Cisco Innovations

Star Tseng

Senior Consult, Xander Int'l Corp.

Star_tseng@xander.com.tw

Sep 2015

Cisco's innovation →Unified Access

Cisco Unified Access = Innovation

One Network

Converged Access

Common LAN and WLAN fabric (UADP ASIC) – Common OS (Cisco IOS®) – SDN Ready (API/SDK)

Gigabit Wi-Fi

802.11ac standard leadership – The transformational technology for the new Gigabit Wi-Fi edge

AVC

Application visibility and control across the LAN and WLAN, using 1000+ dynamically updated signatures

SSO

Stateful switchover for nonstop operation of both the LAN and WLAN

BSD

Bonjour Services Directory – Multicast DNS discovery and advertisement

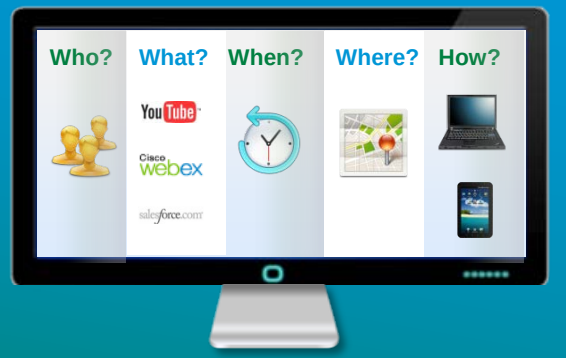
CMX

Cisco® Connected Mobile Experiences – Advanced location services and analytics for business intelligence

Cisco CleanAir®

Automatic chip-level innovation for interference mitigation and RF reconfiguration

One Policy & One Management



Cisco Identity Services Engine (ISE)

Cisco Prime™

Converged Access

Common Fabric for LAN and WLAN

Cisco Unified Access™ Data Plane ASIC (UADP)

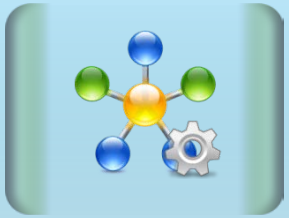
Programmable

SDN Ready

Common Cisco IOS for LAN and WLAN

Show Clear Save Set

Ping Run Config Debug AP



Operational Consistency (same well-known commands)

Wireless Mobility Controller Copy ?

dot11 Antenna Rename

Wireless Management Interface

*Cisco VNI Study 2012

Gigabit Wi-Fi (802.11ac)

- 802.11ac is the transformational technology for the Gigabit Wi-Fi Edge
- Cisco is the leader of the 802.11ac amendment to the 802.11 standard
- Industry's only future-ready modular radio platform
- Supports 802.11b/g/n, 802.11a/n, and 802.11ac
- Support for Wave 1 and Wave 2 modules

2
802.11
1997

11
802.11b
1999

54
24
802.11a/g
2003

600
450
300
65
802.11n
2007

Std Max
Product Max
Typical
Minimum

6900
1300
870
290
Gigabit Ethernet Uplink
802.11ac Wave 1
2013

6900
3500*
1730*
290
2 Gigabit Ethernet Uplinks
802.11ac Wave 2
2015

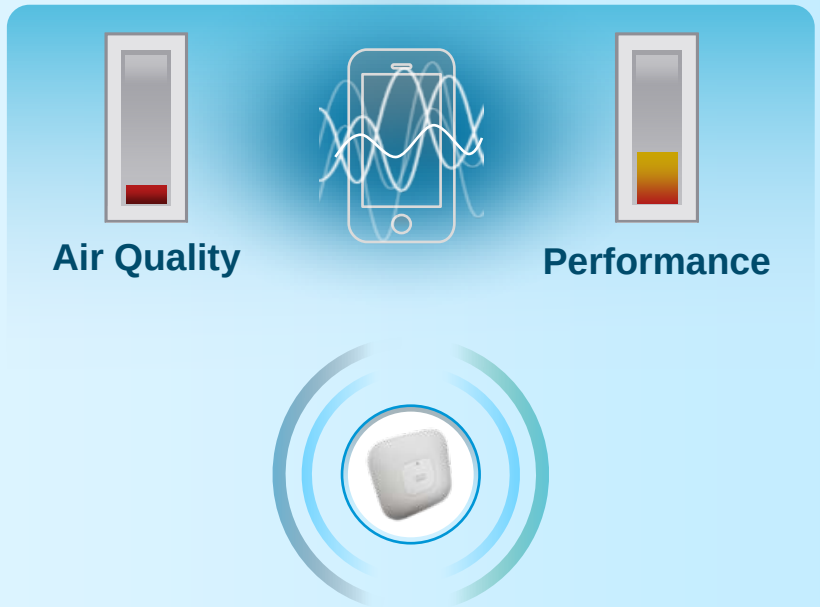
8 Spatial Streams
3 Spatial Streams
1 Spatial Stream

*Assuming 160 MHz is available and suitable.

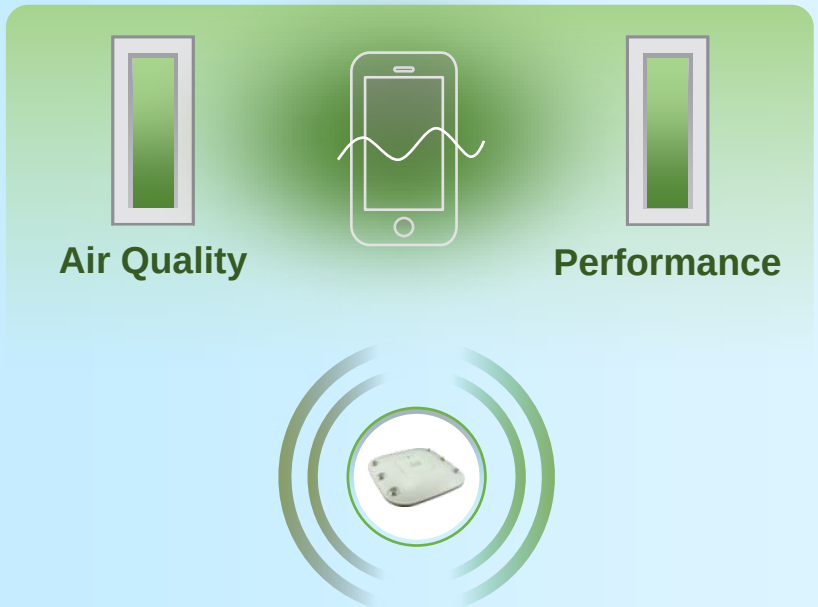
Cisco CleanAir

Before: Wireless Interference Decreases Reliability and Performance

After: Cisco CleanAir® Mitigates RF Interference, Improving Reliability and Performance



Improved Client Performance



CleanAir = Chip-Level Automatic Interference Mitigation

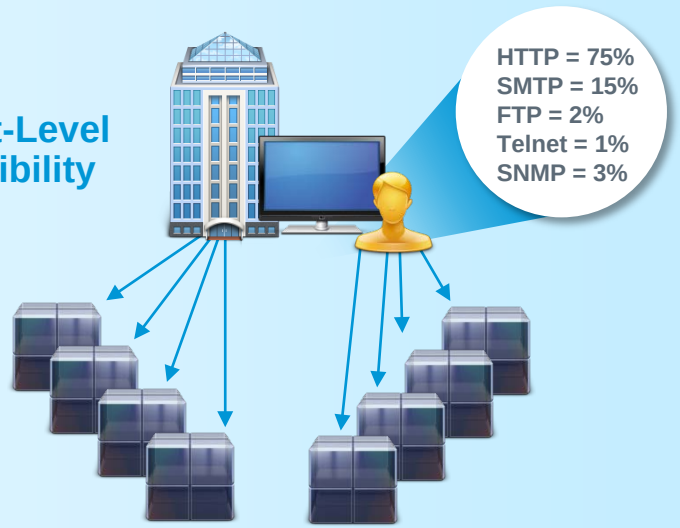
Application Visibility And Control (AVC)

Before: Application View and Control Based on Layer 4 Port Sessions

After: Network-Based Application Recognition – NBAR2 Deep Packet Inspection and App ID

Visibility into the port-level interaction but not the applications running within the port

Port-Level Visibility



Layer 4 Port Session Visibility and Control

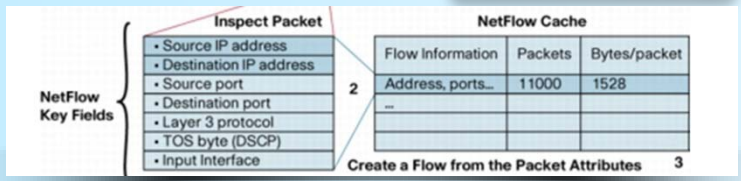
Improved Visibility and Control

Wireless LAN Controller

Real Time
Interactive
Non-Real Time
Background

NBAR2 LIBRARY
Deep Packet Inspection

POLICY
Packet Mark and Drop



View, Control, and Troubleshoot – End User Application Experience

AVC = Identify, Analyze, and Control Application Traffic

Cisco Identity Services Engine (ISE)

Before: Separate Policy and Guest Management

After: Unified Context-Based Policy Management for Employees and Guests Across the Network

Wired | Wireless | WAN

Unified Policy Management

Account for Every Device and Block Unwanted Devices

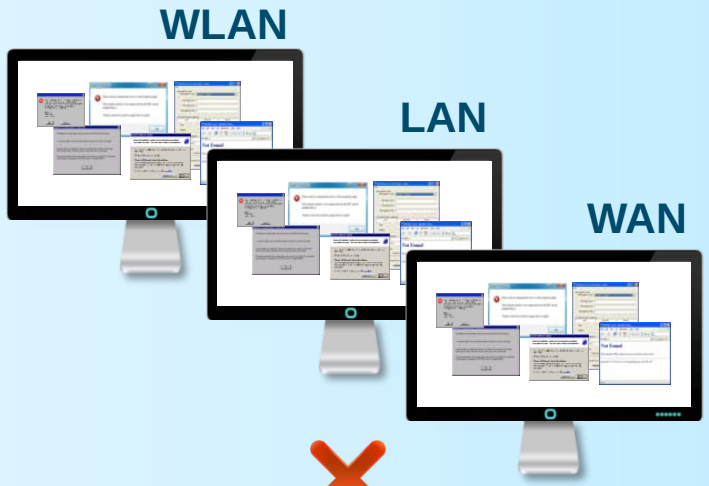
AAA + Profiling, Provisioning, and Posturing = Secure BYOD

ISE = Unified LAN, WLAN, and WAN Policy Management

Cisco Prime Infrastructure

Before: Separated Management

After: Comprehensive User and Unified Access
Network Visibility and Advanced Troubleshooting



Siloed: Inefficient operational model

Repetitive: Manual correlation of data

Error Prone: Consumes time and resources

Unified Network Management

WLAN
LAN
WAN
+
Identity

Simple: Improves IT efficiency

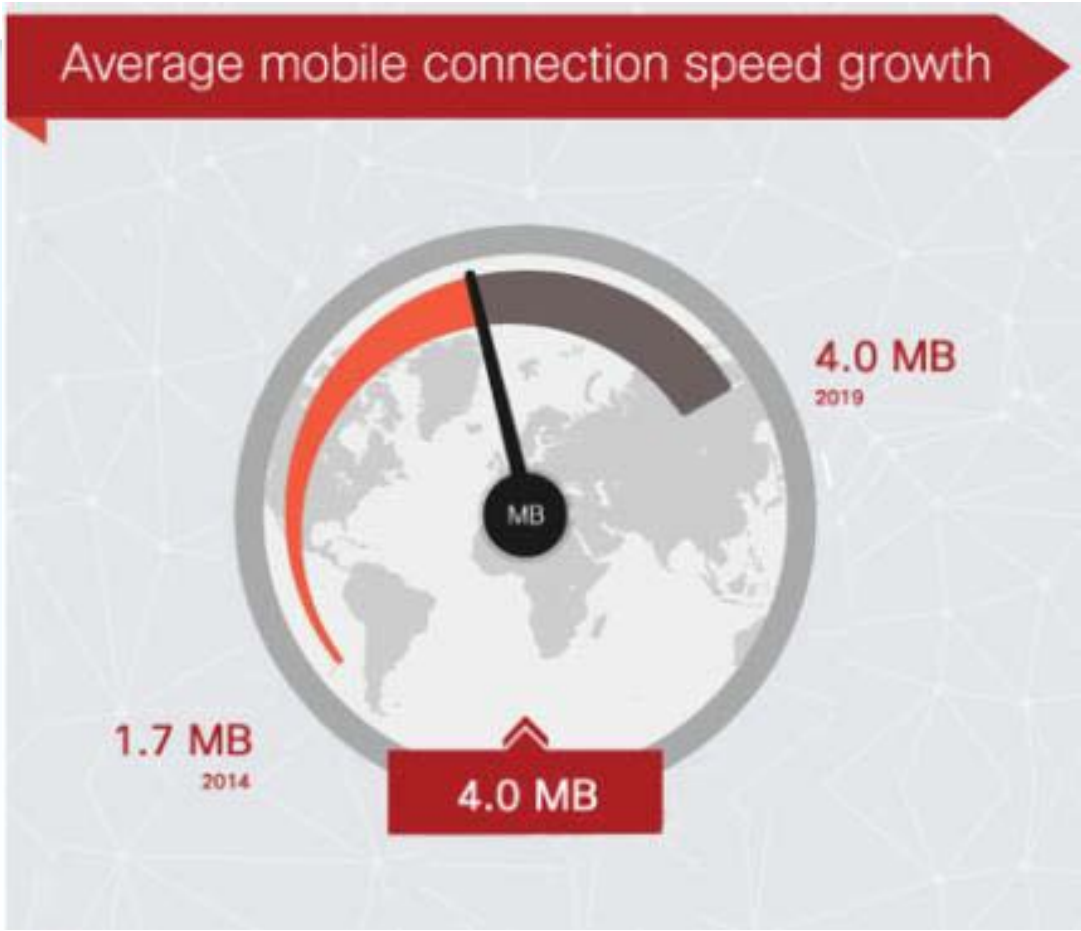
Unified: Single view of all user access data

Advanced Troubleshooting:
Less time and resources consumed

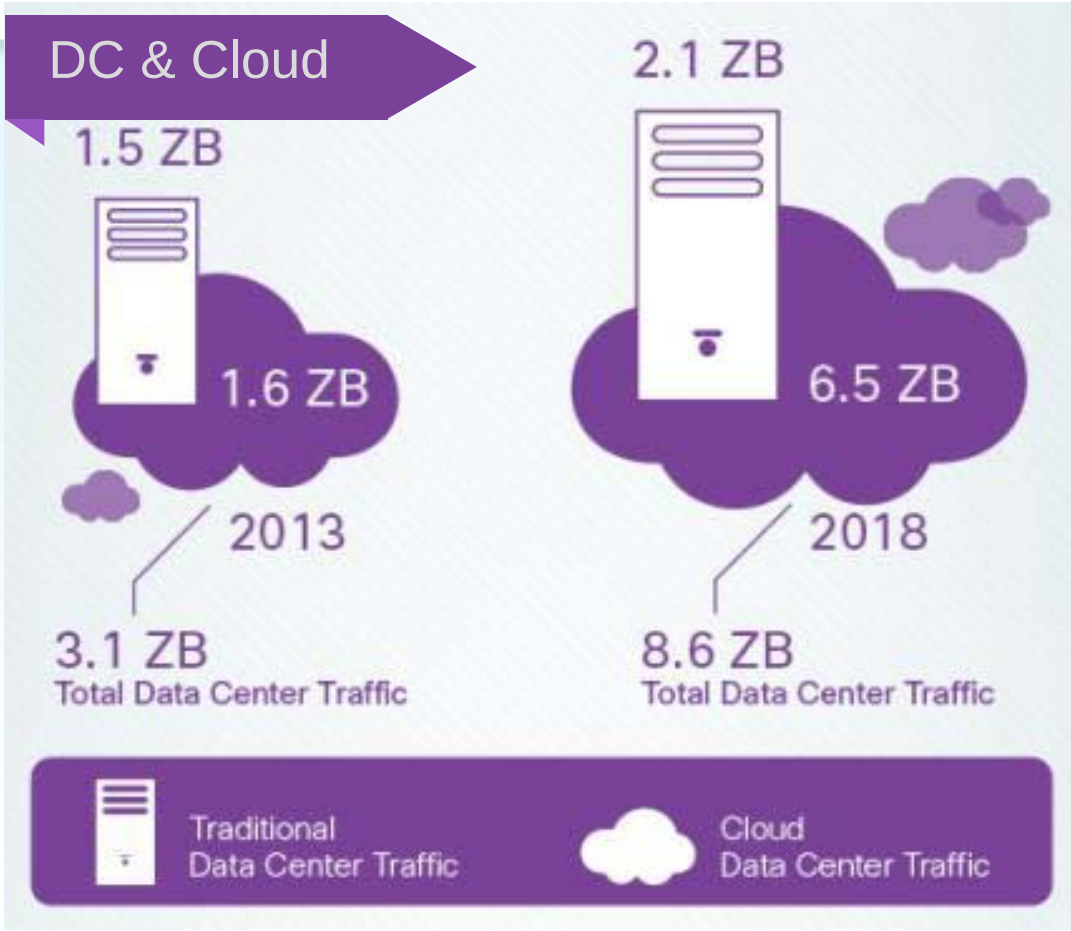
Cisco Prime™ Infrastructure = Unified LAN, WLAN, and WAN Network Management

Cisco's innovation
→Intelligent WAN(iWAN)

Traffic Growth

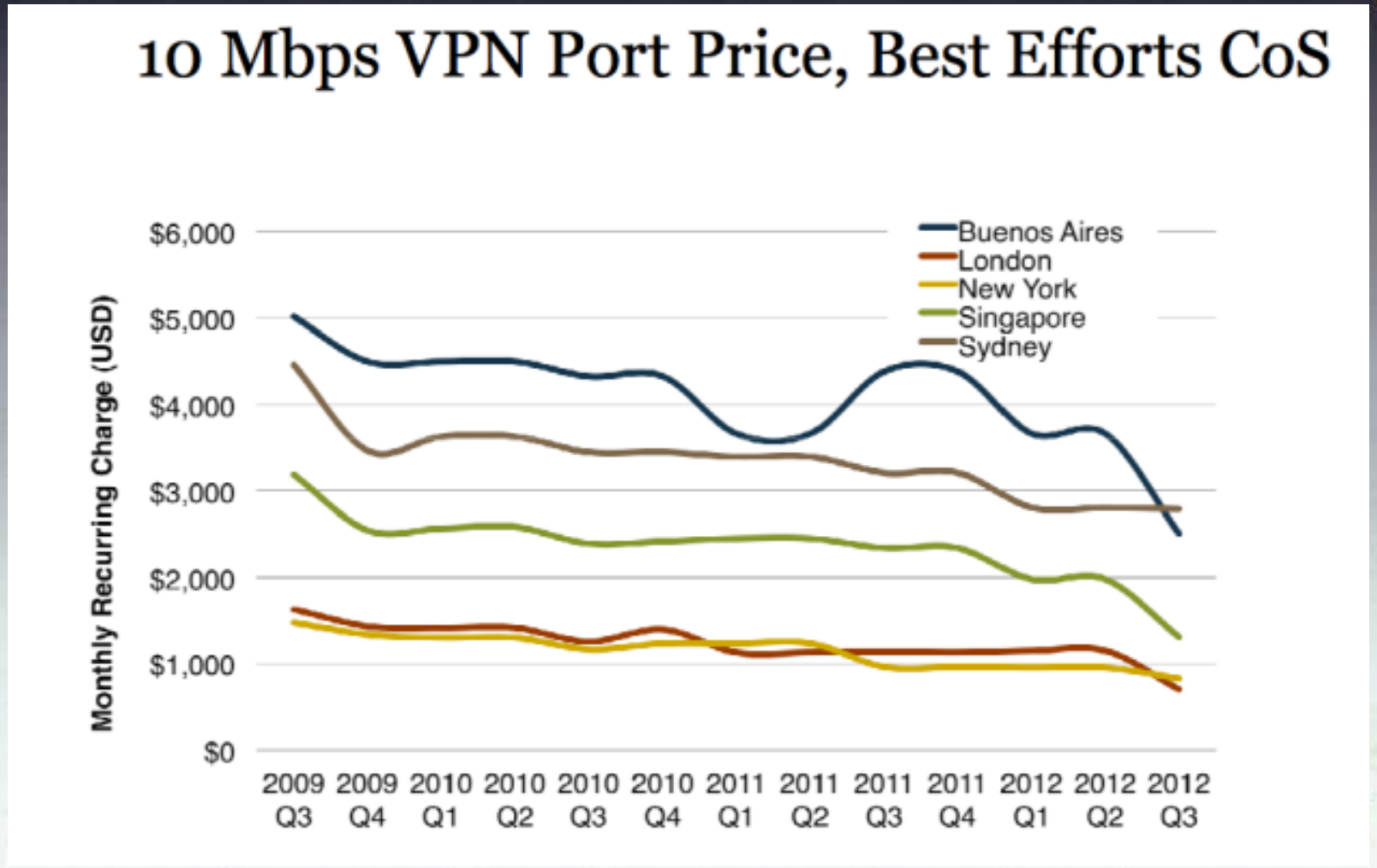


That’s 10,000 3.5” floppies/day



that’s 9 trillion hours of HD

Cost of Bandwidth



Cisco Intelligent WAN

Transport Independent

Provider Flexibility
Modular Design
Common Operational Model

Intelligent Path Control

Load Balancing
Policy-Based Path Selection
Network Availability

Application Optimization

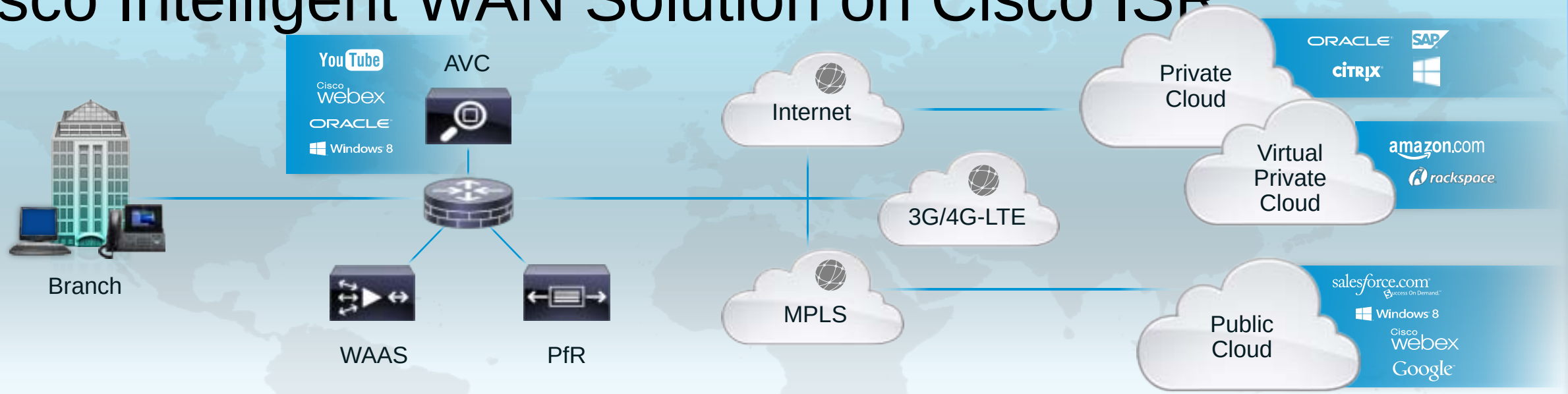
Application Visibility
App Acceleration
Intelligent Caching

Secure Connectivity

Scalable, Strong Encryption
App-Aware Threat Defense
Cloud Web Security

Secure, Reliable and High Performance Application Experience
on **Any Device**, over **Any Connection**, to **Any Cloud**

Cisco Intelligent WAN Solution on Cisco ISR



Transport Independent

- Consistent operational model
- Simple provider migrations
- Scalable and modular design
- DMVPN IPsec overlay design

Intelligent Path Control

- Application best path based on delay, loss, jitter, path preference
- Load balancing for full utilization of all bandwidth
- Improved network availability
- Performance Routing (PfR)

Application Optimization

- **AVC:** Application monitoring with Application Visibility and Control
- **WAAS:** Intelligent Edge Caching with Akamai Connect
- **WAAS:** Application Acceleration and bandwidth savings

Secure Connectivity

- Certified strong encryption
- Comprehensive threat defense with ASA and IOS firewall/IPS
- Cloud Web Security (CWS) for scalable secure direct Internet access

The WAN and the Application Challenge?

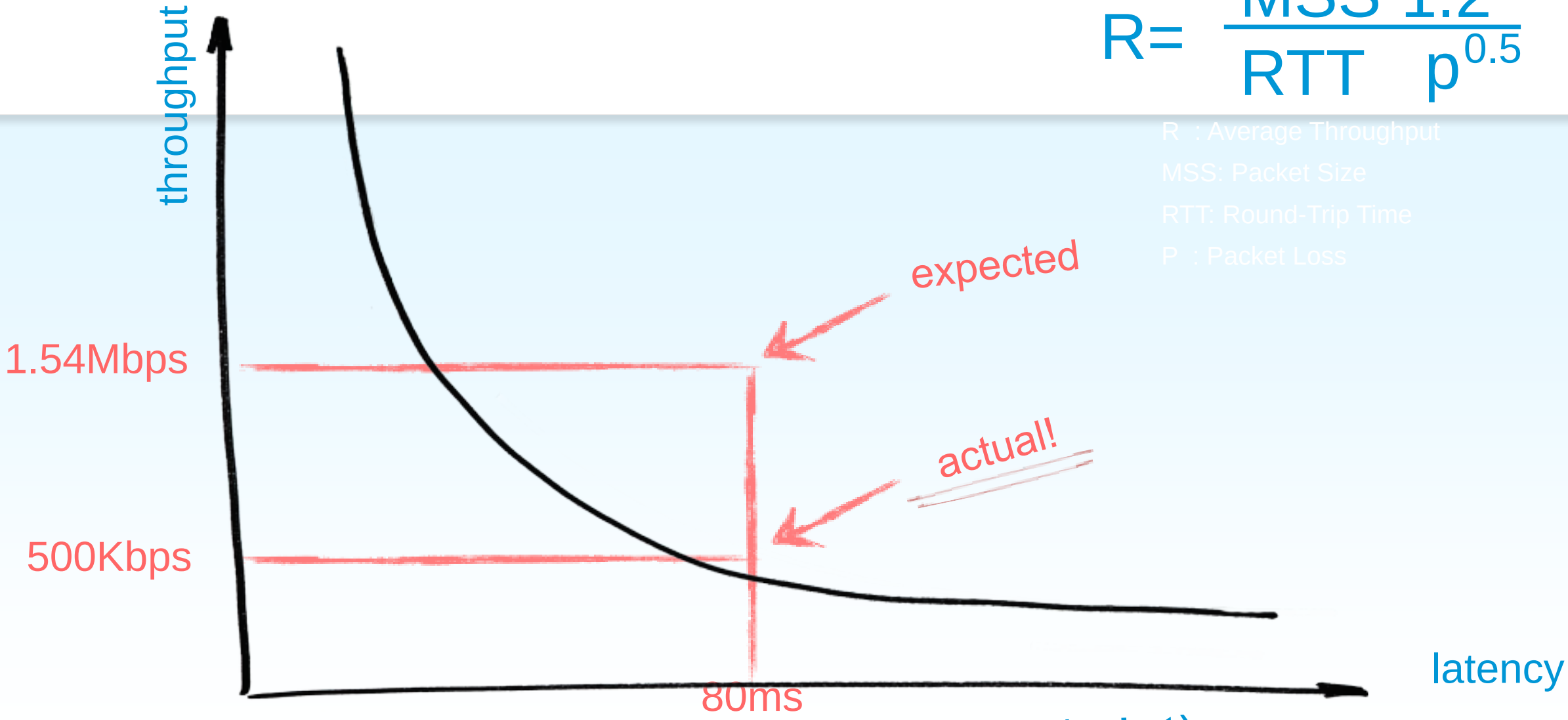
$$R = \frac{MSS\ 1.2}{RTT\ \ p^{0.5}}$$

R : Average Throughput

MSS: Packet Size

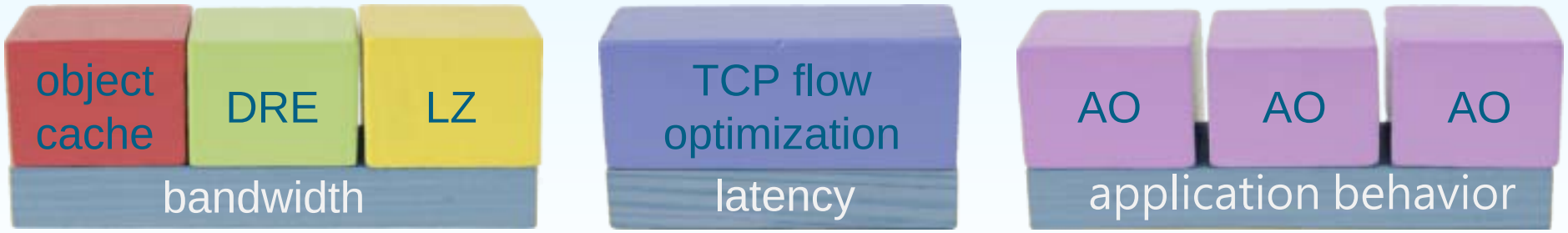
RTT: Round-Trip Time

P : Packet Loss

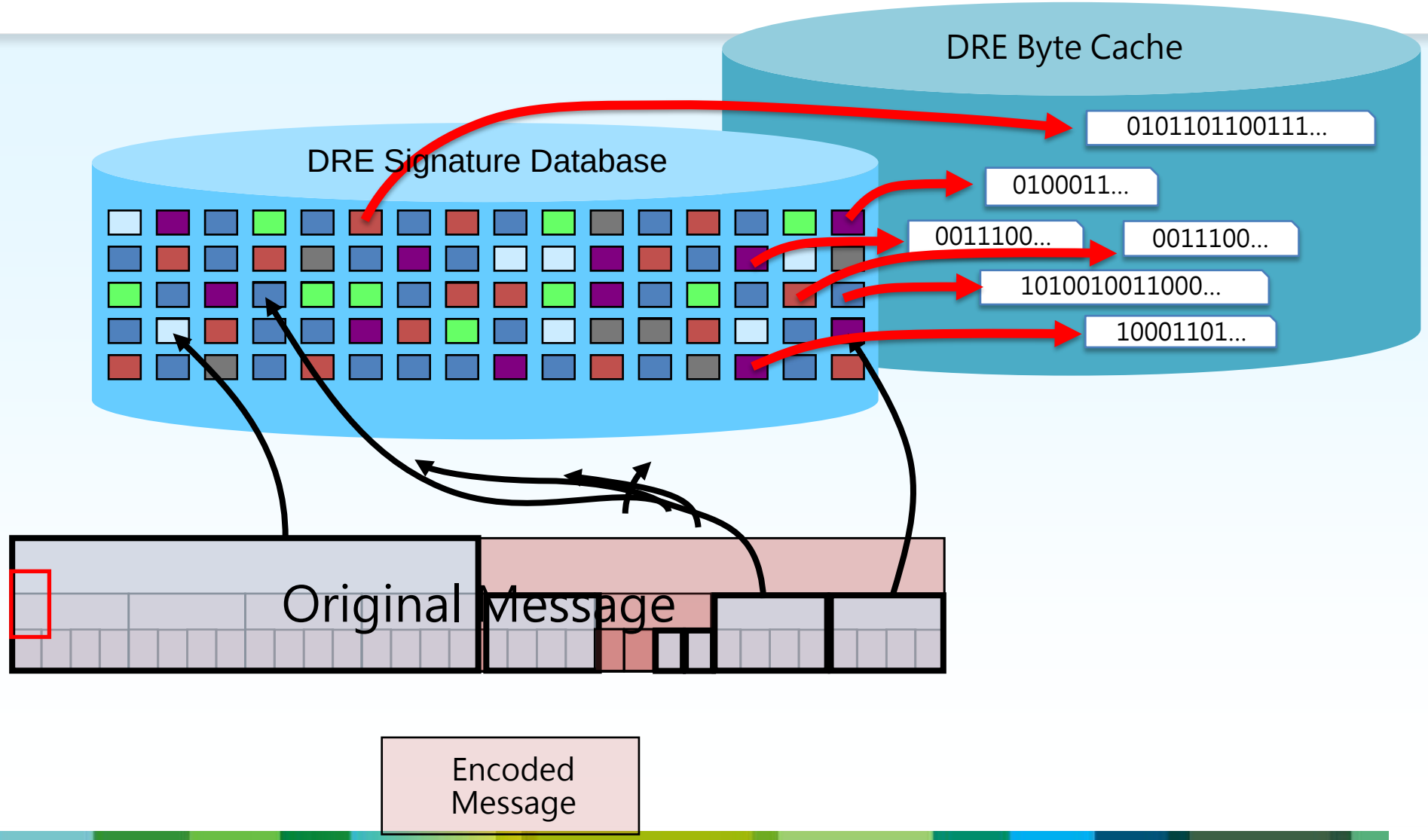


as latency increases, throughput drops (a lot)

Building Blocks of WAAS



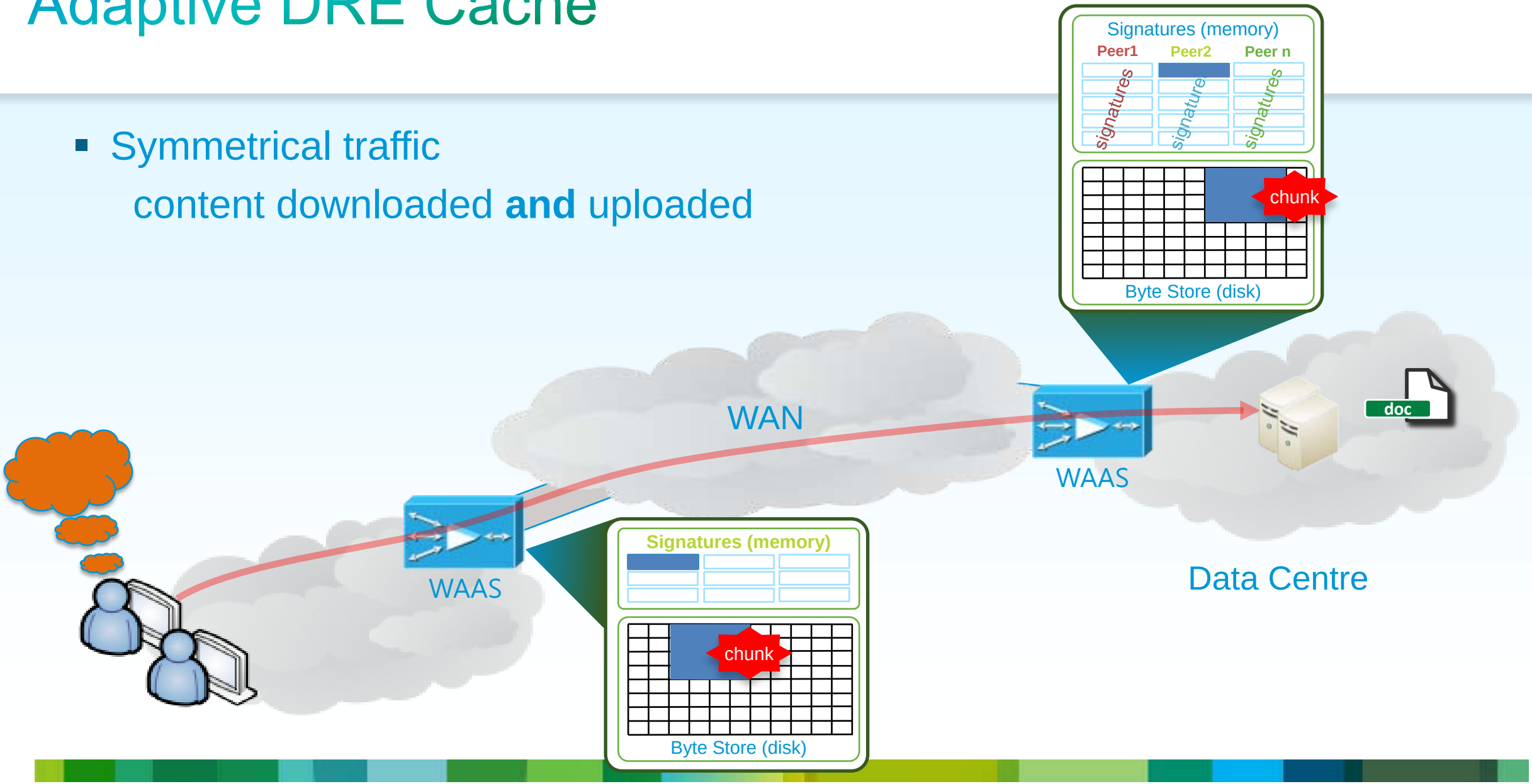
DRE Pattern Matching



Adaptive DRE Cache

- Symmetrical traffic

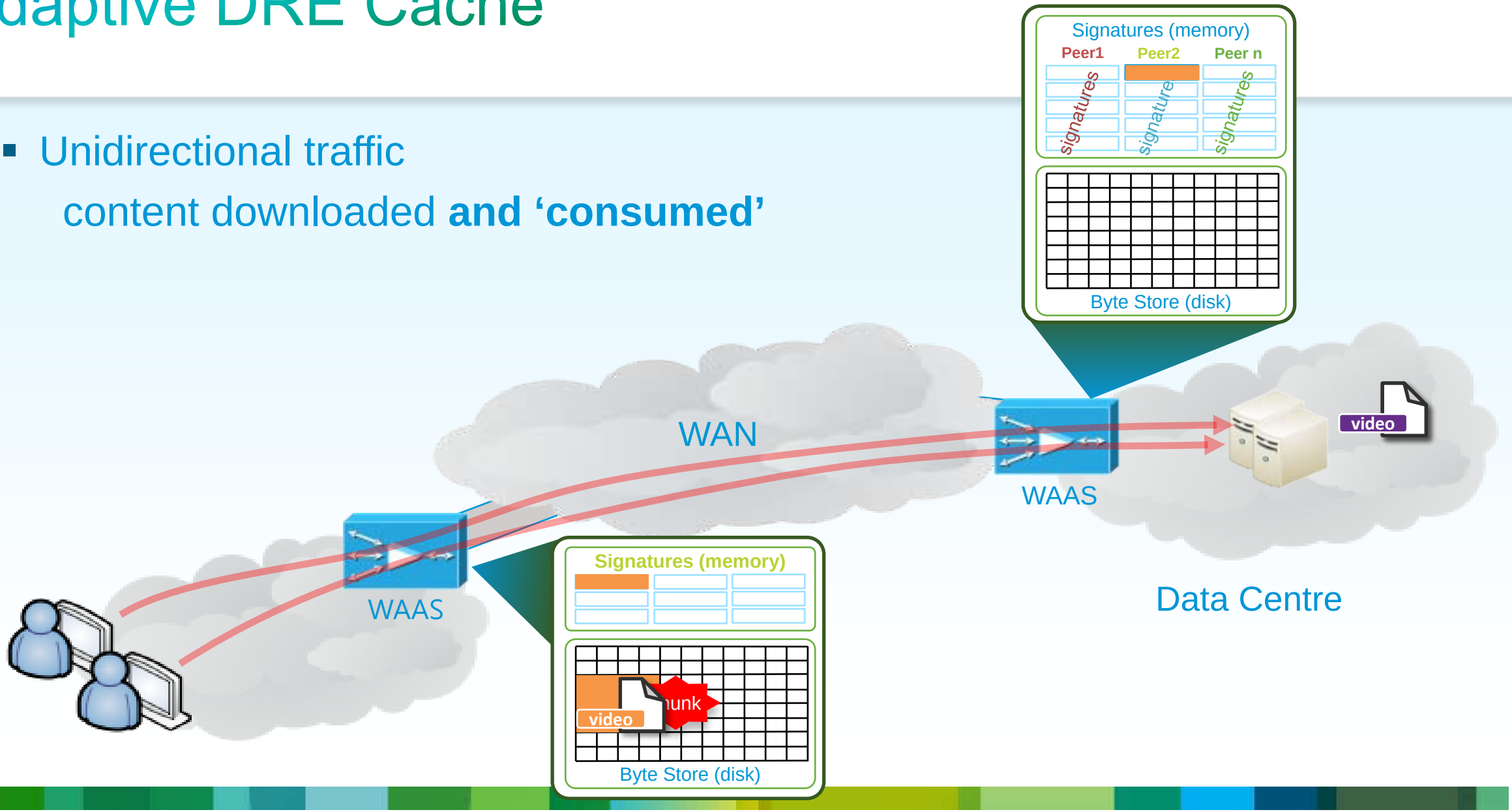
  content downloaded **and** uploaded



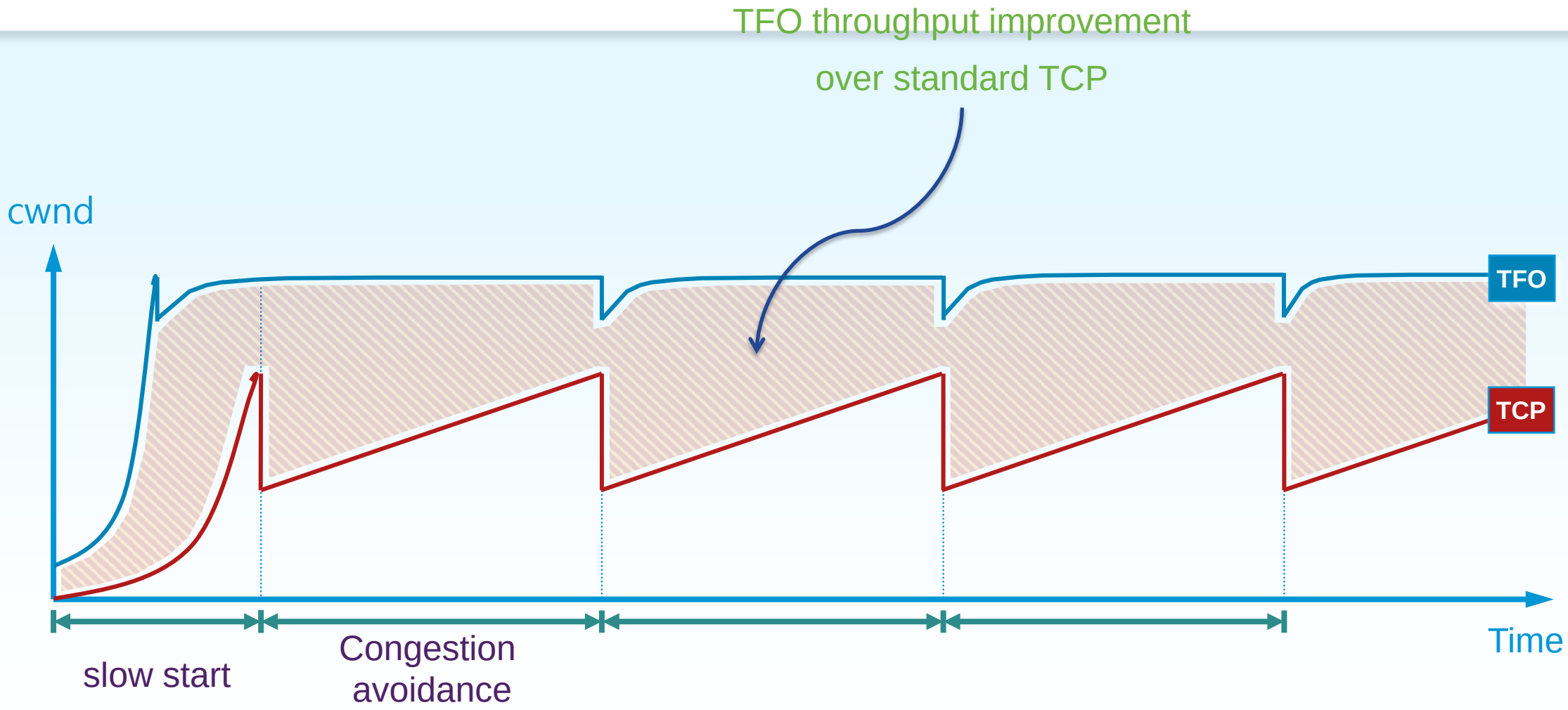
Adaptive DRE Cache

- Unidirectional traffic

  content downloaded **and 'consumed'**

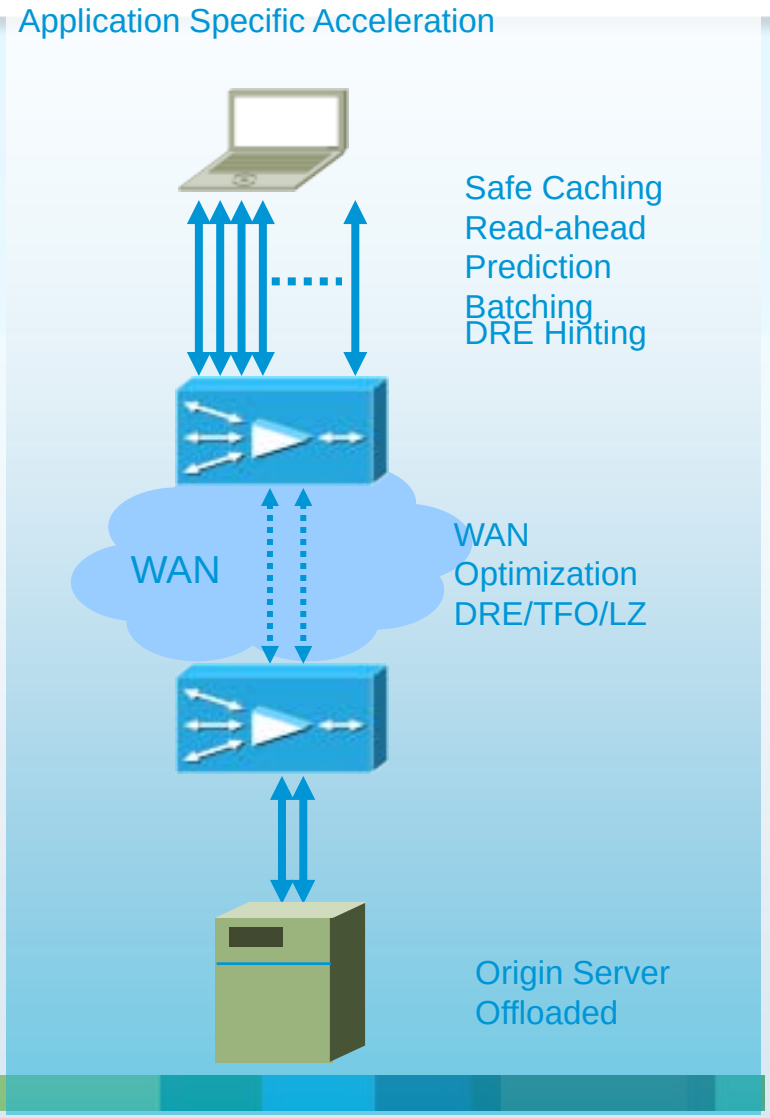


TCP Flow Optimizations



Application-Specific Acceleration

- Application and protocol awareness
  - Eliminate unnecessary chatter
  - Save WAN bandwidth
  - Pre-populate edge cache as necessary
  - Enable disconnected operations
- Intelligent protocol acceleration
  - Read-ahead, prediction, and batching
  - Safe data and metadata caching
  - Improves application response time
  - Provide origin server offload
- DRE Hints
  - Application intelligence signals to DRE & LZ…
    - whether to compress
    - whether to cache

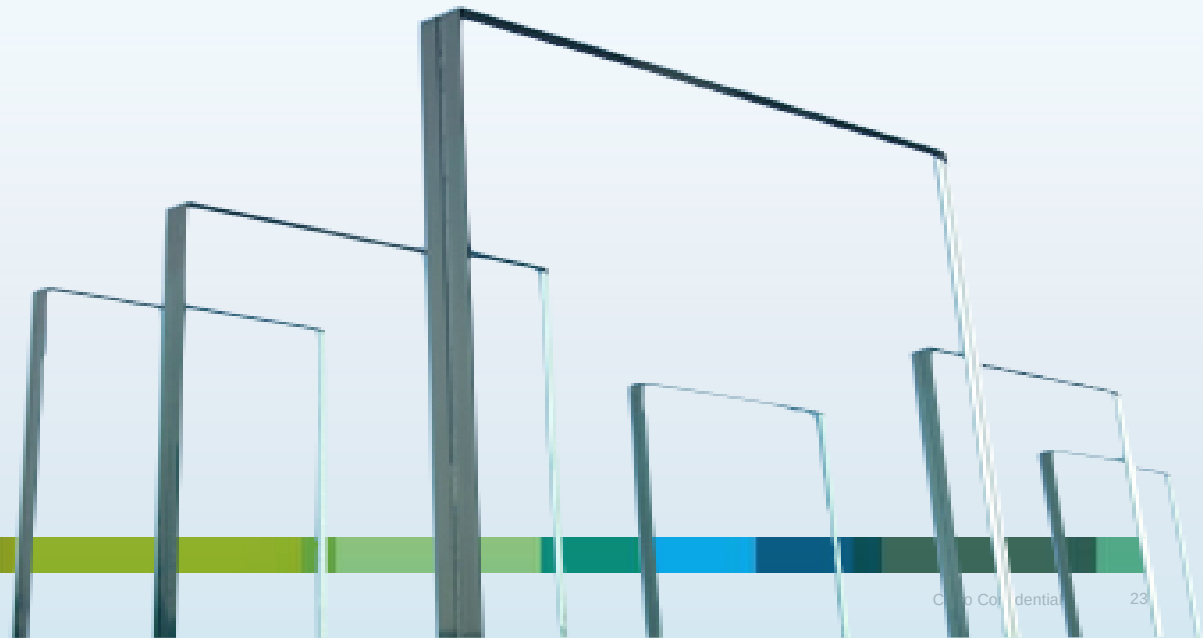


Application Optimizers

SMBv1
SMBv2
SMBv3

- (includes print services and signed)

- MAPI / eMAPI
- HTTP
- HTTPS
- NFS
- Citrix ICA



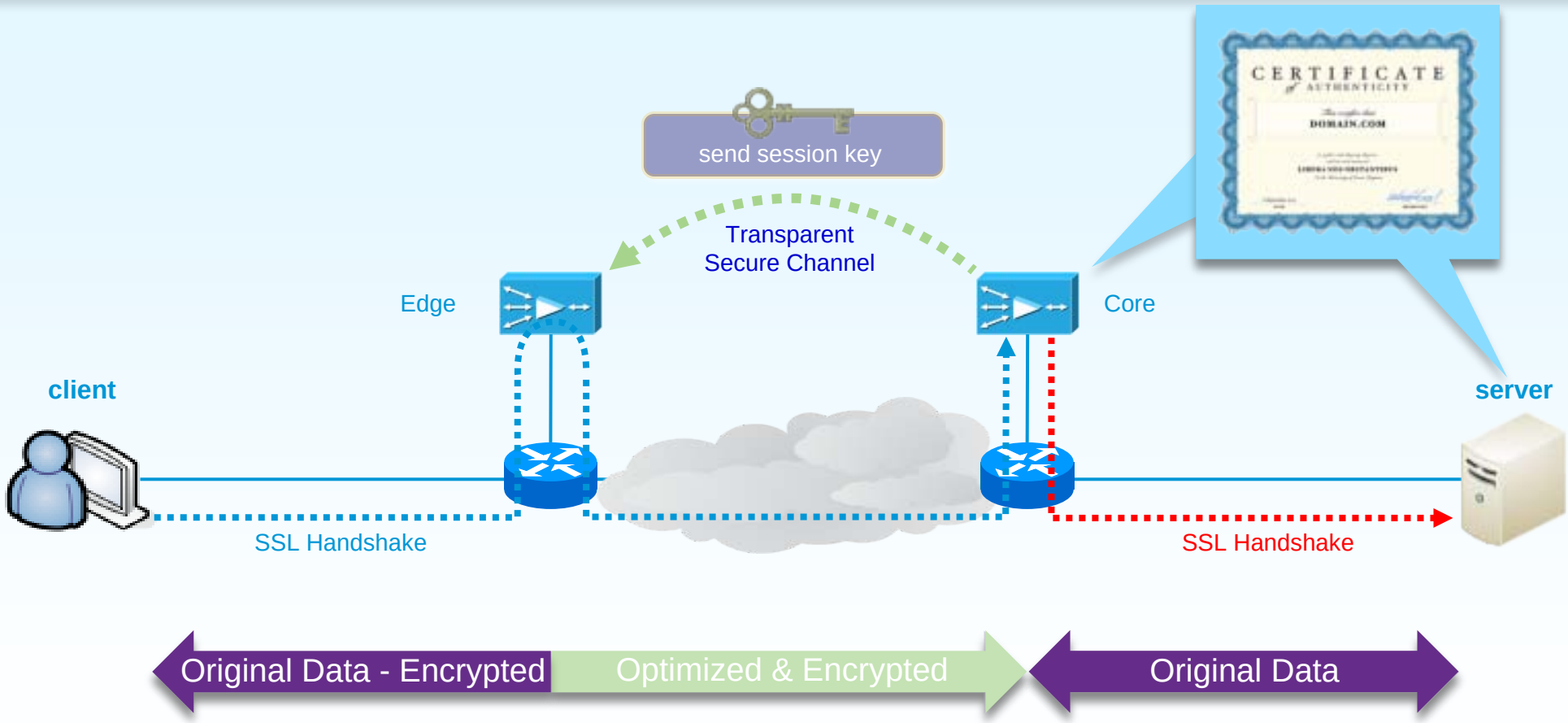
What about …

encrypted traffic?

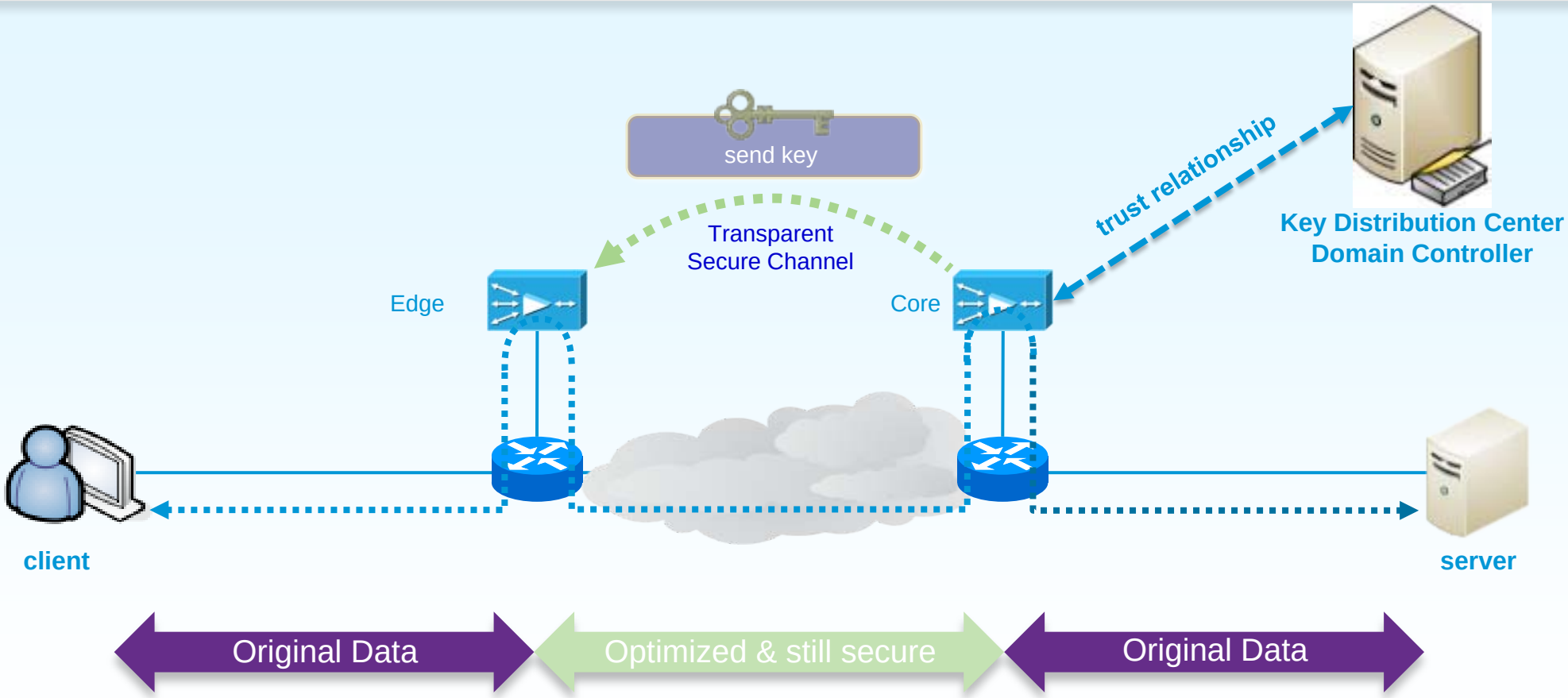
signed traffic?

compressed traffic?

Dealing with Encryption



Microsoft Encryption & Signed traffic



What about compression?

Compress already compressed traffic?

Bad idea…

Better Idea:

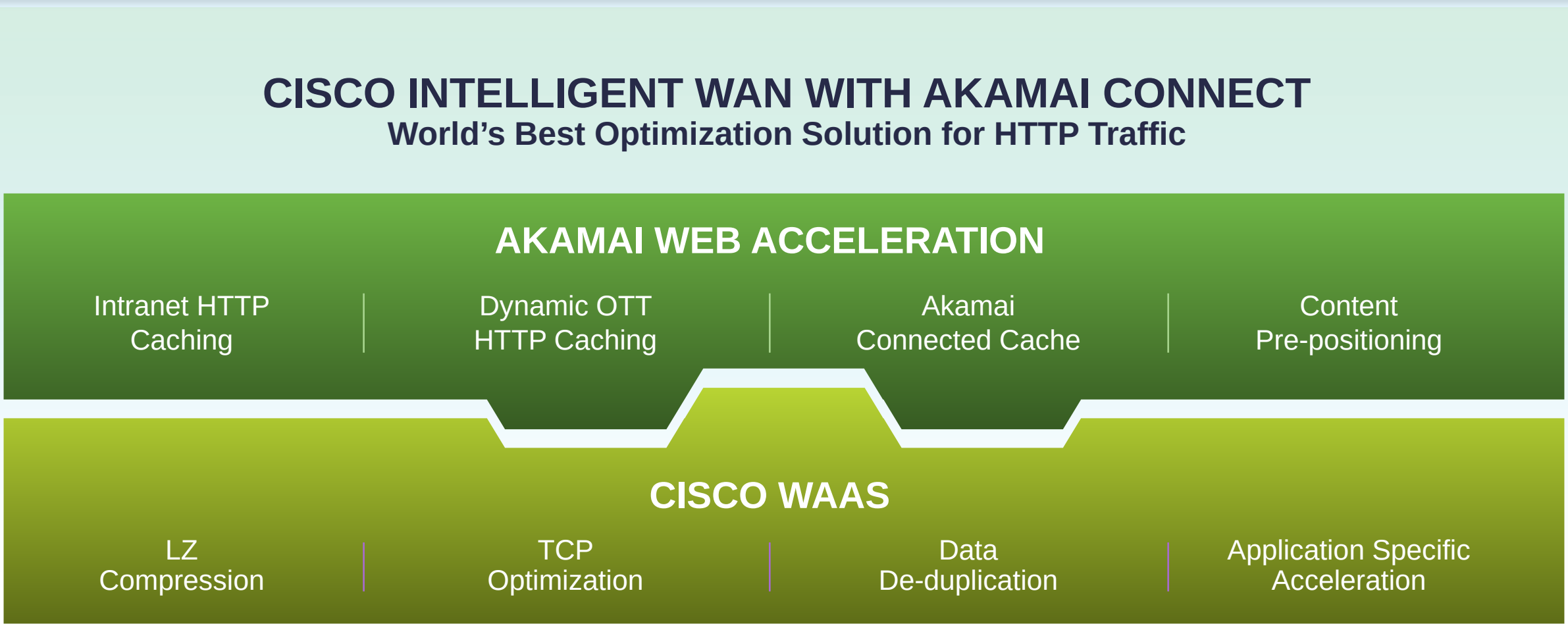
Turn it off!

Why?

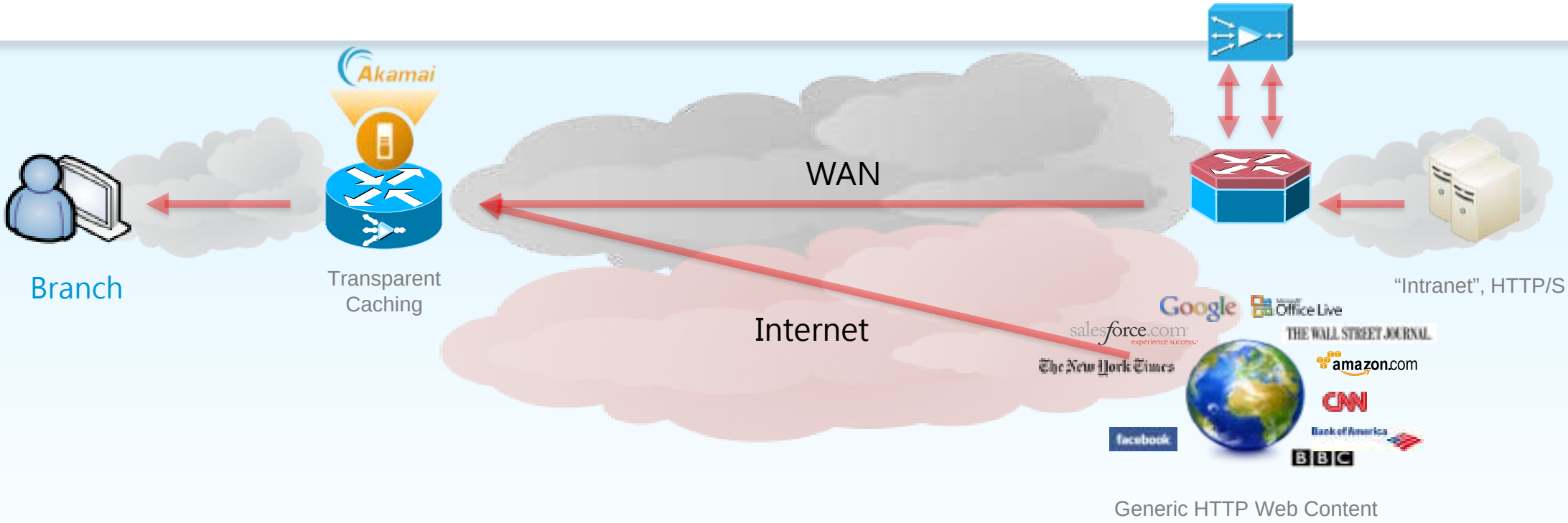
HTTP GZIP, ICA compression, EMSMDB compression

Building On Cisco WAAS Solution

Akamai Caching Enhances the User Experience



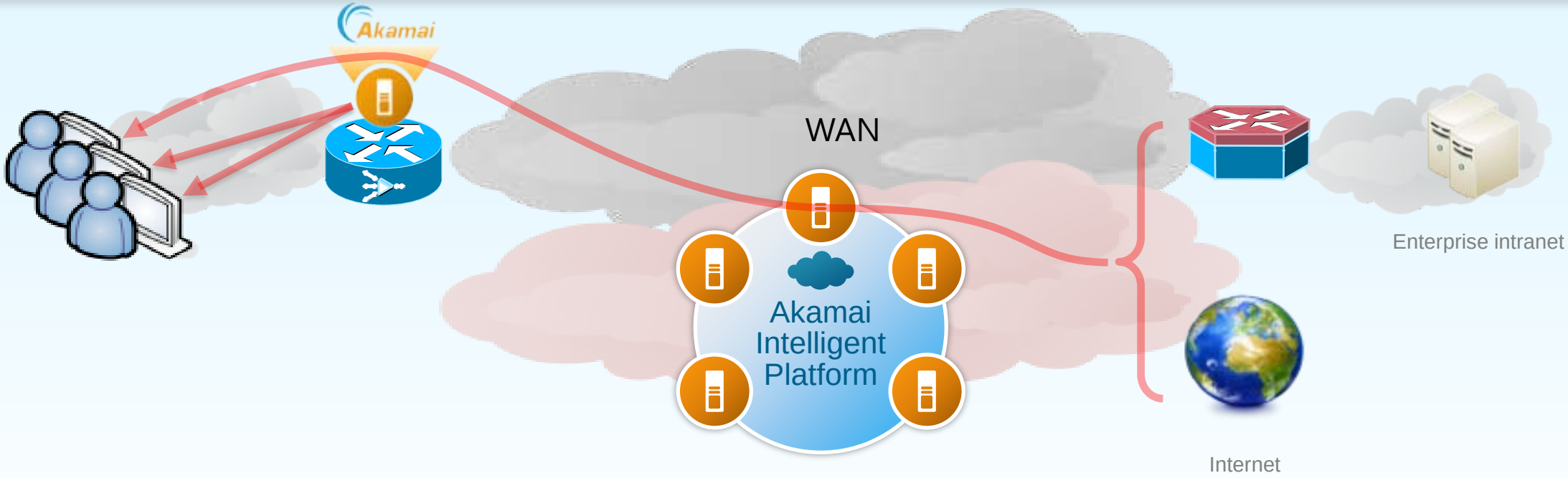
Akamai Connect – Transparent Cache



- Improve User Experience
- Reduce network congestion

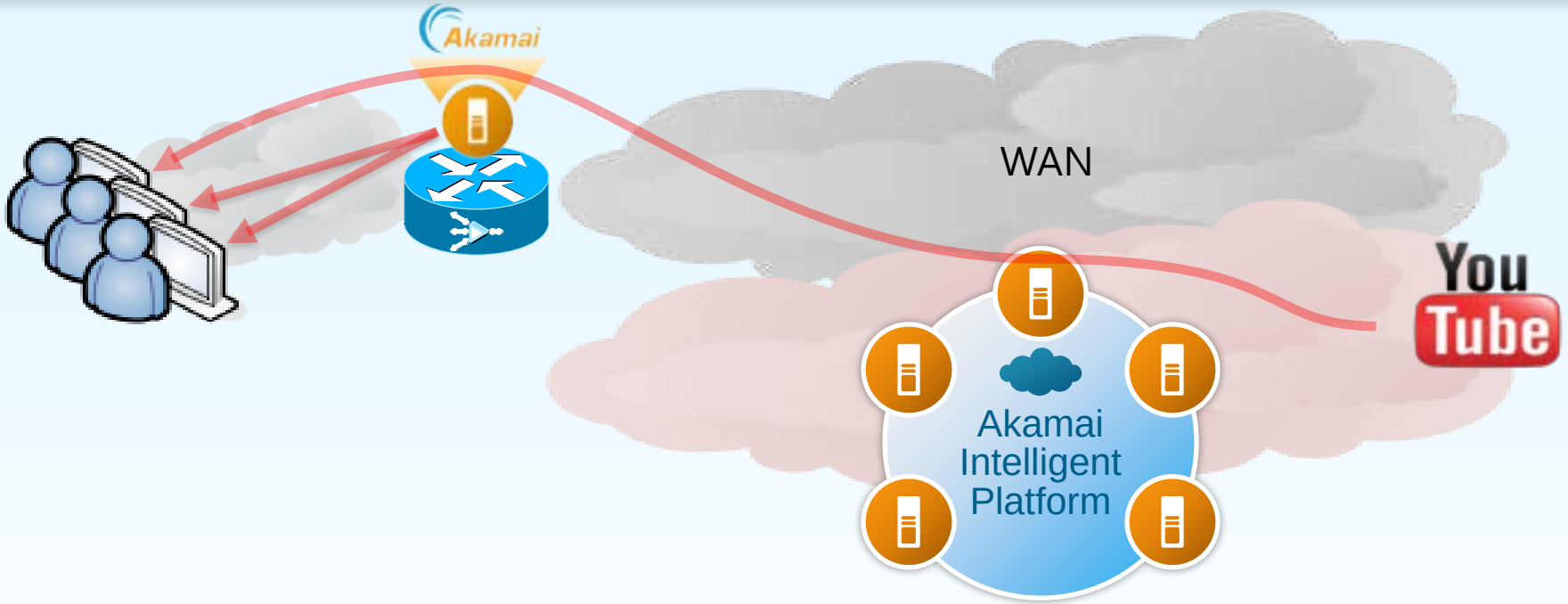
- Akamai smarts for caching
- WAAS provides:
  - SSL Handling
  - Transport Optimization
  - Deduplication

Akamai Connect – Use Case 1



- Generic Web Cache

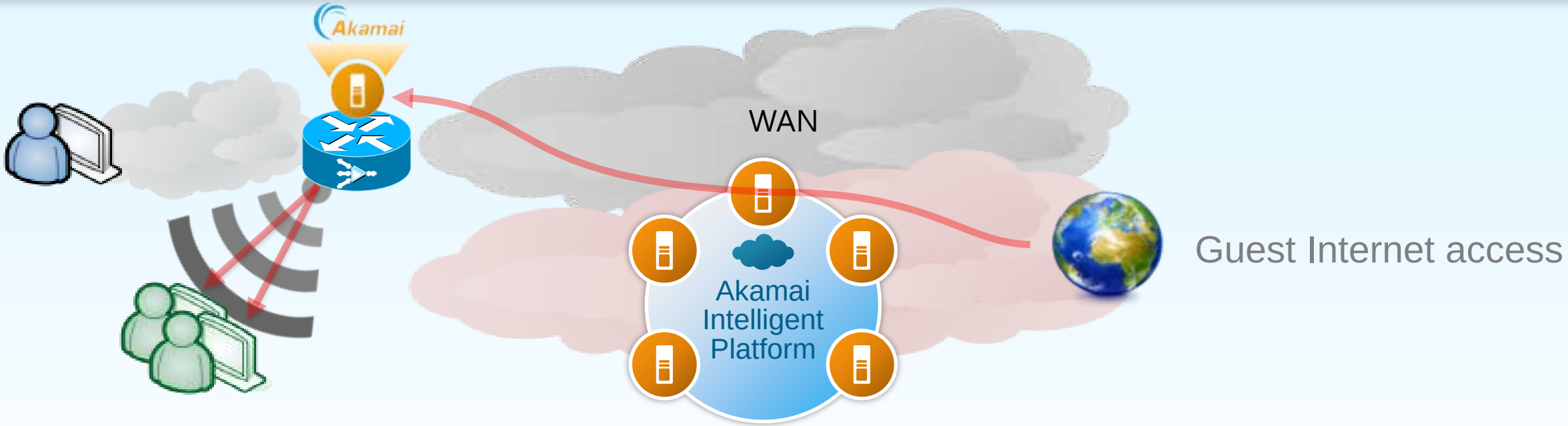
Akamai Connect – Use Case 2



YouTube channel
Training videos
Viral videos

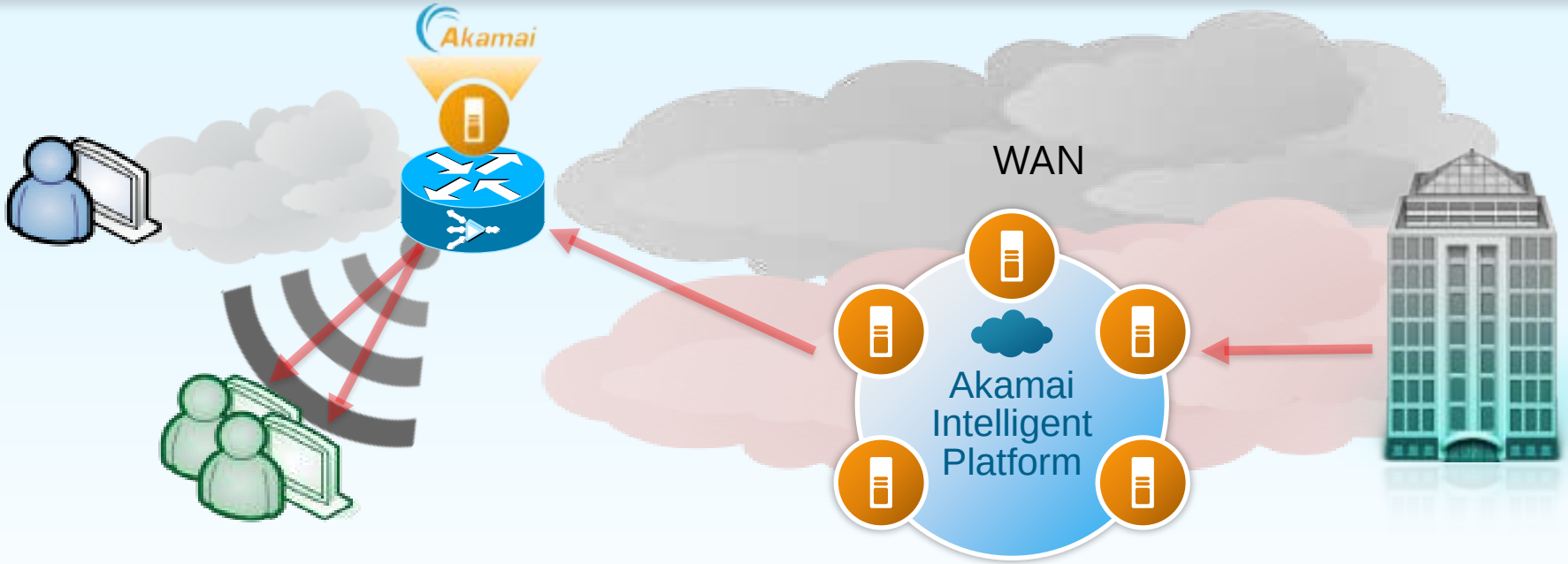
- Generic Web Cache
- Training: over-the-top cache

Akamai Connect – Use Case 3



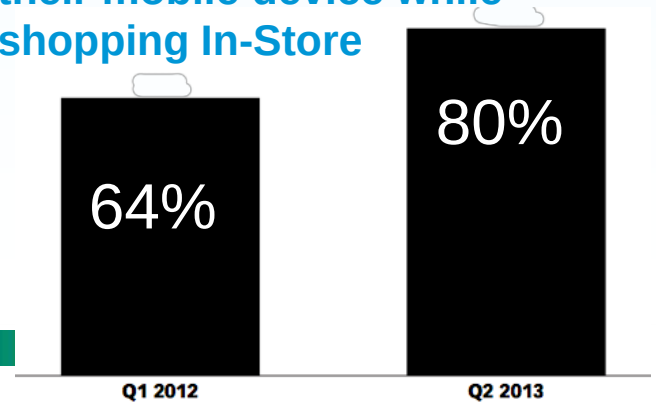
- Generic Web Cache
- Training: over-the-top cache
- Guest Wi-Fi

Akamai Connect – Use Case 4



- Generic Web Cache
- Training: over-the-top cache
- Guest Wi-Fi
- Omnichannel retail

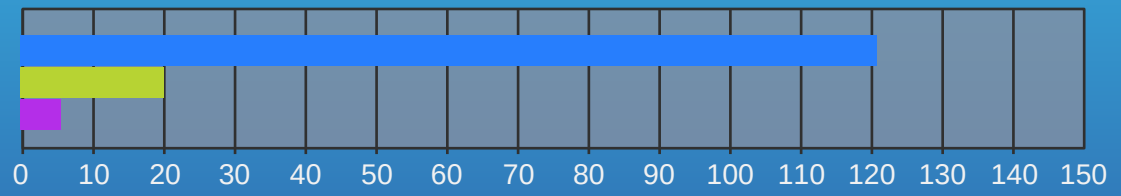
US mobile Wi-Fi users who Use their mobile device while shopping In-Store



But does it work?

WAAS Delivers User Experience at Scale

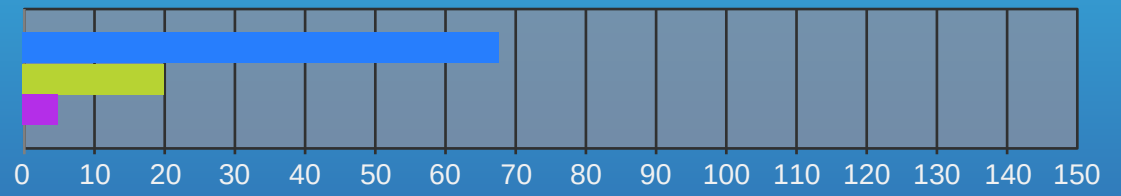
Email



- Send and Receive Email over native WAN
- First Optimized with WAAS
- Second Pass Optimized with WAAS

24x FASTER

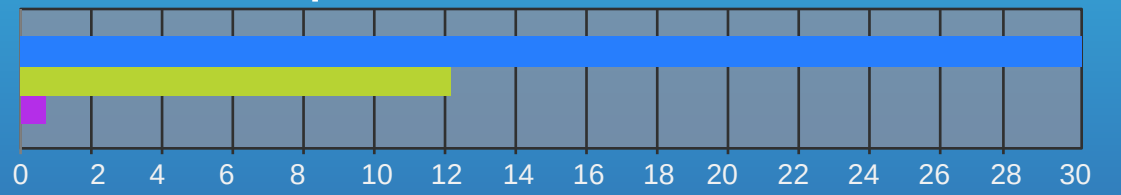
File Services



- File Drag and Drop Over native WAN
- First Optimized with WAAS
- Second Pass Optimized with WAAS

17x FASTER

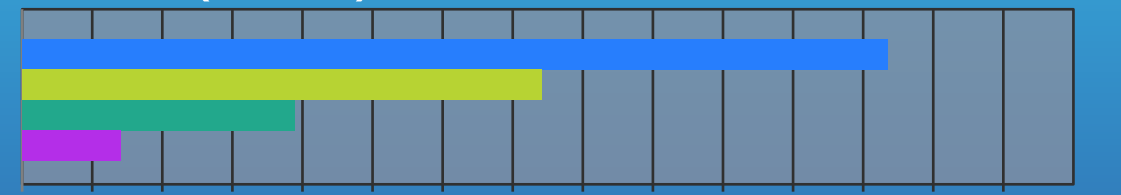
MS Sharepoint



- Sharepoint File Download over Native WAN
- First Pass Optimized with WAAS
- Second Pass Optimized with WAAS

30x FASTER

VDI (Citrix)



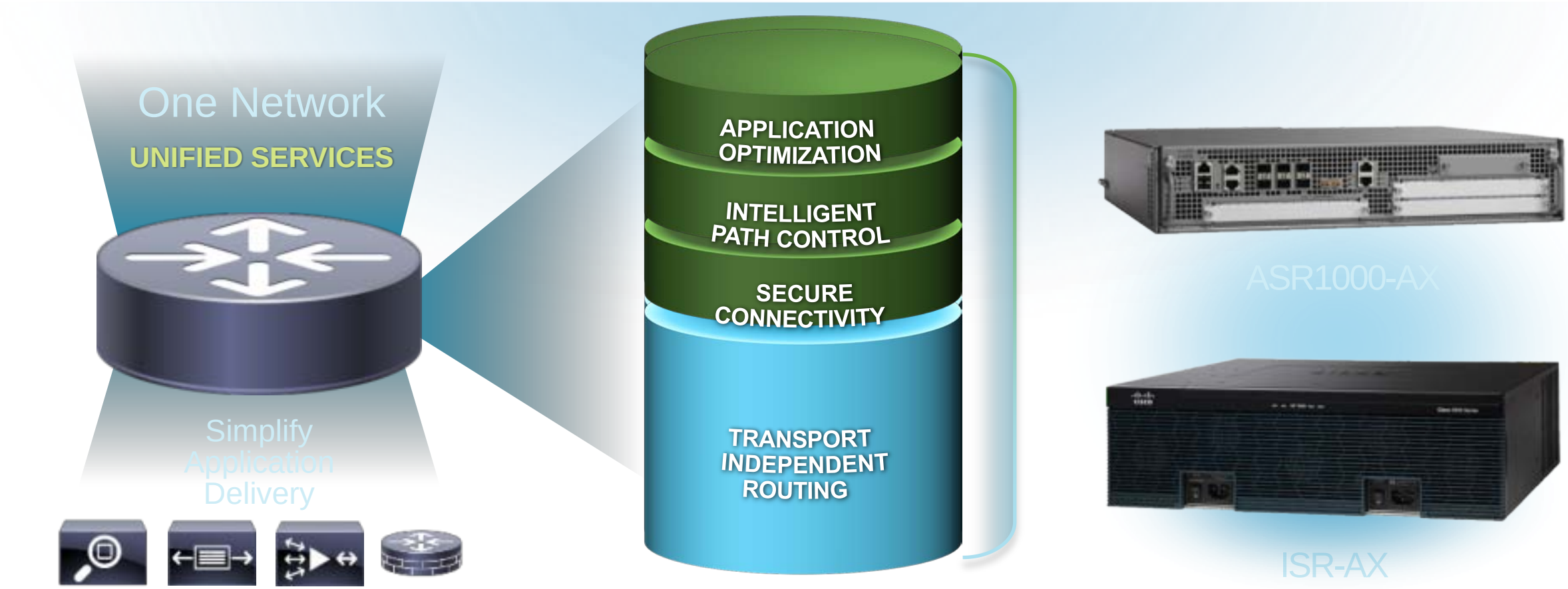
- Launch Citrix XenDesktop Over Native Citrix ICA/SSL
- Launch Citrix XenDesktop with WAAS
- Site Navigation Over Native Citrix ICA/SSL
- Site Navigation with WAAS

3-8x FASTER

Deployment Options: Evolution of Integration

Start with Cisco AX Routers

IWAN Capabilities Embedded in the Network Services Platform



Cisco AX Routers ISR-4000-AX | 3900-AX | 2900-AX | 1900-AX | 800-AX | ASR1000-AX

Cisco Branch Router Evolution

Support UCS E-series

Cisco 2500
Cisco's first family of branch routers for 23 different deployments

1993

Cisco 2600
Superseded 2500. Considered one of Cisco's premier products.

1998

ISR G1 family
1800, 2800, 3800
The first architecture custom designed for integrated services

2004

ISR G2 family
800*, 1900, 2900 & 3900
Taking the ISR concept to the next level

2009

ISR 4451-X
First ISR based on IOS XE

2013

ISR 4431 & 4300 family
Making for a complete ISR 4000 family

2014

- Not shown here: 700, 1600, 1700, 4000/4500, 3600 & 3700 series routers

*ISR800 series do not support UCS E-series

New Cisco ISR 4000 Series

Turbo Charging the Intelligent WAN

1000+ Customers

ISR 4451
1-2Gbps

ISR 4431
500-1000 Mbps

ISR 4351
200-400 Mbps

ISR 4331
100-300 Mbps

ISR 4321
50-100 Mbps

Now Available

Award Winning Architecture
4-10X Faster
Cisco ONE Software

Delivering a High Quality Experience Across All Branches

Cisco UCS E-Series Servers

Cisco UCS E-Series Servers

Scalability

Cisco UCS-E140S

- Service Module
- Vmware, Hyper-V, Citrix Certified
- Intel E3 4 Core Processor
- vWLC, vWAAS, Physical Security

Cisco UCS-E160D

- Service Module
- Vmware, Hyper-V, Citrix Certified
- Intel E5 6 Core Processor
- vWLC, vWAAS, Virtual Desktops, Physical Security

Cisco UCS-E180D

- Service Module
- Vmware, Hyper-V, Citrix Certified
- Intel E5 8 Core Processor
- vWLC, vWAAS, Virtual Desktops, Physical Security, Security applications

Performance

Cisco UCS E-Series Single-Wide Blade

Compact Blade Housed in Cisco ISR G2 and ISR 4000 Chassis – UCS-E140S M2

8, 12, and 16 GB DRAM options

Maximum 65 W power draw 80 percent less than server

Intel® Xeon® E3 Family quad-core processor

Configuration and management through CIMC

Remote and schedulable power management

Two SD cards: One for the CIMC and temporary storage of OS and one for a blank virtual drive

One external and two internal GE ports

Up to 2 SATA, SAS, or SSD hard drives

10/100 Ethernet management port

USB 2.0 port for external device connectivity

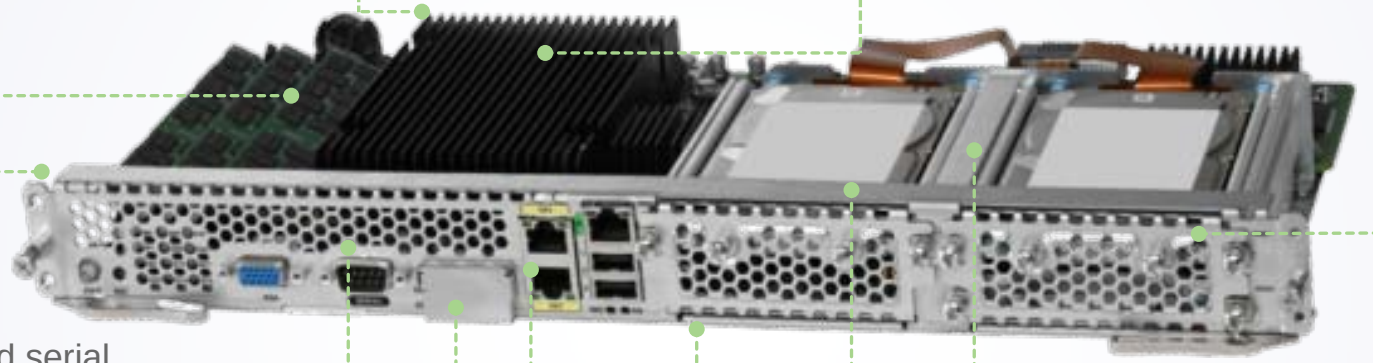
KVM console connector

On-board hardware RAID 0/1 with hot-swappable capability

Wire-free, plug-and-play modularity, low shipping weight (2.5 lb/1.1 kg)

Cisco UCS E-Series Double-Wide Blade

Multipurpose Blade Housed in ISR G2 and ISR 4000 Chassis – UCS-E160DM2/UCS-E180DM2



8 GB – 96* GB DRAM options

Maximum 130 W power draw, 80 percent less than server

Intel Xeon E5-2400 Quad Core/Six-Core/Eight-Core Processor

Remote and schedulable power management

Out-of-band configuration and management through CIMC

Front-panel VGA, 2 USB, and serial console connectors

Up to 3 SATA, SAS, SSD hard drives or 2 HDD and a PCIe card

Two SD Cards: one for the CIMC and temporary storage of OS and one for a blank virtual drive

On-board hardware RAID 0, 1, and 5 configuration options with hot-swappable capability

Two external and two internal GE ports with TCP/IP acceleration

Wire-free, plug-and-play modularity, low shipping weight (7 lb / 3.2 kg)

Hardware Comparison Matrix (UCS E-Series)

	UCS-E140S M2	UCS-E160D M2	UCS-E180D M2
Processor	Intel Xeon E3-1105C v2 (1.8 GHz)	Intel Xeon E5-2418L v2 (2.0 GHz)	Intel Xeon E5-2428L v2 (1.8 GHz)
Core/vCPU	4/8	6/12	8/16
Memory	8 - 16 GB	8 - 96 GB	8 - 96 GB
Storage	Up to 3.6 TB (2 HDD bays) SATA, SAS, SED, SSD	Up to 5.4 TB (3 HDD bays) SATA, SAS, SED, SSD	Up to 5.4 TB (3 HDD bays) SATA, SAS, SED, SSD
RAID	RAID 0 & RAID 1	RAID 0, RAID 1 & RAID 5	RAID 0, RAID 1 & RAID 5
Network Port	Internal: 2 GE Ports External: 1 GE Port	Internal: 2 GE Ports External: 2 GE Ports	Internal: 2 GE Ports External: 2 GE Ports
Platforms	4451-X, 4351, 4331, 2911,2921, 2951, 3925,3945,3925E, 3945E	4451-X, 4351, 2911,2921, 2951, 3925,3945,3925E, 3945E	4451-X, 4351, 2911,2921, 2951, 3925,3945,3925E, 3945E

UCS E-Series in an ISR Chassis

ISR	UCSE 140S M2	UCSE 160D M2	UCSE 180D M2	Max Modules / Router
2911	Yes	No	No	1 SW
2921	Yes	Yes	No	1 SW or 1 DW
2951	Yes	Yes	No	2 SW or 1 DW
3925	Yes	Yes	Yes	2 SW or 1 DW & 1 SW
3925E	Yes	Yes	Yes	2 SW or 1 DW & 1 SW
3945	Yes	Yes	Yes	4 SW or 2 SW & 1 DW
3945E	Yes	Yes	Yes	4 SW or 2 SW & 1 DW
ISR 4451-X	Yes	Yes	Yes	2 SW or 1 DW
ISR 4431	No	No	No	NA
ISR 4351	Yes	Yes	Yes	2 SW or 1 DW
ISR 4331	Yes	No	No	1 SW
ISR 4321	No	No	No	NA

Cisco UCS E-series Network Compute Engine

Scalability

Available 3QCY15

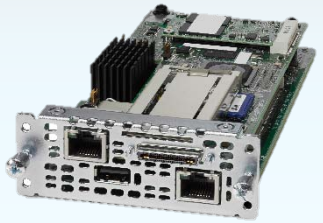
Cisco UCS-EN 120E

(Supported on ISR-G2 Only

- Enhanced HWIC
- Virtualization Enabled
- Network Compute Applications
  - vWLC, vWAAS

Cisco UCS-EN 140N

(Supported on ISR4000 Only



- NIM network compute module
- Virtualization Enabled
- Network Compute Applications
  - vWLC, vWAAS

Cisco UCS-EN 120S

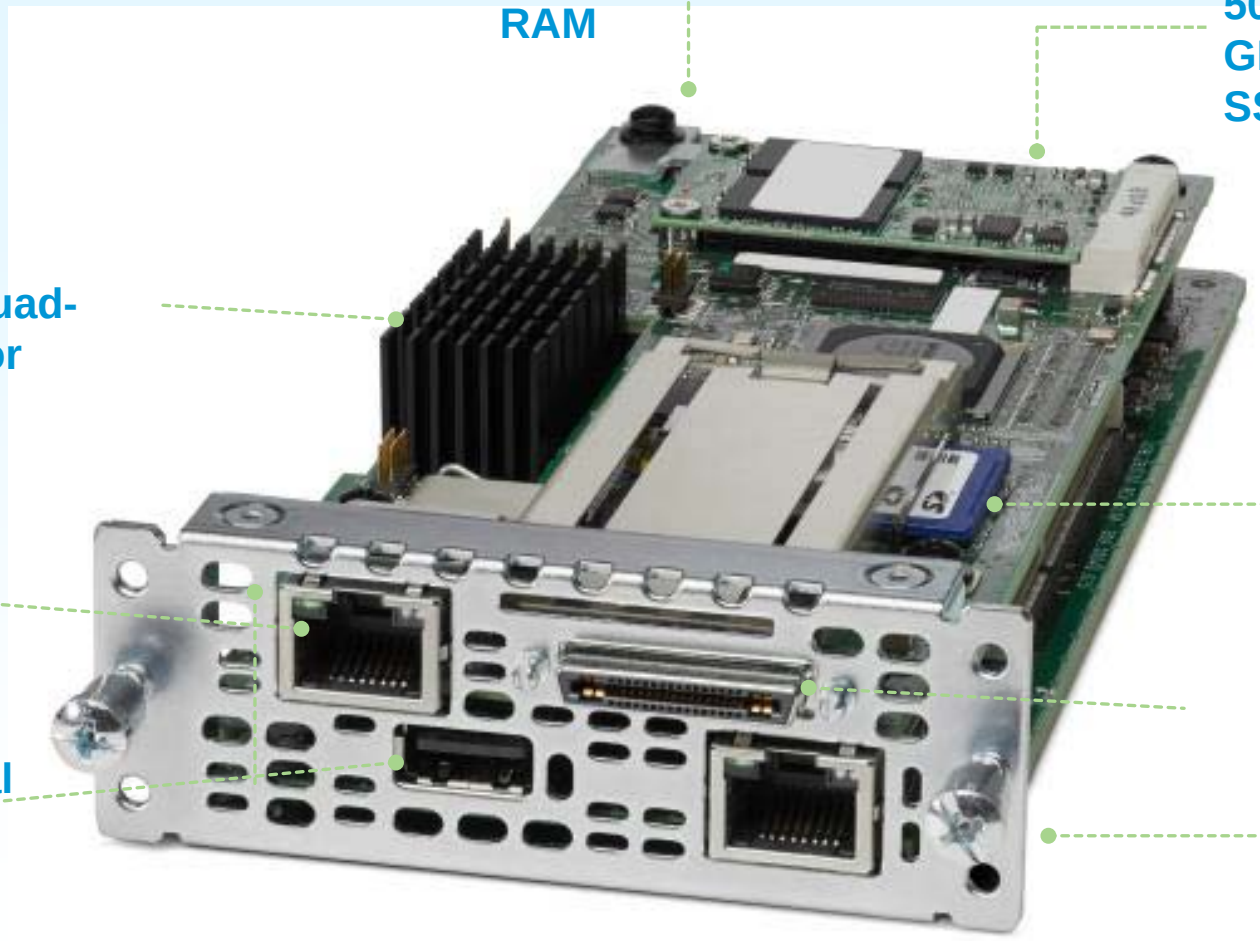
- Service Module
- VMware and Hyper-V Certified
- Network Compute Applications – vWLC, vWAAS

Performance

Cisco UCS E-Series Network Compute Engine

Compact, Multipurpose Blade Housed in ISR 4000 – UCS-EN140N M2

Target Launch
AugustCY15'



Up to 8 GB RAM

50, 100, 200 GB mSATA SSD Options

Intel® Atom Quad-core processor

One 2GB SD card for CIMC

Dedicated Management Port

KVM console connector

USB 2.0 port for external device connectivity

One External Gigi Ethernet Interface

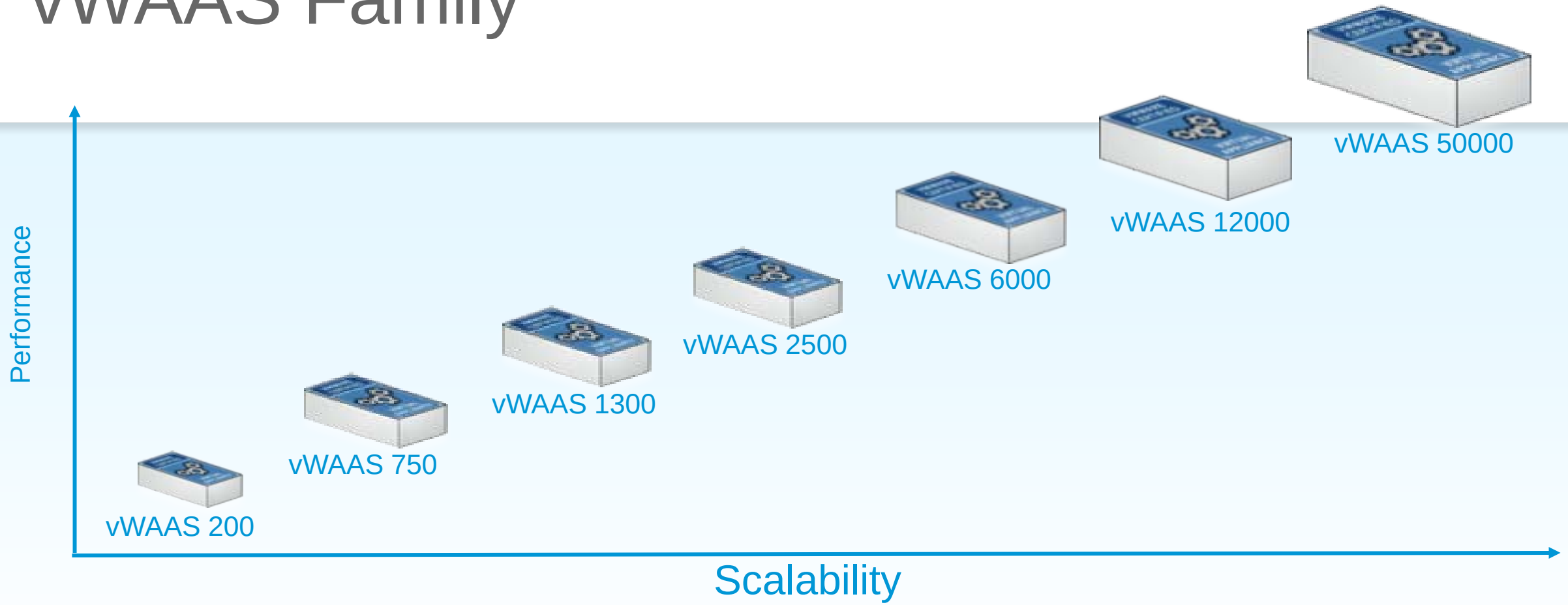
Hardware Comparison Matrix (UCS E-Series NCE)

	UCS-EN120S M2	UCS-EN140N (Only on ISR4000)	UCS-EN120E (only on ISRG2)
Processor	Intel Pentium B925C (2.0 GHz)	Intel Atom C2518 (1.7 GHz)	Intel Atom C2358 (1.7 GHz)
Core	2	4	2
Memory	8 - 16 GB	8GB	8GB
Storage	500 GB- 2 TB (2 HDD) SATA, SAS	50GB – 200GB	50GB – 200GB
RAID	RAID 0 & RAID 1	NA	NA
Network Port	Internal: 2 GE Ports External: 1 GE Port	Internal: 2 GE Ports External: 1 GE Port	Internal: 2 GE Ports External: 1 GE Port
Platforms	2911, 2921, 2951, 3925,3945, 3925E, 3945E, 4451-X, 4351, 4331	4451, 4431, 4351, 4331, 4321	1921, 1941,2911, 2921, 2951, 3925,3945,3925E, 3945E

Definitions ISR4K Application Optimization Options

- Basic = Router with IP Base license
- IWAN Base = Router with AX license which includes data and security features to run AVC, PfR, and DMVPN
- IWAN Advanced (ISRWAAS) = Router with AX license + Memory, Flash, SSD Bundle (e.g. ISR4350-MEM-MSATA) required to run ISR-WAAS
- IWAN Advanced (ISRWAAS + Akamai) = Same as above + AKC license = to the ISR-WAAS connection count
- IWAN Advanced (vWAAS) = Router with AX license + UCSE-140SM2 with recommend configuration for redundancy and ability to run more than just vWAAS -- 2 x 1TB HD, 16GB memory, Cisco Installed ESXi, ESXi host license from Cisco, and vWAAS pre-installed
- IWAN Advanced (vWAAS + Akamai) = Same as above + AKC license = to the vWAAS connection count

vWAAS Family



- ‘Personality’ encapsulated in OVF file
- DAS or SAN for DRE
- Leverages Nexus 1000v and vPath
- Suited to Multi-tenancy & Elastic Provisioning

Appliance Options

2 Gbps
150,000

WAVE-8541

1 Gbps
60,000

WAVE-7571

500 Mbps
18,000

WAVE-7541

200 Mbps
6,000

WAVE-694

100 Mbps
1,300

WAVE-594

20 Mbps
400

WAVE-294

Performance

Scalability

Cisco's innovation →Total Security

Why AMP?

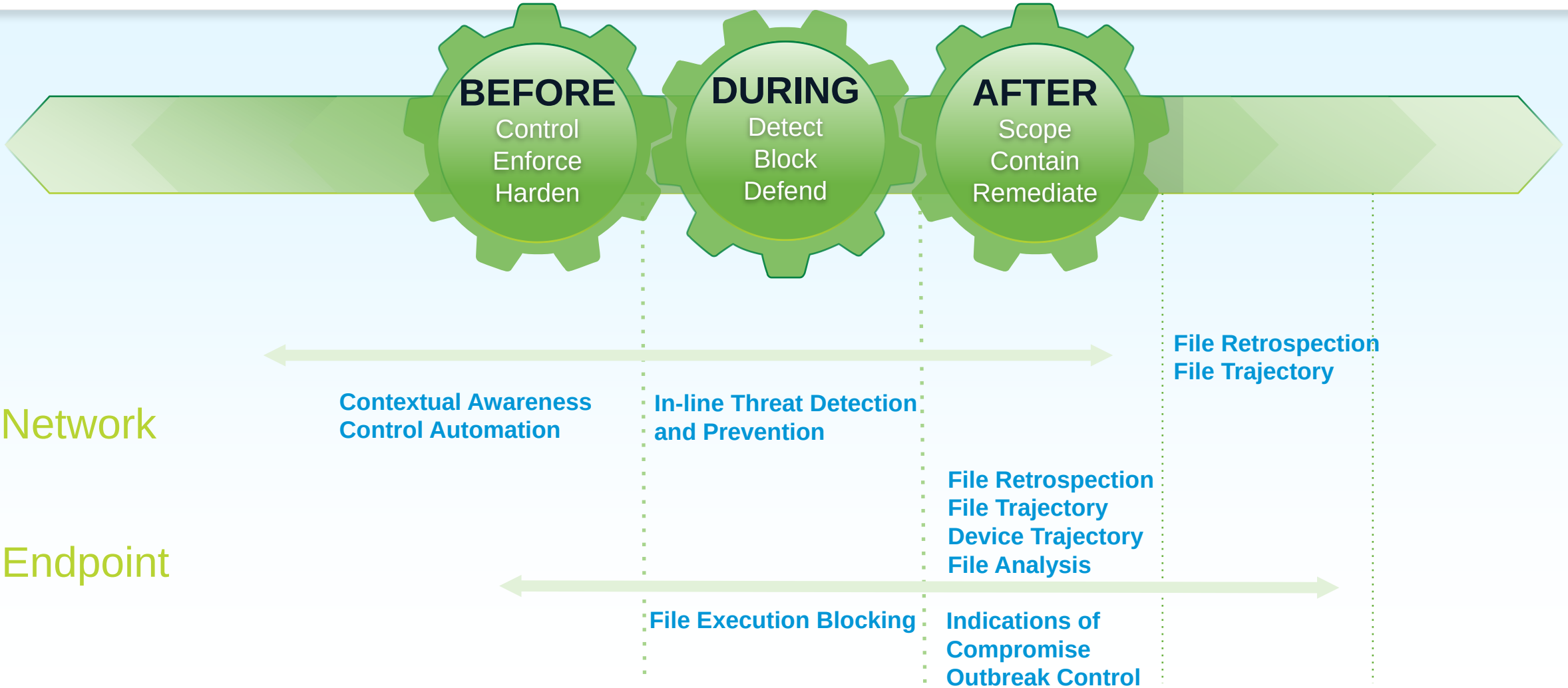
Attackers are determined and resourceful

- Malware still getting on devices, detection not 100%
- Point-in-time detection is not sufficient
- Integrated response required to be effective
- Advanced Malware Protection must be pervasive

AMP solves business problems

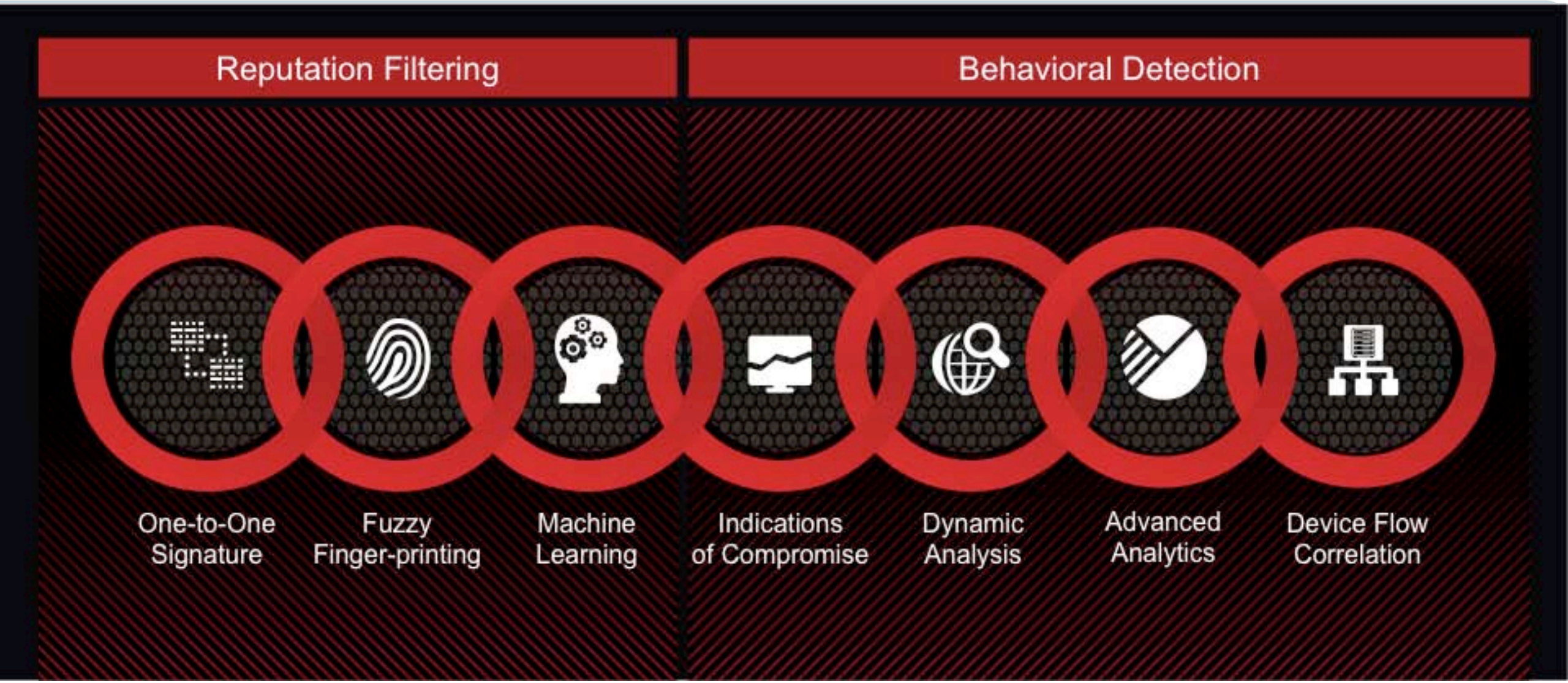
- Where do I start?
- What is the scope and how bad is the situation?
- What was the point and method of entry?
- Can I control and remediate across gateways, networks, and endpoints?

Comprehensive Security Solutions



Cisco AMP
Features and Design

Reputation Filtering and Behavioral Detection

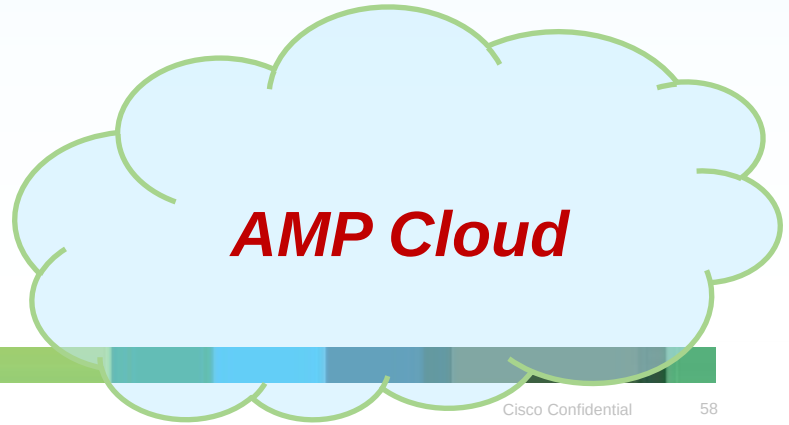


Spero Engine: Big Data and Machine Learning

- Spero is one of the detection engines in the AMP Cloud
  - Provides zero-day detection
- Creates a *feature print* of a file
  - Structural information
  - Referred DLLs
  - PE header
- Send this *feature print* to the AMP Cloud
  - Matches machine learned data trees and returns disposition
- Spero is available in AMP for Network and Windows Endpoint Connectors

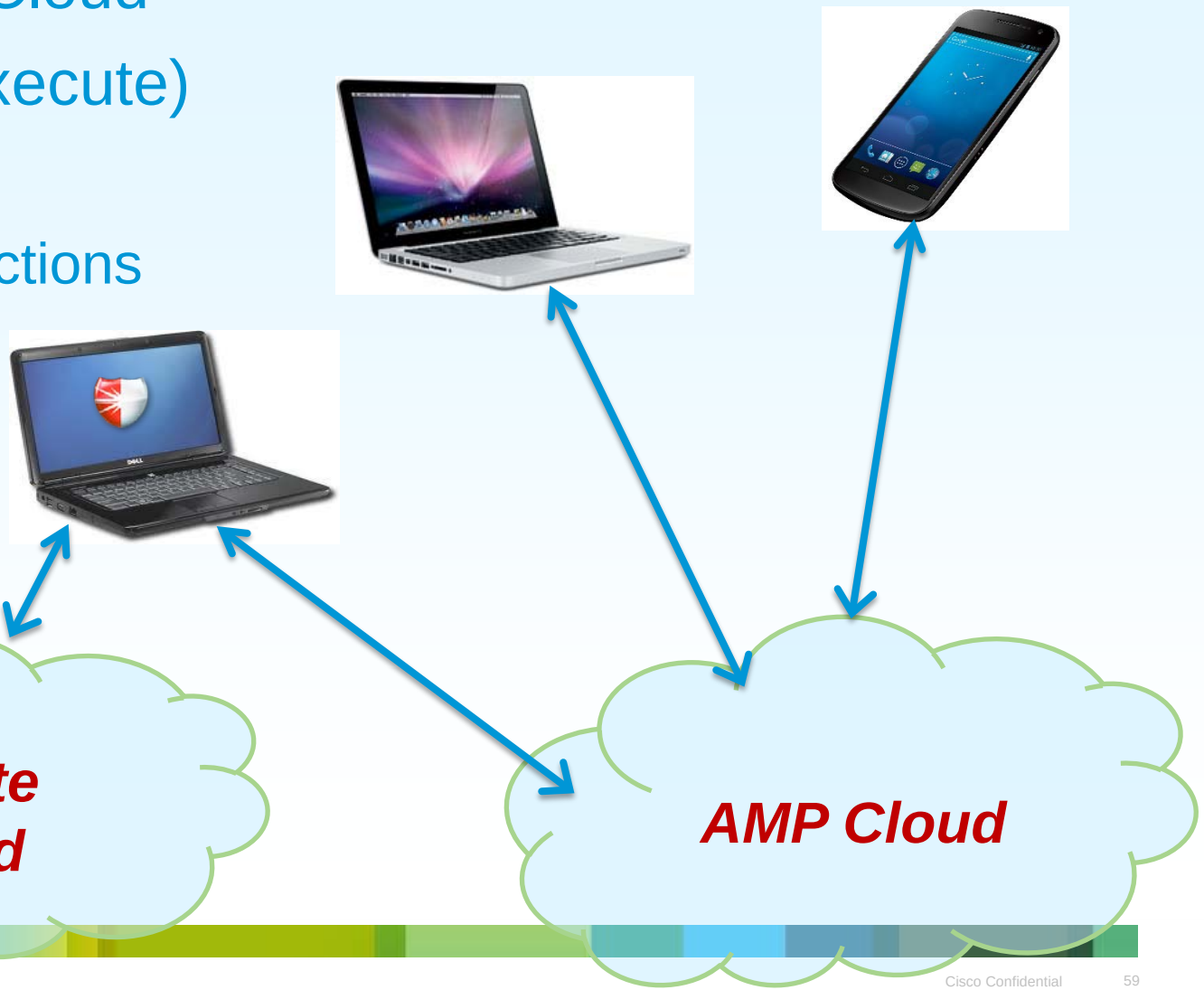
AMP Cloud Features

- Admin Portal – Deployment and Management
- Network and Endpoint Protection
- Tracking and Outbreak Control
  - Device Trajectory(設備軌跡)
  - File Trajectory(檔案軌跡)
  - Threat Root Cause
- Offloads Heavy Analysis from the Connector
- Collective Security Intelligence(CSI)



AMP for Endpoints

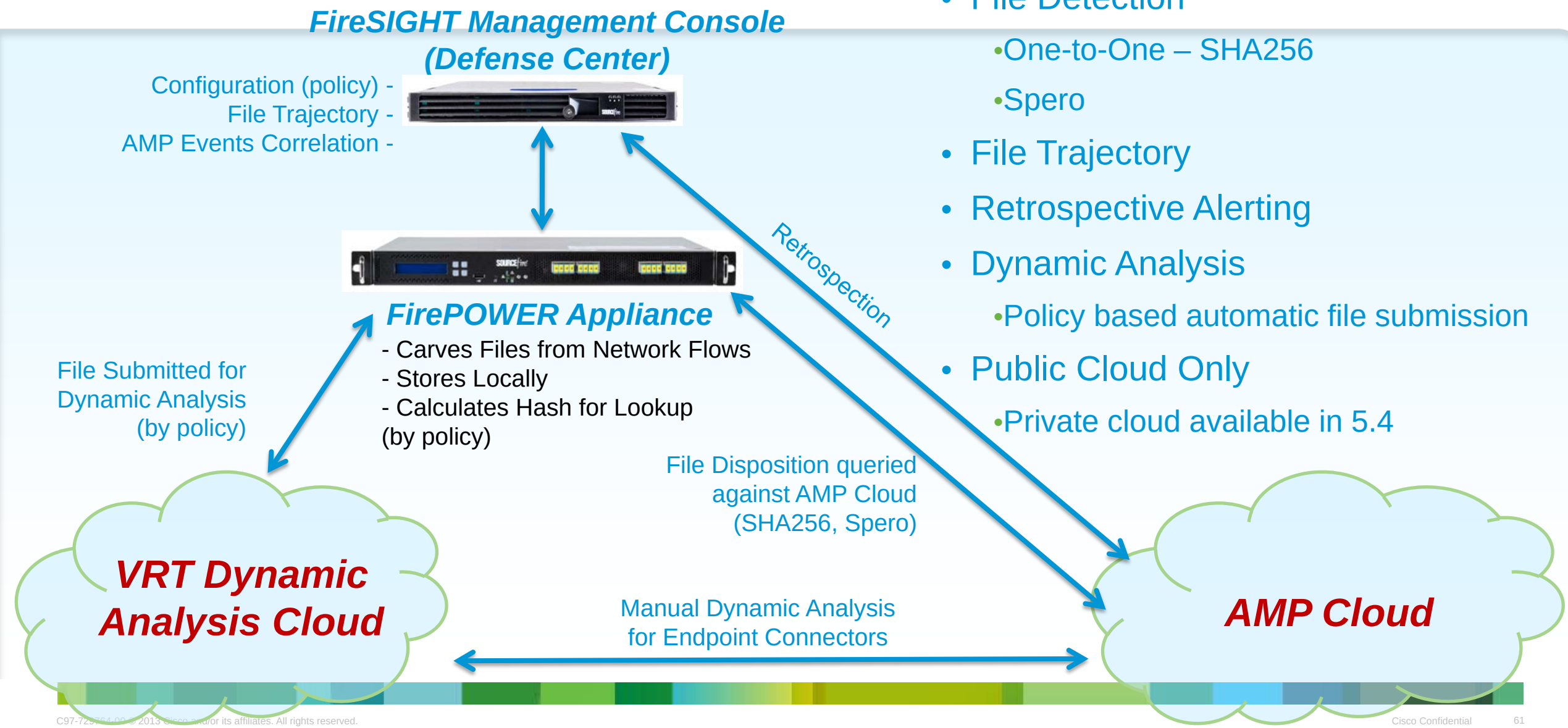
- Managed and Deployed from the Cloud
- File Activity (Created/Edit/Move/Execute)
  - One-to-One/Spero/Ethos
  - Simple and Advanced Custom Detections
- Retrospective(回顧機制) Alerting and Quarantine
- Application Control
- Network Flow Correlation
  - Black/White Lists
- Dynamic Analysis



AMP for Endpoints Capabilities

Capabilities	Windows	Mac	Android
Hash Lookups	SHA256	SHA256	SHA1
Ethos	✓	✗	✗
Spero	✓	✗	✗
Simple Custom Detections	✓	✓	✓
Advanced Custom Detections	✓	✓	✗
Retrospective Alerting	✓	✓	✓
File Quarantine	✓	✓	✗
Device Flow Correlation	✓	✓	✗
Application Control	✓	✓	✗
Supported Clouds	Public, Private	Public	Public

AMP for Networks



- Managed by FireSIGHT Management Center
- File Detection
  - One-to-One – SHA256
  - Spero
- File Trajectory
- Retrospective Alerting
- Dynamic Analysis
  - Policy based automatic file submission
- Public Cloud Only
  - Private cloud available in 5.4

AMP for Networks Integrated with AMP for Endpoints

FireSIGHT Management Console (Defense Center)

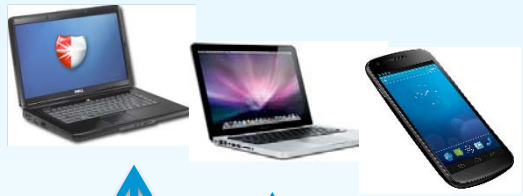
Configuration (policy) -
File Trajectory -
AMP Events Correlation -

Link to AMP Public Cloud for Endpoint Connector Events

Retrospection

FirePOWER Appliance

- Carves Files from Network Flows
- Stores Locally
- Calculates Hash for Lookup (by policy)



Endpoint Connectors

File Submitted for Dynamic Analysis (by policy)

File Disposition queried against AMP Cloud (SHA256, Spero)

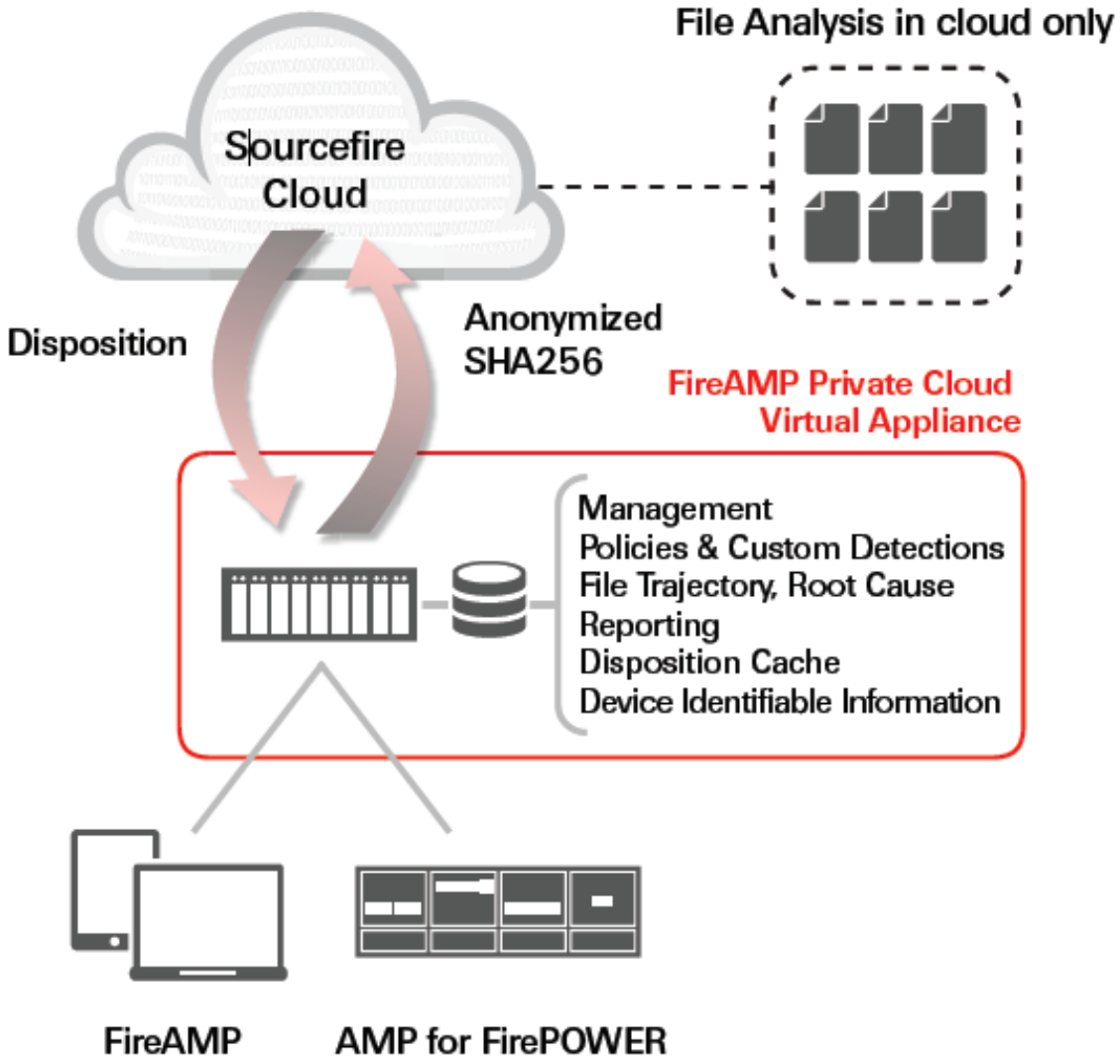
VRT Dynamic Analysis Cloud

Manual Dynamic Analysis for Endpoint Connectors

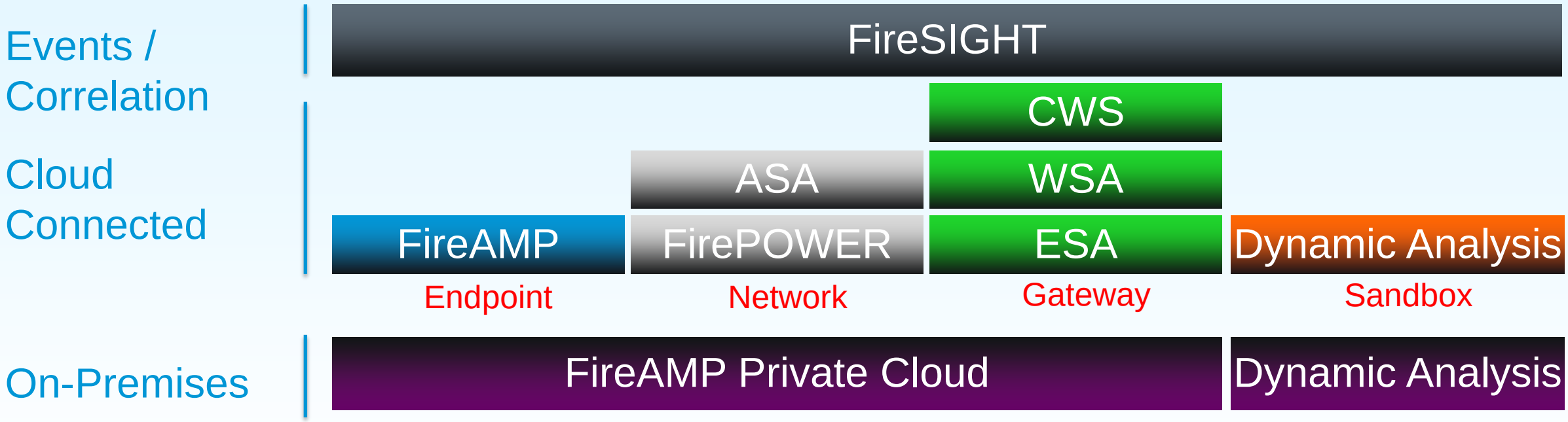
AMP Cloud

FireAMP Private Cloud Design

- Admin portal for rapid deployment and management
- Anonymized file disposition lookups
- Retrospective Analysis
- Device Trajectory
- File Trajectory
- Root Cause
- Tracking and Outbreak Control

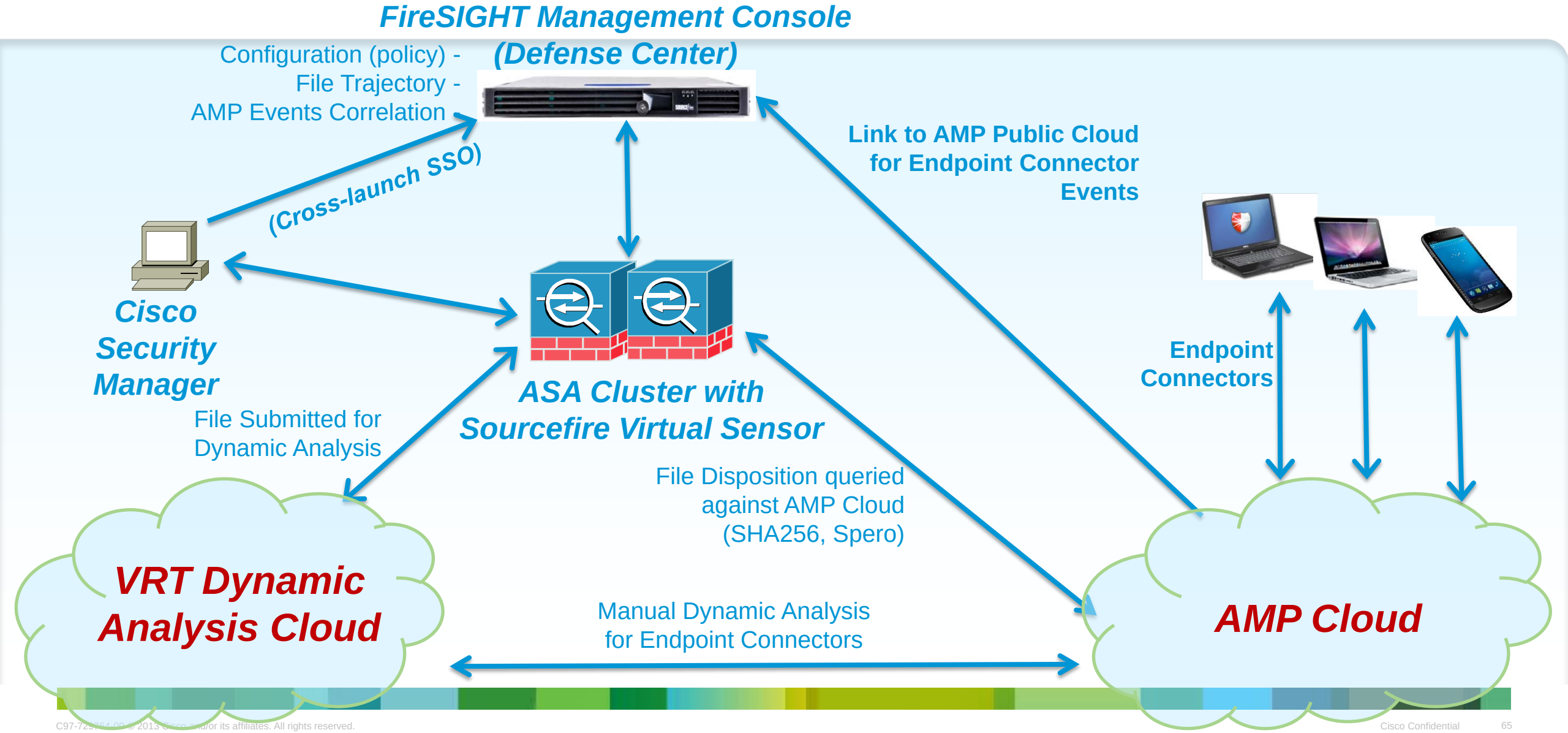


AMP Everywhere



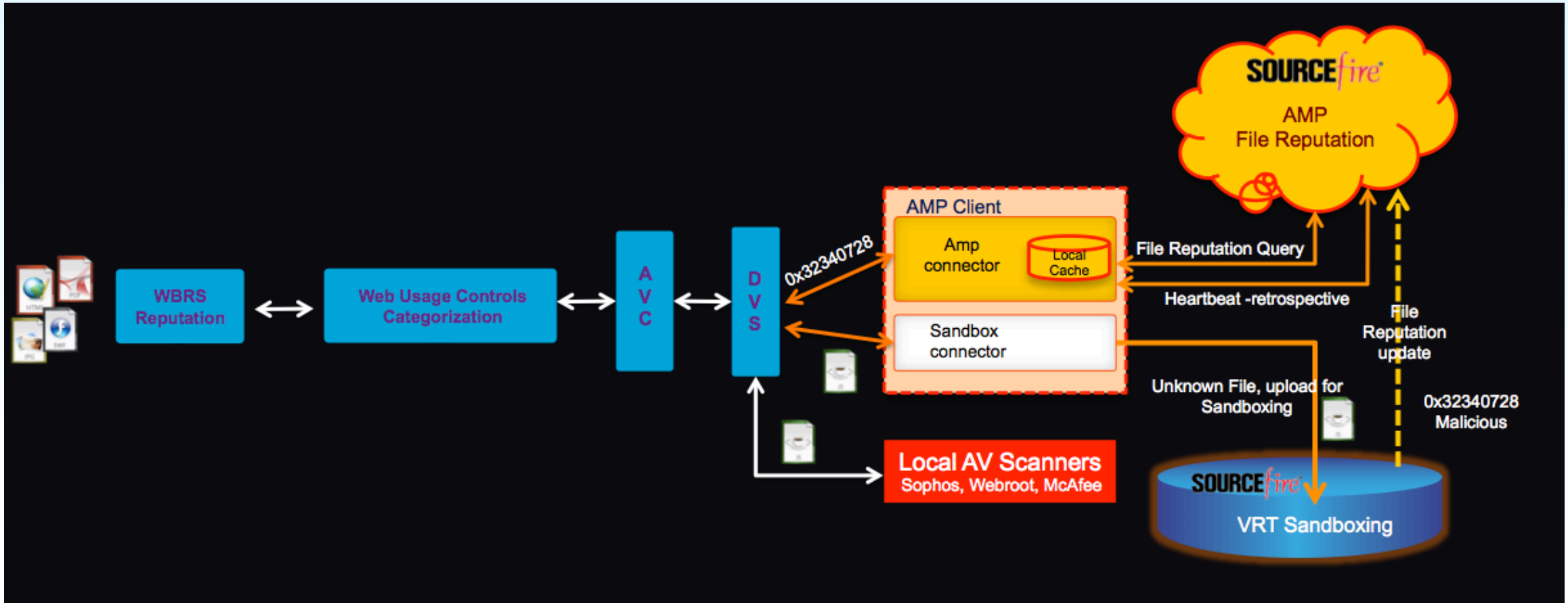
Out-scoping the competition.
Cisco has the most comprehensive strategy for Advanced Malware Protection.

FirePOWER Services on the ASA



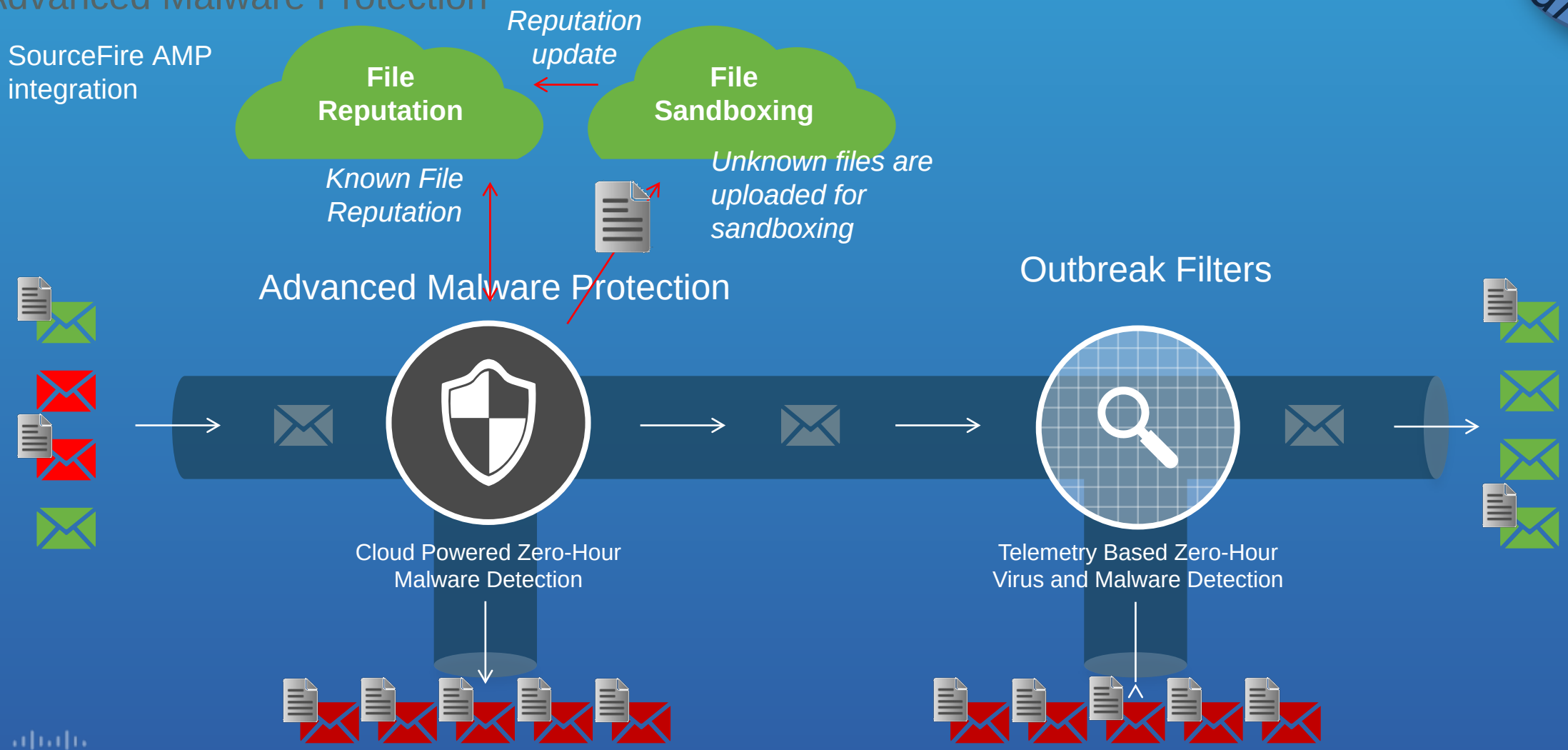
WSA AMP Integration

- Available with AsyncOS 8.0.5



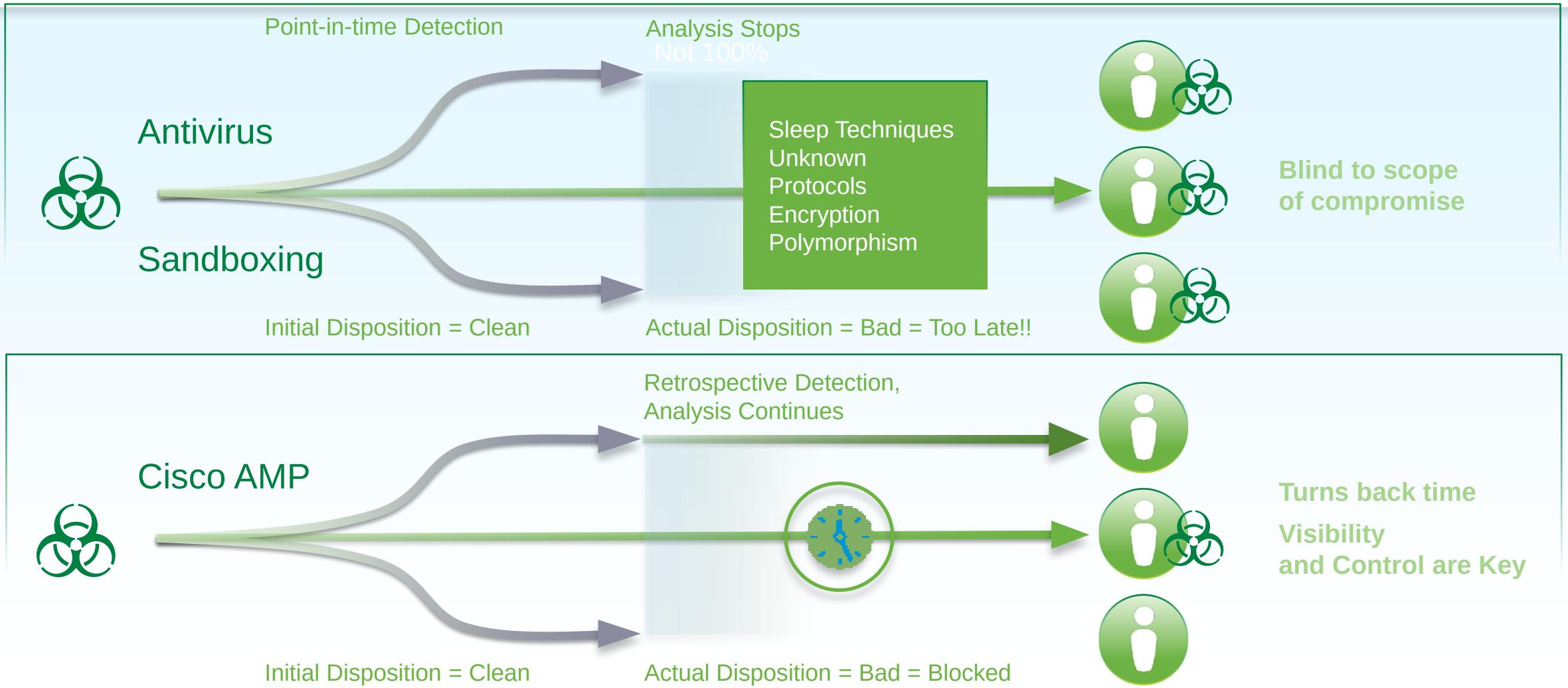
Cisco Zero-Hour Malware Protection

- Advanced Malware Protection



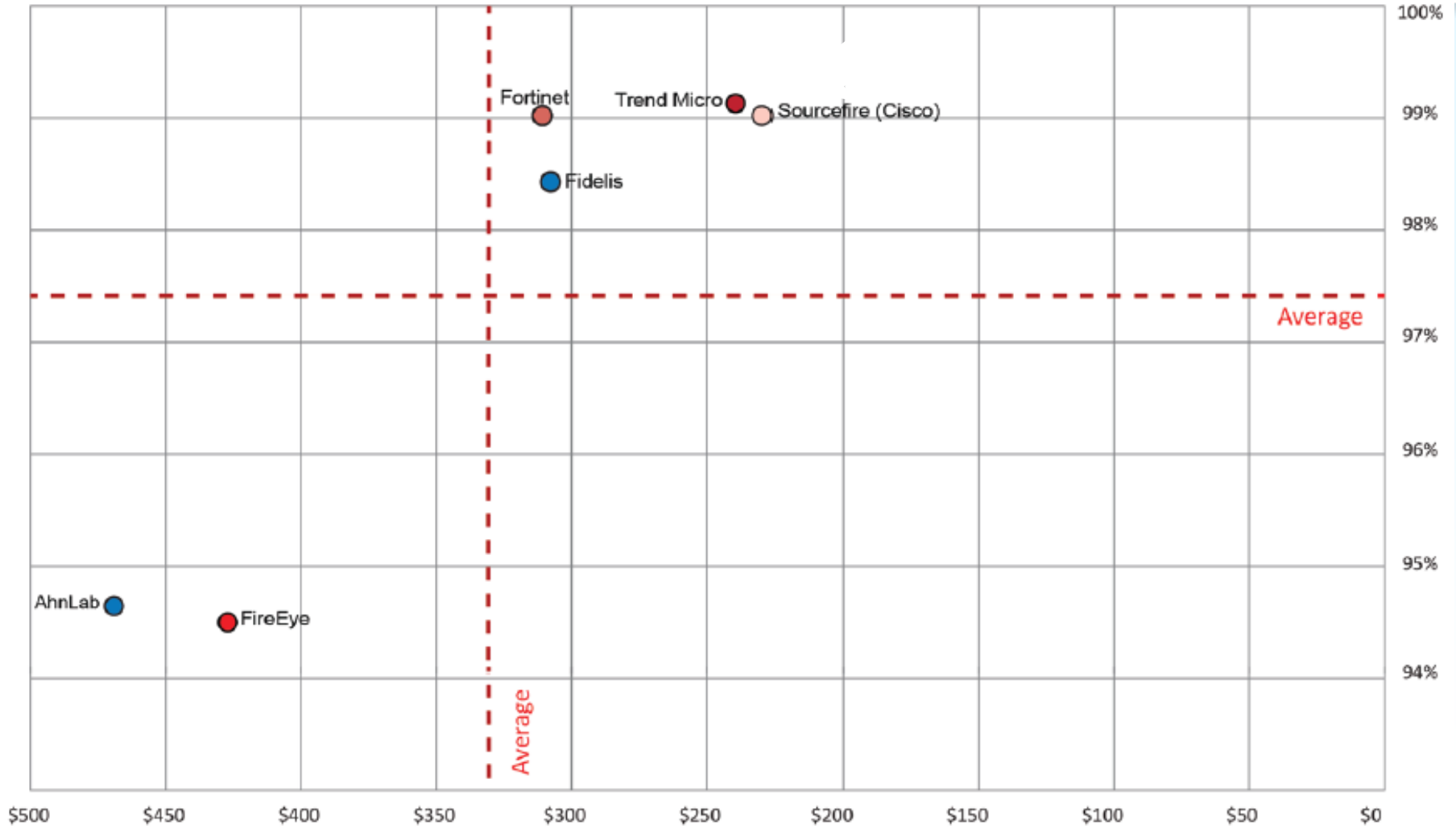
Unique Business Value

Beyond the Event Horizon



NSS Report

NSS Labs Security Value Map (SVM) for Breach Detection Systems



Cisco Advanced Malware Protection

Best Protection Value

99.0% Breach Detection Rating

Lowest TCO per Protected-Mbps

Thank you.