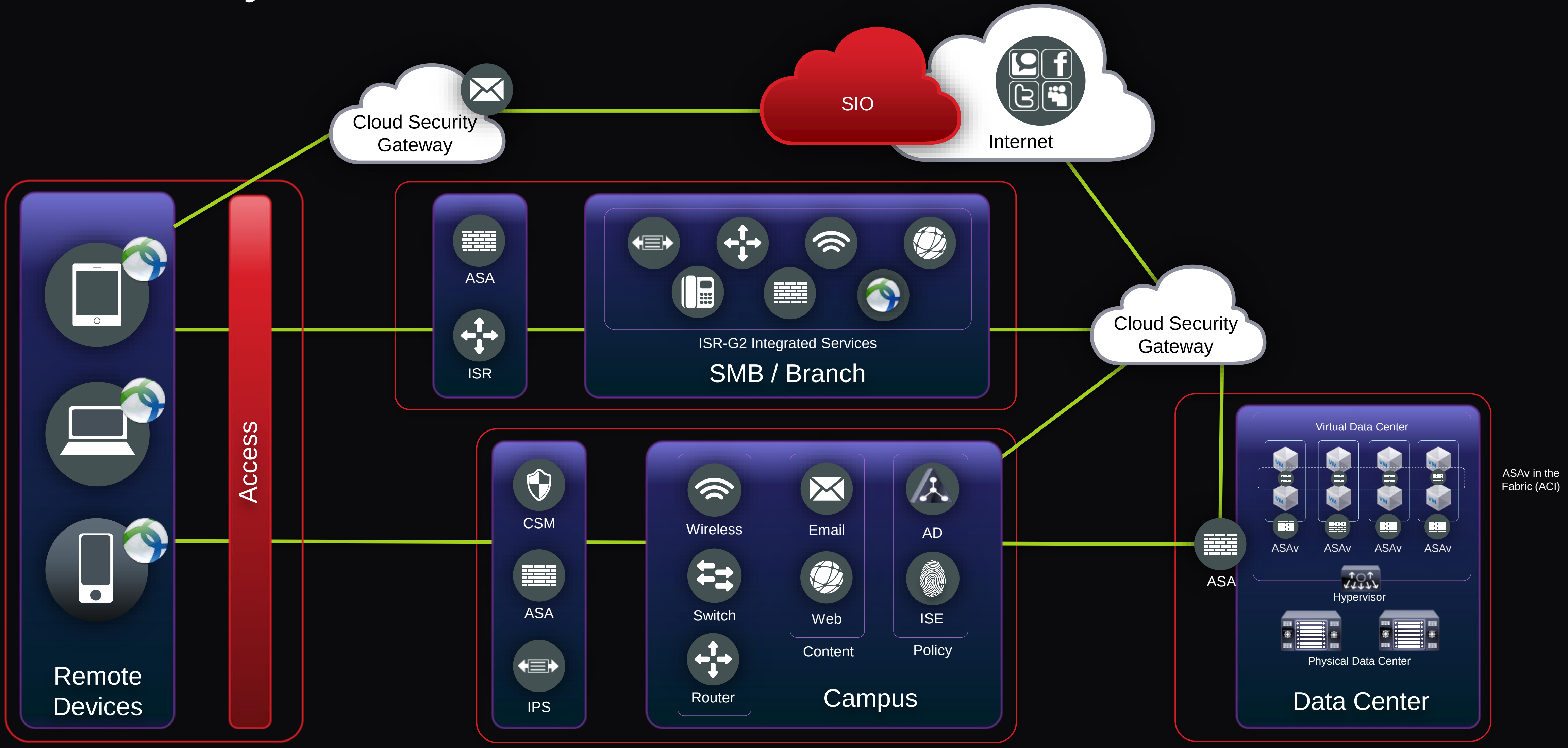
Swiss Networking Day 2014

Cloud Cyber Security Service: Enabling Seamless Distributed Architectures

Markus Frey
Consulting System Engineer

8. Mai 2014

Cisco Security Architecture



Agenda

Threat Landscape

Cisco Security Intelligence in the Cloud

Seamless Distributed Architectures

Future ?

Agenda

Threat Landscape

Cisco Security Intelligence in the Cloud

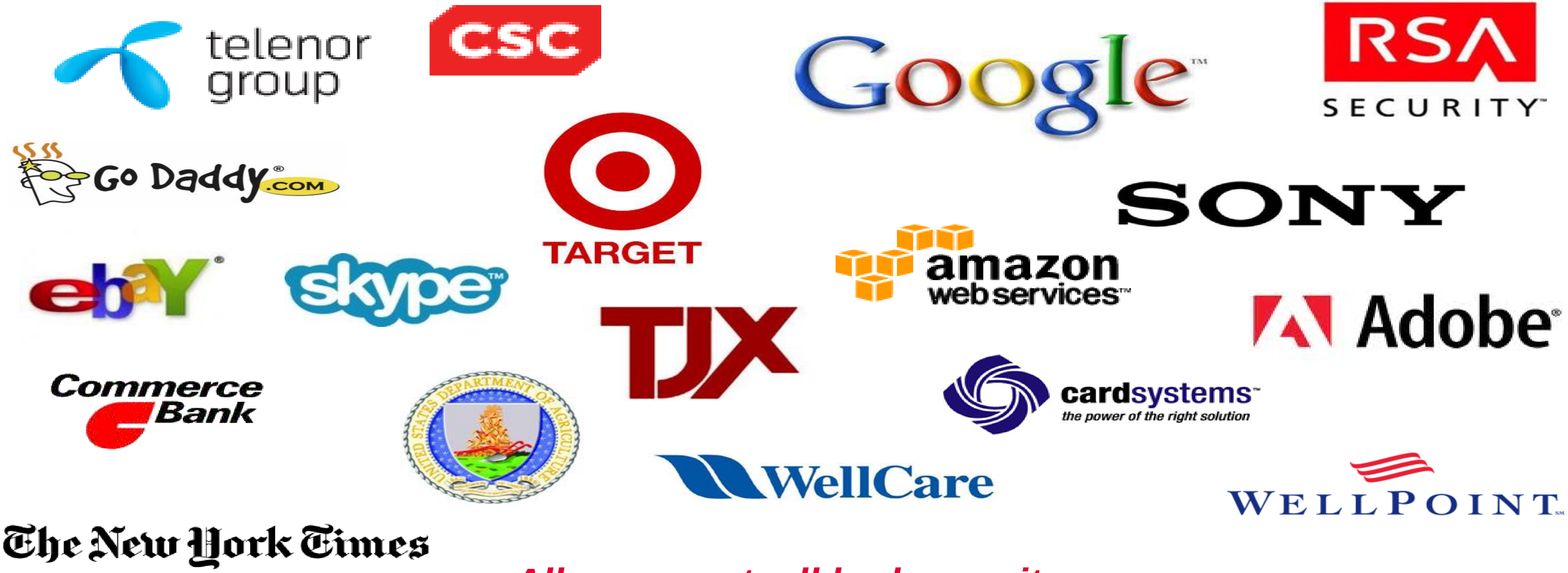
Seamless Distributed Architectures

Future ?

Customers are challenged with today’s evolving threat landscape

- Malware Infections
- Acceptable Use Violations
- Data Loss

Today’s Reality…



All are smart, all had security,
All were seriously compromised.

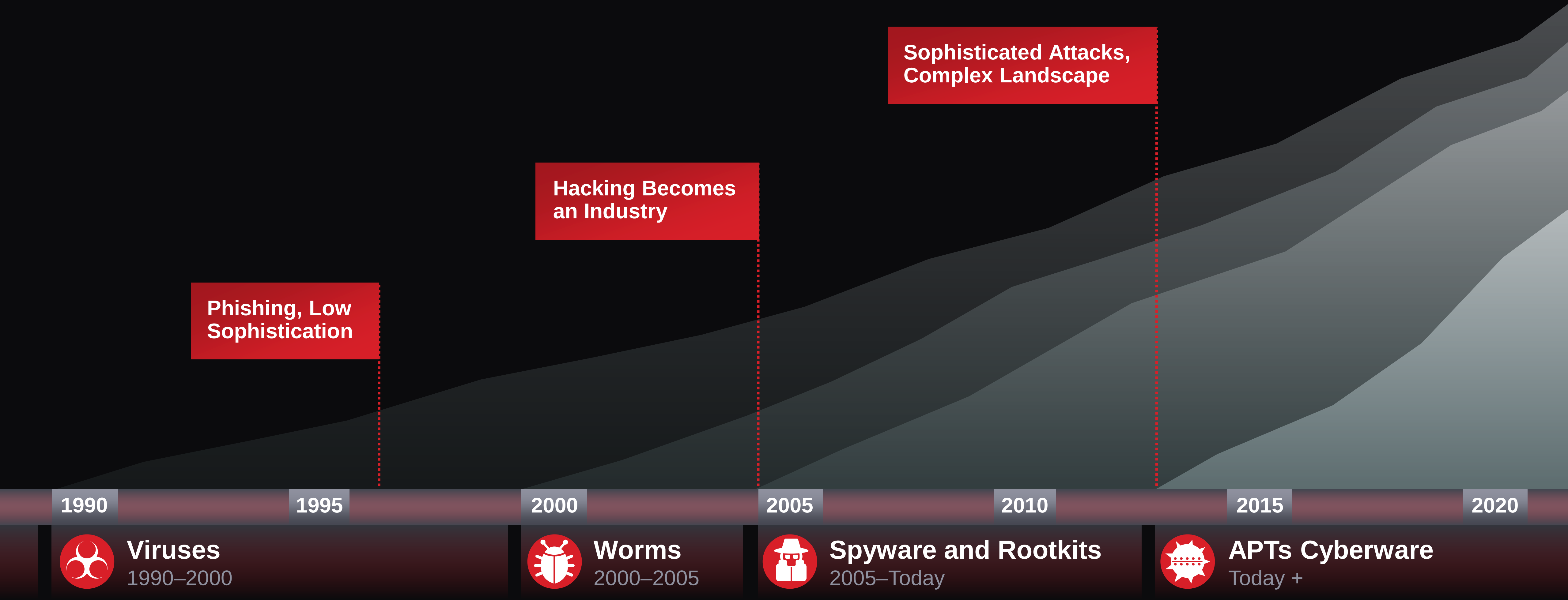
The Security Problem

Changing
Business Models

Dynamic
Threat Landscape

Complexity
and Fragmentation

The Industrialization of Hacking



Phishing, Low Sophistication

Hacking Becomes an Industry

Sophisticated Attacks, Complex Landscape

Viruses
1990–2000

Worms
2000–2005

Spyware and Rootkits
2005–Today

APTs Cyberware
Today +

Agenda

Threat Landscape

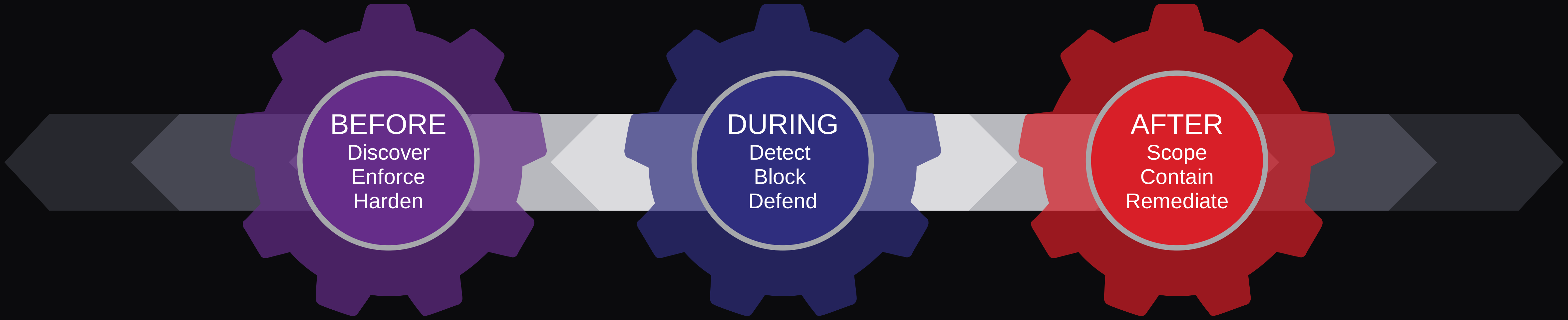
Cisco Security Intelligence in the Cloud

Seamless Distributed Architectures

Future ?

To defend against advanced threats requires greater visibility and control

Attack Continuum



Network

Endpoint

Mobile

Virtual

Cloud

Email & Web

Point-in-time

Continuous

Cisco Security Intelligence in the Cloud

Cisco® SIO

Email Endpoints Web Networks IPS Devices

1.6 million
global sensors

100 TB
of data received per day

150 million+
deployed endpoints

600+
engineers, technicians, and researchers

35%
worldwide email traffic

13 billion
web requests

24x7x365
operations

40+
languages

Cisco Collective Security Intelligence

Cisco Security Devices

+

AMP

Advanced Malware Protection

Sourcefire VRT® (Vulnerability Research Team)

180,000+ File Samples per Day

FireAMP™ Community

Advanced Microsoft and Industry Disclosures

Snort and ClamAV Open Source Communities

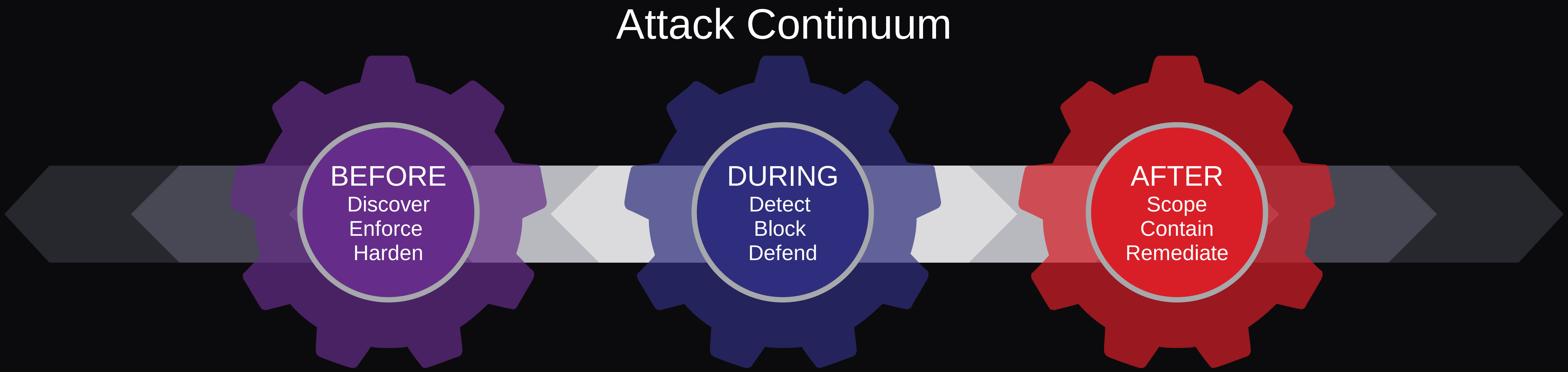
Honeypots

Sourcefire AEGIS™ Program

Private and Public Threat Feeds

Dynamic Analysis

Cisco Web Security with AMP (advanced malware protection) defends across the full attack continuum



Web Reputation	Malware Signature	File Retrospection
Usage Controls	File Reputation	Threat Analytics
Application Controls	File Sanboxing	Actionable Reporting

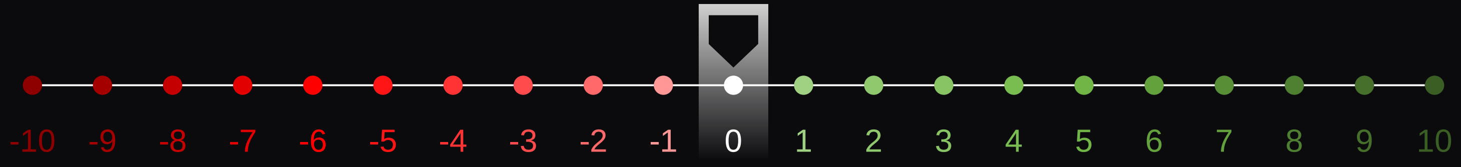
Reputation Analysis

The power of real-time context

BEFORE
Discover
Enforce
Harden

DURING
Detect
Block
Defend

AFTER
Scope
Contain
Remediate



IP Reputation Score

17.0.2.12

Kiev

HTTPS

Web server
< 1 Month

010 10010111001 10 100111 010 000100101 110011 011001110100001100000 0011101 1100001110001110 1001 1101 1110011 0110011 101000 0110 00 011
0101 1100110 1100 111010000 110 0001110 00111 010011101 11000 0111 000 1101 1110011 0110011 101000 0110 00 0111000 111010011 101 1100001 1
0010 010 10010111001 10 100111 010 00010 0101 110011 011 001 11010000 0 0111010011101 1100001110001110 1001 1101 1110011 0110011 101000 01

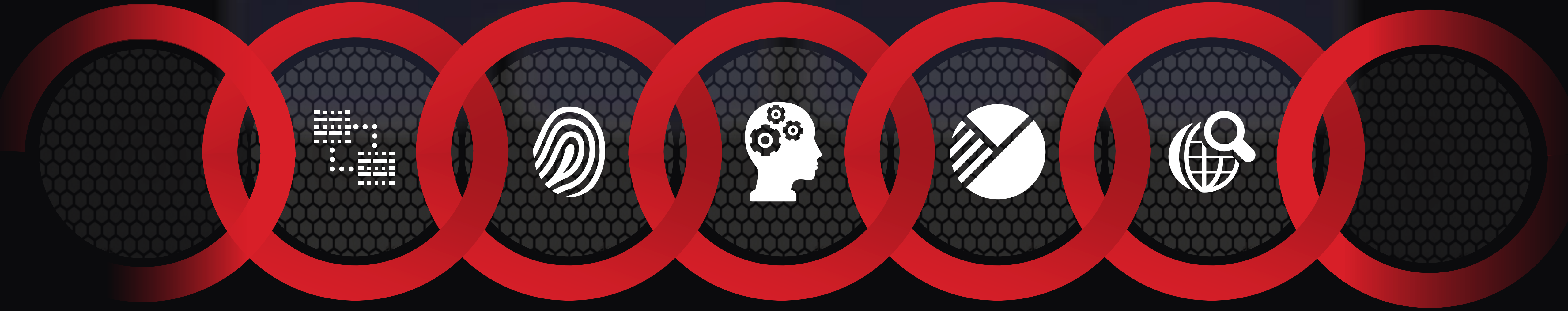
AMP strengthens the first line of detection

BEFORE
Discover
Enforce
Harden

DURING
Detect
Block
Defend

AFTER
Scope
Contain
Remediate

All detection is less than 100%



One-to-One Signature

Fuzzy Finger-printing

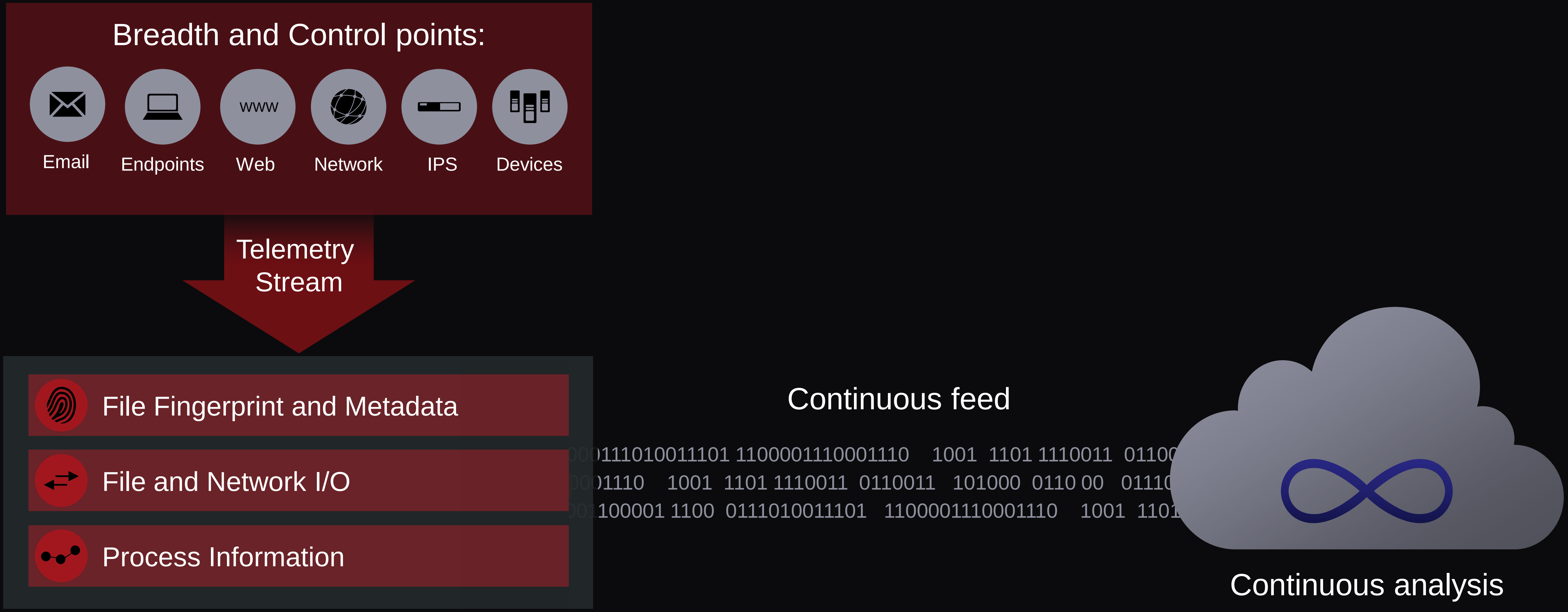
Machine Learning

Advanced Analytics

Dynamic Analysis

Reputation Filtering and File Sandboxing

But most importantly AMP provides continuous retrospective security


Breadth and Control points:

Email

Endpoints

Web

Network

IPS

Devices

Telemetry Stream

File Fingerprint and Metadata

File and Network I/O

Process Information

Continuous feed

Continuous analysis

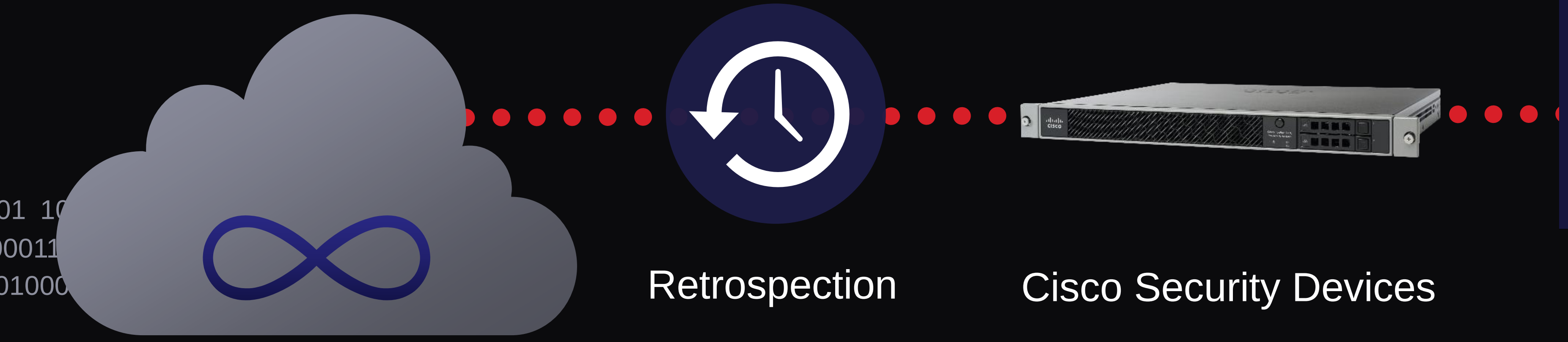
That continues to analyze what happens along the attack continuum

BEFORE
Discover
Enforce
Harden

DURING
Detect
Block
Defend

AFTER
Scope
Contain
Remediate

Detects malicious files that initially pass through perimeter defenses



Retrospection

Cisco Security Devices

- Proactive Blocking
- URL Tracking
- Extensive Reporting
- Remediation Prioritization

Supported Actions

Agenda

- Threat Landscape
- Cisco Security Intelligence in the Cloud
- Seamless Distributed Architectures
- Future ?

Flexible Deployment Options

On- and Off-premises

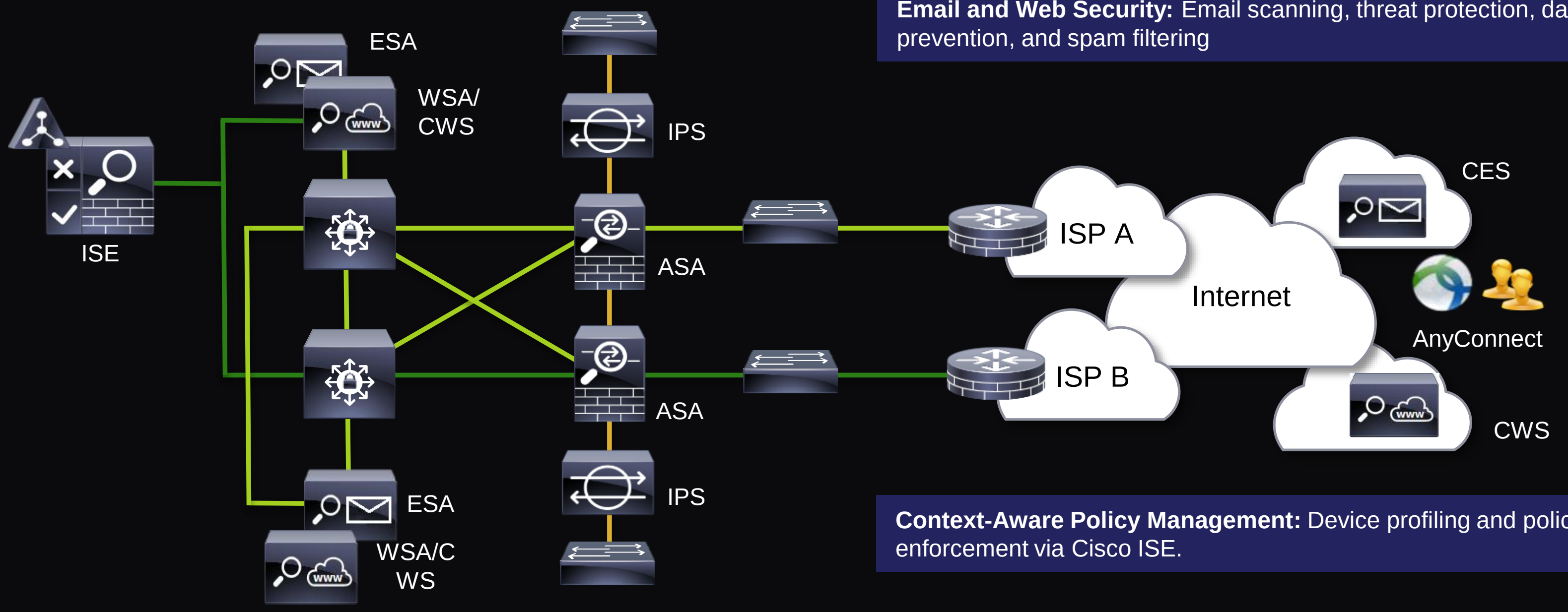
	On-premises	Cloud
Deployment Options	Appliance Virtual NGFW	Cloud
Advanced Malware Protection	Integrated on box – Licensed Plug-in	Integrated - License
Connection Methods	Roaming	Router Firewall / IPS Appliance Roaming
Redirectors	WCCP PAC File Explicit	WCCP PAC File Explicit

Securing the Campus and Edge

Layer 2 Security: Layer 2 protection provided by Catalyst Integrated Security Features, including port security, Dynamic ARP inspection, IP source guard, DHCP snooping, private VLANs, QoS, NetFlow, ERSPAN, SPAN, MACsec hop-by-hop encryption. Identity-aware user and device access with TrustSec.

Email and Web Security: Email scanning, threat protection, data loss prevention, and spam filtering

Firewall and IPS: NGFW protection w/context, app inspection, and policy. NGIPS traffic inspection, including signature matching, event correlation, advanced malware protection, and reputation filtering



Remote Access: Authenticated and encrypted granular user/group-based access control. AnyConnect VPN.

Context-Aware Policy Management: Device profiling and policy enforcement via Cisco ISE.

Context-based Edge Security: User/app/device/policy. SIO and cloud-based policy/ anti-malware protection. Hybrid-Hosted Email Security and encryption

Network Foundation Protection: Device hardening, data, control and management plane protection. 802.1X-based access control with Cisco ISE and TrustSec.

Secure WAN and DMZ: Data confidentiality and integrity with IPSec VPN and PKI.

Agenda

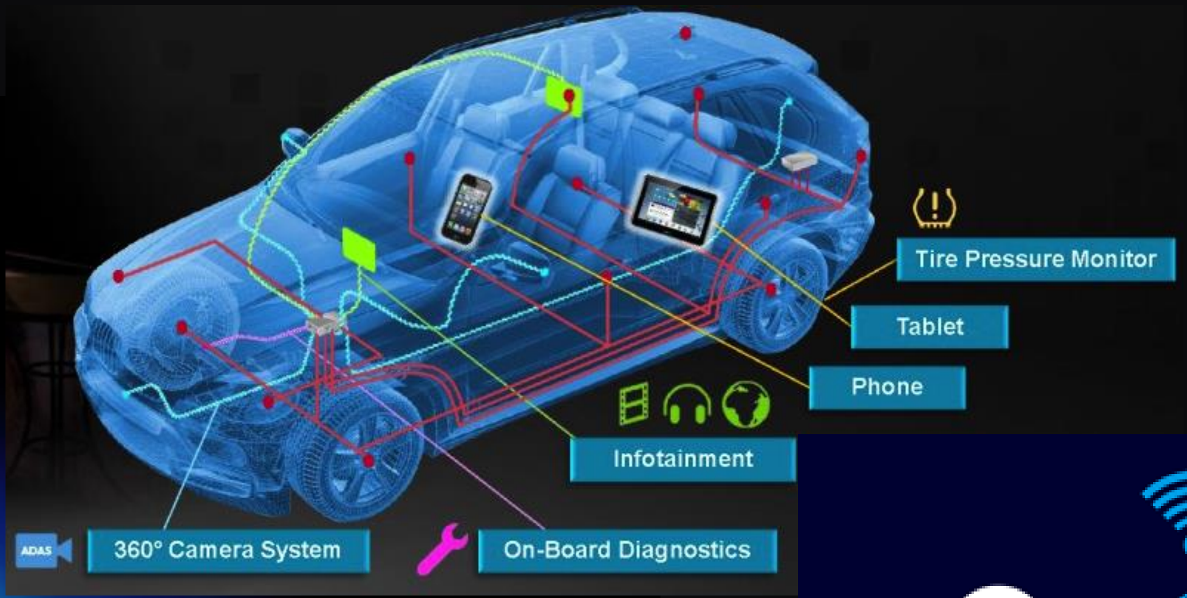
Threat Landscape

Cisco Security Intelligence in the Cloud

Seamless Distributed Architectures

Future ?

IoT and Mobile – Massively increasing Attack Surface



Thank You