How to Predict, Detect & Stop threats at the Edge and Behind the Perimeter even in encrypted traffic without decryption

Nikos Mourtzinos, CCIE #9763
Cisco Cyber Security Sales Specialist

April 2018

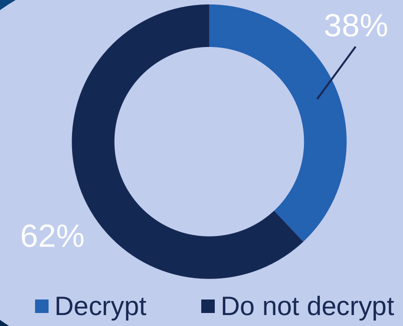
New threat landscape

81% of organizations have been victims of a cyber attack

41% of attackers used encryption to evade detection

64% cannot detect malicious content in encrypted traffic

Organizations are at risk



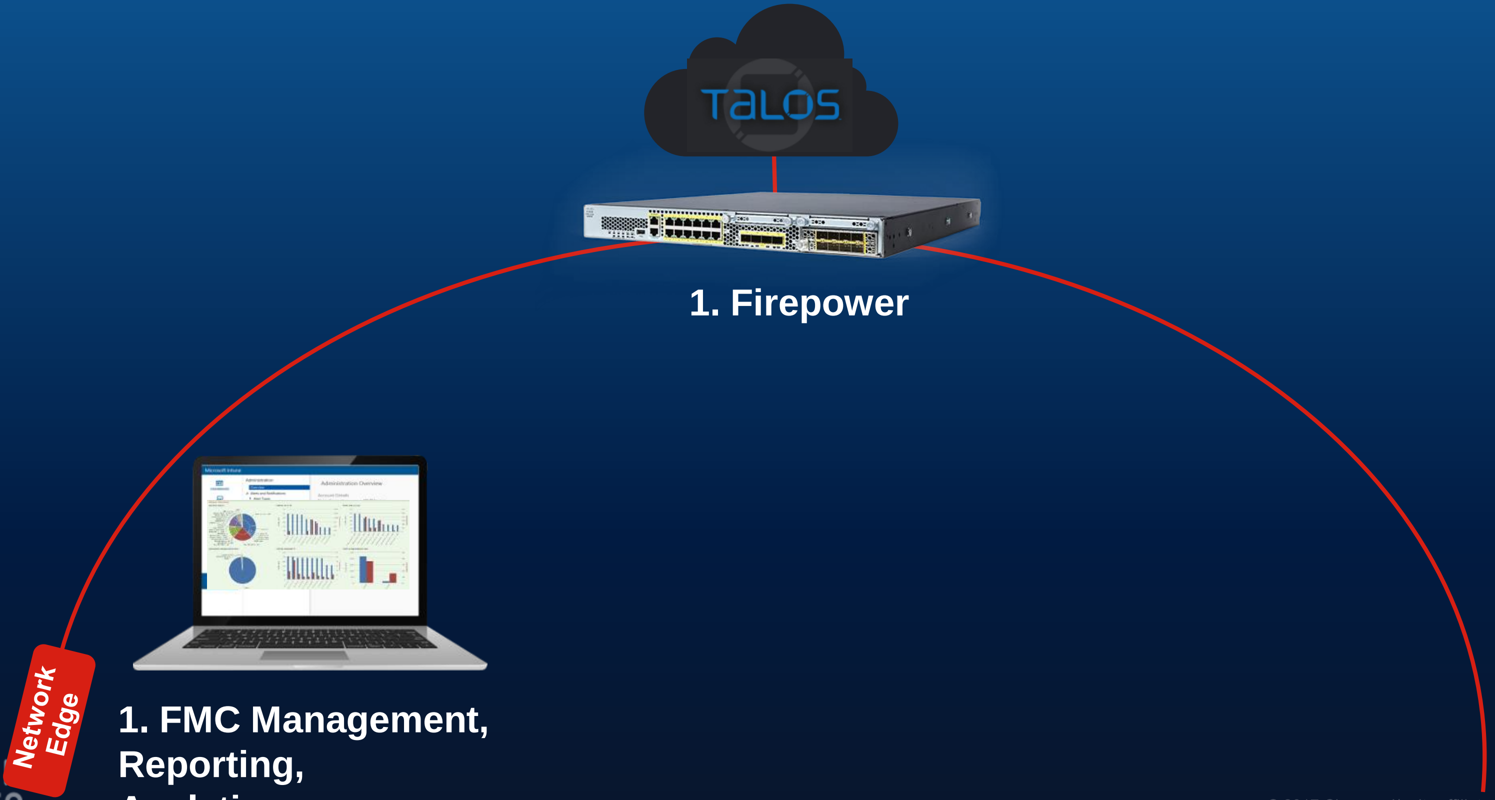
New attack vectors

- Employees browsing over HTTPS: Malware infection, covert channel with command and control server, data exfiltration
- Employees on internal network connecting to DMZ servers: Lateral propagation of encrypted threats

Source: Ponemon Report, 2016

1. Firepower

Security Architecture



1. Firepower

Network Edge

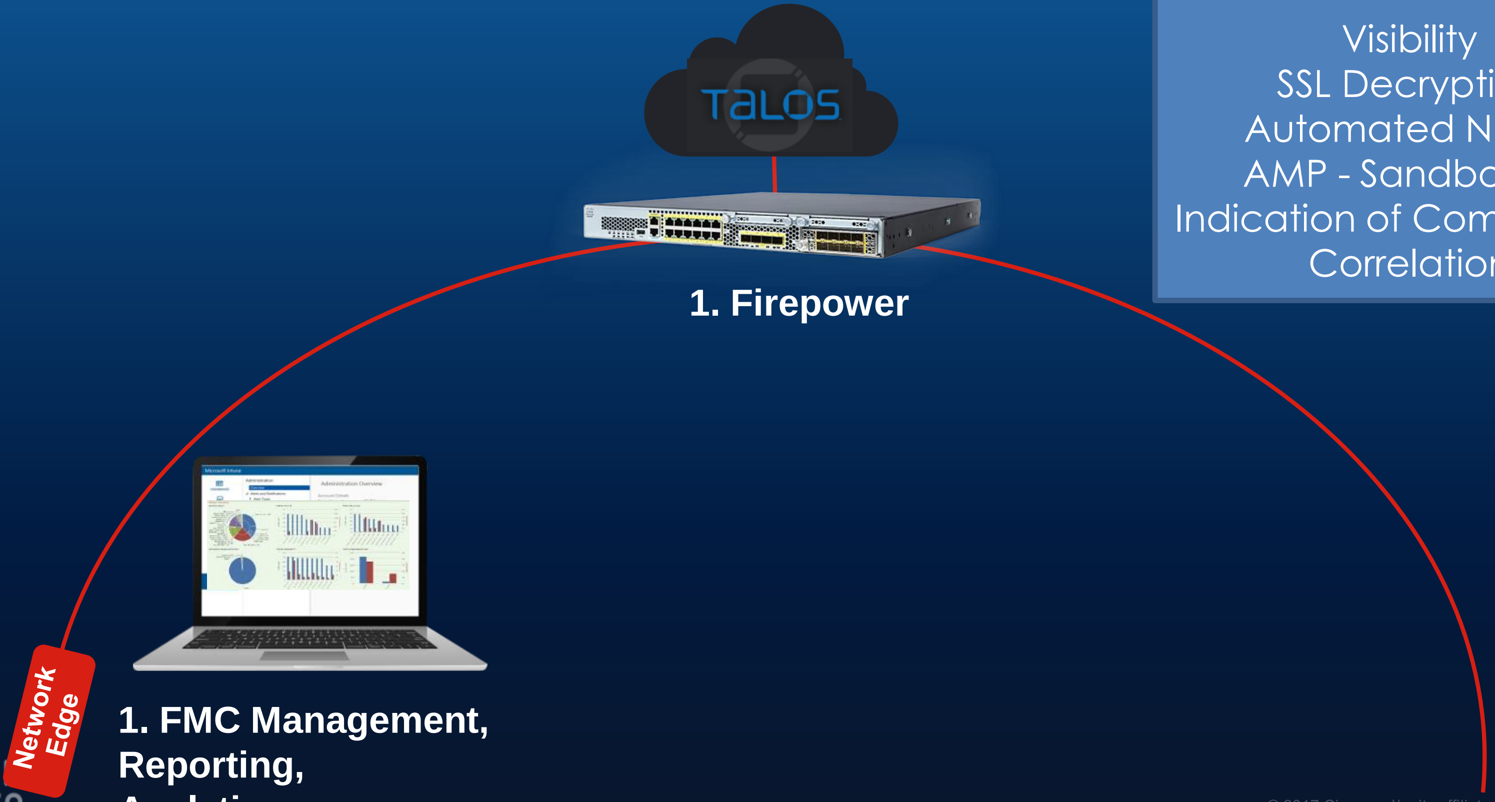
1. FMC Management, Reporting, Analytics

1. Firepower

Security Architecture

Perimeter

Visibility
SSL Decryption
Automated NGIPS
AMP - Sandboxing
Indication of Compromise
Correlation

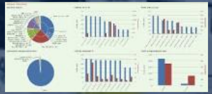


1. Firepower

**1. FMC Management,
Reporting,
Analytics**

IPS configuration

- Security Specialist to know customer environment
- Write down all vulnerabilities
- Select 10.000 IPS signatures out of 50.000+ available
- Configure



- Achieve high security effectiveness to block attacks

September 2017 – Kick off

Mon	Tue	Wed	Thu	Fri	Sat	Sun
28	29	30	31	1 Kick-off	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

September 2017 – Know the environment

Mon	Tue	Wed	Thu	Fri	Sat	Sun
28	29	30	31	1 Kick-off	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

September 2017 – Locate Vulnerabilities

Mon	Tue	Wed	Thu	Fri	Sat	Sun
28	29	30	31	1 Kick-off	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

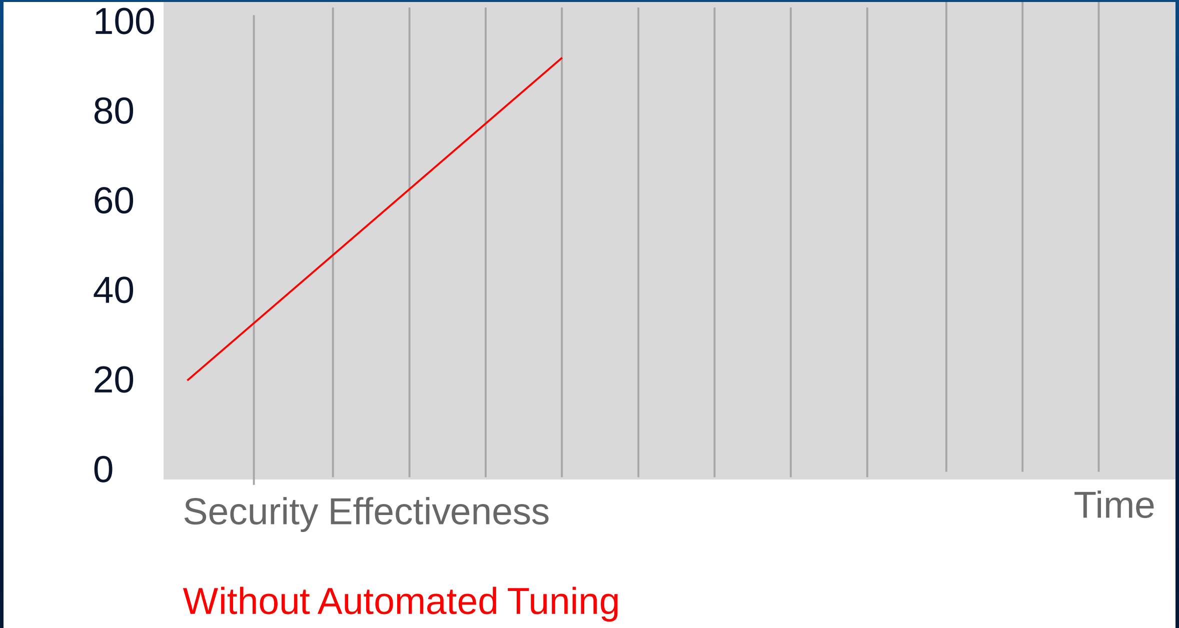
September 2017 – Select Signatures

Mon	Tue	Wed	Thu	Fri	Sat	Sun
28	29	30	31	1 Kick-off	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

September 2017 – Configure Hardware & Software

Mon	Tue	Wed	Thu	Fri	Sat	Sun
28	29	30	31	1 Kick-off	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

IPS Tuning


100
80
60
40
20
0
Security Effectiveness
Time
Without Automated Tuning

Environment Changes !

August						
Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	**5**
6	7	8	9	10	11	**12**
13	14	15	16	17	18	**19**
20	21	22	23	24	25	**26**
27	28	29	30	31		

IPS Tuning is required !!!!

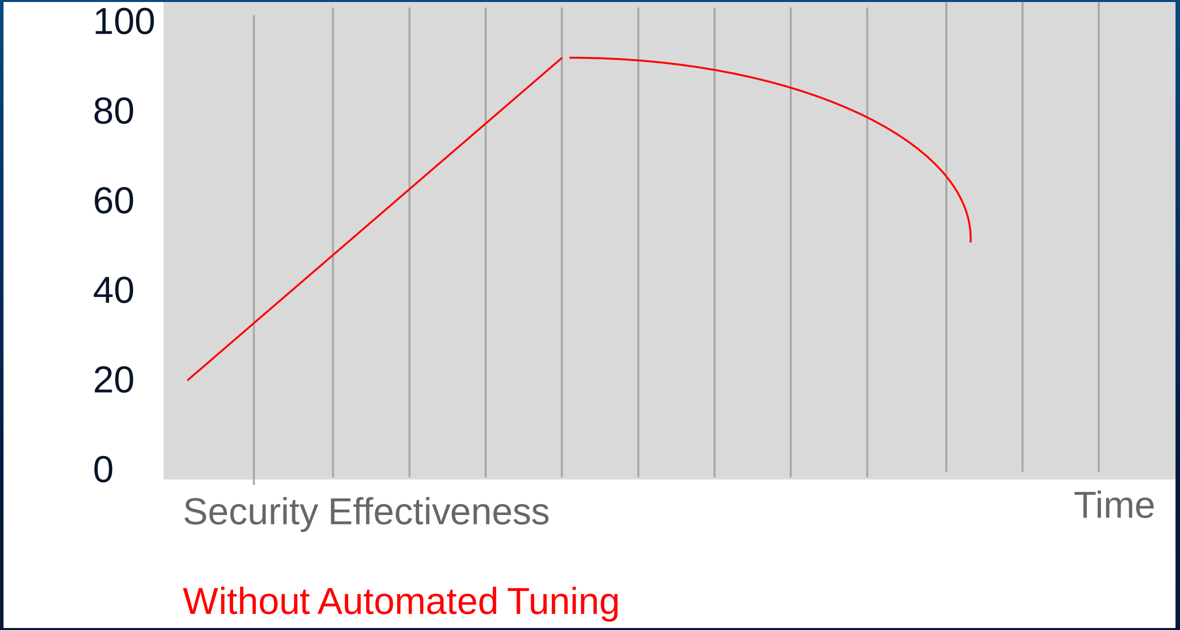
NSS IPS Test Key Findings:
Protection varied widely between **31%** and **99,5%**.

Tuning is required, and is ***most important*** for remote attacks against servers and their applications**.**

Complex Operations & Increases Costs

IPS Tuning

Organizations that do not tune could be missing numerous “catchable” attacks.



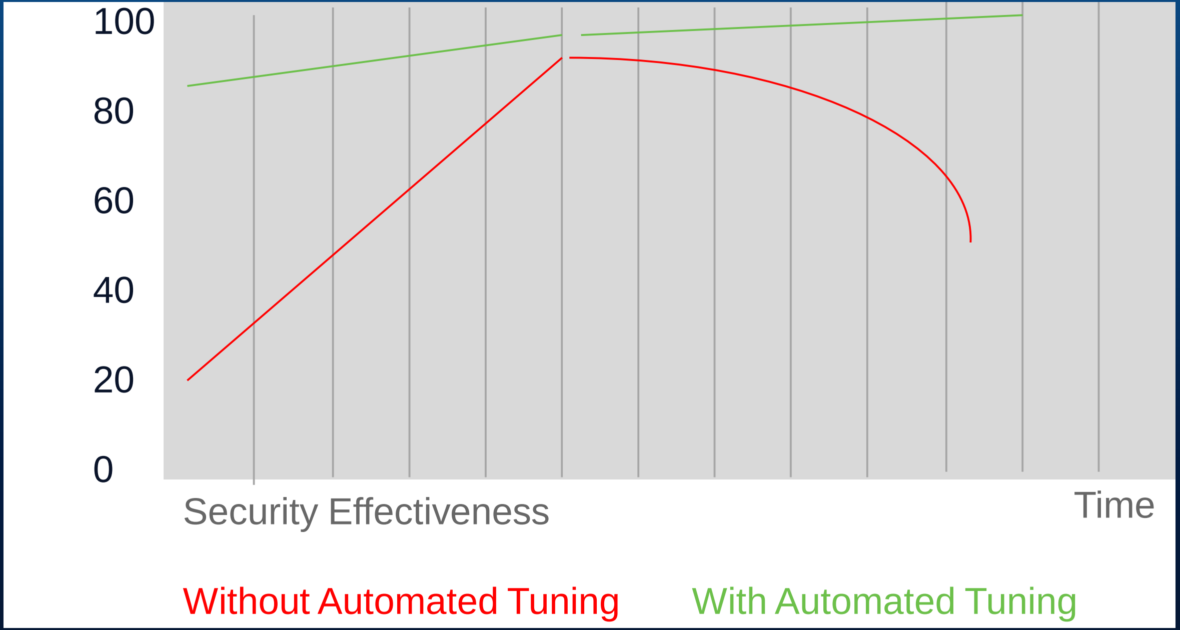
Automated Tuning

Adjust IPS policies automatically based on network changes

Automated NGIPS Tuning

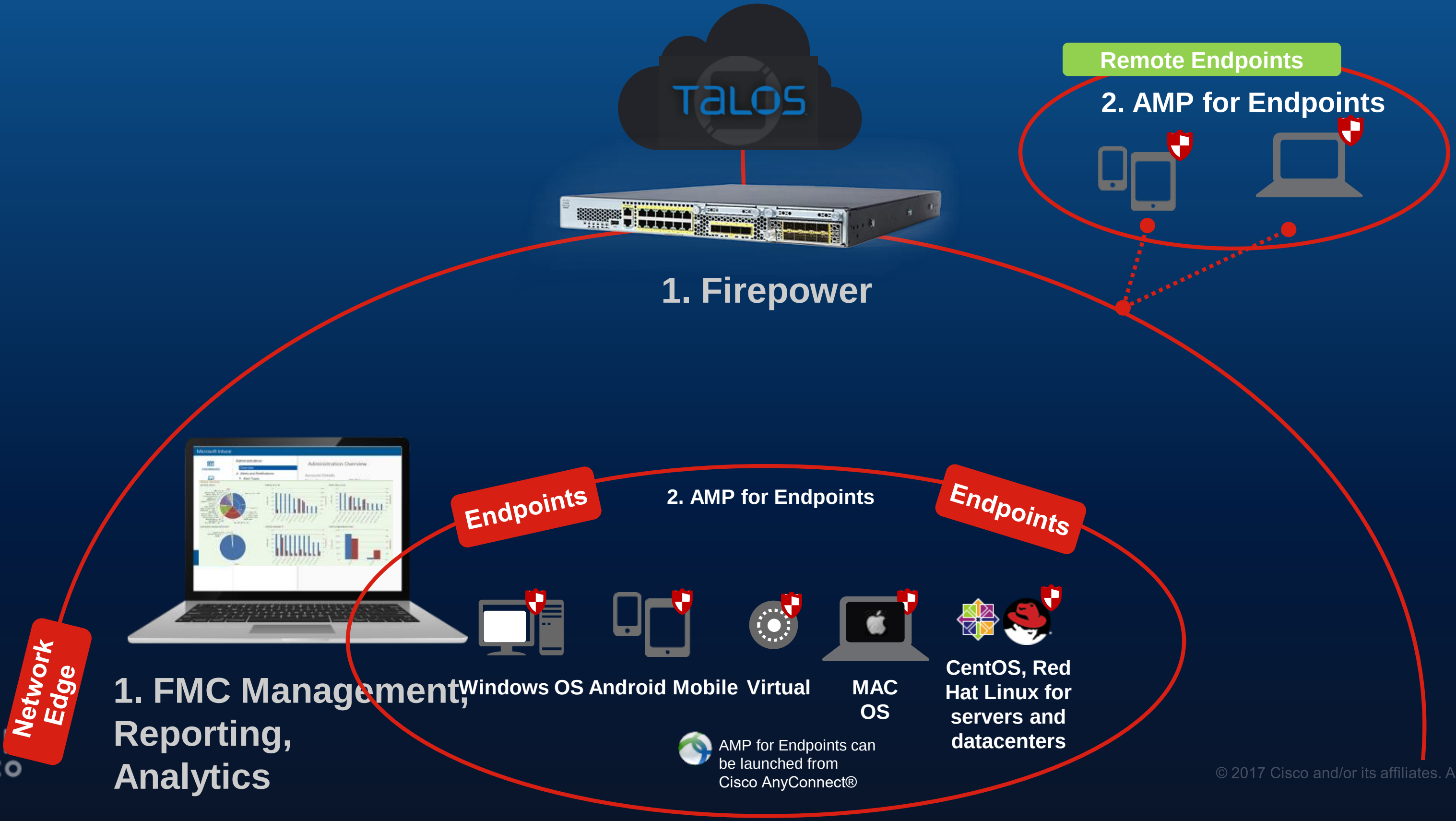
- Automated Recommended Rules based on Organization's Infrastructure
- Automated IPS Policies based on Changes
- Simplifies Operations & Reduces Costs

Automated NGIPS Tuning



Security Architecture

1. Firepower
2. AMP for endpoint



Talos

Remote Endpoints

2. AMP for Endpoints

1. Firepower

Endpoints

2. AMP for Endpoints

Endpoints

Network Edge

1. FMC Management, Reporting, Analytics

Windows OS

Android Mobile

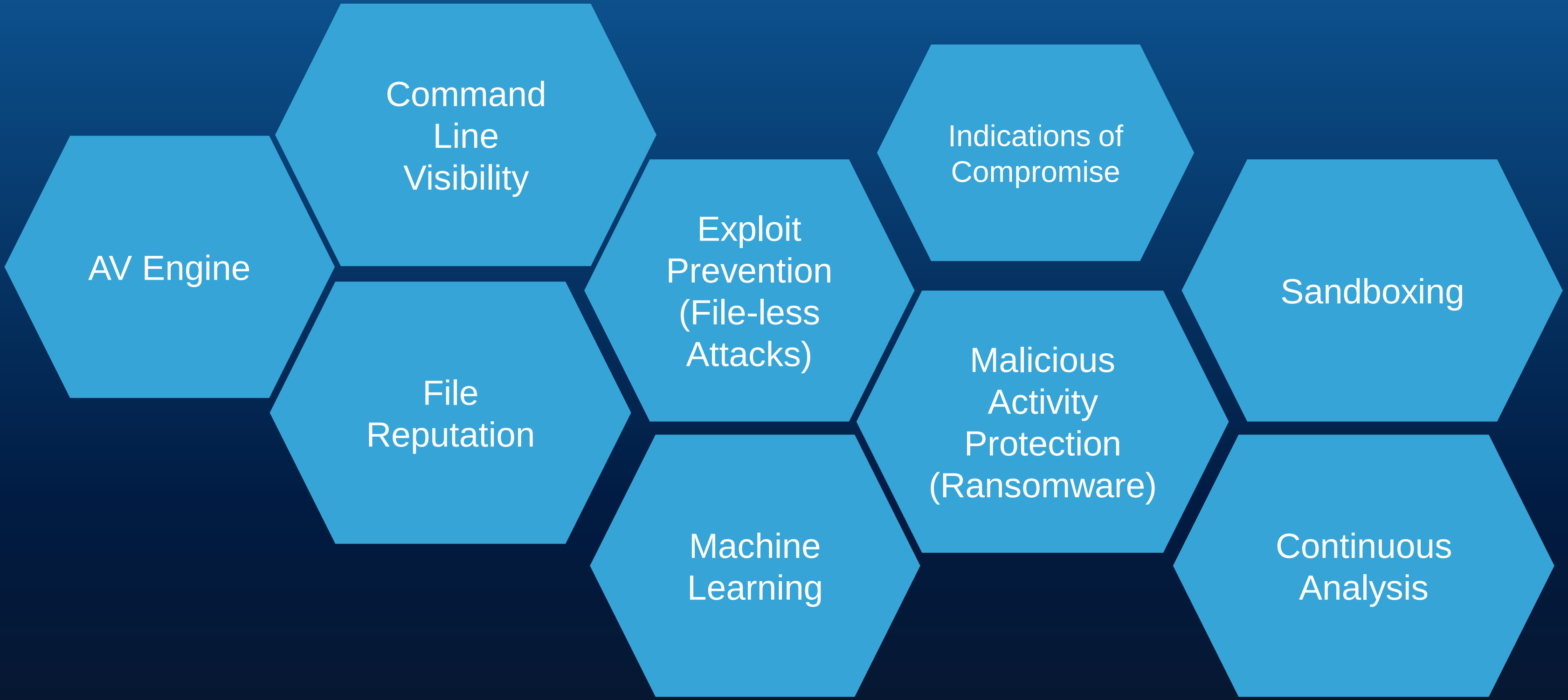
Virtual

MAC OS

CentOS, Red Hat Linux for servers and datacenters

AMP for Endpoints can be launched from Cisco AnyConnect®

What do you get with AMP for Endpoints ?



AV Engine

Command Line Visibility

File Reputation

Exploit Prevention (File-less Attacks)

Machine Learning

Indications of Compromise

Malicious Activity Protection (Ransomware)

Sandboxing

Continuous Analysis

What do you get with AMP for Endpoints ?

Command Line Visibility

AV Engine

File Reputation

Exploit Prevention (File-less Attacks)

Machine Learning

Indications of Compromise

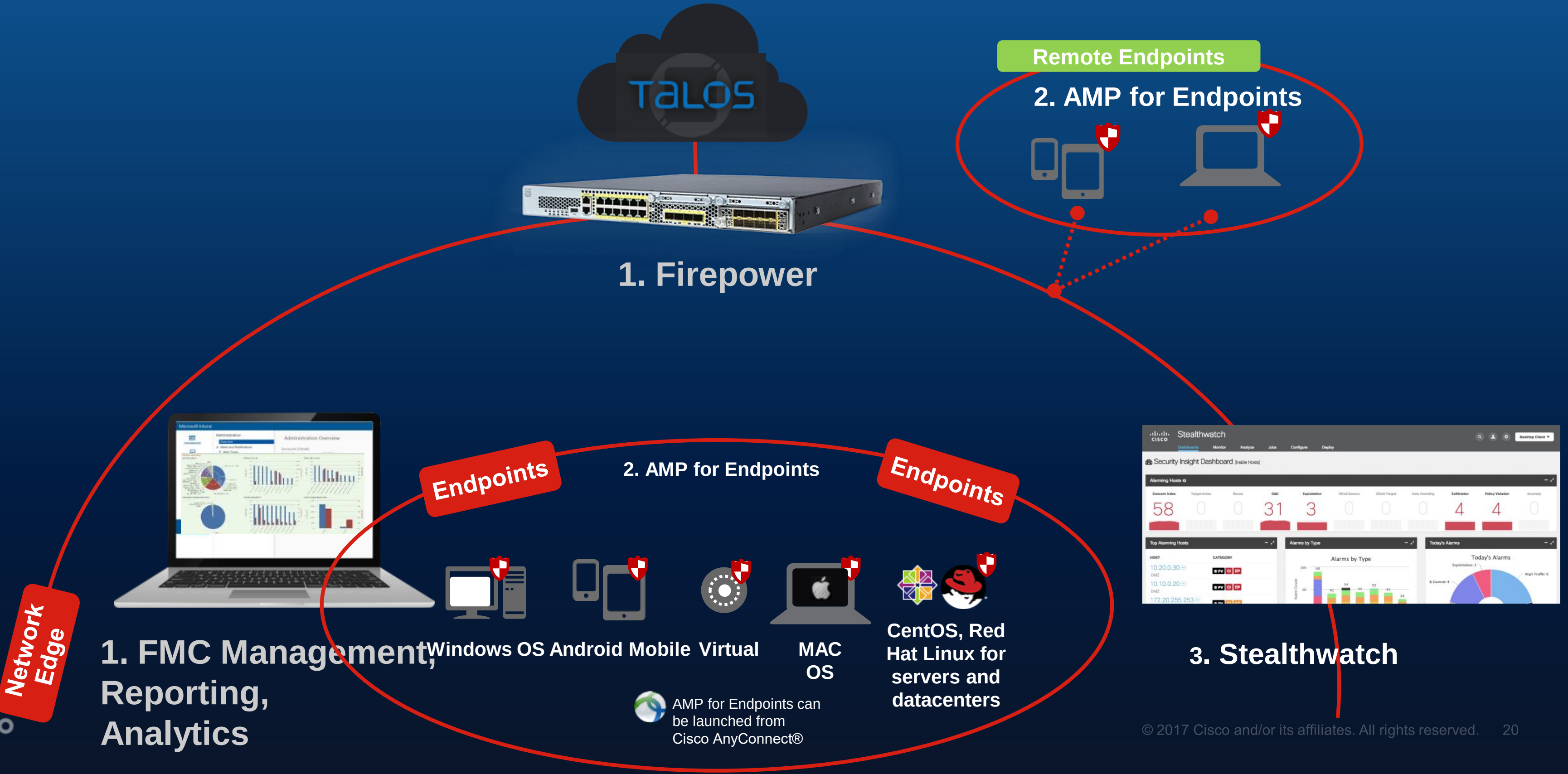
Malicious Activity Protection (Ransomware)

Sandboxing

Continuous Analysis

Security Architecture

1. Firepower
2. AMP for endpoint
3. Stealthwatch



Remote Endpoints

2. AMP for Endpoints

1. Firepower

Endpoints

2. AMP for Endpoints

Endpoints

Network Edge

1. FMC Management, Reporting, Analytics

Windows OS

Android Mobile

Virtual

MAC OS

CentOS, Red Hat Linux for servers and datacenters

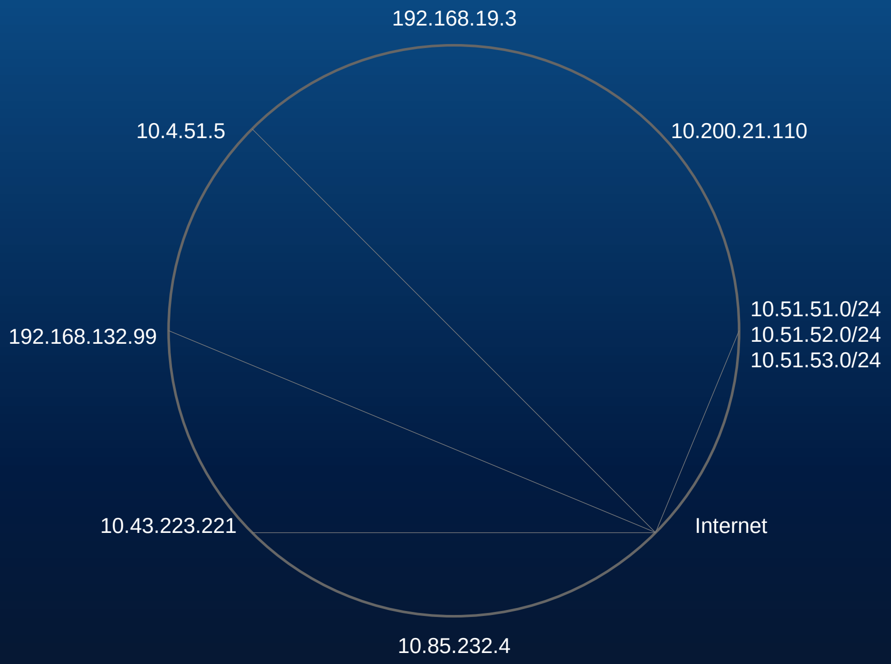
AMP for Endpoints can be launched from Cisco AnyConnect®

3. Stealthwatch

Organization with Only Perimeter Visibility

Visibility available for traffic transiting through perimeter

Many devices in your network without visibility

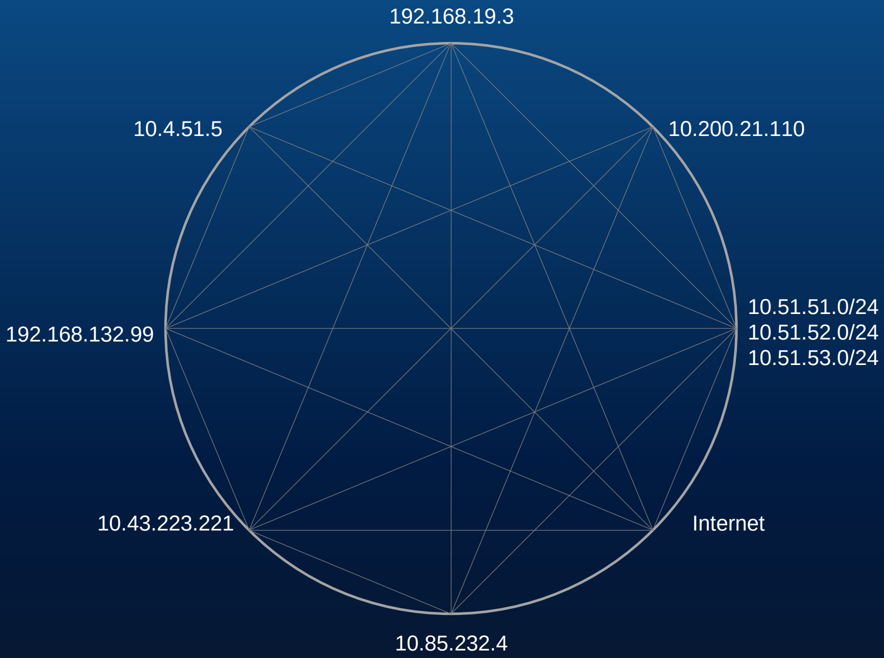


Enabling Visibility Inside Your Organization

KNOW
every host

RECORD
every conversation

EVERYTHING
on the network

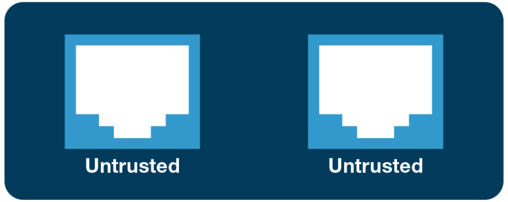


Forrester’s Zero Trust Framework

Zero trust operates under the principle of “never trust, always verify,” which means that trust is never assumed for any device or user on the system.

In Zero Trust, All Interfaces Are Untrusted

No More Chewy Centers: The Zero Trust Model Of Information Security

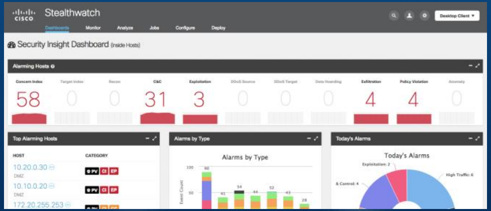


56682

Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

Next Generation Cyber Threat Defense

Cisco StealthWatch



Security Insight Dashboard (Inside Hosts)

Alarming Hosts

Concern Index	Target Index	Recon	C&C	Exploitation	DDoS Source	DDoS Target	Data Hoarding	Exfiltration	Policy Violation	Anomaly
58	0	0	31	3	0	0	0	4	4	0

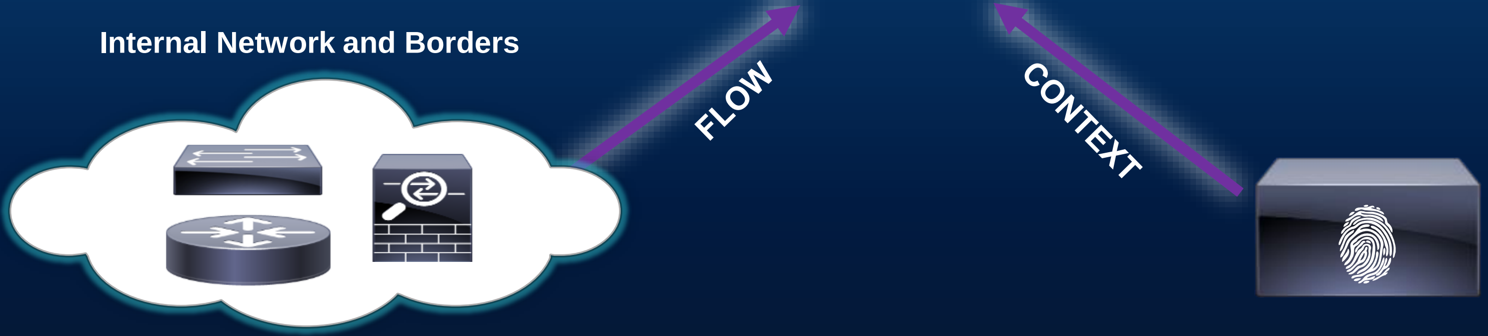
Top Alarming Hosts

HOST	CATEGORY
10.20.0.30 DMZ	PV CI EP
10.10.0.20 DMZ	PV CI EP
172.20.255.253	

Alarms by Type

Today's Alarms

- Aggregating, analyzing NetFlow
- Network Behavior - Baseline
- Anomaly Detection Algorithms
- Insider Threats



Internal Network and Borders

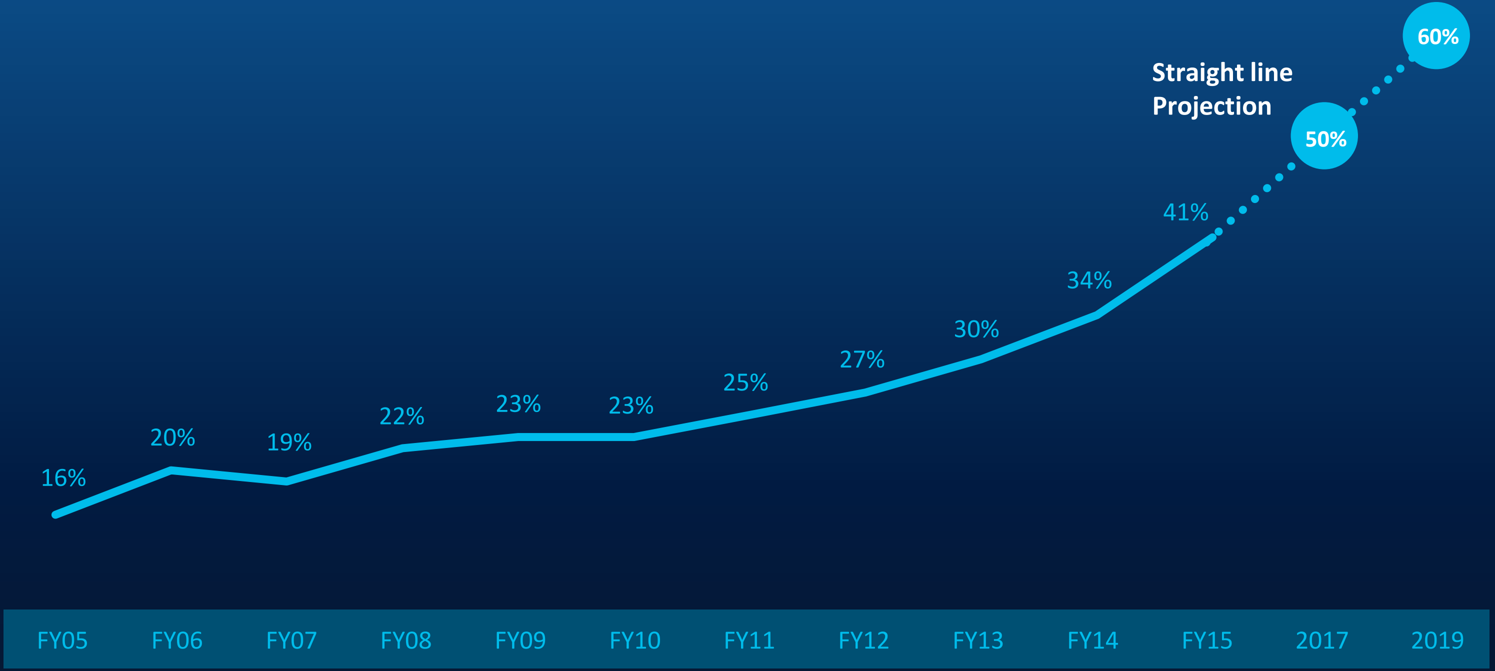
NetFlow Telemetry

Switches, Routers, and Firewalls

Cisco Identity Services Engine

Identity, Device, Posture

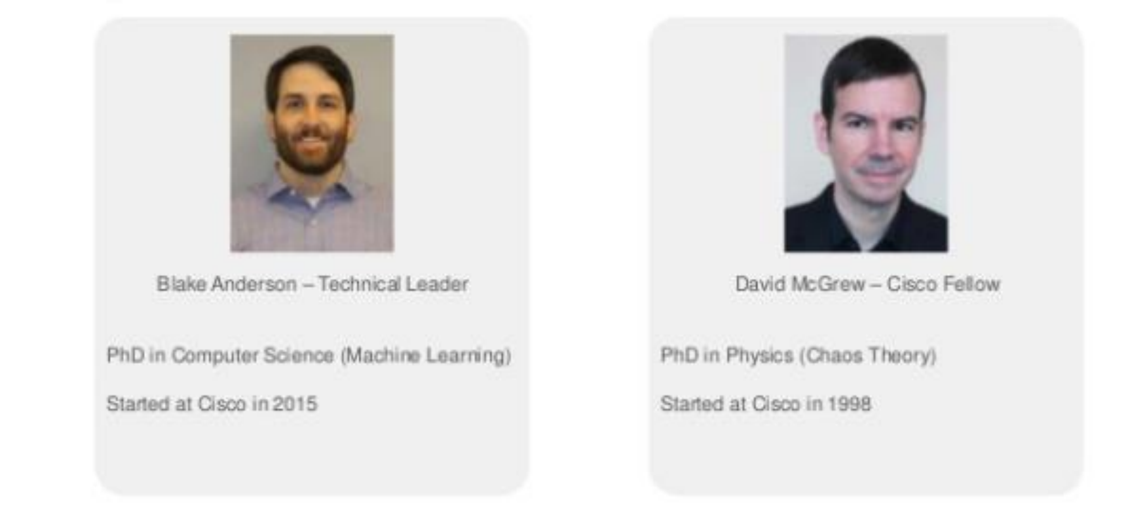
Encryption Is Changing The Threat Landscape



Source: Thales and Vormetric

▬ Extensive deployment of encryption

Encrypted Traffic Analytics
Published research– 18 patents filed



Blake Anderson – Technical Leader

PhD in Computer Science (Machine Learning)

Started at Cisco in 2015

David McGrew – Cisco Fellow

PhD in Physics (Chaos Theory)

Started at Cisco in 1998

"Identifying Encrypted Malware Traffic with Contextual Flow Data"

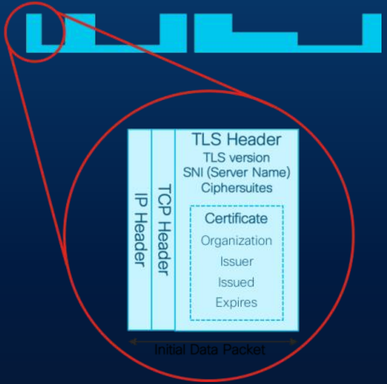
AISec '16 | Blake Anderson, David McGrew (Cisco Fellow)

Industry’s first solution with ability to find threats in encrypted traffic without decryption

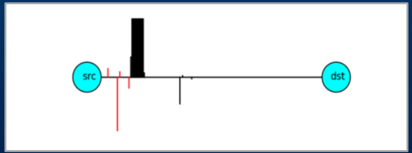
Initial Data Packet

Sequence of Packet Lengths and Times

Threat Intelligence Map



Initial Data Packet



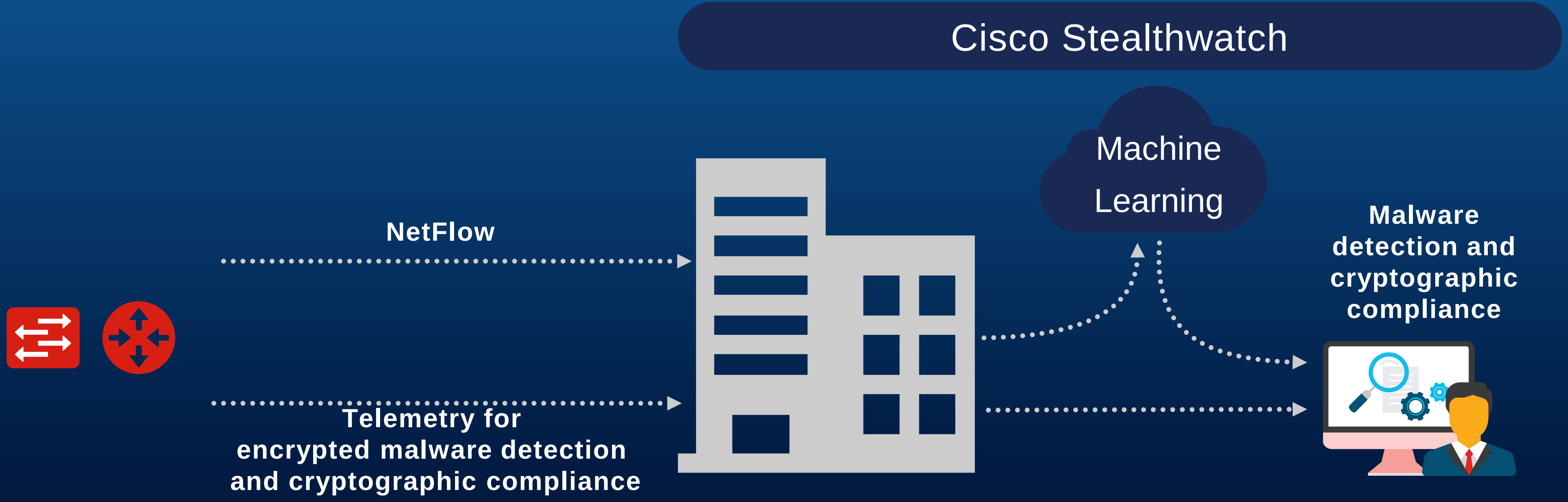
C2 message

Data exfiltration

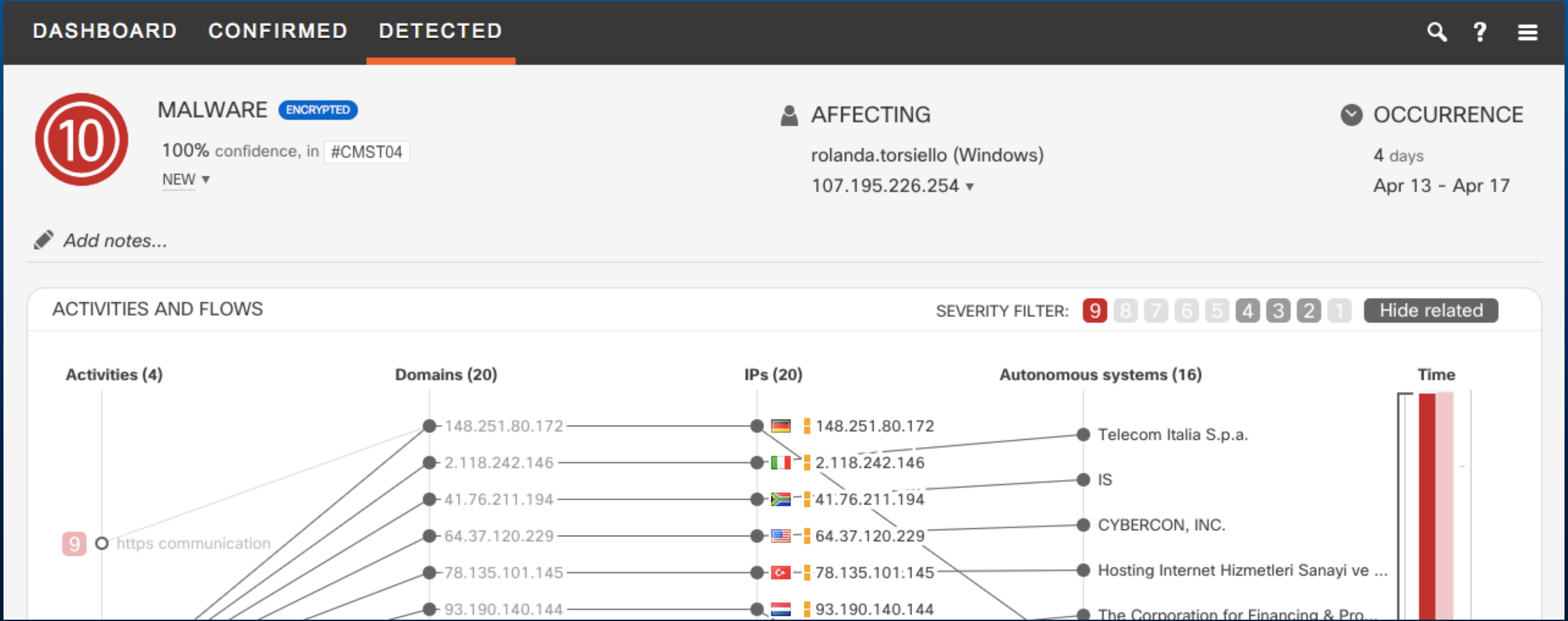
Self-Signed certificate

Broad behavioral information about the servers on the Internet.

Malware in Encrypted Traffic


Cisco Stealthwatch
Machine Learning
NetFlow
Telemetry for encrypted malware detection and cryptographic compliance
Malware detection and cryptographic compliance

Malware in Encrypted Traffic



10

MALWARE ENCRYPTED

100% confidence, in #CMST04

NEW ▾

AFFECTING

rolanda.torsiello (Windows)
107.195.226.254 ▾

OCCURRENCE

4 days
Apr 13 - Apr 17

Add notes...

ACTIVITIES AND FLOWS

SEVERITY FILTER: 9 8 7 6 5 4 3 2 1

Activities (4)

9 https communication

Domains (20)

148.251.80.172
2.118.242.146
41.76.211.194
64.37.120.229
78.135.101.145
93.190.140.144

IPs (20)

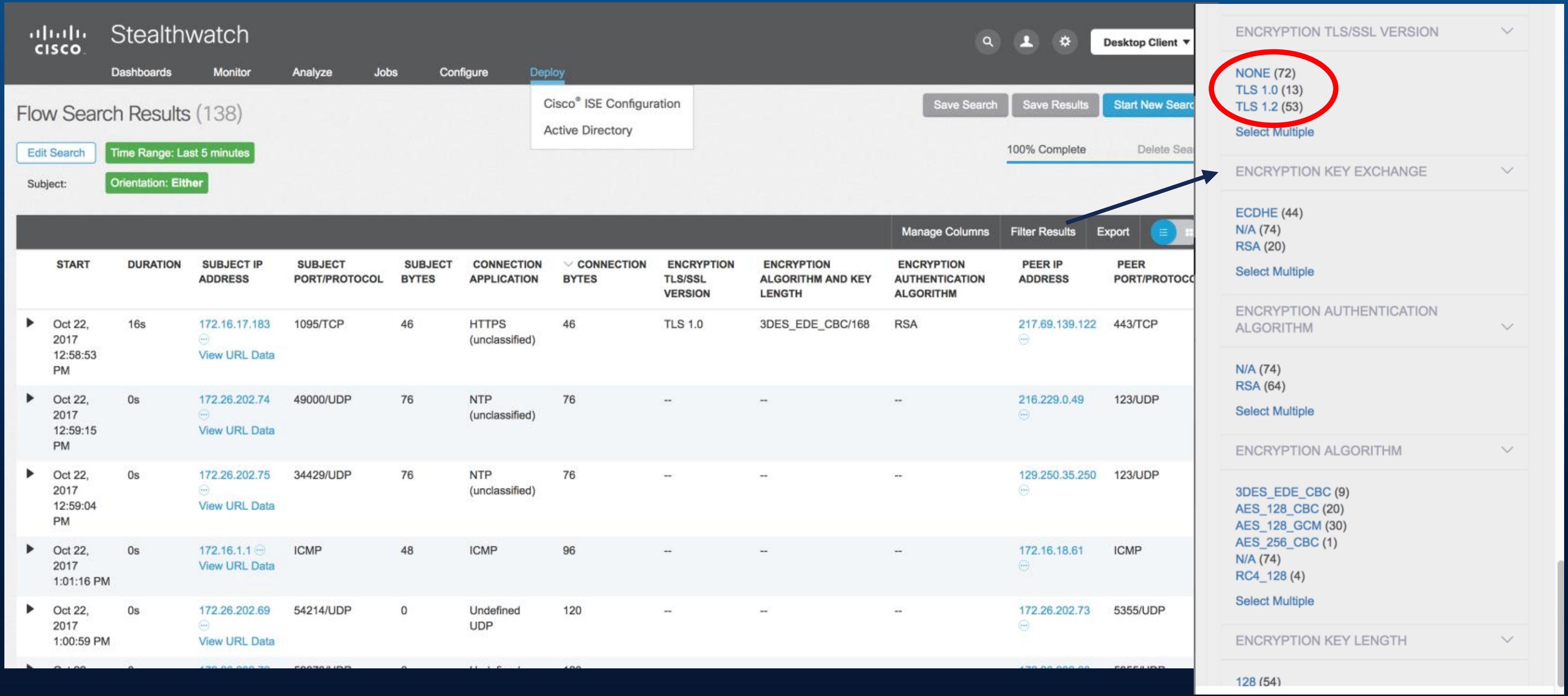
148.251.80.172
2.118.242.146
41.76.211.194
64.37.120.229
78.135.101:145
93.190.140.144

Autonomous systems (16)

Telecom Italia S.p.a.
IS
CYBERCON, INC.
Hosting Internet Hizmetleri Sanayi ve ...
The Corporation for Financing & Pro...

Time

Cryptographic Compliance
Flow search results



Flow Search Results (138)

Edit Search | Time Range: Last 5 minutes

Subject: Orientation: Either

START	DURATION	SUBJECT IP ADDRESS	SUBJECT PORT/PROTOCOL	SUBJECT BYTES	CONNECTION APPLICATION	CONNECTION BYTES	ENCRYPTION TLS/SSL VERSION	ENCRYPTION ALGORITHM AND KEY LENGTH	ENCRYPTION AUTHENTICATION ALGORITHM	PEER IP ADDRESS	PEER PORT/PROTOCO
Oct 22, 2017 12:58:53 PM	16s	172.16.17.183 View URL Data	1095/TCP	46	HTTPS (unclassified)	46	TLS 1.0	3DES_EDE_CBC/168	RSA	217.69.139.122	443/TCP
Oct 22, 2017 12:59:15 PM	0s	172.26.202.74 View URL Data	49000/UDP	76	NTP (unclassified)	76	--	--	--	216.229.0.49	123/UDP
Oct 22, 2017 12:59:04 PM	0s	172.26.202.75 View URL Data	34429/UDP	76	NTP (unclassified)	76	--	--	--	129.250.35.250	123/UDP
Oct 22, 2017 1:01:16 PM	0s	172.16.1.1 View URL Data	ICMP	48	ICMP	96	--	--	--	172.16.18.61	ICMP
Oct 22, 2017 1:00:59 PM	0s	172.26.202.69 View URL Data	54214/UDP	0	Undefined UDP	120	--	--	--	172.26.202.73	5355/UDP

ENCRYPTION TLS/SSL VERSION

- NONE (72)
- TLS 1.0 (13)
- TLS 1.2 (53)
- Select Multiple

ENCRYPTION KEY EXCHANGE

- ECDHE (44)
- N/A (74)
- RSA (20)
- Select Multiple

ENCRYPTION AUTHENTICATION ALGORITHM

- N/A (74)
- RSA (64)
- Select Multiple

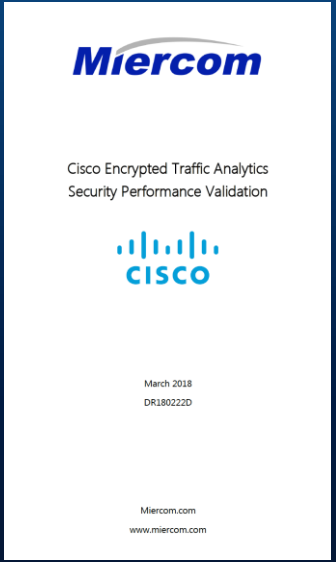
ENCRYPTION ALGORITHM

- 3DES_EDE_CBC (9)
- AES_128_CBC (20)
- AES_128_GCM (30)
- AES_256_CBC (1)
- N/A (74)
- RC4_128 (4)
- Select Multiple

ENCRYPTION KEY LENGTH

- 128 (54)

Encrypted Traffic Analytics receives “Miercom Performance Verified” Certification



Cisco Encrypted Traffic Analytics
Security Performance Validation

March 2018
DR180222D

Miercom.com
www.miercom.com

Key Conclusions

36% higher rate detection finding 100% of threats

https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/miercom-report-eta-perf.pdf

Security Architecture

1. Firepower
2. AMP for endpoint
3. Stealthwatch

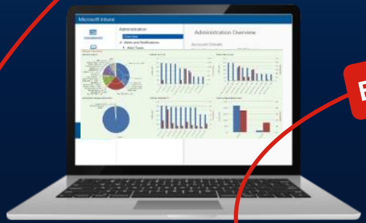
1. Firepower

Re

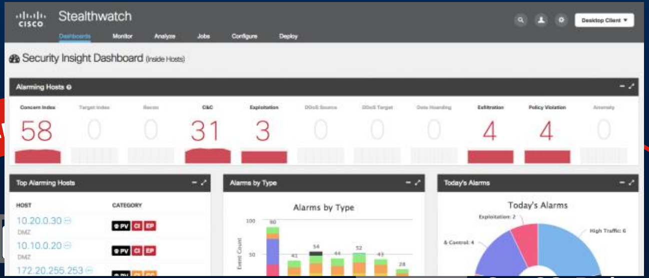
2.

Perimeter

Visibility
Automated NGIPS
AMP - Sandboxing
Indication of Compromise
Correlation



Er



Security Insight Dashboard (Inside Hosts)

Alarming Hosts

Concern Index	Target Index	Recon	C&C	Exploitation	DDoS Source	DDoS Target	Data Hoarding	Exfiltration	Policy Violation	Anomaly
58	0	0	31	3	0	0	0	4	4	0

Top Alarming Hosts

HOST	CATEGORY
10.20.0.30 DMZ	PV CI EP
10.10.0.20 DMZ	PV CI EP
172.20.255.253	[illegible]

Network Edge

1. FMC Management, Reporting, Analytics

Windows OS Android Mobile Virtual

MAC OS

CentOS, Red Hat Linux for servers and datacenters

AMP for Endpoints can be launched from Cisco AnyConnect®

Inside the Organization

Know every host

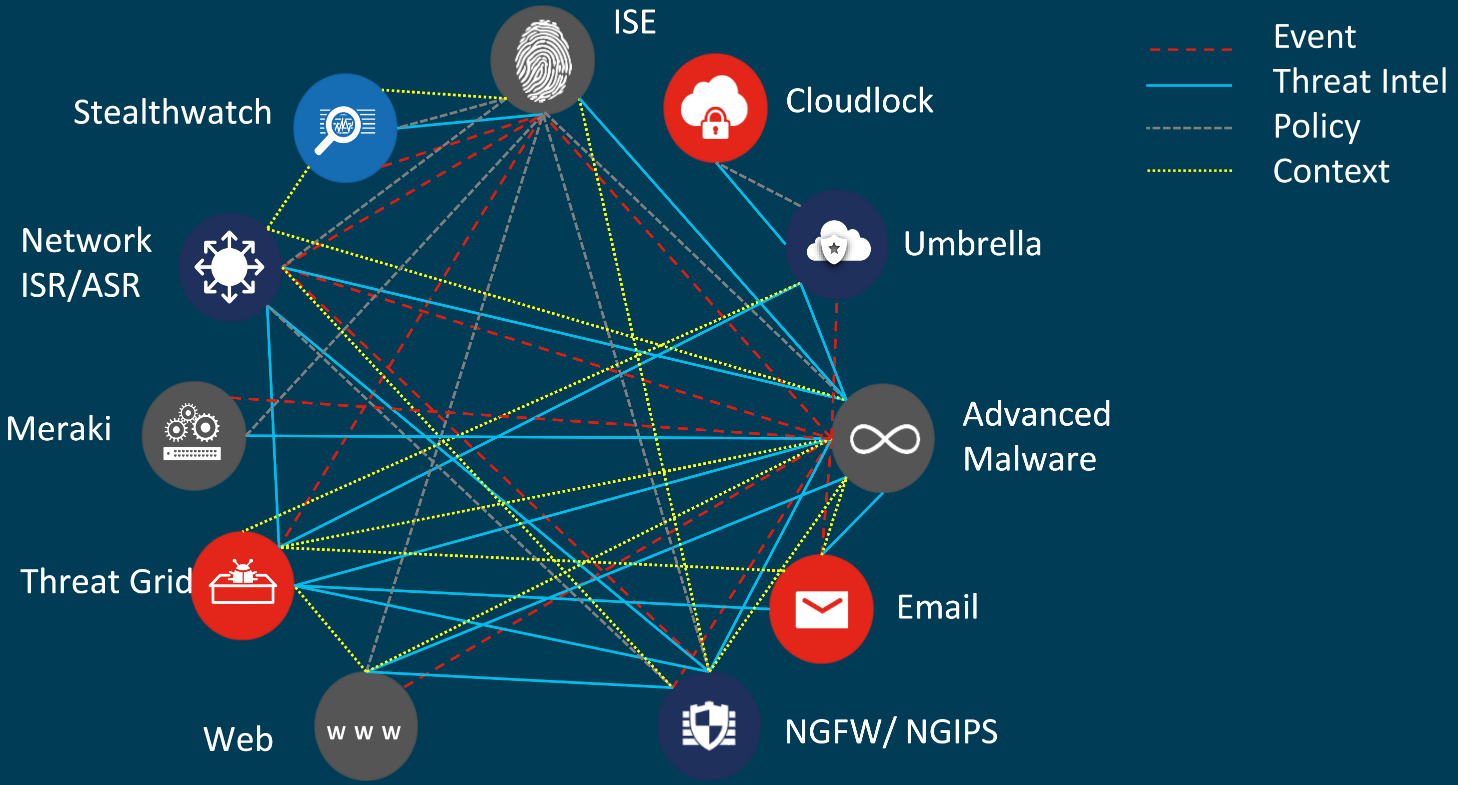
Record every conversation

Everything on the network

Cisco Integrated Security Portfolio

- It’s our #1 differentiator
- It solves a vital customer problem: complexity

Cisco's Integrated Security Portfolio works in concert to prevent breaches, automate response, and detect and stop threats fast



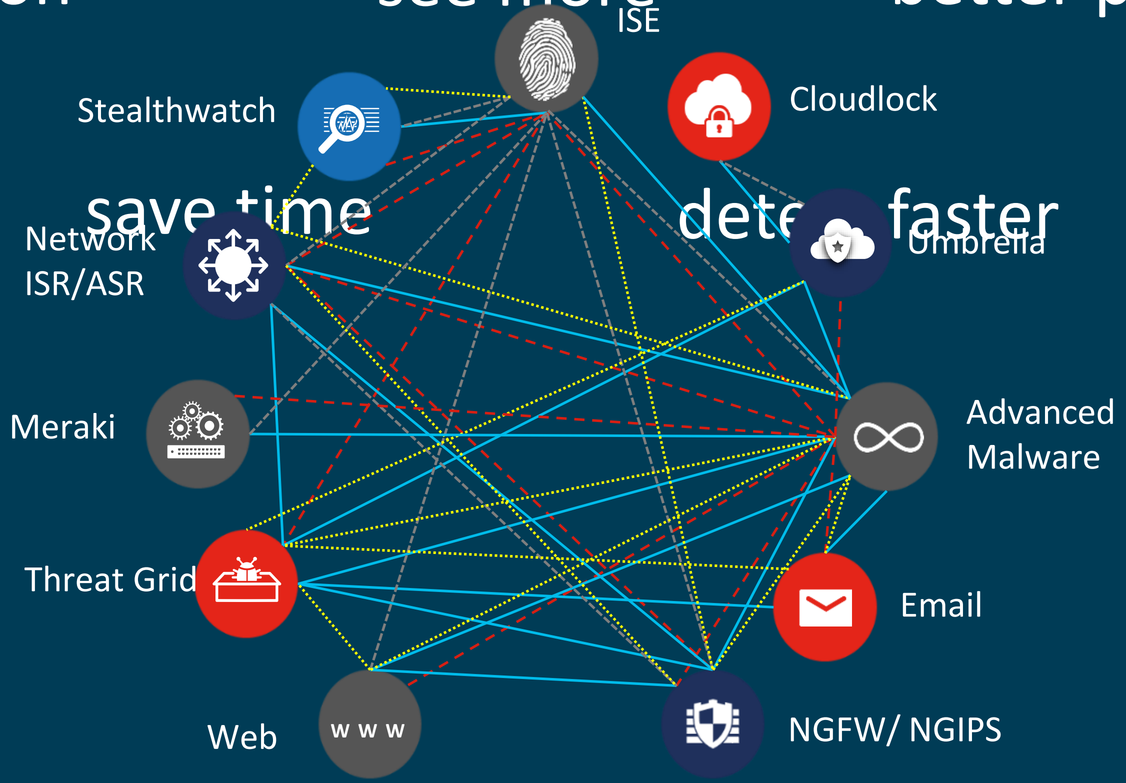
automation

see more

better protection

save time

dete faster



Ecosystem and Integration

Vulnerability Management

- Outpost24
- RAPID7
- SAINT
- tenable network security
- QUALYS
- Greenbone
- Network Critical
- POSITIVE TECHNOLOGIES
- tripwire

Packet Brokering

- GARLAND
- Interface Masters Technologies Innovative Network Solutions
- A10
- IXIA
- VSS monitoring
- Gigamon

IAM/SSO

- SECUREAUTH
- NetIQ
- Ping Identity

Network Infrastructure & Policy Management

- HYTRUST Cloud Under Control
- embrane
- VCE The Virtual Computing Environment Company
- tufin Making Security Manageable
- Symantec
- algosec
- FIREMON
- skybox security
- CITRIX
- UBIqube
- f5

Performance Management & Visualization

- LiveAction Simplifying the Network
- hyperglance

Custom Detection

- radware
- SOPHOS
- P1 Security Priority One Security
- skyhigh
- elastica
- ARBOR NETWORKS

Mobility

- airwatch by vmware
- SOTI
- MobileIron
- Tangoe
- JAMF software
- SAP
- ABSOLUTE
- Good
- MaaS360 by Fiberlink

Firewall/Access Control

- IMPERVA
- Infoblox
- BAYSHORE
- Check Point Software Technologies Ltd.

Packet Capture & Forensics

- NETSCOUT
- endace
- NEXT COMPUTING
- savvius

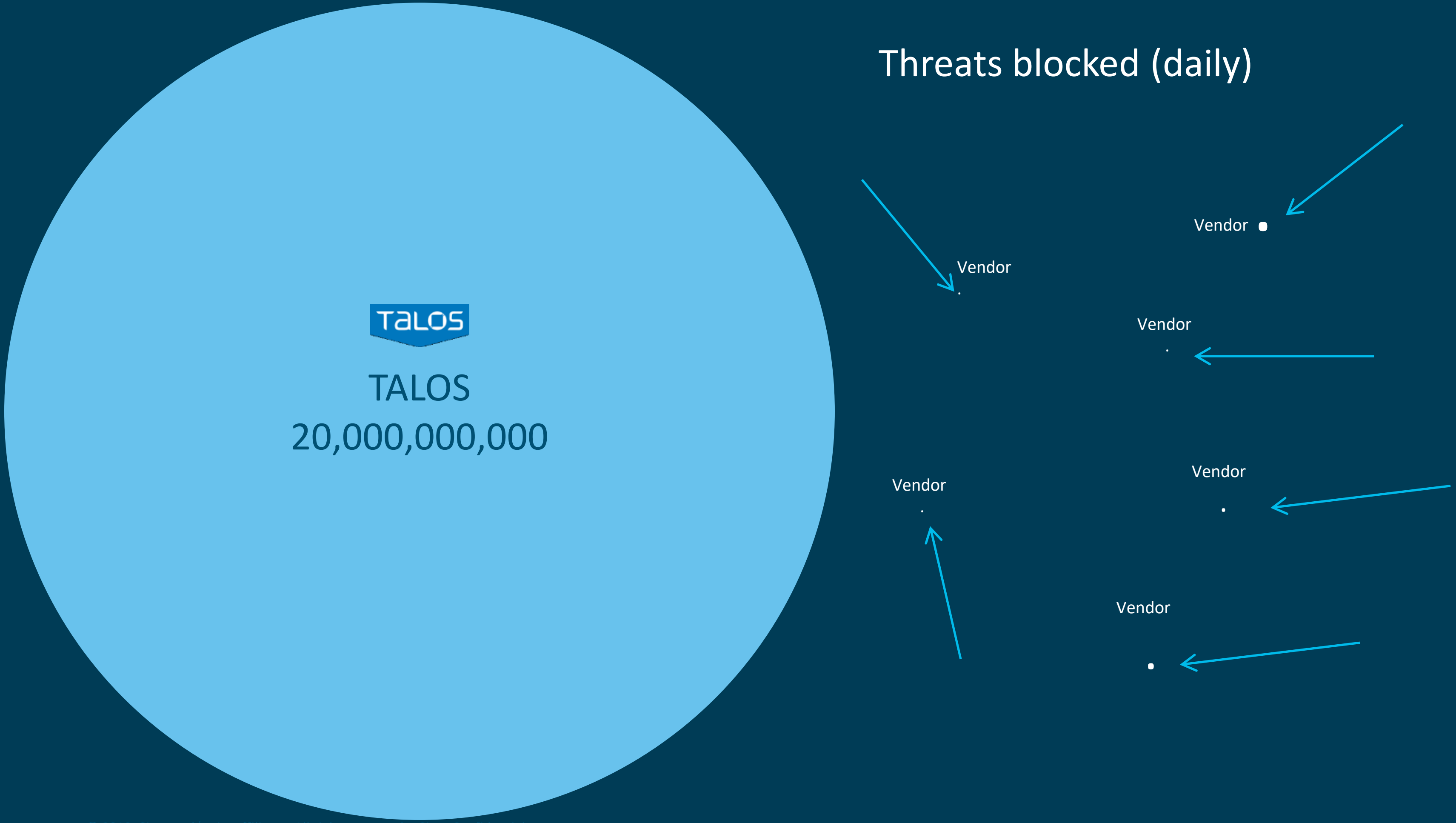
Remediation & Incident Response

- THREATCONNECT
- GUIDANCE SOFTWARE

SIEM & Analytics

- Huntsman
- EIQ
- ArcSight
- ACUITY SYSTEMS
- TIBCO
- E8 SECURITY
- 1Labs
- FIDELIS CYBERSECURITY
- BLACKHAWK NETWORK
- HAWK NETWORK DEFENSE
- splunk>
- Trustwave
- FORTSCALE
- LogRhythm
- BlackStratus
- invincea
- RSA SECURITY
- Trustwave
- Symantec

Threats blocked (daily)



Questions

1. Can your firewall talk to the rest of your security ecosystem to improve visibility, increase speed to detection and response, and automate tasks?
2. How do you protect yourself from traffic the firewall doesn't see?
3. How do you protect devices when they are off the corporate network?
4. Are you prepared for Ransomware infections?
5. What if you ARE breached…What do you do next?

Get started with Cisco Security today

1

Learn more about how Cisco Security can work with your business

2

Schedule a Proof Of Value to identify areas in your business where visibility or control is lacking

Nikos Mourtzinos, CCIE #9763
Cyber Security Sales Specialist
nmourtzi@cisco.com
Linkedin nmourtzi
Twitter: @nmourtzinos