect
Block
Defend

AFTER
Scope
Contain
Remediate

VPN

- Cisco AnyConnect VPN

UTM

- Meraki MX

NAC + Identity Services

- Cisco Identity Services Engine (ISE)
- Cisco Access Control Server (ACS)

NGFW

- Cisco ASA 5500-X Series
- Cisco ASA 5500-X w/ NGFW license
- Cisco ASA 5585-X w/ NGFW blade
- FirePOWER NGFW

NGIPS

- Cisco ASA 5500-X integrated IPS
- FirePOWER NGIPS
- FirePOWER NGIPS w/ Appl. Control
- FirePOWER Virtual NGIPS

Email Security

- Cisco Email Security Appliance (ESA)
- Cisco Virtual Email Security Appliance
- Cisco Cloud Email Security

Web Security

- Cisco Web Security Appliance (WSA)
- Cisco Virtual Web Security Appliance
- Cisco Cloud Web Security

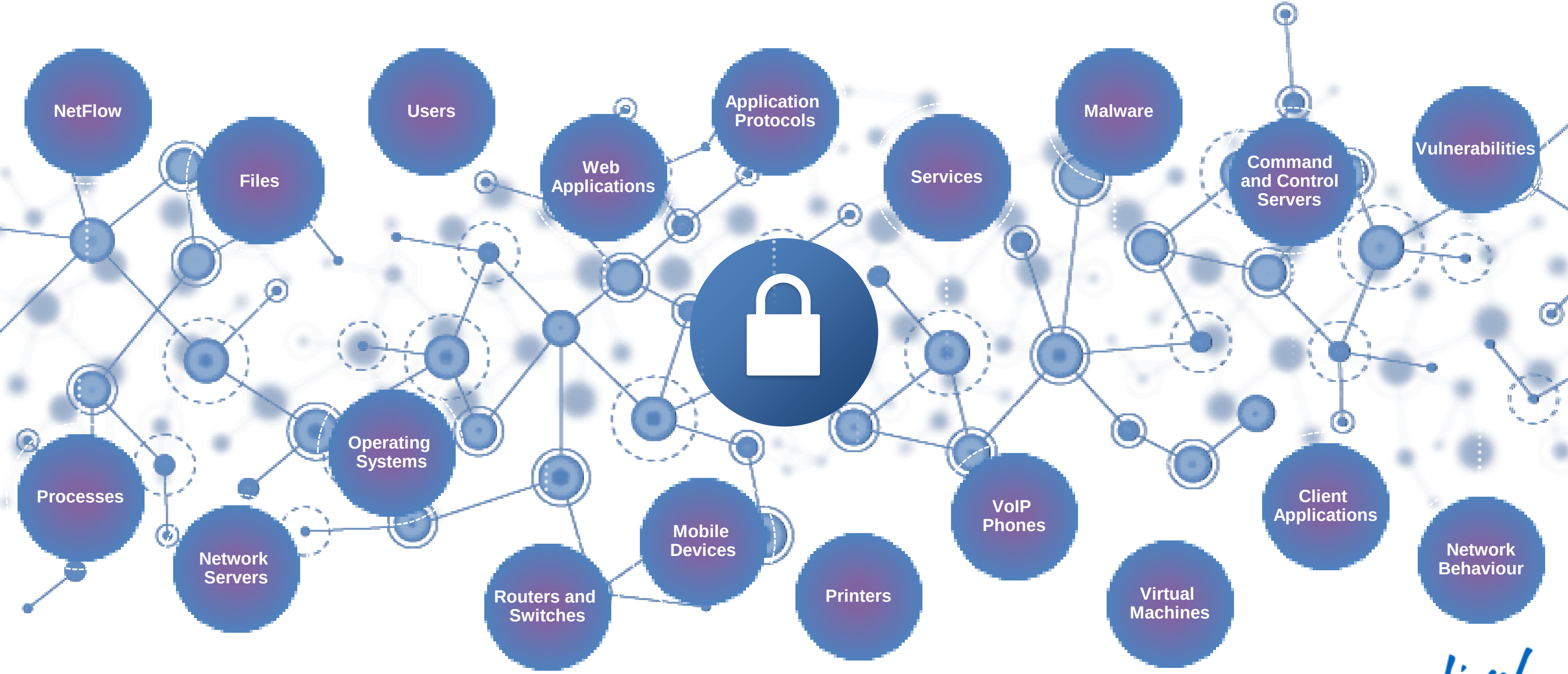
Advanced Malware Protection

- FireAMP
- FireAMP Mobile
- FireAMP Virtual

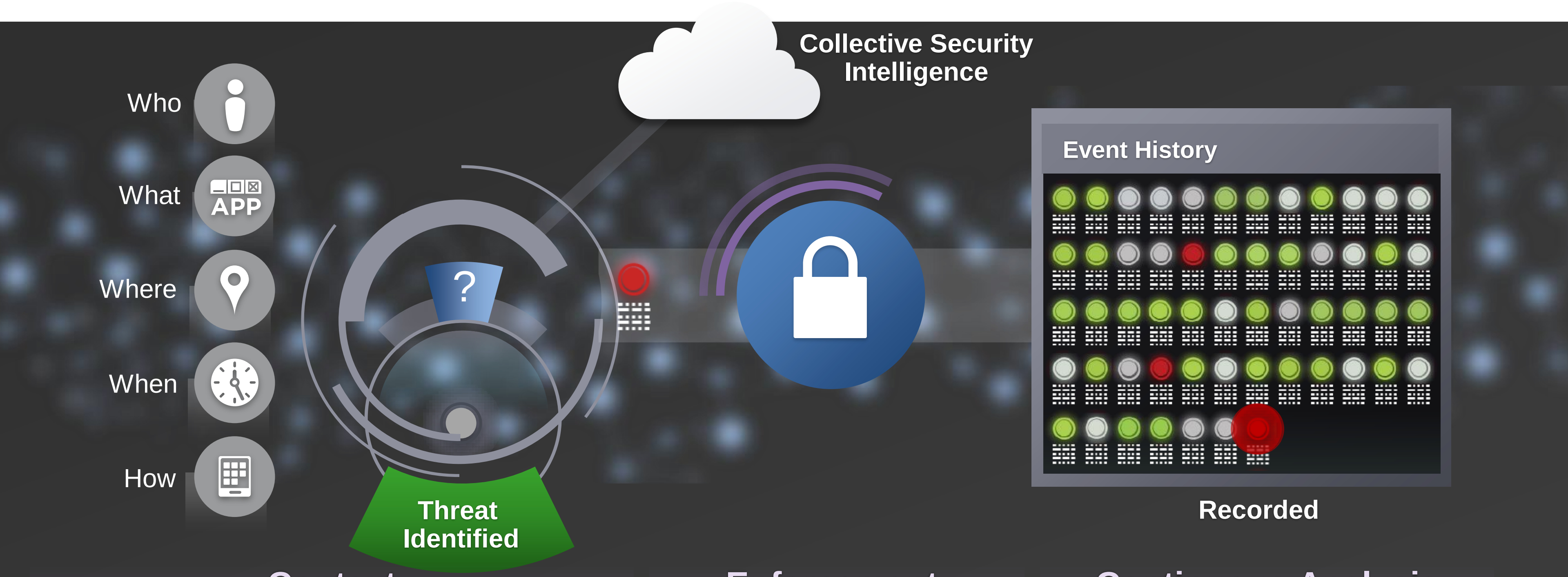
Network Behaviour Analysis

- Cyber Threat Defence
- Cisco SIO
- FireSight
- SIEM Integration

Visibility: Cisco Sees More than the Competition



Detect, Understand and Stop Threats



Context

ISE + Network, Appliances (NGFW/NGIPS)

Enforcement

AMP, CWS, Appliances

Continuous Analysis

AMP, Threat Defence

The Security Perimeter in the Cloud

Collective Security Intelligence

Telemetry Data

Threat Research

Advanced Analytics

The Distributed Perimeter

Cloud Connected Network

Mobile

Router

Firewall

3M+
Cloud Web Security Users

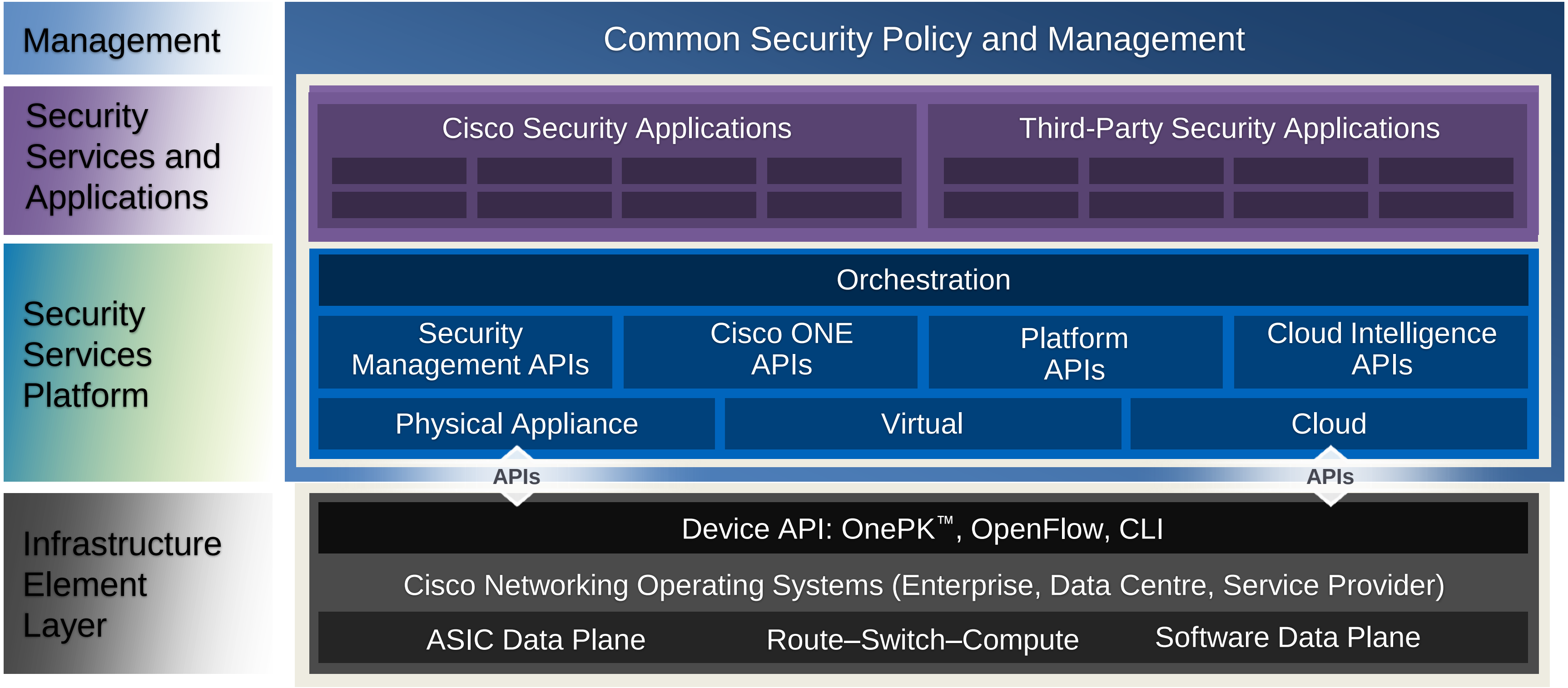
6 GB
Web Traffic Examined, Protected Every Hour

75M
Unique Hits Every Hour

10M
Blocks Enforced Every Hour

Cisco live!

Platform-Based Security Architecture



Management

Common Security Policy and Management

Security Services and Applications

Cisco Security Applications

Third-Party Security Applications

Security Services Platform

Orchestration

Security Management APIs

Cisco ONE APIs

Platform APIs

Cloud Intelligence APIs

Physical Appliance

Virtual

Cloud

APIs

APIs

Infrastructure Element Layer

Device API: OnePK™, OpenFlow, CLI

Cisco Networking Operating Systems (Enterprise, Data Centre, Service Provider)

ASIC Data Plane

Route–Switch–Compute

Software Data Plane

Reduce Complexity & Increase Capability Through Platforms

Collective Security Intelligence

Centralised Management

Appliances, Virtual

Network Control Platform

Appliances, Virtual

Device Control Platform

Host, Mobile, Virtual

Cloud Services Control Platform

Hosted

Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2014 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 21 March 12:00pm - 2:00pm

Learn online with Cisco Live!

Visit us online after the conference for full access to session videos and presentations. www.CiscoLiveAPAC.com cisco TM