



*TOMORROW
starts here.*

Cisco *live!*



Cisco + SourceFire: Threat-Centric Security Approach

BRKSEC-2061

Jatin Sachdeva (CISSP, CISA, CEH, GWAPT, GSEC, SFCE)
Security Architect, Cisco ANZ

#clmel

Cisco *live!*

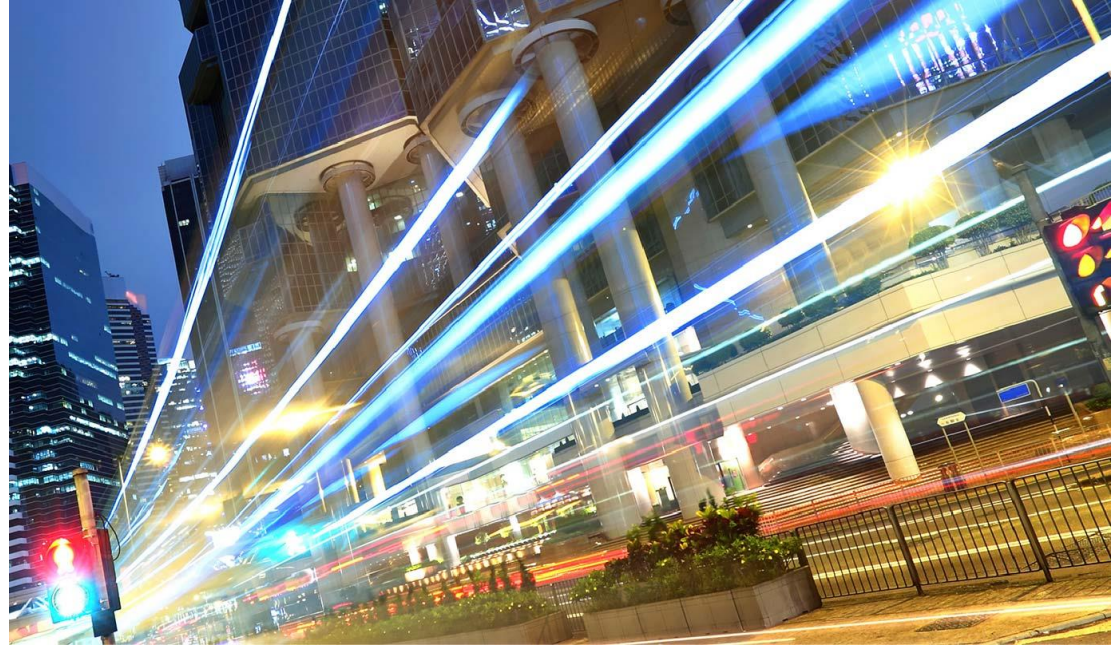
Agenda

- Today's Security Challenges
- A Threat-Centric and Operational Security Model
- Next Generation Firewall & IPS
- Content security & Advanced Malware Prevention
- Network as a Distributed Firewall
- Network as a Visibility Sensor
- Reducing Complexity and Increasing Capability
- It takes an Architecture
- Summary



Session Objective

Provide a quick review of today's dynamic threat landscape and outline the Cisco threat-centric and operational security model that spans a range of attack vectors to address the full attack continuum – before, during, and after an attack.





Security Perspective

The Problem is **THREATS**

Today's Advanced Malware is Not Just a Single Entity



100 percent of companies surveyed by Cisco have connections to domains that are known to host malicious files or services. (2014 CASR)

It is a Community that hides in plain sight

Missed by Point-in-time

Outsight

Top Cyber Risks for Users



Untrustworthy sources



Clickfraud and Adware



Outdated browsers



10%

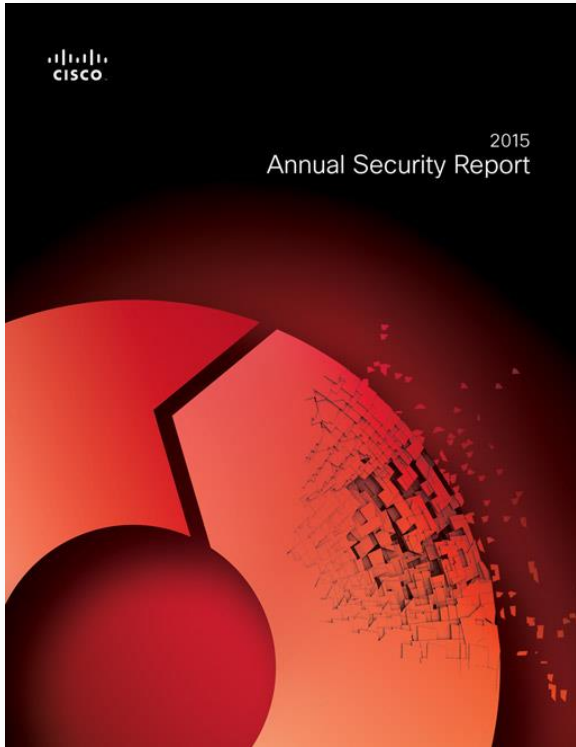
IE requests
running latest
version

64%

Chrome requests
running latest
version

The Challenges Come from Every Direction





Cisco 2015 Annual Security Report

Now available:

cisco.com/go/asr2015

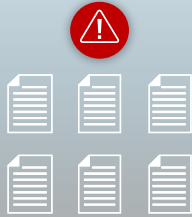
Impact of a Breach

Breach occurs



START

60% data in breaches is stolen in **hours**



HOURS

54% of breaches remain undiscovered for **months**



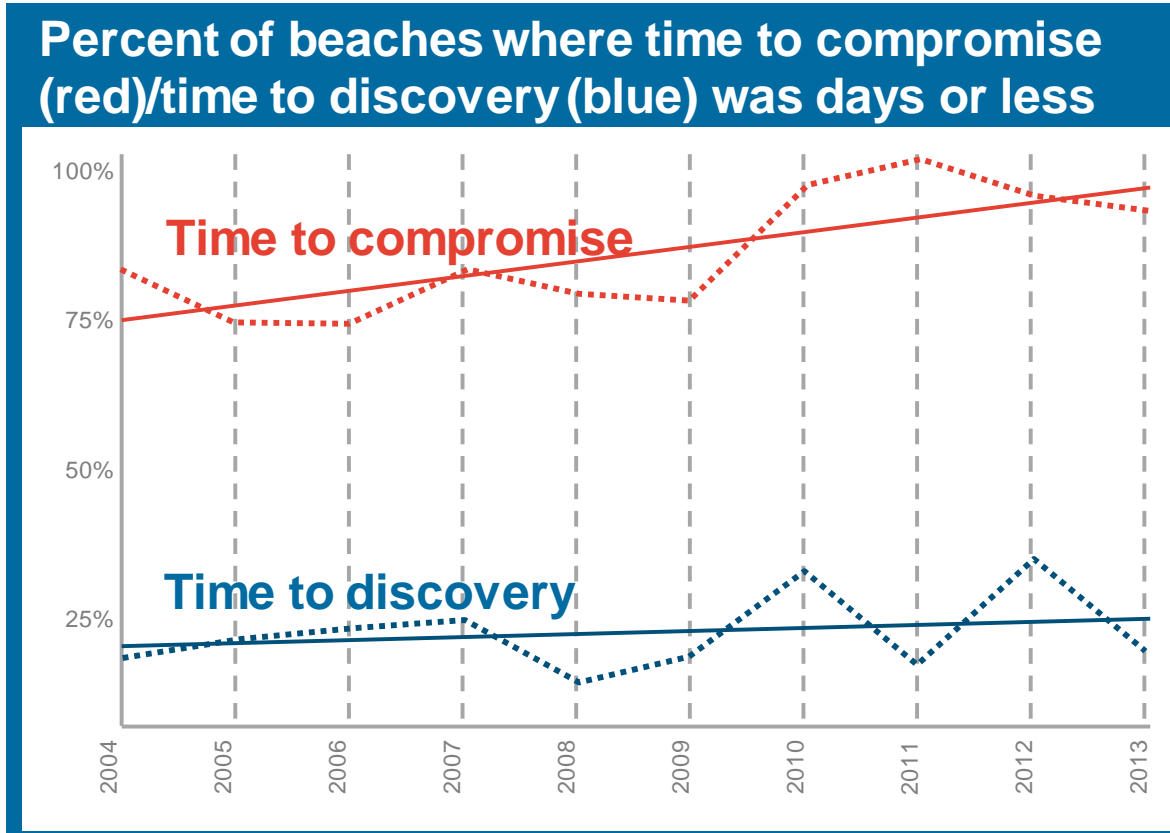
MONTHS

Information of up to **750 million** individuals on the black market over last three **years**



YEARS

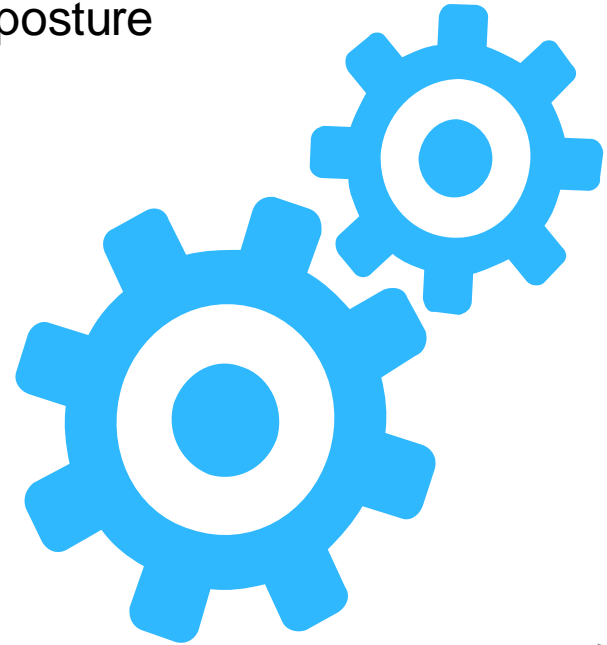
Breach/Detection Time Delta is Not Improving



Why?

The Configuration Problem

- Poor awareness of true operational environment
- Change to environment requiring configuration/posture changes unrecognised
- Detection content unavailable
 - 0-day
- No anomaly detection mechanisms in place





Defenders

Less than half of security practitioners leverage known effective practices

SecOps



Identity Administration and Provisioning	43%
Patching and configuration as defence	38%
Pentesting	39%
Quarantine malicious applications	55%

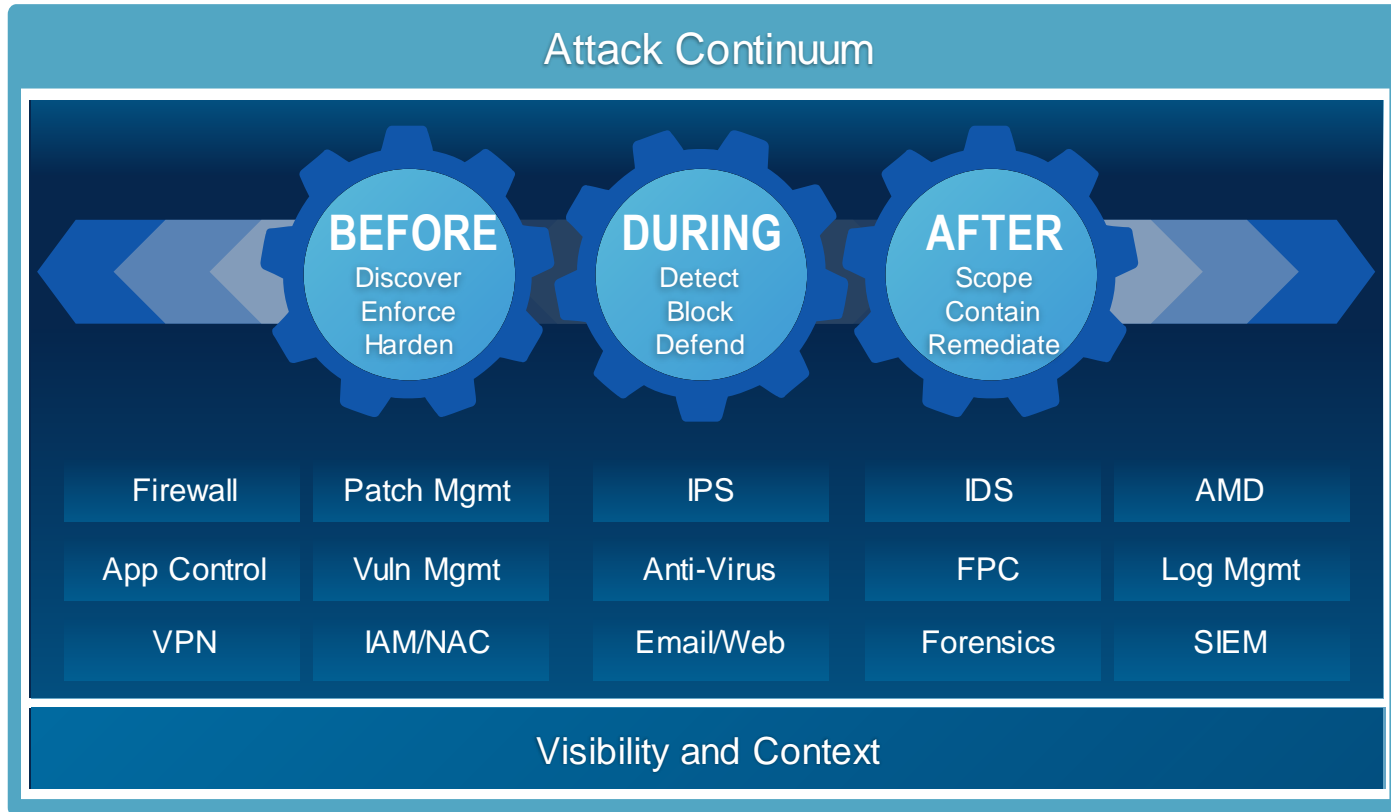
If you knew you were going to be compromised, would you do security differently?

Addressing The Configuration Problem

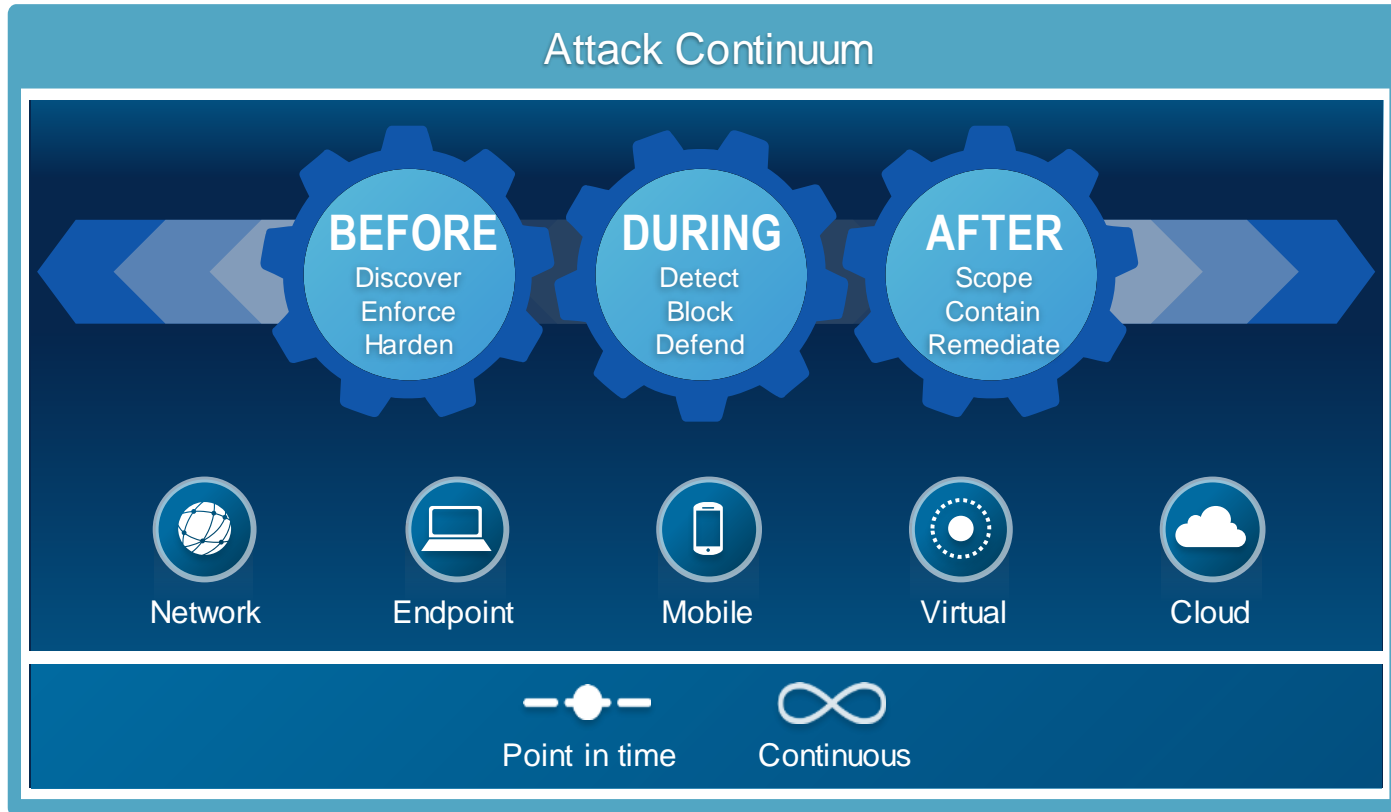
- Visibility Architecture
 - Collect context about the operational environment
 - Continuously in real-time
 - Visibility data is used to recommend configuration of security infrastructure
 - Real-time notifications of change to drive real-time change in security posture
- Content
 - Rapid development and dissemination of updated detection is a fundamental
 - Vendor
 - Security operations teams



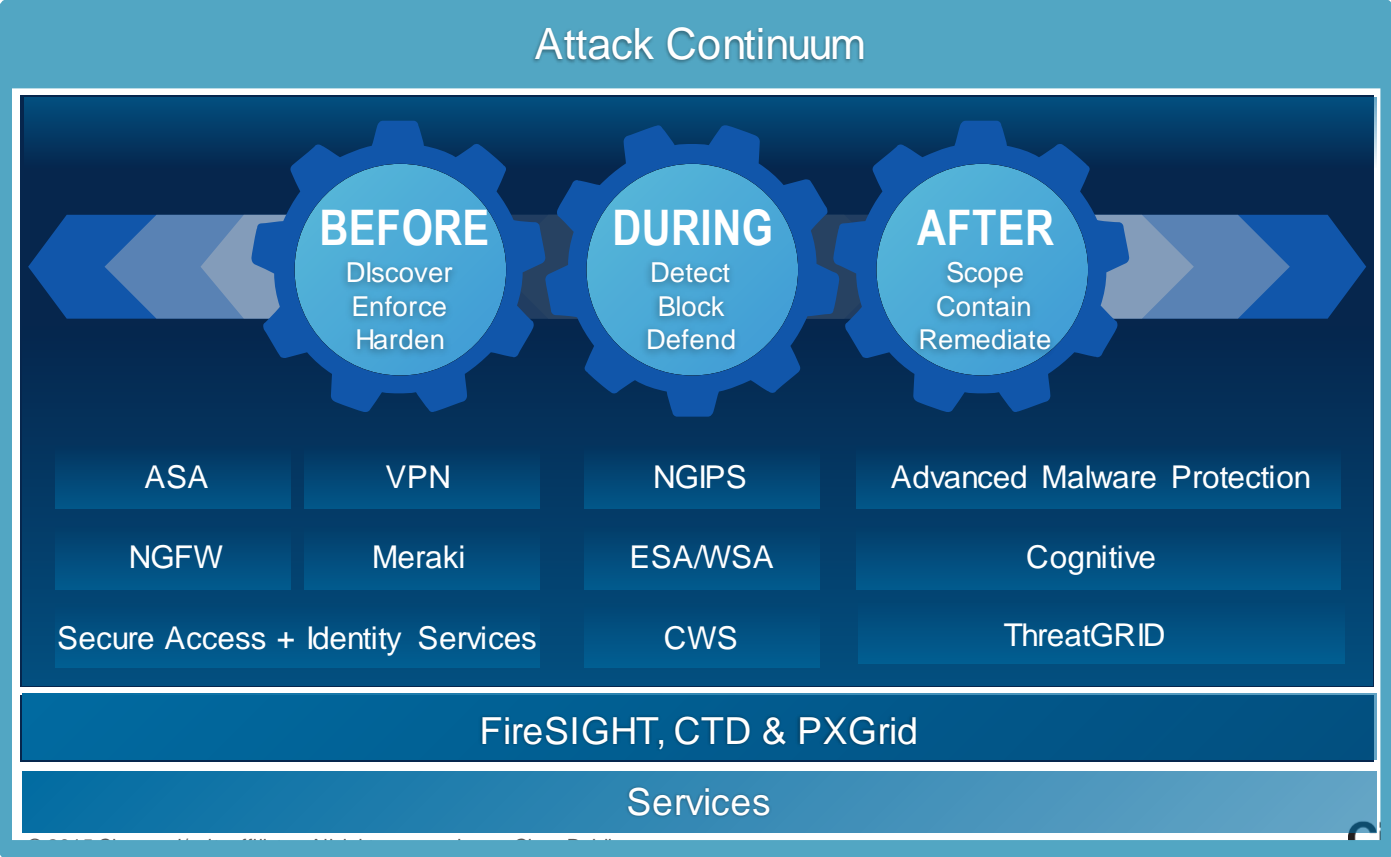
A Threat-Centric and Operational Security Model



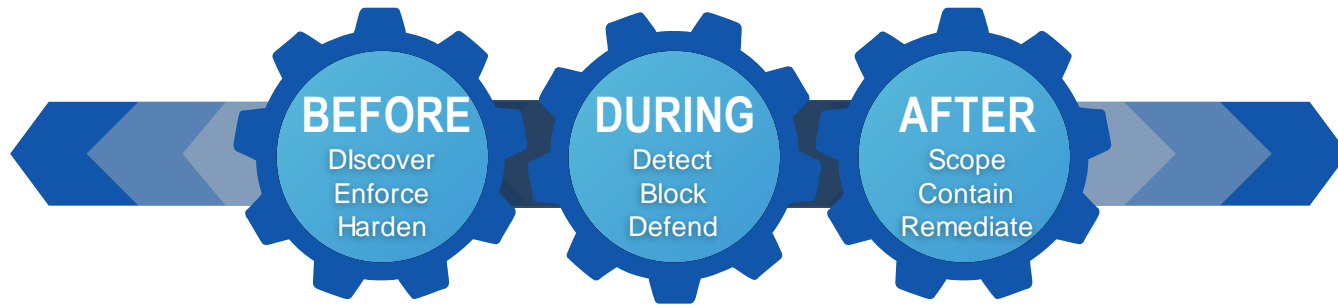
A Threat-Centric and Operational Approach



Cisco: Covering the Entire Continuum



Building a Threat-Centric Cisco Security Architecture



Attack Continuum



Next Generation Firewall and Intrusion Prevention System

Cisco NGFW / NGIPS Offerings

FirePOWER NGIPS

- Best-of-Breed NGIPS for Advanced Threat Protection
- Scalability up to 60Gbps+
- Application and Identity Aware
- Lower TCO Through Automation

Embedded Advanced Malware Prevention (AMP)

- Class-leading advanced malware solution
- File reputation and sandboxing
- Malware Forensics reports
- Malware and file Retrospection
- Cisco AMP Everywhere ensures pervasive coverage

Cisco NGFW ASA w/ FirePOWER Services

- Only threat-focused NGFW to cover full attack continuum
- Available on existing ASA-x platforms
- Integrated NGIPS + AMP
- Ultra-Granular Policies: App, Identity, Risk, Business Relevance

Common NGIPS and AMP code base
Common Threat Management– FireSIGHT
Common Collective Security Intelligence



ASA with FirePOWER Services Best-in-Class NGFW

New ASA
Capabilities

Cisco Collective Security Intelligence Enabled



Clustering &
High Availability



Intrusion Prevention
(subscription)



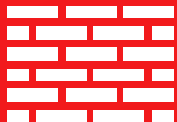
FireSIGHT
Analytics & Automation



Advanced Malware
Protection
(subscription)

WWW

URL Filtering
(subscription)



Network Firewall
Routing | Switching



Application
Visibility & Control



Built-in Network
Profiling



Identity-Policy Control
& VPN

Cisco FireSIGHT Management Automates Operations



Content Security

Email and Web are the Most Prevalent Attack Vectors

Risks

- App development has moved to web and mobile
 - Explosion of
 - Cloud Services
 - Social Networking
 - Email still one of the most critical business applications
- 

- Java exploits represented 93% of all 2014 Indications of Compromise*
- Blended attacks combine social engineering, Phishing and web malware
- Social Networking users increasingly being targeted for data theft and social engineering attacks
- Loss of productivity due to social networking, gaming, etc.

Cisco Content Security Can Help

Cisco Email Security

- Efficient Multi-Scan
- Spam and virus protection
- Email Reputation Filtering
- Spam Image Analysis
- Encryption
- Robust DLP
- URL Scanning

Cisco Advanced Malware Prevention

- Class-leading Anti-malware solution
- File reputation and Sandboxing
- Malware Forensics reports
- Malware File Retrospection
- Cisco AMP Everywhere ensures pervasive coverage

Cisco Web Security

- Safeguards every device, everywhere, all the time
- Acceptable Use Controls
- Web Reputation
- Application Visibility & Control
- Dynamic Content Analysis
- Actionable Reporting
- Threat Analytics

AMP Everywhere
Common Collective Security Intelligence
Systems work together for blended attack protection

Flexible Deployment



Client



Appliance



Virtual

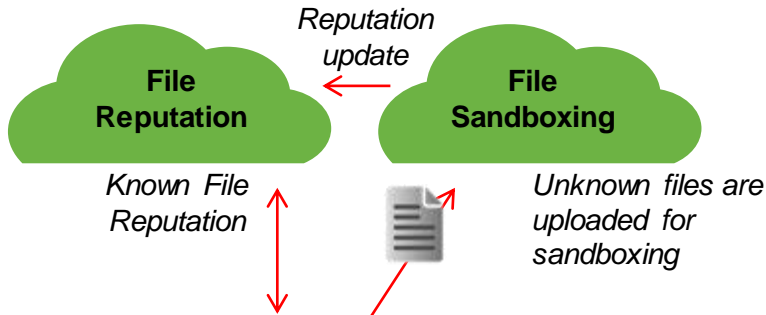


Cloud

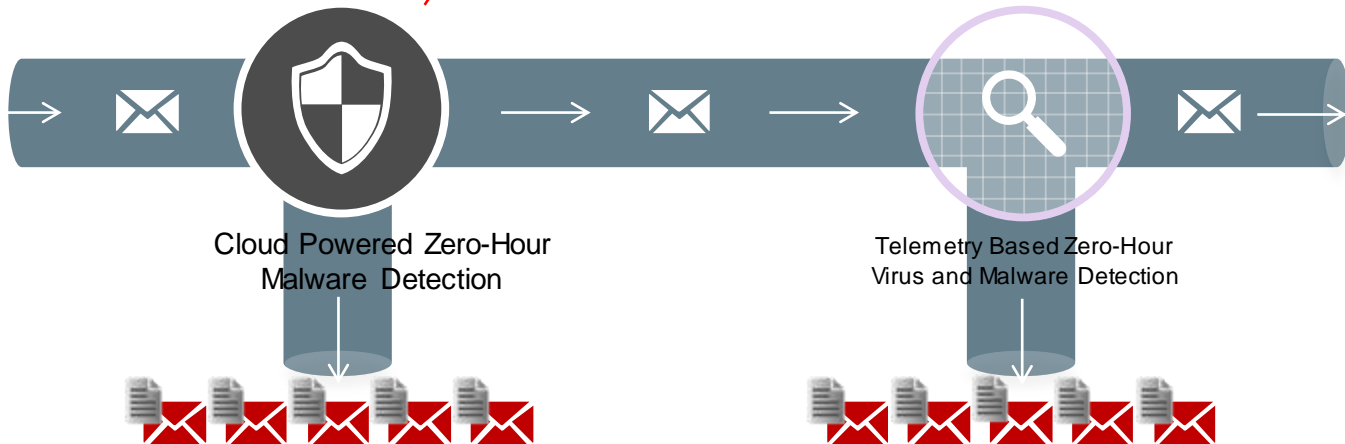
Email Cisco Zero-Hour Malware Protection

Advanced Malware Protection

SourceFire AMP
integration



Outbreak Filters

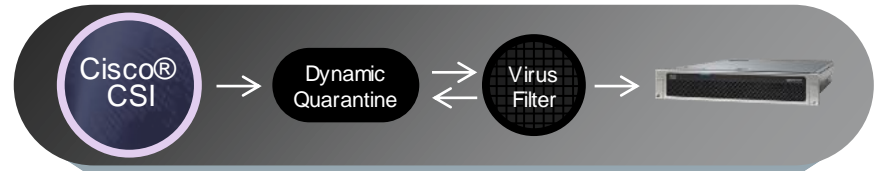


Email Outbreak Filters

Outbreak Filters Advantage

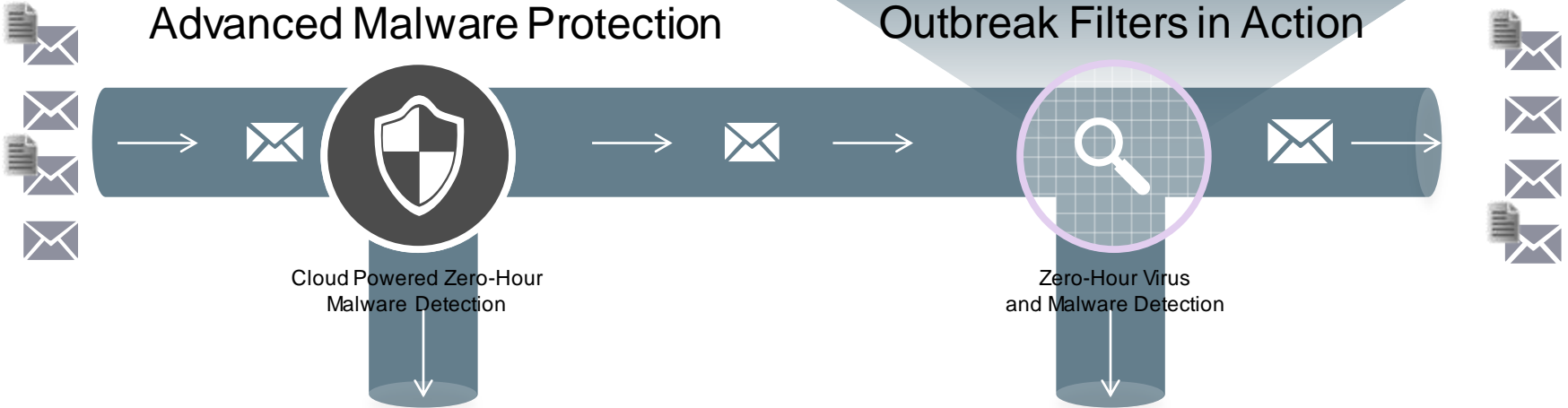
- More protection than just AV alone
- Leverages CSI Telemetry to detect outbreaks
- Average AV signature lead time: Over 13 hours
- Average Cisco lead time: <60mins

<http://www.senderbase.org/static/malware/>



Advanced Malware Protection

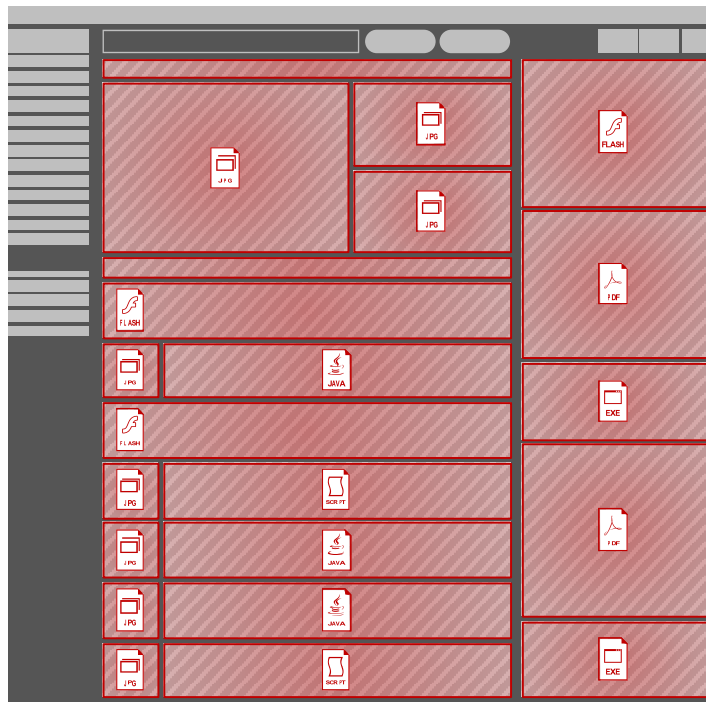
Outbreak Filters in Action



Malware Name	Cisco	Sophos	McAfee	Trend Micro	Symantec
Troj/Agent-AIYV	2014/09/17 09:29 UTC	+0d 11h 36m	Not Published	Not Published	Not Published

Web Pages Contain Hidden Threats

Real-time Sandbox Analysis for Zero-day Defence

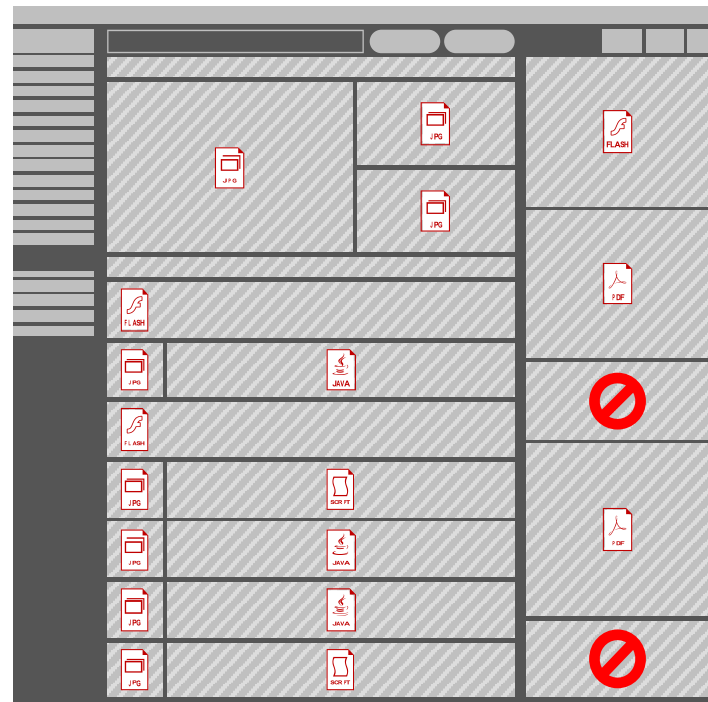


Every object on the page is analysed



Real-time Emulation

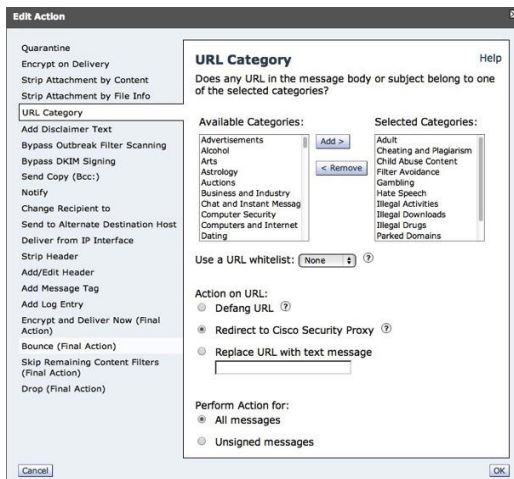
Detects ~20% more threats*



Outstanding Blended Attack Defence

Cisco Email & Web work as a system

Email Contains URL



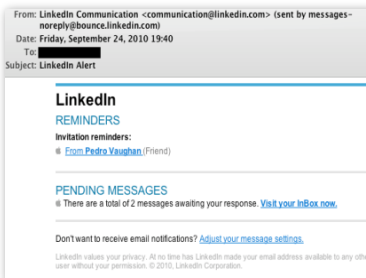
URL Analytics

Cisco Security Intelligence

Send to Cloud

Rewrite

Neutralise



BLOCKEDwww.playboy.comBLOCKED
BLOCKEDwww.proxy.orgBLOCKED

Replace "This URL is blocked by policy"

Automated with Outbreak Filters or Manual



Network as a Distributed Firewall

Protection Against Advanced Persistent Threats

Network Segmentation is critical



Australian Government
Department of Defence
Intelligence and Security

Why is network segmentation and segregation important?

- Once a malicious cyber adversary compromises your network, usually through the compromise of a system under the control of a legitimate user by means of social engineering, they will attempt to move around your network to locate and access the information they are targeting. This is known as propagation of lateral movement.
- In order to minimise the impact of such a compromise, it should be as hard as possible for the malicious cyber adversary to find and access the information they seek and move undetected around a system or network, and remove the information from the network once they locate it.

Verizon DBIR 2014: Recommended Controls

PHISHING ATTACKS	RECOMMENDED CONTROLS Isolating the root cause of an espionage-related breach is a bit of a nightmare. Sure, victims make mistakes (error and otherwise) that are exploited in the process, but the real root issue is a determined, skillful, patient, and well-resourced adversary who will keep poking until he finds (or makes) a hole. With that in mind, let's take a closer look at the holes and other spots these adversaries often take advantage of. First, we'll start with a few blocking and tackling fundamentals that you really ought to be doing regardless of whether or not you're worried about espionage. If you don't do these, all those super-advanced cyberbastic APT kryptolite solutions may well be moot. ✓ Patch ALL THE THINGS! Exploiting browser, OS, and other third-party software (e.g., Flash and Java) vulnerabilities to infect end-user systems is a common initial step for attackers. Keeping everything up to date will make that step a lot harder to take. ✓ Use and update anti-virus (AV) While many proclaim AV is dead, not having it is akin to living without an immune system. It might not protect you from the dreaded zero day, but let's be honest — many espionage victims still fall to one-zero-zero days (or higher). An up-to-date AV (in-line and on the endpoint) can go a long way to detect anomalies in applications and find pesky shells and other malware. ✓ Train users
INSIDER ATTACKS	Beyond the basics, there are some specific practices that organizations concerned with state-affiliated and other determined adversaries should consider. These roughly follow critical points in the path of attack, where victims have the best chance to recognize and respond. ✓ Break the delivery-exploitation-installation chain Users will be phished, and they will eventually click; we've got the data to prove it. Focus on implementing a solution that more completely defends against phishing, such as not relying solely on spam detection and blocklists, but also doing header analysis, pattern matching based on past detected samples, and sandbox analysis of attachments or links included. For more mature organizations, check out the growing collection of Data Execution Prevention (DEP) and Endpoint Threat Detection and Response (ETDR) solutions. We don't promote specific products in this report, but you'll find some good options in this space by starting your search with some of our contributors. ✓ Spot C2 and data exfiltration Collect and/or buy threat indicator feeds. In and of themselves, they aren't intelligence, but they're certainly useful within intelligence and monitoring operations. Monitor and filter outbound traffic for suspicious connections and potential exfiltration of data to remote hosts. In order to do so, you'll need to establish a good baseline of traffic like those indicators you collected/bought here. Establish connections among the single best sources in your organization. Compare these to your threat line this data often.
INVESTIGATIVE PRIVILEGE ABUSE	
PHYSICAL THEFT AND LOSS	
MALICIOUS INTERNAL ENDPOINTS	

PAYMENT CARD SKIMMERS	or technology. It's not all about prevention; arm them with the knowledge and skills they need to recognize and report potential incidents quickly.	of data within your organization. Compare these to your threat intelligence, and mine this data often.
CYBER- ESPIONAGE	✓ Segment your network Good network and role segmentation will do wonders for containing an incident, especially where actors intend to leverage access to one desktop as a stepping-stone to the entire network. ✓ Keep good logs Log system, network, and application activity. This will not only lay a necessary foundation for incident response, but many proactive countermeasures will benefit from it as well.	✓ Stop lateral movement inside the network After gaining access, attackers will begin compromising systems across your network. ETDR, mentioned above, can help here too. Two-factor authentication will help contain the widespread and unchallenged re-use of user accounts. We mentioned network segmentation in the basics, but since doing it well is challenging, we'll mention it here again. Don't make it a straight shot from patient zero to a full-fledged plague. Watch for user behavior anomalies stemming from compromised accounts.
DOS ATTACKS		

Cisco Secure Access

Making segmentation easy and dynamic

Identity Services Engine

- Centralised Policy Management
- Allows for dynamic and micro segmentation
- AAA Radius Server
- Guest Access Services
- BYOD Enablement
- MDM Integration
- Device Profiling & Posture assessment
- pxGrid Context Sharing

TrustSec

- Provides dynamic network segmentation
- Access Control using IP/VLAN independent tags
- Simplifies BYOD access and policies
- Provides access policy enforcement on all network devices
- Vast Firewall Rule Simplification

AnyConnect Secure Mobility

- Universal Security Client
- SSLVPN / IPsec
- Mobile Web Security
- Network Access Manager
- Host NAC Agent
- Certificate Provisioning

Common Identity and Context
Common Policy across Wired, Wireless and VPN

Flexible Deployment



Appliance



Virtual



Cloud

Simplification of Access Policy with TrustSec

Firewall Rules

Source		Destination			Action
IP	SGT	IP	SGT	Service	Action
Any	Employee	Any	Biz Server	HTTPS	Allow
Any	Suspicious	Any	Biz Server	Any	Deny

Business Data
App / Storage



- Massive Firewall rule simplification
 - Policy Enforcement regardless of IP address/vlan
- Result: Accelerated service provisioning

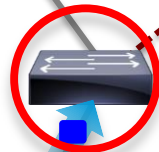
VPN Remote
Access



WLAN
Controller



Corp Asset
Endpoints



Access Switch



ISE
Policy Server



Device Type: Apple Mac
User: Fay
AD Group: Employee
Asset Registration: Yes

Policy Mapping → SGT: **Employee**

- Consistent policy assignment regardless of access method

- Differentiated Network Access based on Context
- Security Group Tag is added to every packet from host

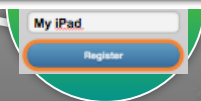
Empower BYOD with ISE & TrustSec

Empowering the User
without sacrificing security

Blacklist
of device



Simple
Certificate
Provisioning



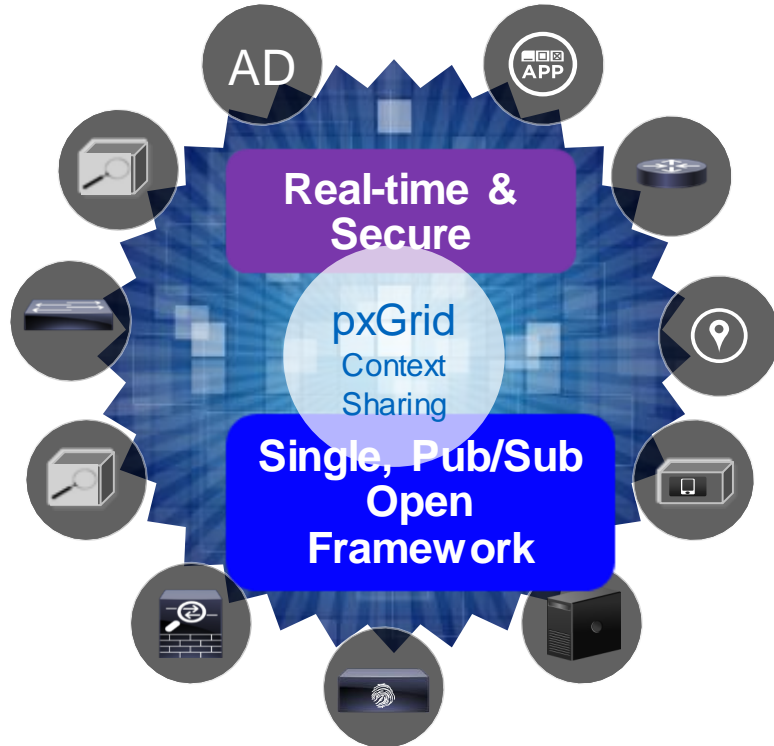
Self Re



- **Reduced Burden on IT Staff**
 - Device On-Boarding
 - MDM / Posture compliance
 - Self Registration
 - Supplicant Provisioning
 - Certificate Provisioning
- **Self Service Model**
 - myDevice Portal for registration
 - Guest Sponsorship Portal
- **Device Black Listing**
 - User initiated control for their devices, black-listing, re-instate, etc
- **Support for:**
 - iOS (post 4.x)
 - MAC OS X (10.6 – 10.9)
 - Android (2.2 and onward)
 - Windows (XP, Vista, win7, win8)

Enabling Network-Wide Identity & Context Sharing

Cisco Platform Exchange Grid – pxGrid



INFRASTRUCTURE FOR A ROBUST SECURITY ECOSYSTEM

- Single framework – develop once, instead of to multiple APIs
- Control what & where context is shared among platforms
- Bi-directional – share and consume context at the same time
- Extremely Scalable
- Integrating with Cisco SDN for broad network control functions

ISE TrustSec

CISCO Identity Services Engine ise admin Logout Feedback

Home Operations Policy Administration Task Navigator

Authentication Authorization Profiling Posture Client Provisioning Security Group Access Policy Elements

Egress Policy Network Device Authorization

Source Tree Destination Tree **Matrix**

Egress Policy (Matrix View)

Edit Add Clear Mapping Configure Push Monitor All Dimension 6X10 Show Policy-View-1

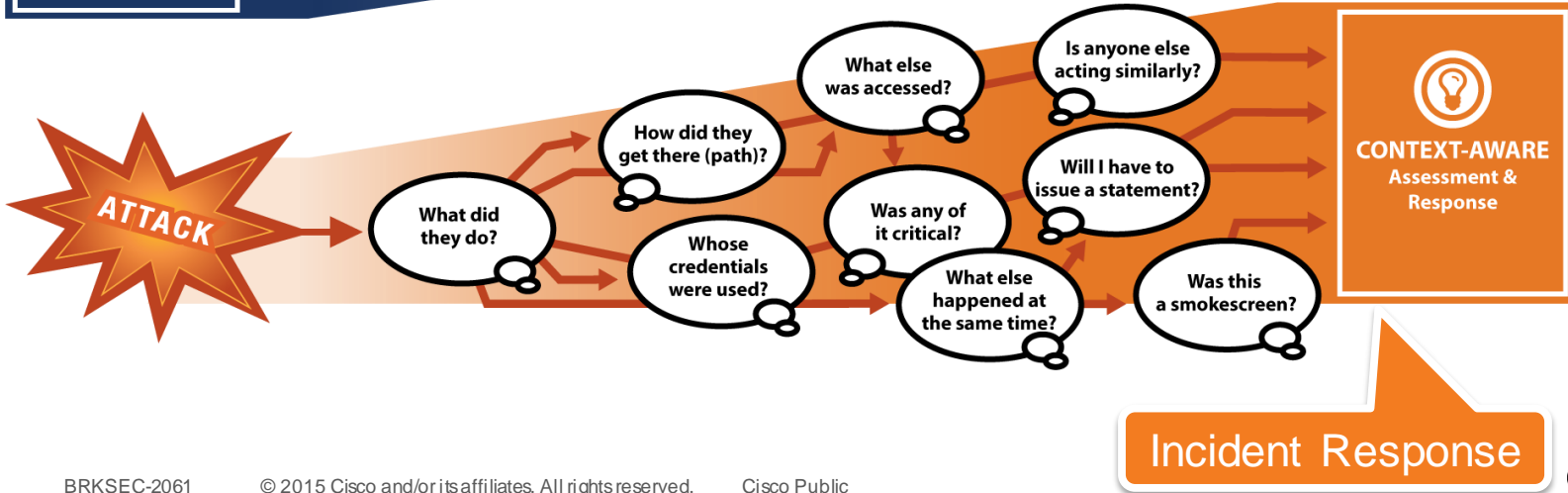
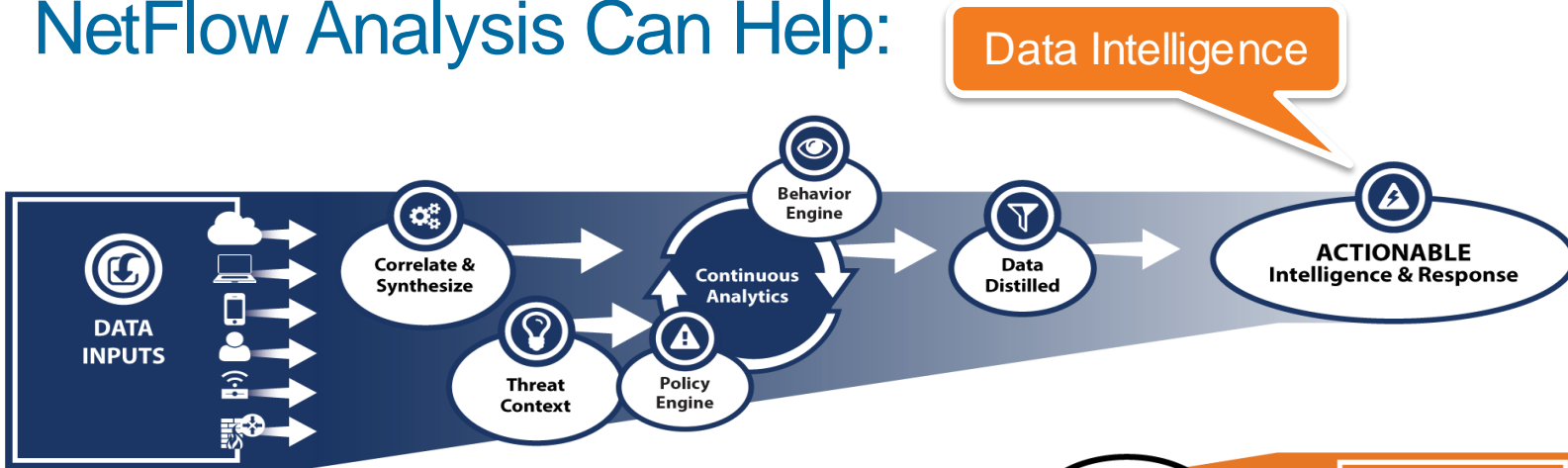
Destination	Web_Servers (7 / 0007)	Time_Card_Server (10 / 000A)	Manager_Portals (9 / 0009)	Employee_Portals (8 / 0008)	CreditCard_Server (11 / 000B)
Unregist_Dev_SGT (3 / 0003)	Enabled SGACLs: Permit IP	Enabled SGACLs: Deny IP	Enabled SGACLs: Deny IP	Enabled SGACLs: Deny IP	Enabled SGACLs: Deny IP
Management_SGT (5 / 0005)	Enabled SGACLs: Permit IP	Enabled SGACLs: Deny IP	Enabled SGACLs: Permit IP	Enabled SGACLs: Permit IP	Enabled SGACLs: Deny IP
Employee_SGT (4 / 0004)	Enabled SGACLs: Permit IP	Enabled SGACLs: Permit IP	Enabled SGACLs: Deny IP	Enabled SGACLs: Permit IP	Enabled SGACLs: Deny IP
CC_Scanner_SGT (6 / 0006)	Enabled SGACLs: Deny IP	Enabled SGACLs: Deny IP	Enabled SGACLs: Deny IP	Enabled SGACLs: Deny IP	Enabled SGACLs: Permit IP

Default Enabled SGACLs : Permit IP Description : Default egress rule



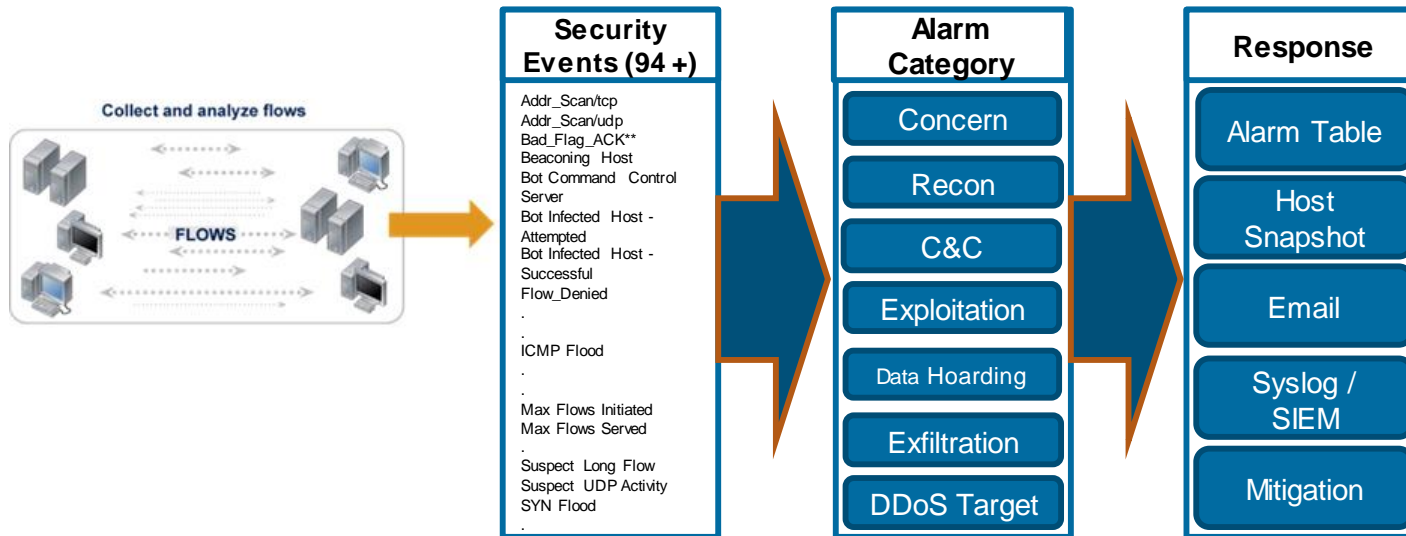
Network as a Visibility Sensor

NetFlow Analysis Can Help:



Behavioural Detection Model

As flows are collected, behavioural algorithms are applied to build “Security Events”. Security Events will add points to an alarm category to allow for easy summarisation higher degree of confidence of the type of activity detected:

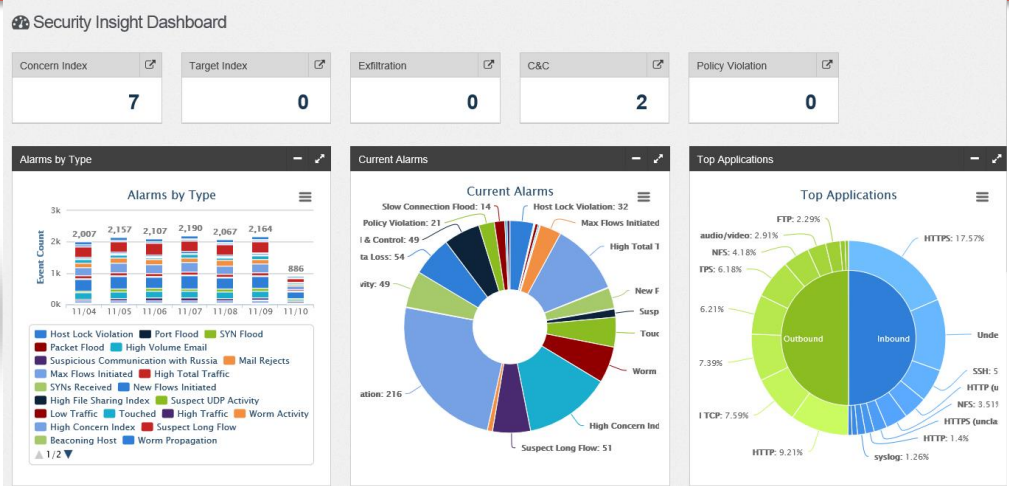


Cyber Threat Defence (CTD) Solution



Advanced Visibility & Investigation

- Partner with Lancope (StealthWatch) to deliver network visibility, security context and intelligence.
- Enhance with Identity, device, application awareness



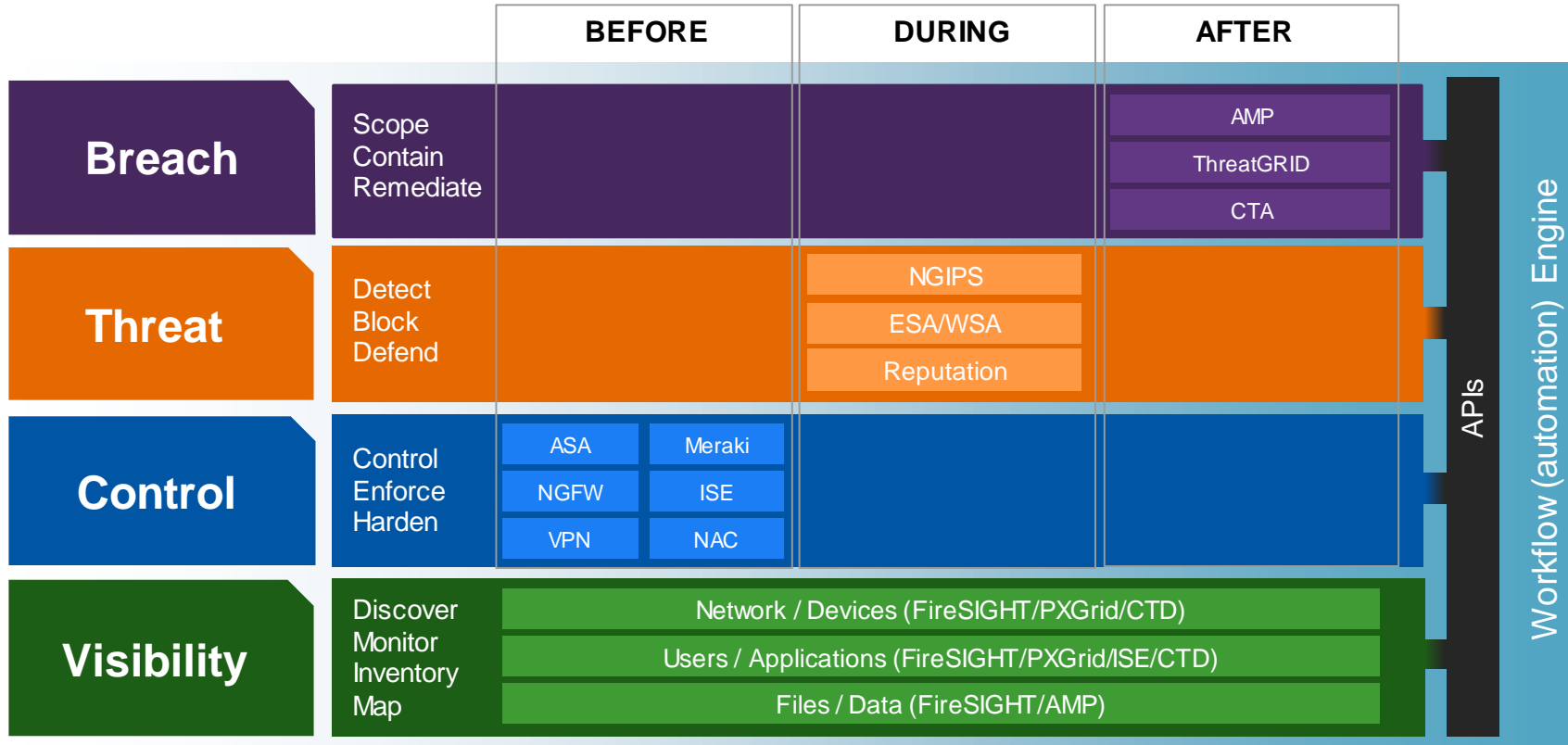


Reducing Complexity and Increasing Capability

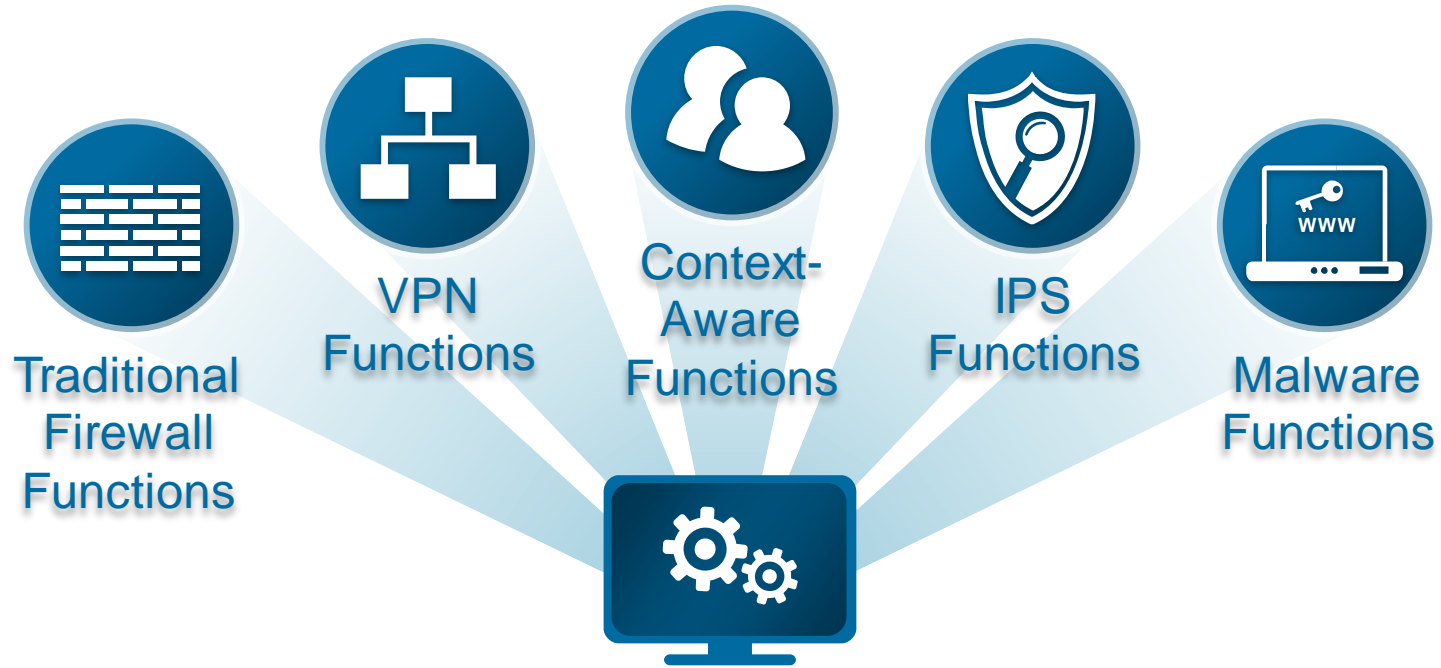
Visibility is the Foundation



Visibility Must Be Pervasive



Today's Security Appliances



We must integrate more effectively to make
more effective security solutions

Two Kinds of Integration

- Front-end integration
 - Most security technologies have information about the environment that they are defending but do not share it
 - Build a Visibility Architecture to collect information about the composition, configuration and change in the environment being defended
- Back-end integration
 - Collect and centralise information about what's happening to the environment and try to figure out what is happening
 - Traditional integration model



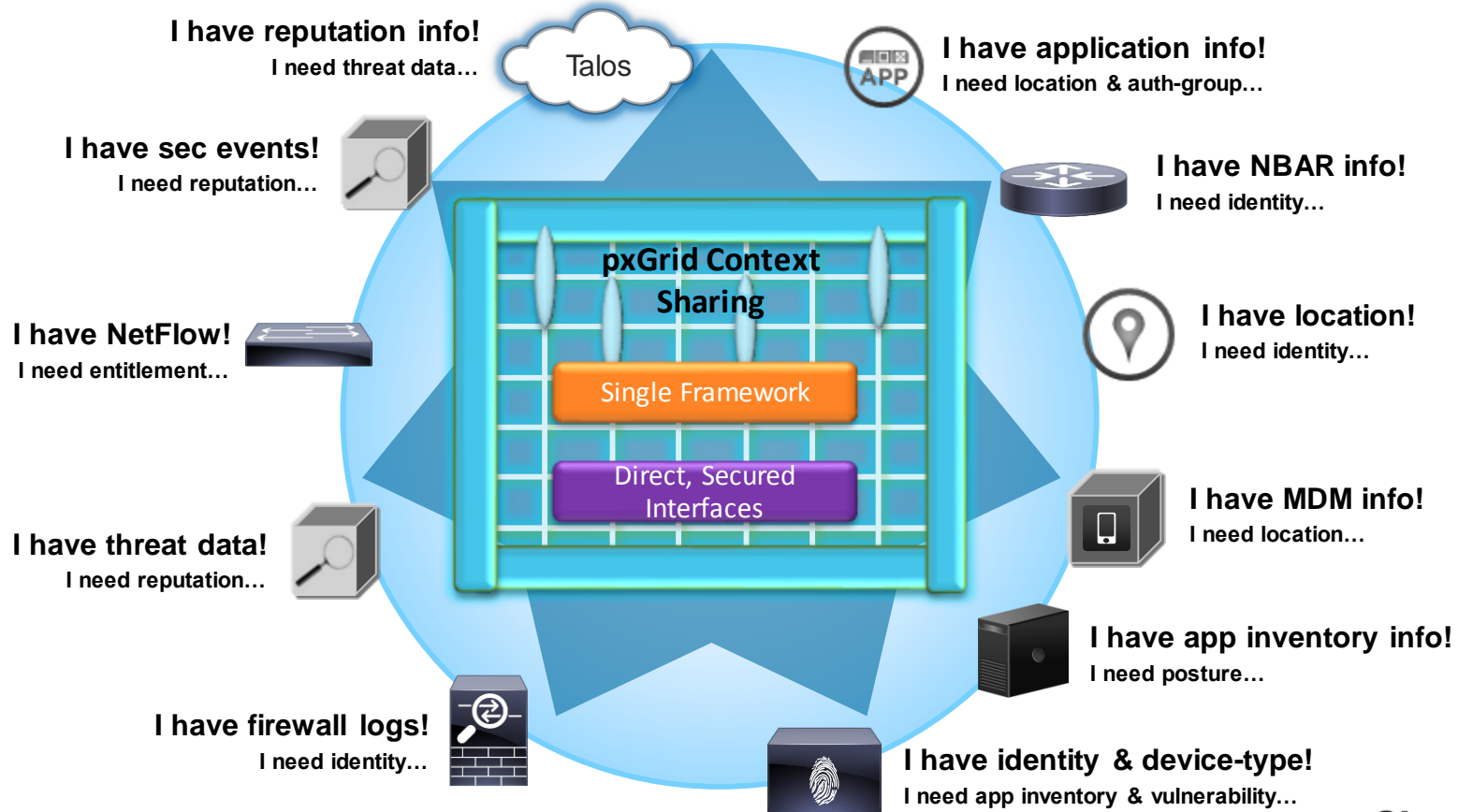
Building a Visibility Architecture

- Why?
 - Automation
 - Contextualisation
 - Anomaly Detection
 - Event-driven Security
- What visibility is important?

Types of Visibility

- Asset/Network
 - Network topology
 - Asset profiles
 - Address
 - Hardware platform/class
 - Operating System
 - Open Ports/Services
 - Vendor/Version of client or server software
 - Attributes
 - Vulnerabilities
- User
 - Location
 - Access profile
 - Behaviours
- File/Data/Process
 - Motion
 - Execution
 - Metadata
 - Origination
 - Parent
- Security
 - Point-in-time events
 - Telemetry
 - Retrospection

Platform Exchange Grid – pxGrid



Cisco FireSIGHT Context Collection Platform

Indications of Compromise (3)

Edit Rule States Mark All Resolved

Category	Event Type	Description	First Seen	Last Seen
Exploit Kit	Intrusion Event - exploit-kit	The host may have encountered an exploit kit	2013-09-17 16:46:28	2013-09-20 06:35:31
CnC Connected	Security Intelligence Event - CnC	The host may be under remote control	2013-09-17 16:52:11	2013-09-20 03:55:45
CnC Connected	Intrusion Event - malware-cnc	The host may be under remote control	2013-09-17 20:09:23	2013-09-19 17:32:49

malware Backdoors

- Exploit Kits
- Web App Attacks
- CnC Connections
- Admin Privilege Escalations

Connections to Known CnC IPs

malware Detections

- Office/PDF/Java Compromises
- Malware Executions
- Dropper Infections

Cisco FireSIGHT Fuels Automation

Impact Assessment and Recommended Rules Automate Routine Tasks

The screenshot displays the Cisco FireSIGHT interface. On the left, a window titled "Intrusion Events" shows a bar chart for "Last 1 hour" and a "Total" column. Below the chart are five rows of event data, each with a colored circle (1-4) and a corresponding bar chart. The "All" row is at the bottom. On the right, a "Policy Information" window is open, showing details for the "Default Production Demo Lab IPS Policy".

Policy Information

Name: Default Production Demo Lab IPS Policy

Description: Sourcefire Provided. For best results, do not modify.

Drop when Inline:

Base Policy: Security Over Connectivity

The base policy is up to date (Rule Update 2013-10-09-004-vrt)

This policy defines 0 variables

This policy has 9038 enabled rules

- 558 rules generate events
- 8480 rules drop and generate events

FireSIGHT recommends 7154 rule state settings for 7430 hosts

- Set 214 rules to generate events
- Set 3550 rules to drop and generate events
- Set 3390 rules to disabled

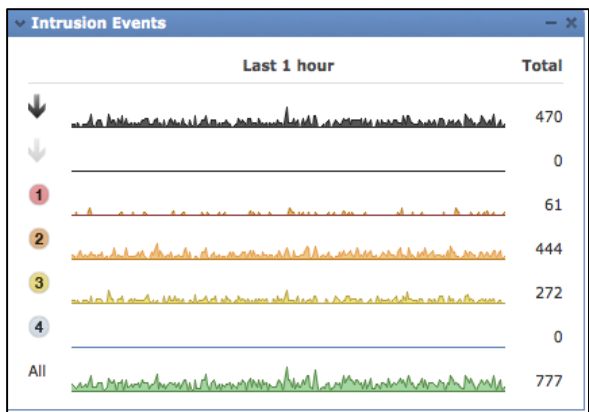
Policy is not using the recommendations. Click to change recommendations






Last generated: 2013 Oct 10 10:15:33

Buttons: Commit Changes, Discard Changes

Impact Assessment

Correlates all intrusion events to an impact of the attack against the target



IMPACT FLAG	ADMINISTRATOR ACTION	WHY
	Act Immediately, Vulnerable	Event corresponds to vulnerability mapped to host
	Investigate, Potentially Vulnerable	Relevant port open or protocol in use, but no vuln mapped
	Good to Know, Currently Not Vulnerable	Relevant port not open or protocol not in use
	Good to Know, Unknown Target	Monitored network, but unknown host
	Good to Know, Unknown Network	Unmonitored network

FireSIGHT Brings Visibility

CATEGORIES	EXAMPLES	Cisco FireSIGHT	TYPICAL IPS	TYPICAL NGFW
Threats	Attacks, Anomalies	✓	✓	✓
Users	AD, LDAP, POP3	✓	✗	✓
Web Applications	Facebook Chat, Ebay	✓	✗	✓
Application Protocols	HTTP, SMTP, SSH	✓	✗	✓
File Transfers	PDF, Office, EXE, JAR	✓	✗	✓
Malware	Conficker, Flame	✓	✗	✗
Command & Control Servers	C&C Security Intelligence	✓	✗	✗
Client Applications	Firefox, IE, BitTorrent	✓	✗	✗
Network Servers	Apache 2.3.1, IIS4	✓	✗	✗
Operating Systems	Windows, Linux	✓	✗	✗
Routers & Switches	Cisco, Nortel, Wireless	✓	✗	✗
Mobile Devices	iPhone, Android, Jail	✓	✗	✗
Printers	HP, Xerox, Canon	✓	✗	✗
VoIP Phones	Cisco, Avaya, Polycom	✓	✗	✗
Virtual Machines	VMware, Xen, RHEV	✓	✗	✗

OpenAppID – First OSS Application and Control

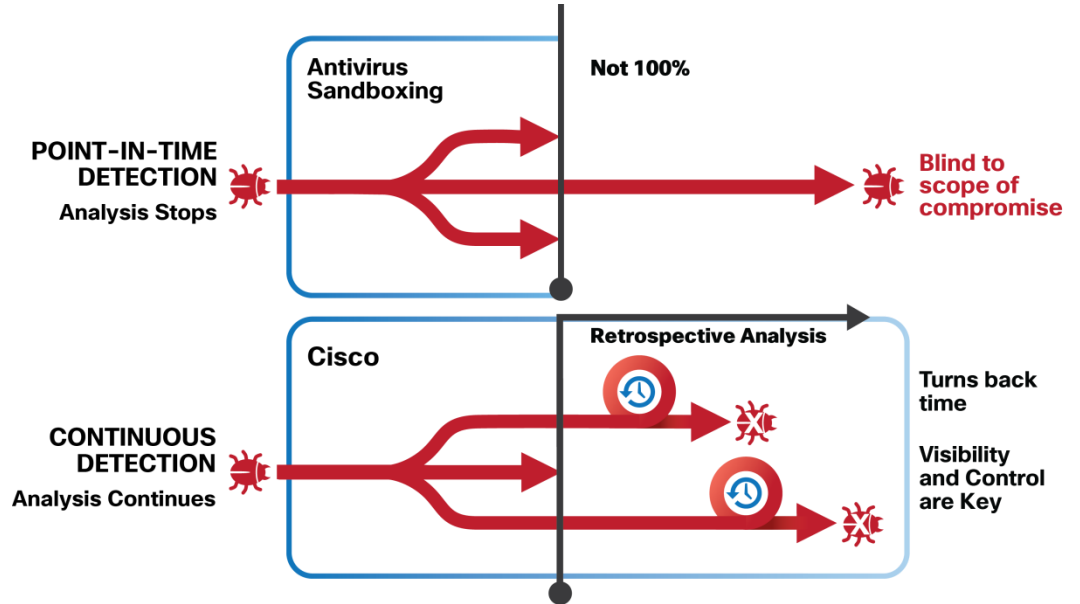
- OpenAppID Language Documentation
 - Accelerate the identification and protection for new cloud-delivered applications
- Special Snort engine with OpenAppID preprocessor
 - Detect apps on network
 - Report usage stats
 - Block apps by policy
 - Snort rule language extensions to enable app specification
 - Append 'App Name' to IPS events
- Library of Open App ID Detectors
 - Over 1000 new detectors to use with Snort preprocessor
 - Extendable sample detectors



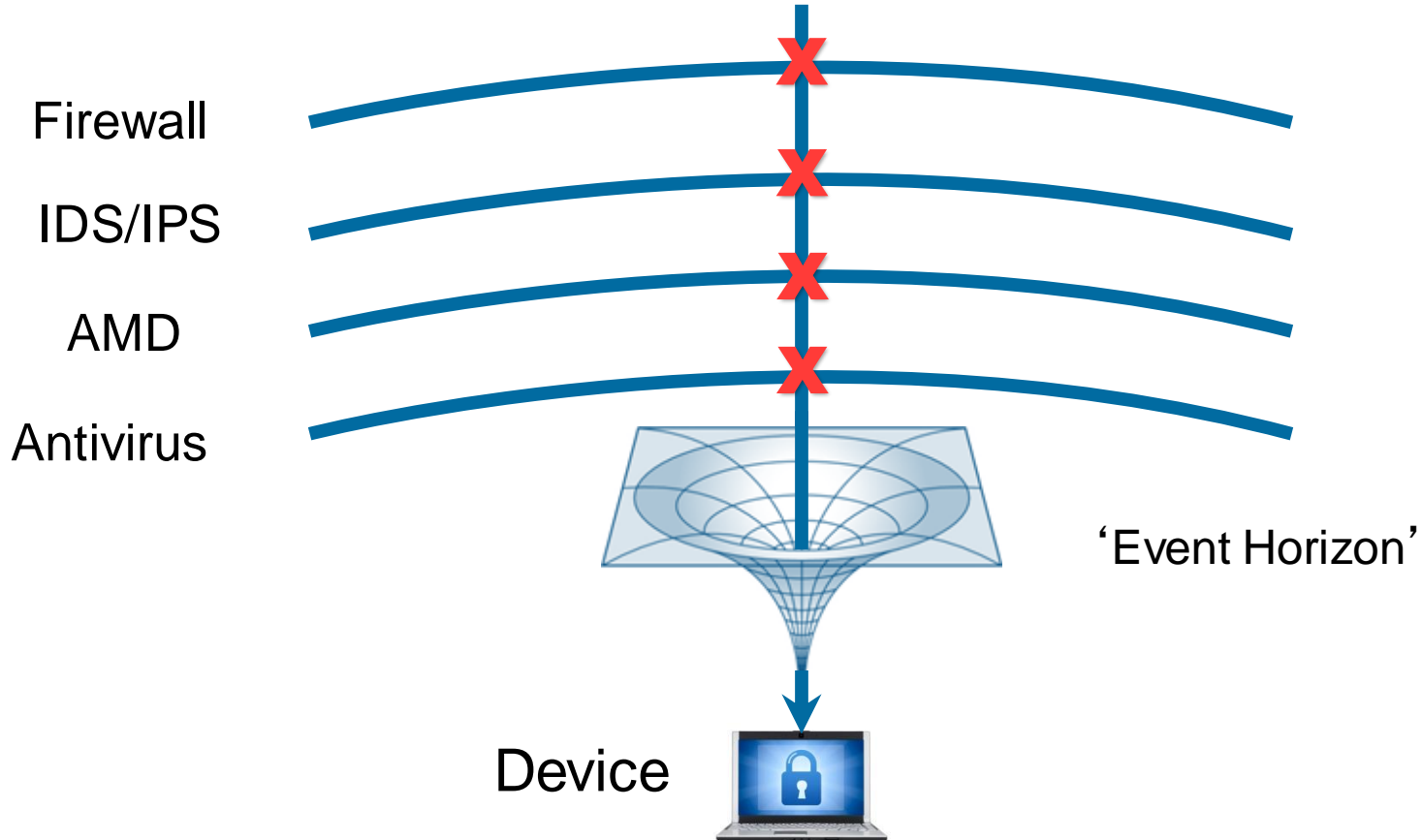
Available now at Snort.org

The Event Horizon Problem

- Point-in-time
 - Events generated as they're discovered
 - Discovery (detection) failure = false negative
 - Brittle.
- Continuous (Telemetry)
 - Specific event types are continuously recorded and analysed
 - Structural (signatures)
 - Behavioural (activities)



The Event Horizon



Beyond The Event Horizon

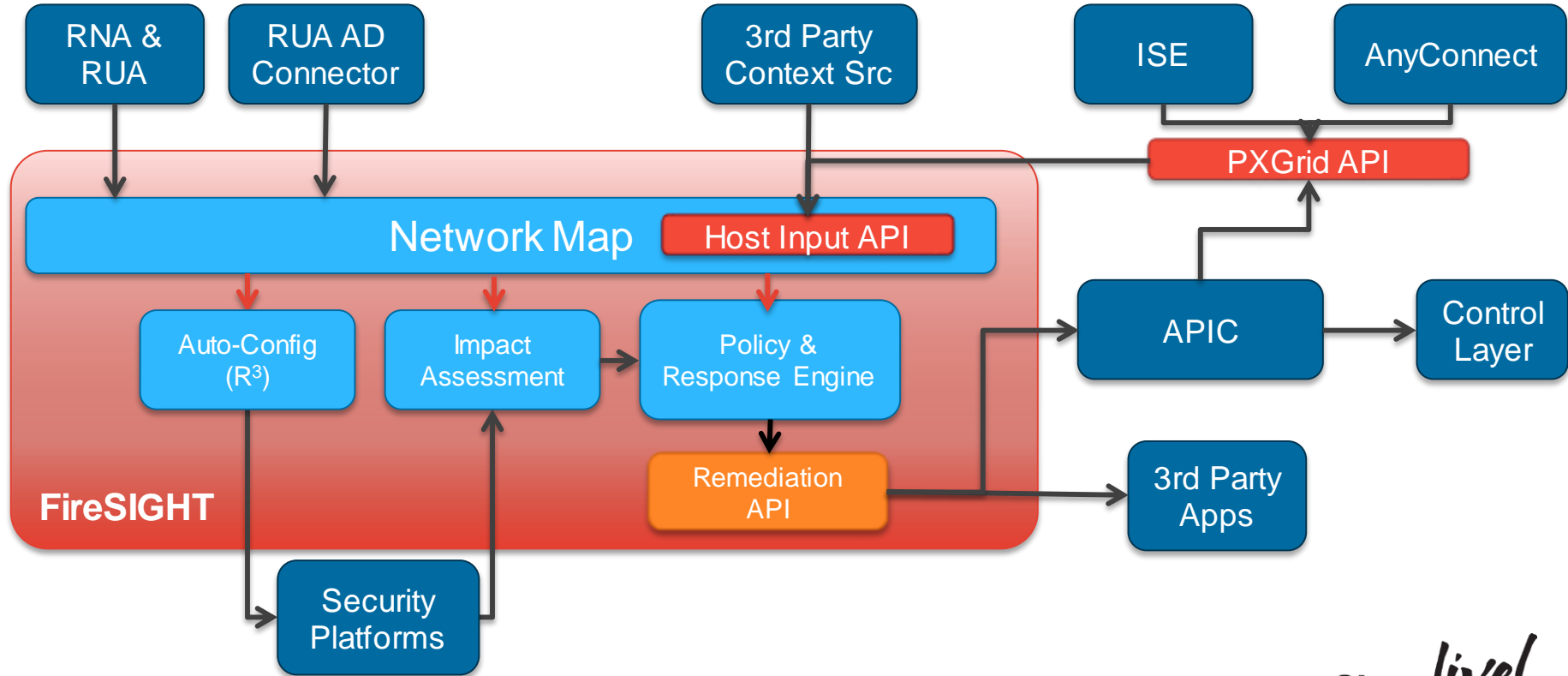
- Continuous Capability is needed for the world in which you *will* be compromised
 - Streaming telemetry
 - Continuous analysis
 - Real-time and retrospective security with the full spectrum of controls available at *any time*



The Threat-Centric Model

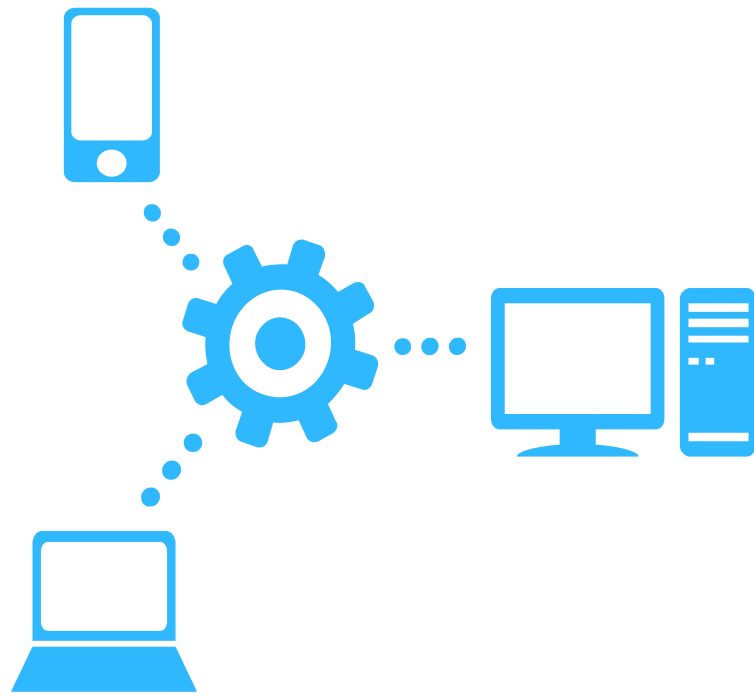


Visibility Layer Concept

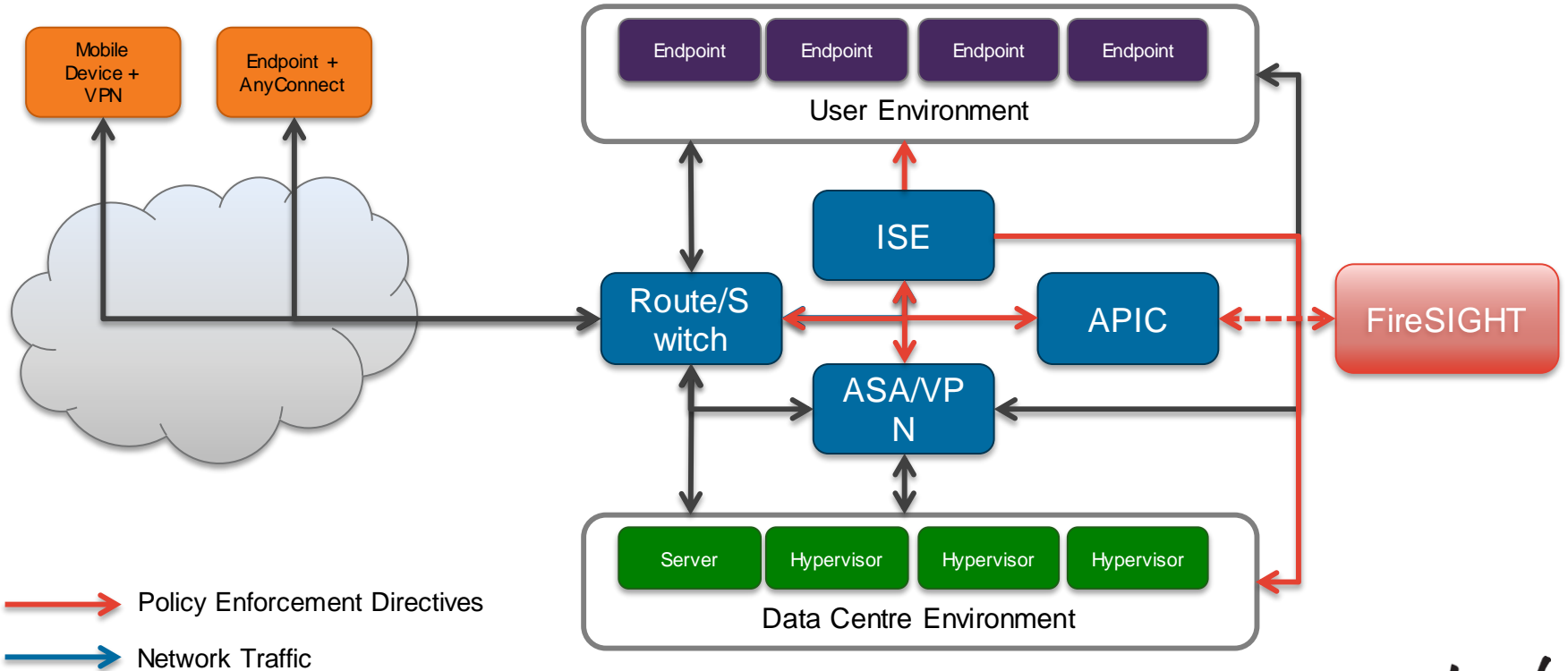


Control

- Control is about defining & managing the interactions between users, applications, devices, and data
- Access control & segmentation
- Policy enforcement
- Asset hardening & management
- User management



Control Layer Concept

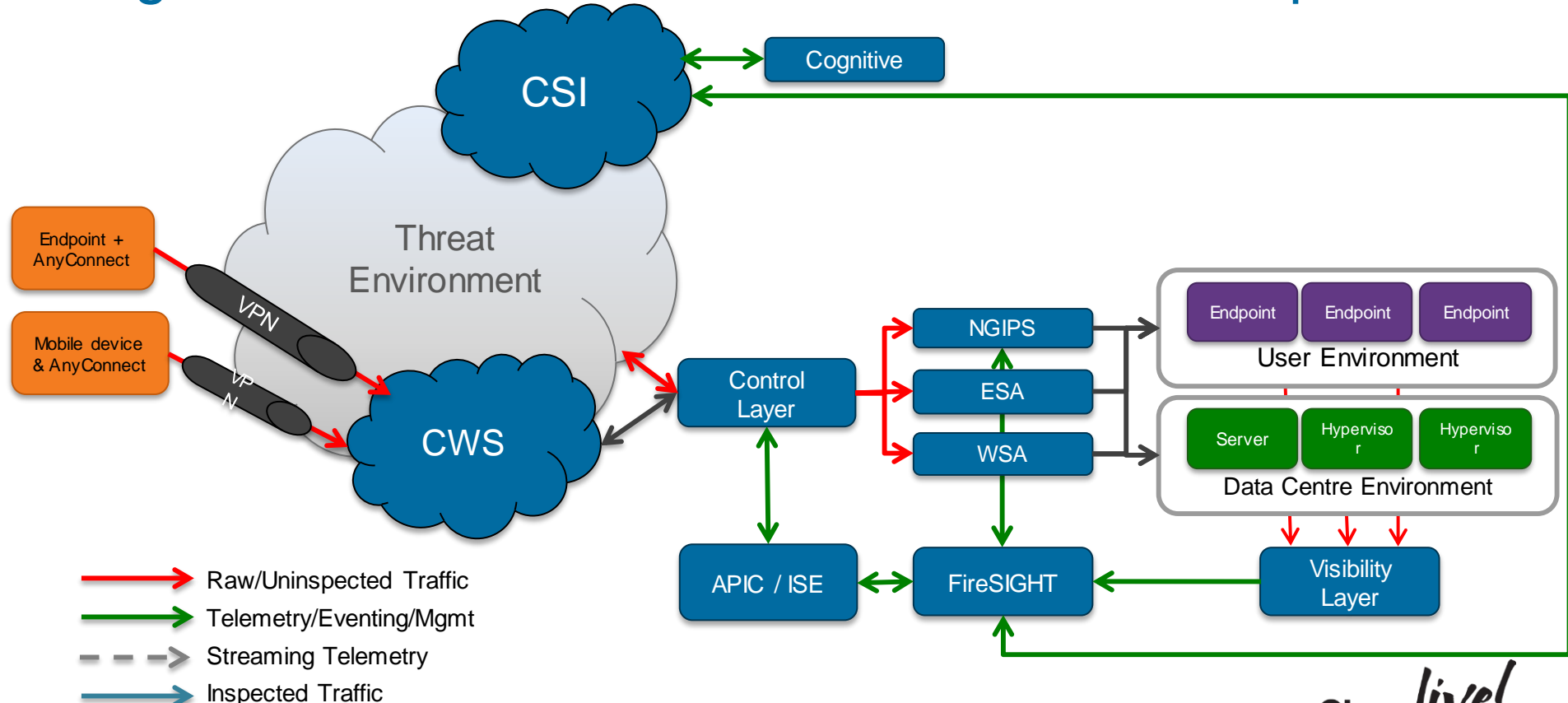


Threat and Breach

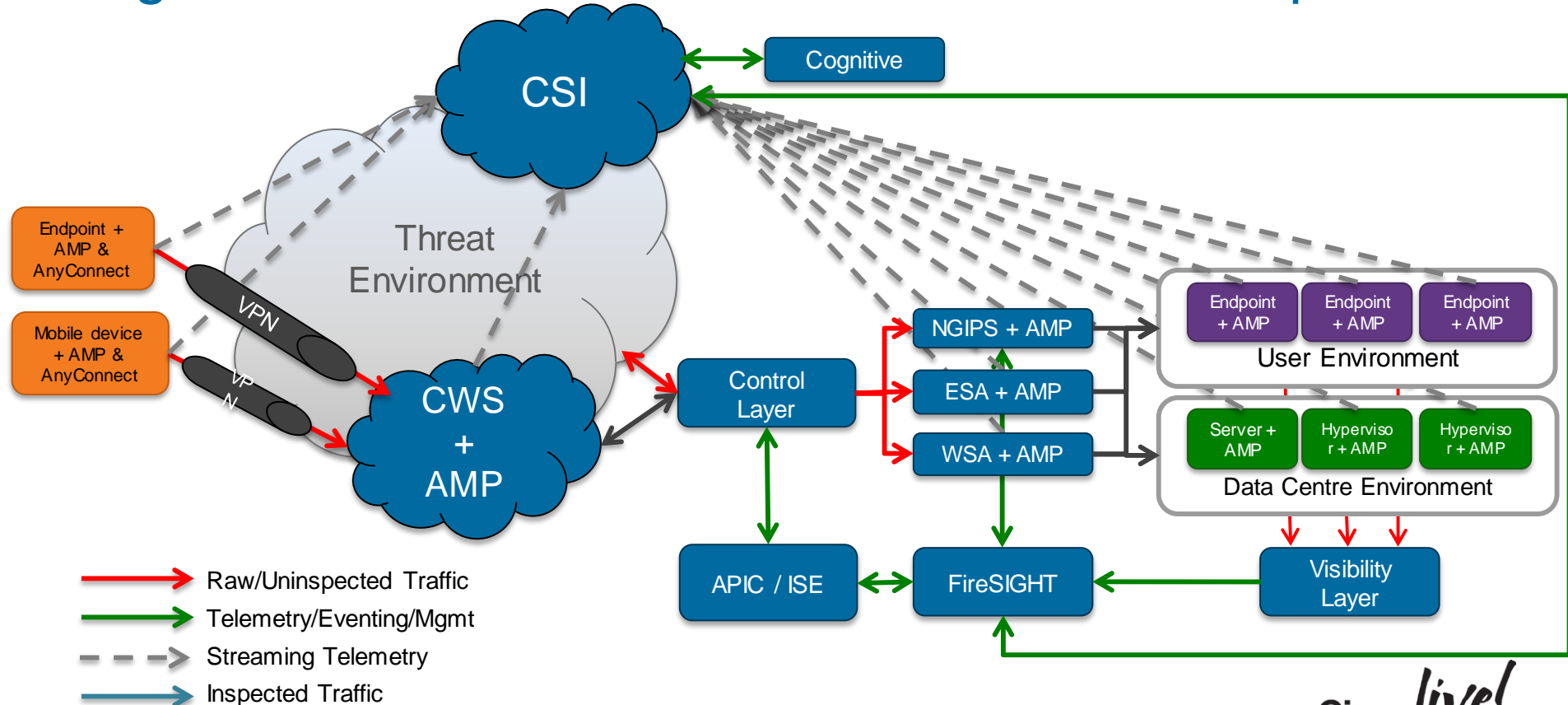
- Detection & Response are critical functions today
- Being able to detect in a “relevant timeframe”
- Timeframe of response
 - “The Golden Hour”



Integrated Threat Defence Architecture Concept



Integrated Threat Defence Architecture Concept

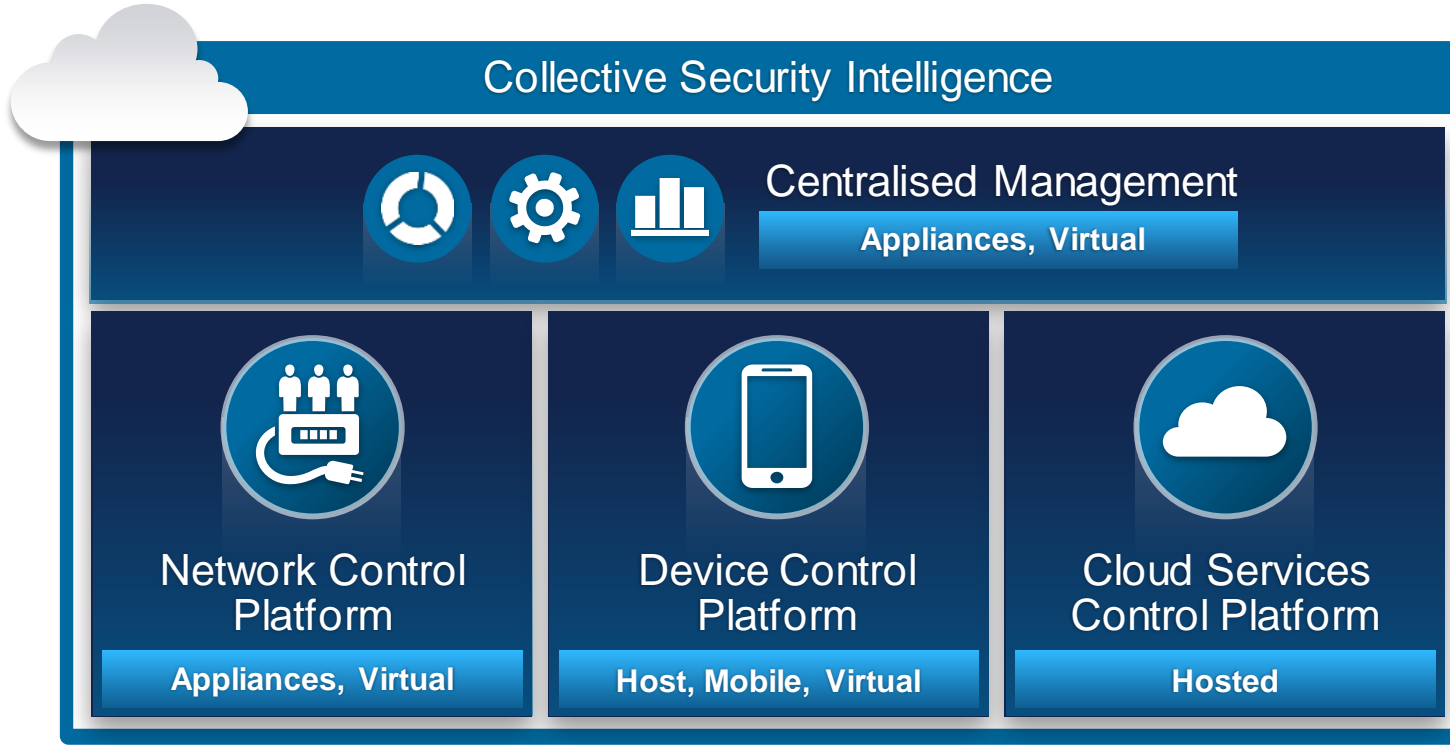


Challenges

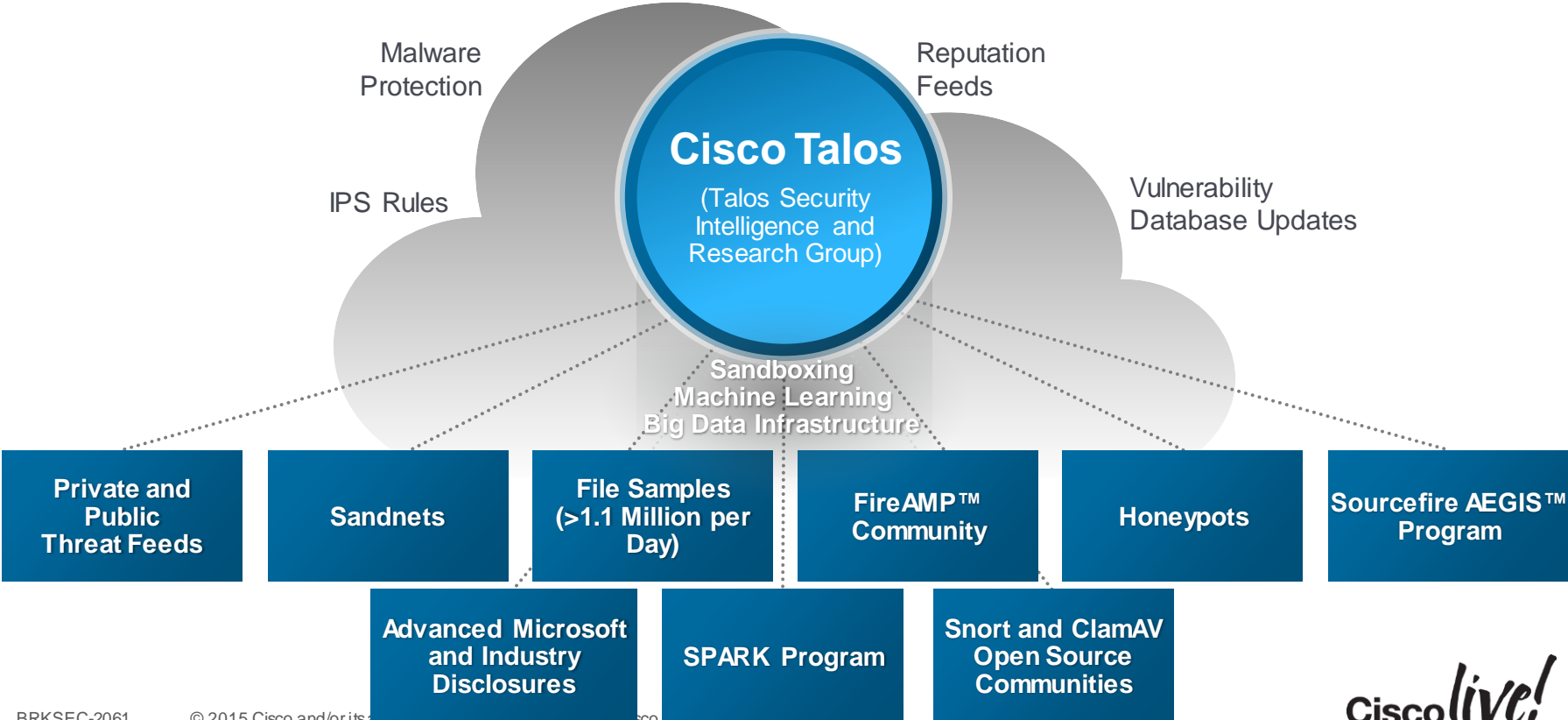
- None of this works if everything has to be there for any of it to work
- Each product must stand alone as the best in its class
- When Cisco products are brought together they gain capability through leveraging each other's visibility and control mechanisms

Our fundamental job is to reduce complexity and increase capability

Reduce Complexity and Increase Capability



Collective Security Intelligence



A long-exposure photograph of a city street at night. The foreground is dominated by vibrant, multi-colored light trails from moving vehicles, creating a sense of motion and energy. In the background, modern city buildings are illuminated with various lights, and a pedestrian bridge spans across the street. The overall scene is a dynamic urban landscape.

It Takes an Architecture

Cisco *live!*

Start with Best-of-breed Products

*The **NGFW** Security Value Map shows the placement of Cisco ASA with FirePOWER Services and the FirePOWER 8350 as compared to other vendors. All three products achieved **99.2** percent in security effectiveness and now all can be confident that they will receive the best protections possible regardless of deployment.*

*Cisco Advanced Malware Protection (**AMP**) has the lowest TCO of any product tested. It is also a leader in security effectiveness achieving detection of **99** percent of all tested attacks AMP excelled in time-to-detection, catching threats faster than competing Breach Detection Systems.*

Based on individual and comparative testing of vendors in the IPS market Cisco FirePOWER **NGIPS** leads the Security Value Map and provides the best protection possible while also leading the class in total cost of ownership.*

Source: Independent Competitive Testing done by NSS Labs

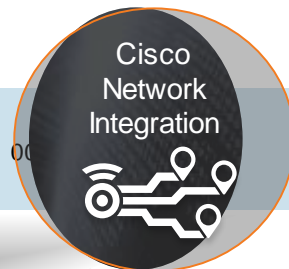
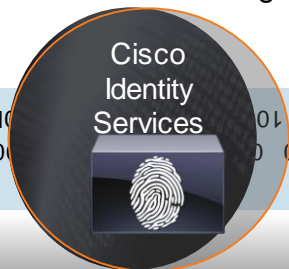
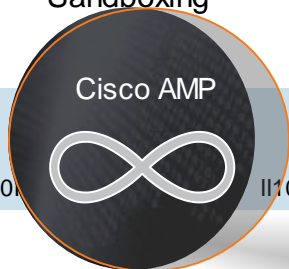
Working Together to Create a Security Architecture

Malware Prevention / Sandboxing

Context-aware Segmentation

Common Identity, Policy and Context Sharing

Wired/Wireless and VPN



Context Pervasive & Integrated Across the Portfolio Visibility



Cisco ASA w/FirePOWER



Cisco NGIPS



Cisco Web & Email Security



Cisco AMP Client

Superior Intelligence to Battle Advanced Threats

Cisco®
SIO

1.6 million
global sensors

35%
worldwide email traffic

100 TB
of data received per day

13 billion
web requests

150 million+
deployed endpoints

24x7x365
operations

600+
engineers, technicians,
and researchers

40+
languages

Talos
Cisco Collective
Security Intelligence



Pervasive across Portfolio

Sourcefire
VRT®

180,000+ File Samples per Day

FireAMP™ Community, 3+ million

Advanced Microsoft
and Industry Disclosures

Snort and ClamAV Open Source Communities

Honeypots

Sourcefire AEGIS™ Program

Private and Public Threat Feeds

Dynamic Analysis

Enhance with Cisco Security Services



Custom Threat Intelligence

Technical Security Assessments



Integration Services

Security Optimisation Services



Managed Threat Defence

Remote Managed Services

Only Cisco Delivers

Unmatched
Visibility



Global Intelligence
With the Right
Context

Consistent
Control



Consistent Policies
Across the
Network and
Data Centre

Advanced Threat
Protection



Detects and Stops
Advanced Threats

Complexity
Reduction



Fits and Adapts
to Changing
Business Models

Related Sessions

- BRKSEC-1030 - Introduction to the Cisco Sourcefire NGIPS – Gary Spiteri
- BRKSEC-2021 - Firewall Architectures in the Data Centre and Internet Edge - Goran Saradzic
- BRKSEC-2028 - Deploying Next Generation Firewall with ASA and Firepower Services – Jeff Fanelli
- BRKSEC-2044 - Building an Enterprise Access Control Architecture Using ISE and TrustSec – Imran Bashir
- BRKSEC-2664 - Cisco Sourcefire Advanced Malware Protection (AMP) - Jay Tecksingani
- BRKSEC-2690 - Deploying Security Group Tags – Kevin Regan
- BRKSEC-2691 - Identity Based Networking: IEEE 802.1X and Beyond – Hari Prasad Holla
- BRKSEC-2902 - Embrace Cloud Web Security With Your Cisco Network – Hideyuki Kobayashi
- BRKSEC-3770 - Advanced Email Security with ESA – Joe Montes
- BRKSEC-3771 - Web Security Deployment with WSA – ChooKai Kang

Continue Your Education

- Demos in the Cisco Campus
- Walk-in Self-Paced Labs
- Meet the Expert 1:1 meetings



Q & A

Cisco *live!*

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2015 T-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
<http://showcase.genie-connect.com/clmelbourne2015>
- Visit any Cisco Live Internet Station located throughout the venue

T-Shirts can be collected in the World of Solutions on Friday 20 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



Thank you.

Cisco *live!*



CISCO

Session Abstract

BRKSEC-2061: Cisco + SourceFire: Threat-Centric Security Approach

Jatin Sachdeva, Security Architect, Cisco ANZ

To truly protect against all possible attack vectors, IT professionals must accept the nature of modern networked environments and devices and start defending them by thinking like defenders responsible for securing their infrastructure. Critical to accomplishing this is first understanding the modern threat landscape and how a threat-centric approach to security can increase the effectiveness of threat prevention. This technical session will provide a "how to" with the Cisco Security portfolio, provide an update on the Cisco and Sourcefire security architectures and integrations, and also detail current threats based on research from Cisco's Talos Security Intelligence & Research Group. By attending this session, Security, Network and IT architects, will benefit from learning approaches that protect their environments across the attack continuum - before, during and after an attack.



CISCO