



Next Generation Firewall

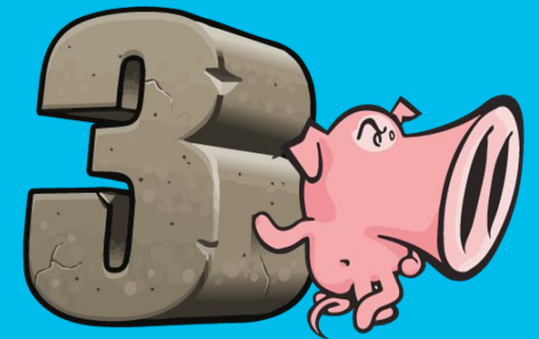
Anticipate, block, and respond to threats

Luc Billot

Cyber Security Technical Architect - Cisco

April 2019

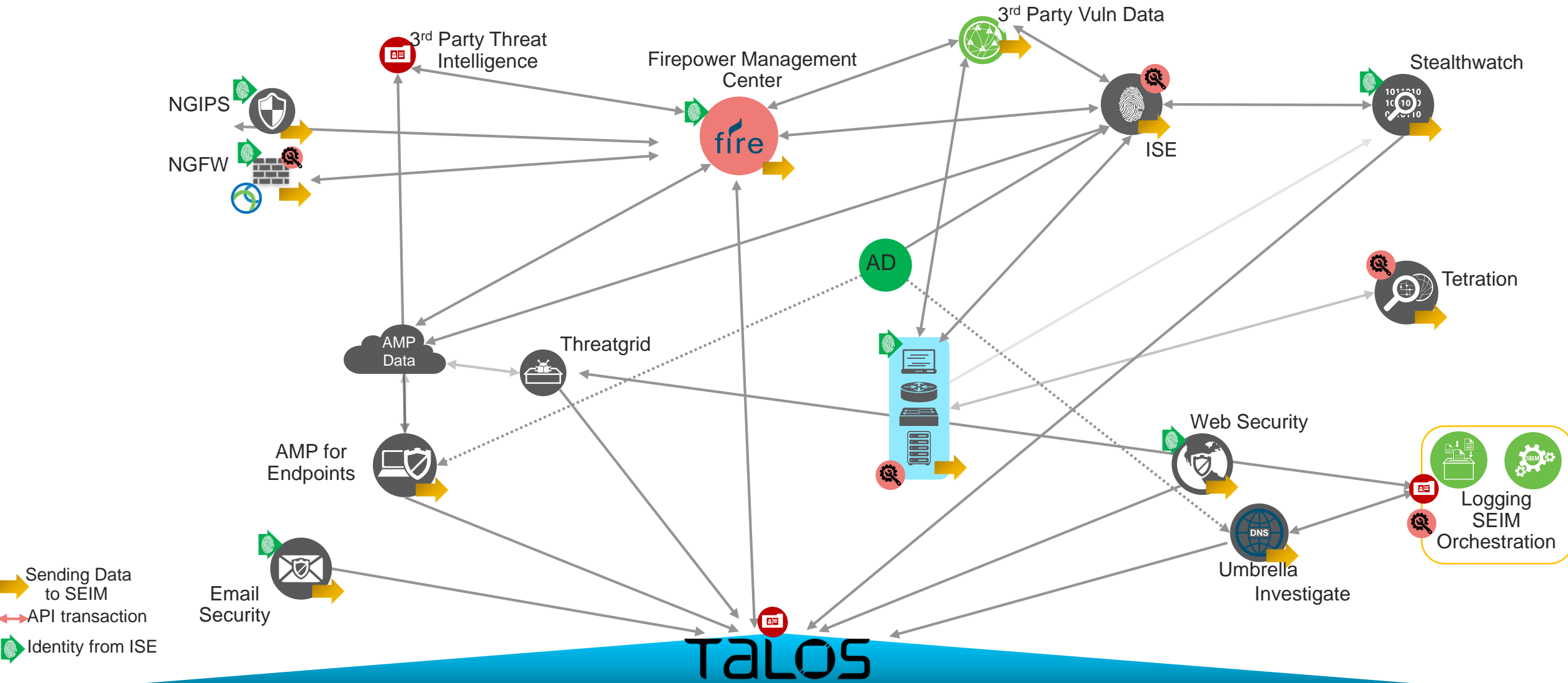
Why Cisco Bought SourceFire ?



It is a 2.7 Billion \$
question...

- SNORT
- VRT
- Immunet
- ClamAV
- FirePower
- FireSight

Security is an Integration Game



Cisco Firewalls have you covered

WannaCry
May 2017

NotPetya
June 2017

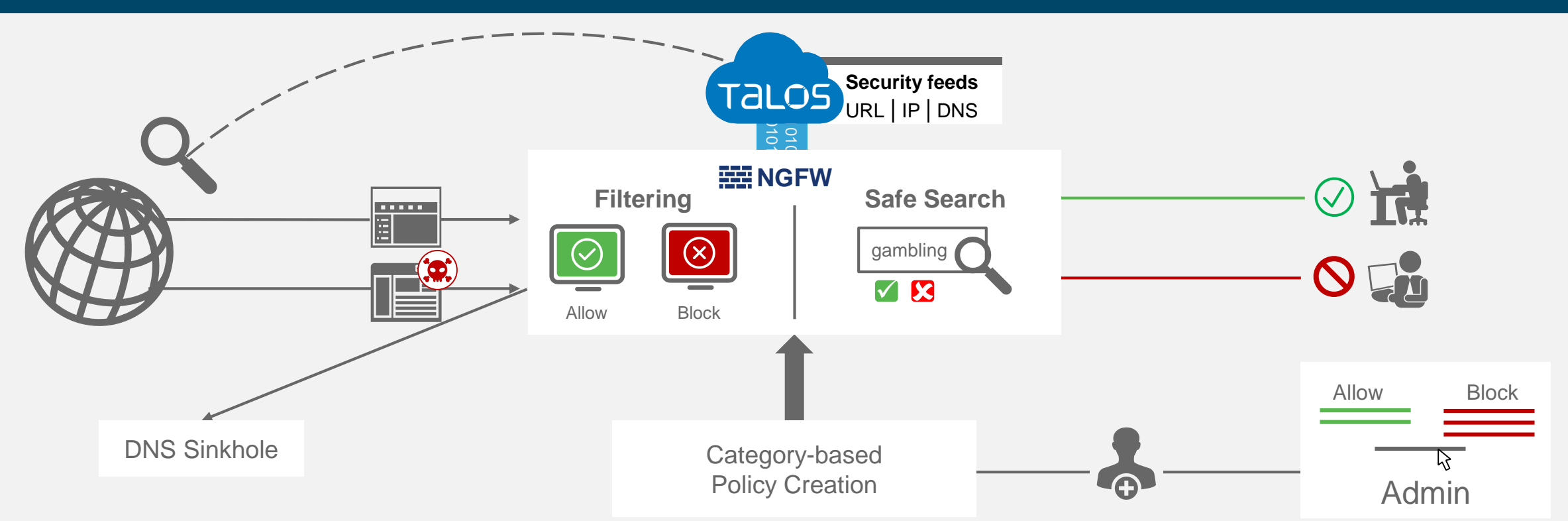
VPNFilter
May 2018

Product	Protection	Protection	Protection
AMP	✓	✓	✓
CWS	✓	N/A	✓
Firewall	✓	✓	✓
Threat Grid	✓	✓	✓
Umbrella	✓	N/A	✓
WSA	✓	N/A	✓

Automatic Threat Prevention

Block or allow access to URLs and domains

Security Intelligence, URL Filtering, DNS Sinkhole



Classify **280M+** URLs

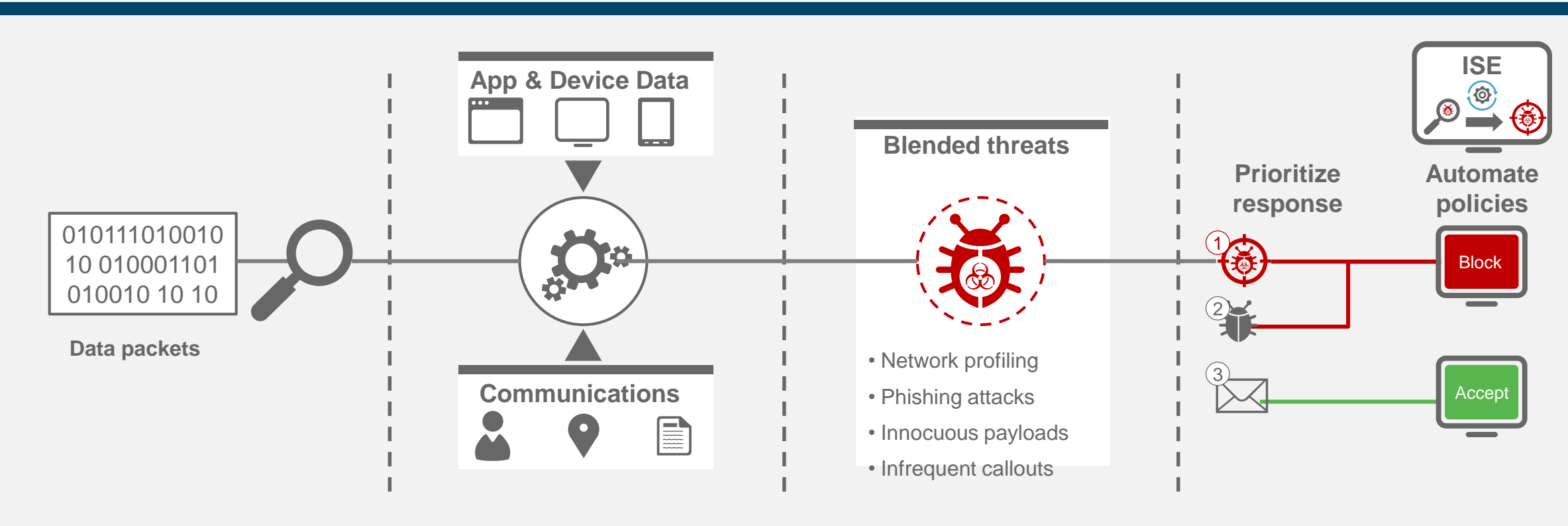
Filter sites using **80+** categories

Manage Acceptable Use Policy

Block latest malicious URLs

Understand threat details and quickly respond

Next-Generation Intrusion Prevention System (NGIPS)



Scan network traffic

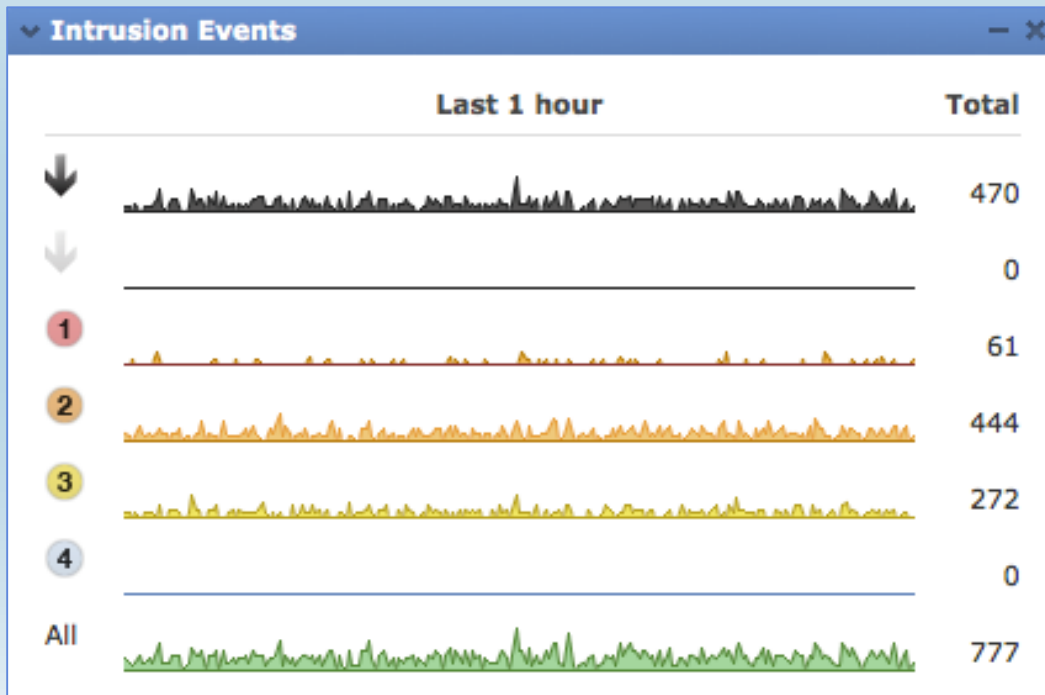
Correlate data

Detect stealthy threats

Respond based on priority

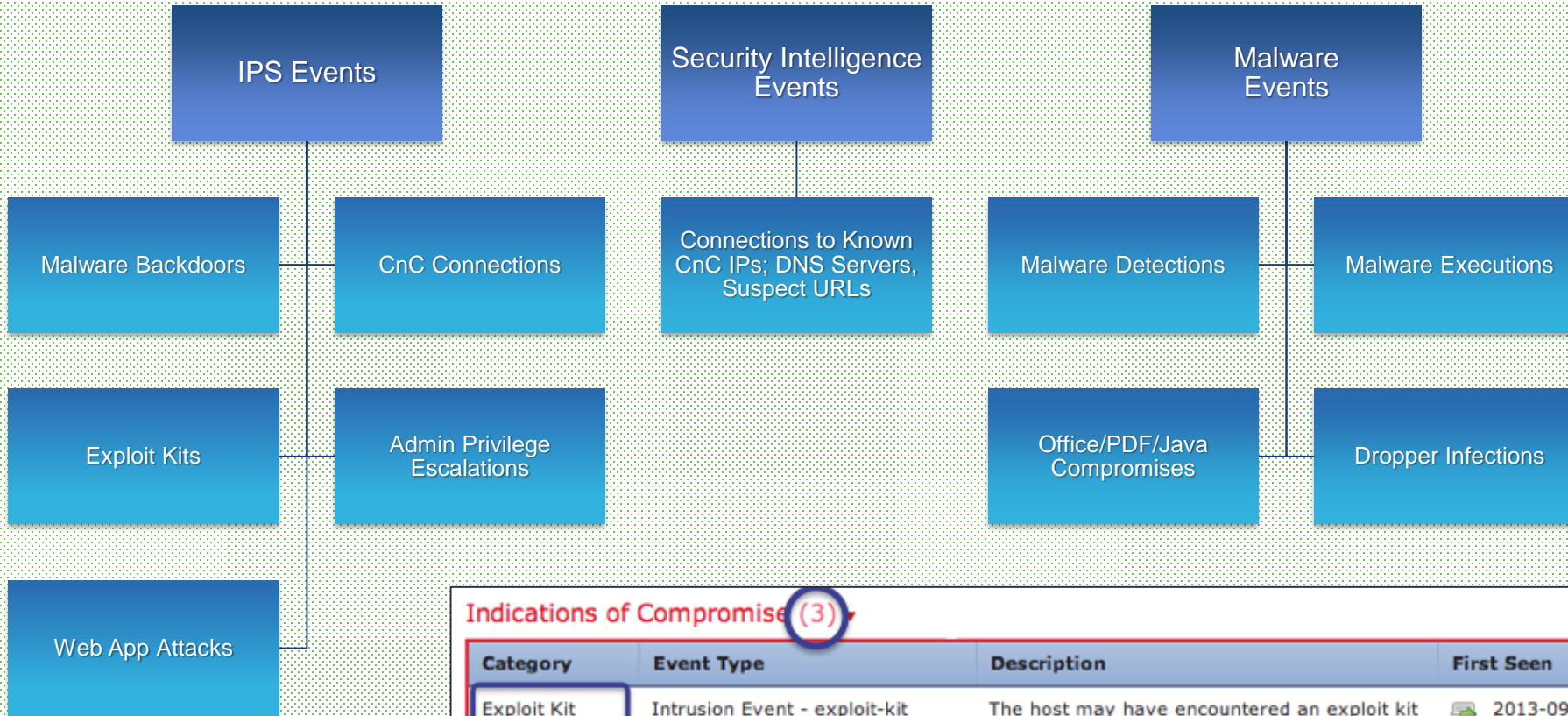
Automated Impact Assessment

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



Impact Flag	Administrator Action	Why
1	Act immediately; vulnerable	Event corresponds to vulnerability mapped to host
2	Investigate; potentially vulnerable	Relevant port open or protocol in use, but no vulnerability mapped
3	Good to know; currently not vulnerable	Relevant port not open or protocol not in use
4	Good to know; unknown target	Monitored network, but unknown host
0	Good to know; unknown network	Unmonitored network

Indications of Compromise (IoCs) Detection & Threat Correlation



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

Firepower Recommendations Knows what I Do Not

Firepower Recommended Rules Configuration < Back

Firepower changed 8413 rule states for 95 hosts View Recommended Changes

- Set 182 rules to generate events View
- Set 8231 rules to drop and generate events View
- Set 0 rules to disabled View

Policy is using the recommendations. Click to change recommendations
Last generated: 2017 Jan 10 11:17:30

Include all differences between recommendations and rule states in policy reports

Advanced Settings

Networks to Examine

Networks

(Single IP address, CIDR block, or comma-separated list)

Firepower Recommended Rules Configuration

Recommendation Threshold
(By Rule Overhead)

None Low Medium High

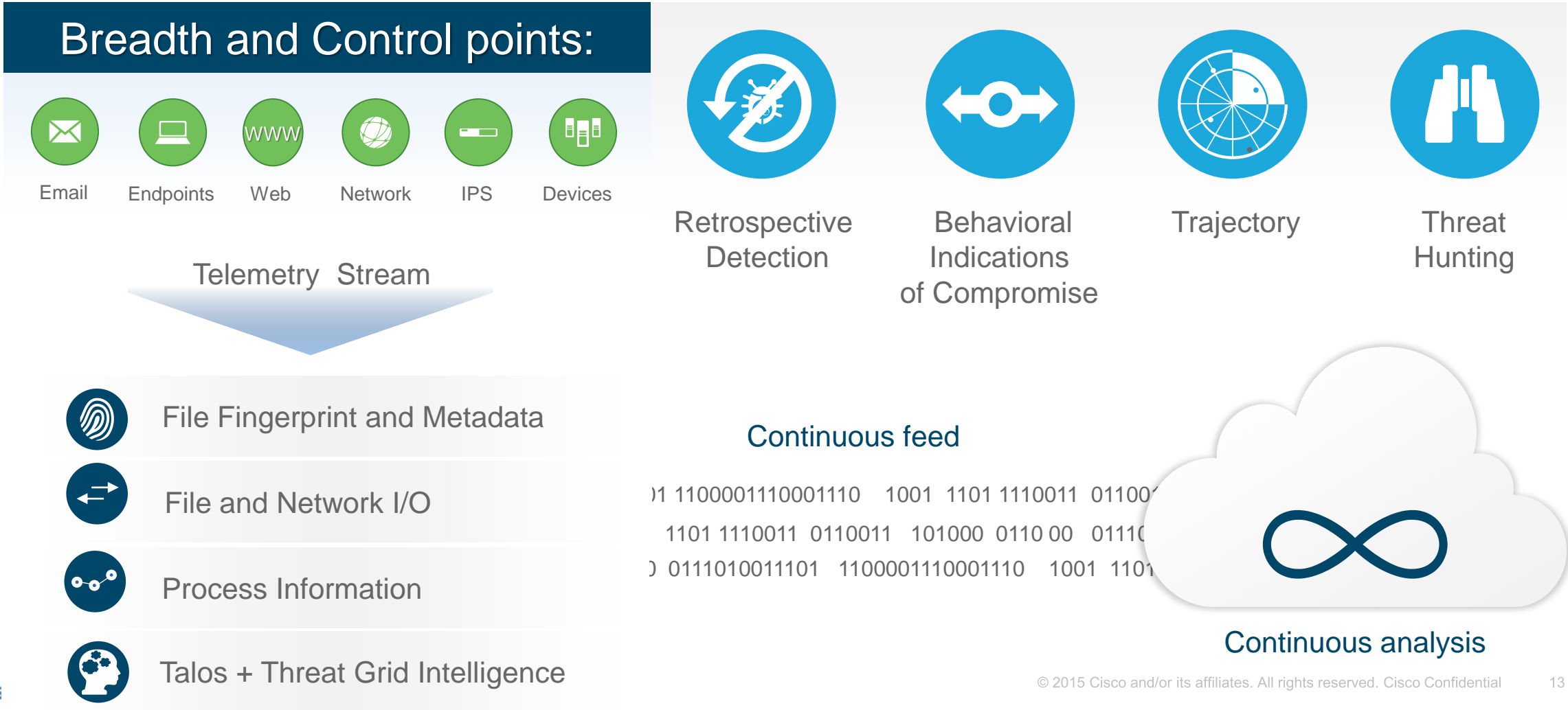
Accept Recommendations to Disable Rules

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

12

Uncover hidden threats in the environment

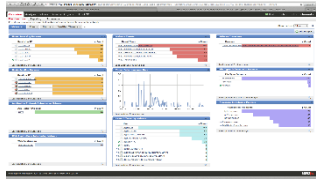
Advanced Malware Protection (AMP)



AMP in Action



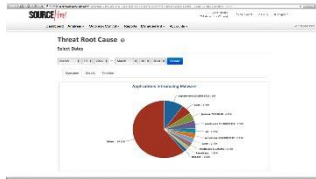
Who



Focus on these users first



What



These applications are affected



Where



The breach impacted these areas



When



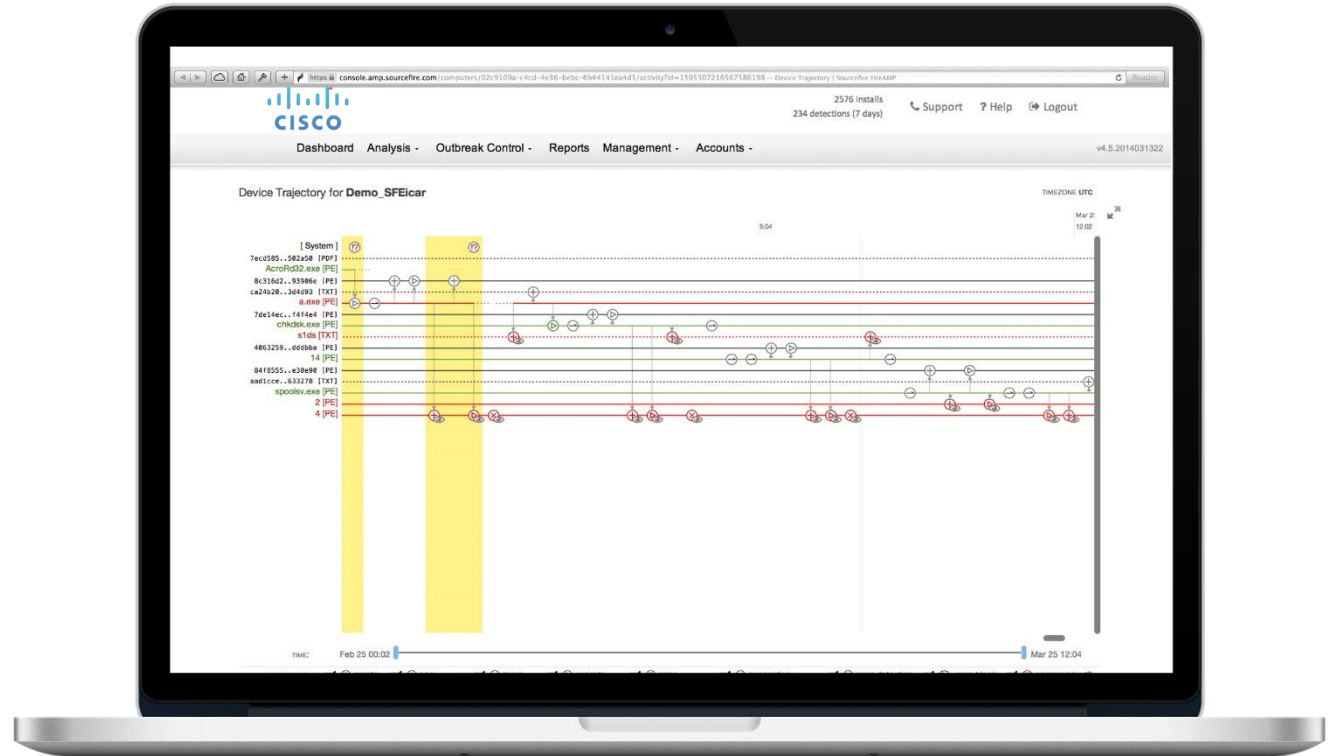
This is the scope of exposure over time



How
CISCO



Here is the origin and progression of the threat



**Network and Endpoint Correlation
IN FIREPOWER MANAGEMENT CENTER**

The results speak for themselves

4.6 Hours

Median time to detection
with Cisco security*

Weeks

Industry average time
to detection

* Source: Cisco 2018 Annual CyberSecurity Report



More visibility equals faster time to detection



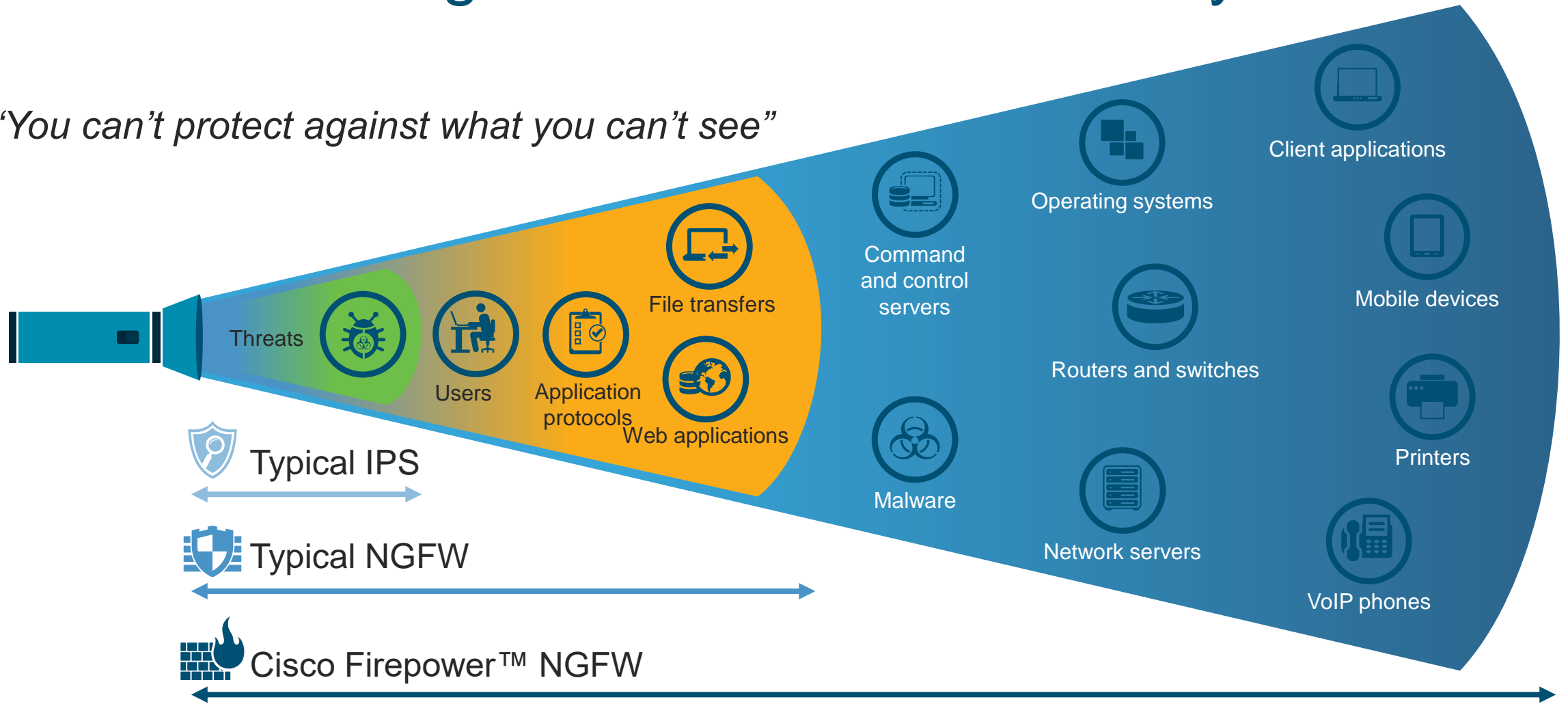
Network and Security
Visibility and Analysis

See more and detect
threats faster

- **Visibility into threat activity** across users, hosts, networks, and infrastructure
- **Network file trajectory** maps how hosts transfer files, including malware files, across your network to scope an attack, set outbreak controls, and identify the source of the threat
- **Centralized management** provides contextual threat analysis and reporting, with consolidated visibility into security and network operations

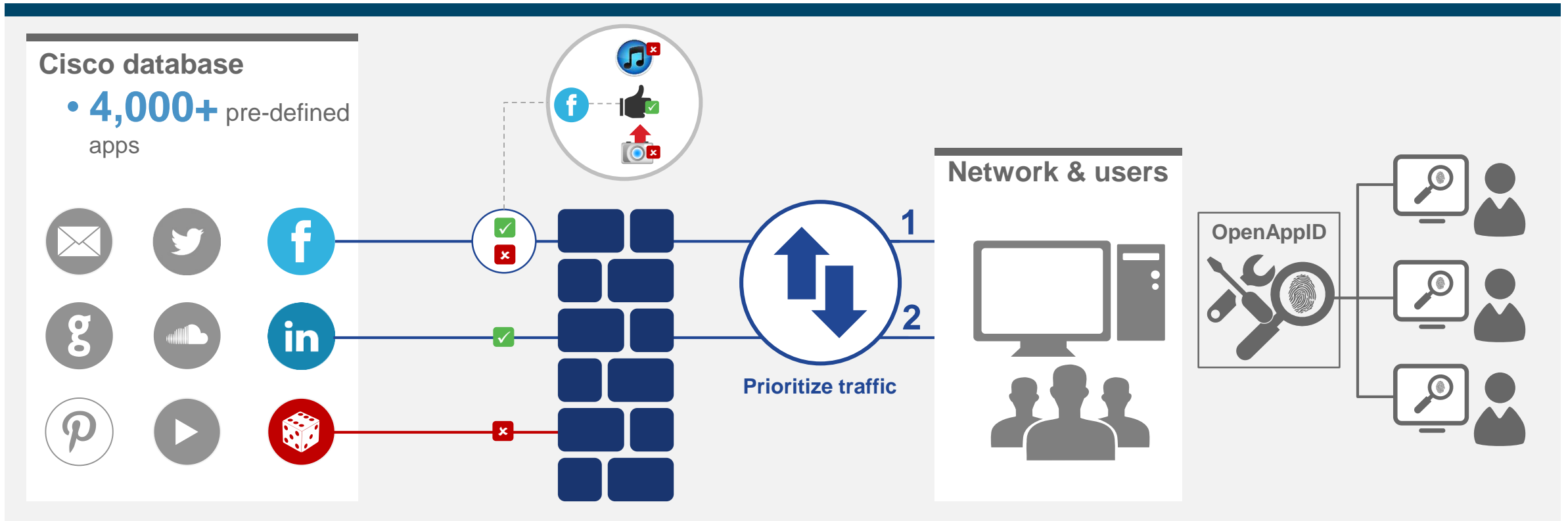
Gain more insight with increased visibility

“You can’t protect against what you can’t see”



Provide next-generation visibility into app usage

Application Visibility & Control



See and understand risks

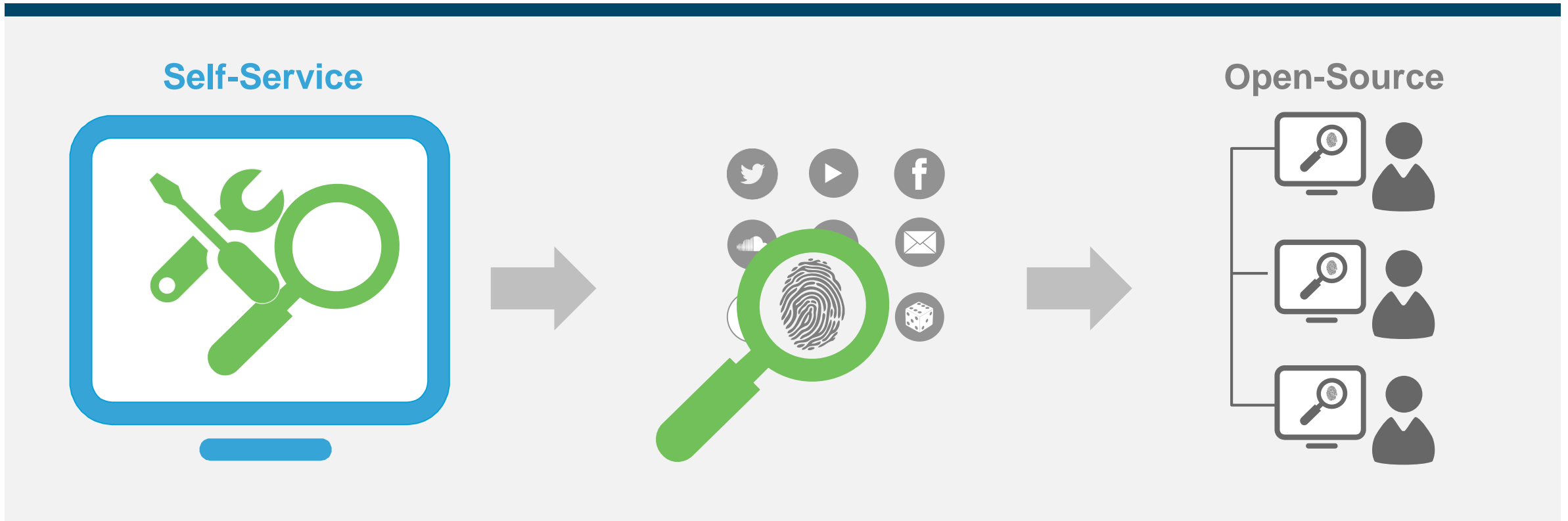
Enforce granular access control

Prioritize traffic and limit rates

Create detectors for custom apps

Extend AVC to proprietary and custom apps

OpenAppID - Crowdsourcing Application Detection



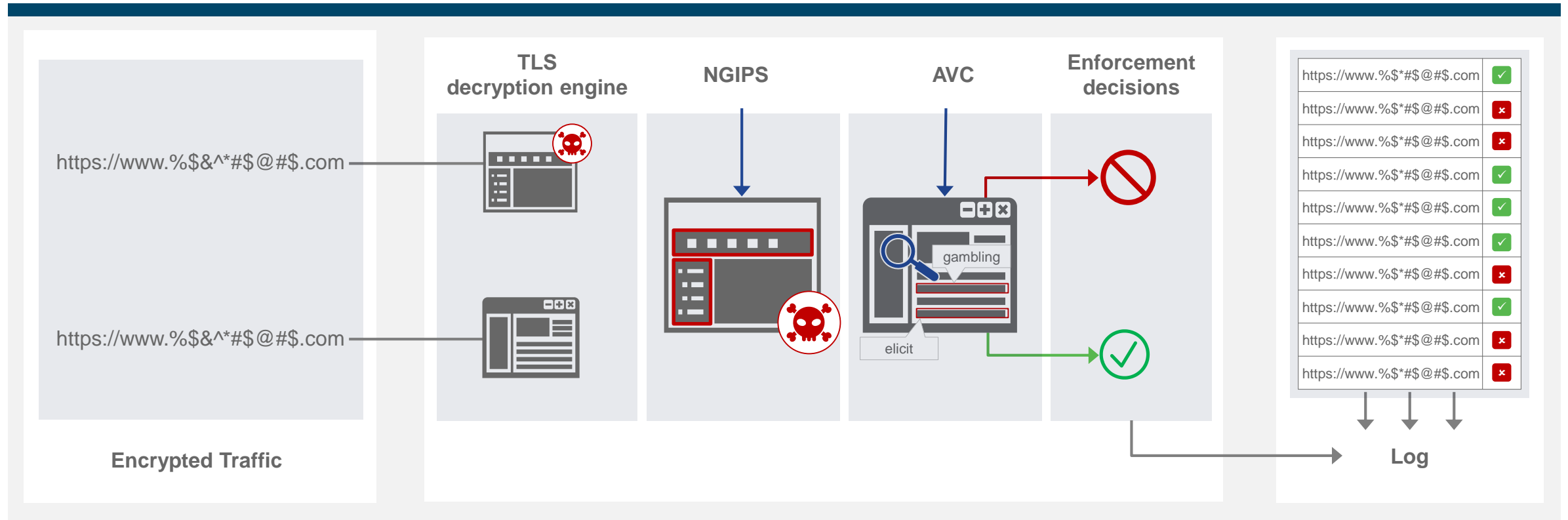
Easily customize application detectors

Detect custom and proprietary applications

Share detectors with other users

Uncover hidden threats at the edge

TLS/SSL decryption engine



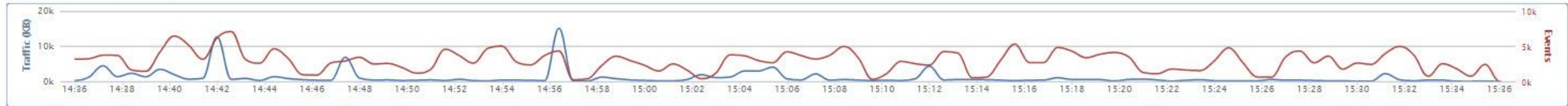
Decrypt traffic in hardware and software

Inspect deciphered packets

Track and log all TLS sessions

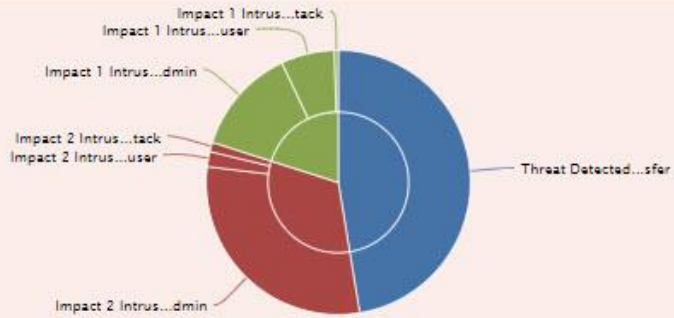
Visibility Provides Context

Traffic and Intrusion Events over Time



Indications of Compromise

Hosts by Indication

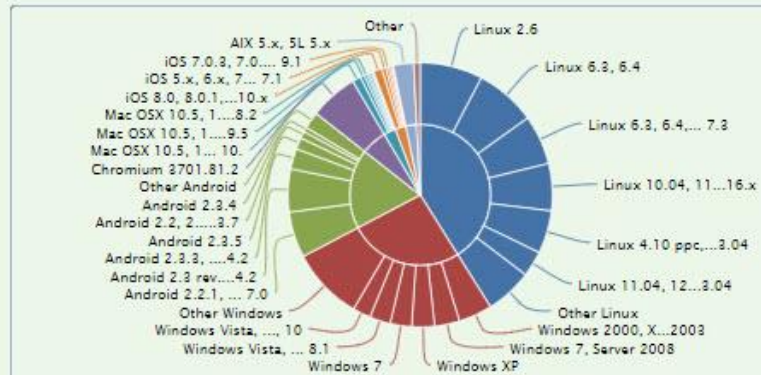


Indications by Host



Network Information

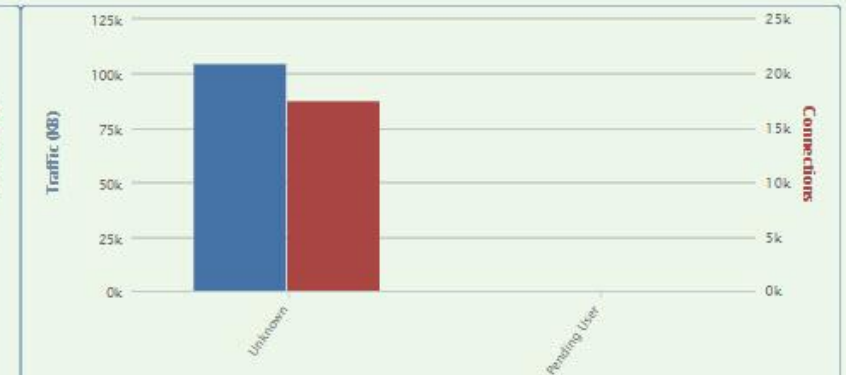
Operating Systems



Traffic by Source IP



Traffic by Source User





Traffic by Destination IP

Traffic by Ingress Security Zone

Detailed Threat Analytics

Event Information ▾

Event	PROTOCOL-SNMP trap udp (1:1419:17)
Timestamp	2018-09-10 14:29:08
Classification	Attempted Information Leak
Priority	medium
Ingress Security Zone	External
Egress Security Zone	Internal
Domain	Global \ Cisco_Backend \ Cisco_SOC
Device	vNGIPS.dcloud.cisco.com
Ingress Interface	eth1
Egress Interface	eth2
Source IP	172.91.41.1
Source Port / ICMP Type	34809 / udp
Source Country	 USA
Destination IP	192.89.41.133
Destination Port / ICMP Code	161 (snmp) / udp
Destination Country	 FIN
Intrusion Policy	[0] Cisco dCloud - IPS Policy - Production
Access Control Policy	Cisco dCloud - ACP - SOC NGIPS
Access Control Rule	Default for Inline Set
Rule	alert udp \$EXTERNAL_NET any -> \$HOME_NET 162 (msg:"PROTOCOL-SNMP trap flow:to_server; metadata:ruleset community, service snmp; reference:bugtraq,4 reference:bugtraq,4089; reference:bugtraq,4132; reference:cve,2002-0012; reference:cve,2002-0013; classtype:attempted-recon; sid:1419; rev:17; gid:1;

Rule Actions

[View Documentation](#)

[Rule Comment](#)

[Edit](#)

[Disable this rule in the current policy \(\[0\] Cisco dCloud - IPS Policy - Production\)](#)

[Set this rule to generate events in the current policy \(\[0\] Cisco dCloud - IPS Policy - Production\)](#)

[Disable this rule in all locally created policies in the current domain](#)

[Set this rule to generate events in all locally created policies in the current domain](#)

[Set this rule to drop the triggering packet and generate an event in all locally created inline policies in the current domain](#)

Set Thresholding Options

▶ in the current policy ([0] Cisco dCloud - IPS Policy - Production)

▶ in all locally created policies in the current domain

Set Suppression Options

▶ in the current policy ([0] Cisco dCloud - IPS Policy - Production)

▶ in all locally created policies in the current domain

Packet Information

FRAME 1 (Expand All)

- ▶ Frame 1: 91 bytes on wire (91 bytes captured (728 bits))
- ▶ Ethernet II (Src: 00:14:2A:93:8D:62, Dst: 00:50:5A:FA:CE:01)
- ▶ Internet Protocol Version 4 (Src: 172.91.41.1, Dst: 192.89.41.133)
- ▶ User Datagram Protocol (Src Port: 34809 (34809), Dst Port: 161 (161))
- ▶ Simple Network Management Protocol
- ▶ Packet Text
- ▼ Packet Bytes

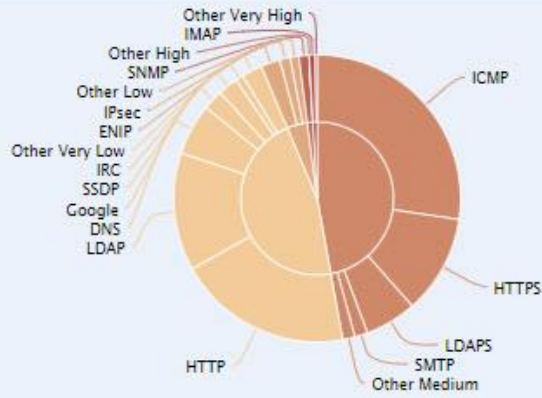
```
0000  00 50 5a fa ce 01 00 14 2a 93 8d 62 08 00 45 00  .PZ.....*..b..E.
0010  00 4d 64 42 40 00 40 11 17 23 ac 5b 29 01 c0 59  .MdB@.@.#.[]..Y
0020  29 85 87 f9 00 a1 00 39 39 11 30 2f 02 01 00 04  )......99.0/....
0030  06 70 75 62 6c 69 63 a1 22 02 04 64 43 2f bf 02  .public."..dC/..
0040  01 00 02 01 00 30 14 30 12 06 0e 2b 06 01 04 01  ....0.0...+....
0050  8f 47 01 01 02 09 02 01 02 05 00                .G.....
```

Visibility Provides Context

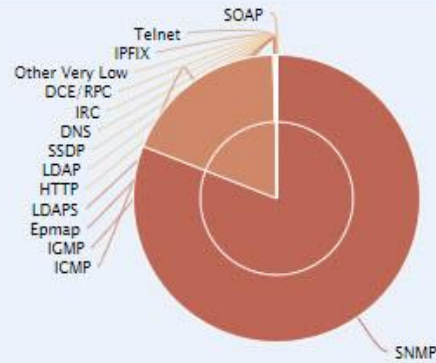
Application Protocol Information

Application Protocol | Client Application | Web Application

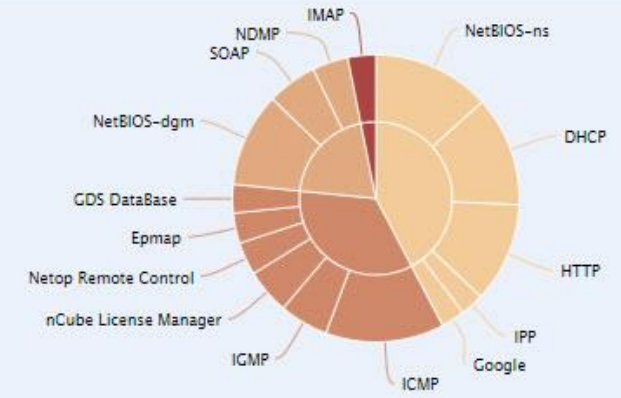
Traffic by Risk and Application



Intrusion Events by Risk and Application



Hosts by Risk and Application



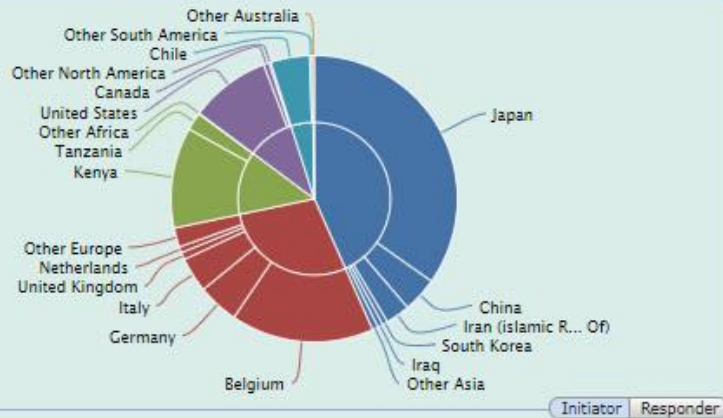
Application Details

Application	Risk	Business Relevance	Category	Hosts
SOAP	Low	Medium	web services provider	61
IGMP	Medium	Medium	network protocols/services	60
nCube License Manager	Medium	Medium	network protocols/services	55
NDMP	Low	High	network protocols/services	44
Netop Remote Control	Medium	Medium	network protocols/services	40
Epmap	Medium	Medium	network protocols/services	37
GDS DataBase	Medium	Medium	network protocols/services	35
IMAP	Very High	Medium	email	34
Google	Very Low	Medium	search engine, web services provider	29

Visibility Provides Context

Geolocation Information

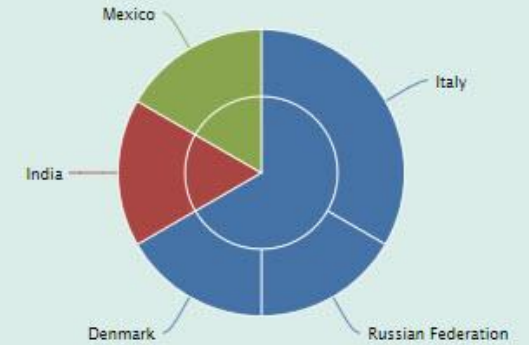
Connections by Initiator Country



Intrusion Events by Source Country

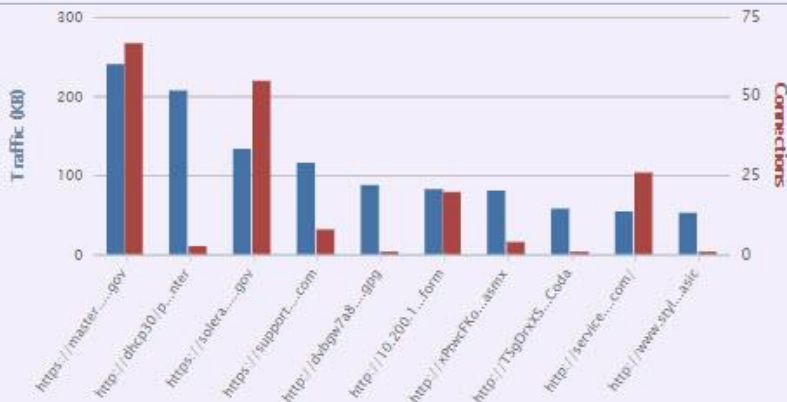


File Events by Sending Country

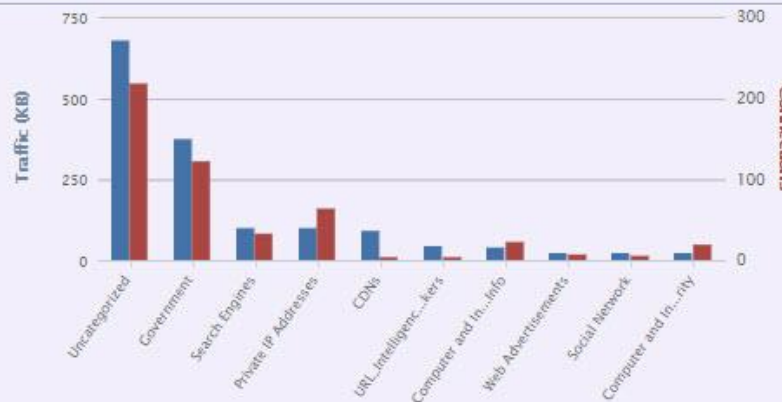


URL Information

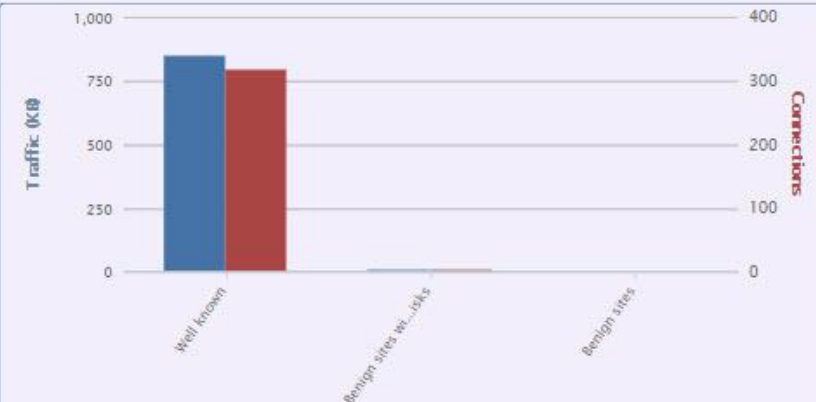
Traffic by URL



Traffic by URL Category



Traffic by URL Reputation



Customizable Monitoring and Reporting

Overview Analysis Policies Devices Objects System Help Global \ demo_user_32

Dashboards Reporting Summary

Summary Dashboard Provides a summary of activity on the appliance

Network Threats Intrusion Events Status Geolocation QoS

Show the Last 1 hour

Add Widgets Report Designer

Unique Applications over Time

Last updated 1 minute ago

Traffic by Application Risk

Risk	Total Bytes (KB)
Medium	12,824.79
Very Low	10,207.78
Low	1,115.68
High	301.83
Very High	130.04

Last updated 2 minutes ago

Traffic by Business Relevance

Business Relevance	Total Bytes (KB)
Medium	17,251.71
High	4,801.26
Very High	2,262.17
Very Low	188.83
Low	76.15

Last updated 1 minute ago

Top Web Applications Seen

Application	Total Bytes (KB)
Google	325.66
ENIP	226.22
IPsec	144.12
Sourcefire.com	119.03
CloudFront	90.31
Y8	84.44
SOAP	57.99
CNN.com	45.68
DCE/RPC	45.25
Pinterest	29.82
DoubleClick	27.38
IGMP	21.84
Yahoo!	17.69
Epmap	17.46
Google Analytics	9.70

Last updated 1 minute ago

Top Server Applications Seen

Application Protocol	Count
DHCP	272
ICMP	252
HTTP	244
IGMP	110
nCube License Manager	108
NDMP	88
Netop Remote Control	79
Epmap	72
GDS DataBase	72
IPP	58

Last updated 2 minutes ago

Top Client Applications Seen

Application	Total Bytes (KB)
Firefox	520.33
Internet Explorer	375.45
SMTP	177.50
Thunderbird	177.50
Chrome	154.35
NetBIOS-ns	97.74
Libwww-Perl	90.31
PS3 web browser	85.23
IMAP	79.24
NetBIOS-dgm	51.87
DCE/RPC	45.25
Mobile Safari	41.87
Pinterest	29.82
Blackberry browser	25.01
Java	21.08

Last updated 1 minute ago

Top Operating Systems Seen

OS Name	Count
Linux	567
Windows	372
Android	254
Chromium	85
Mac OSX	42
iOS	37
ATX	36
FreeBSD	8
Blackberry	2

Last updated 1 minute ago

Closing

Products

<https://www.cisco.com/c/en/us/products/security/firewalls/index.html#~products>

Cisco Firepower® 2100 Series



- Internet edge to small data center environments. Better security, more visibility
- Firewall throughput and sustained performance with threat inspection from 2.0 to 8.5 gigabytes
- Stateful firewall, AVC, NGIPS, AMP, URL filtering

Cisco Firepower 4100 Series



- Internet edge, high-performance enterprise environments
- Firewall throughput and threat inspection from 20 to 60 gigabytes
- Stateful firewall, AVC, NGIPS, AMP, URL filtering, DDoS (Radware vDP)

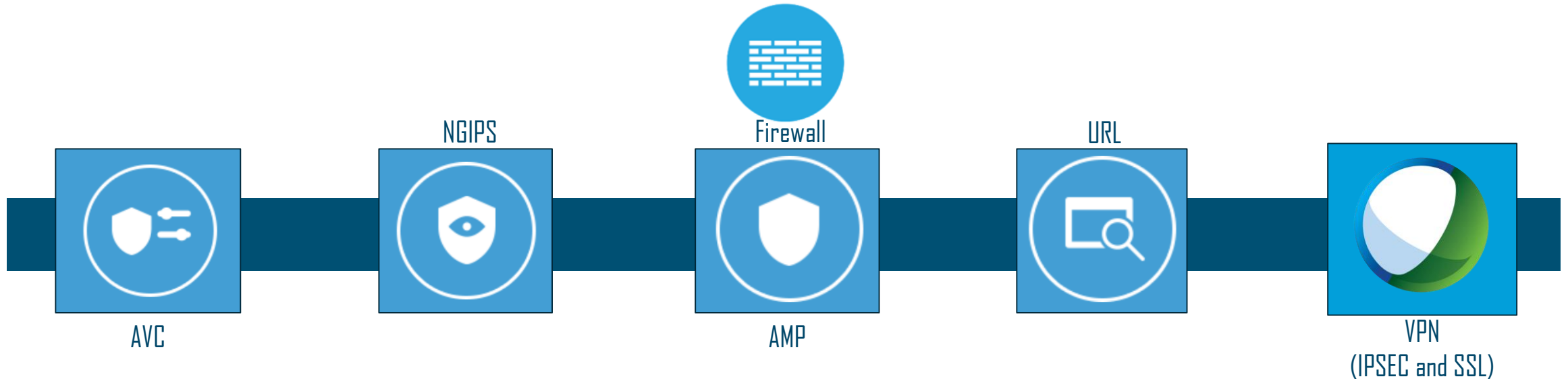
Cisco Firepower 9300 Security Appliance



- Service provider, data center
- Firewall throughput up to 225 gigabytes and threat inspection up to 90 gigabytes
- Firewall, AVC, NGIPS, AMP, URL filtering, DDoS (Radware vDP)

To learn more, visit [Cisco Next-Generation Firewalls](#)

Virtual and Cloud Solutions



vmware®

aws

KVM

Microsoft Azure

Managed by FMC and FDM



