The Power of an Integrated Threat Defense

Save Time and Resources with Cisco Security

Kristy Patullo – Technical Solutions Architect

Greg Girgenti – Security Sales Specialist

October 2019

“Security controls are only as effective as the quality of the threat intelligence they take action upon…”

TALOS

Cisco Security Research

TALOS
Cisco Security Research

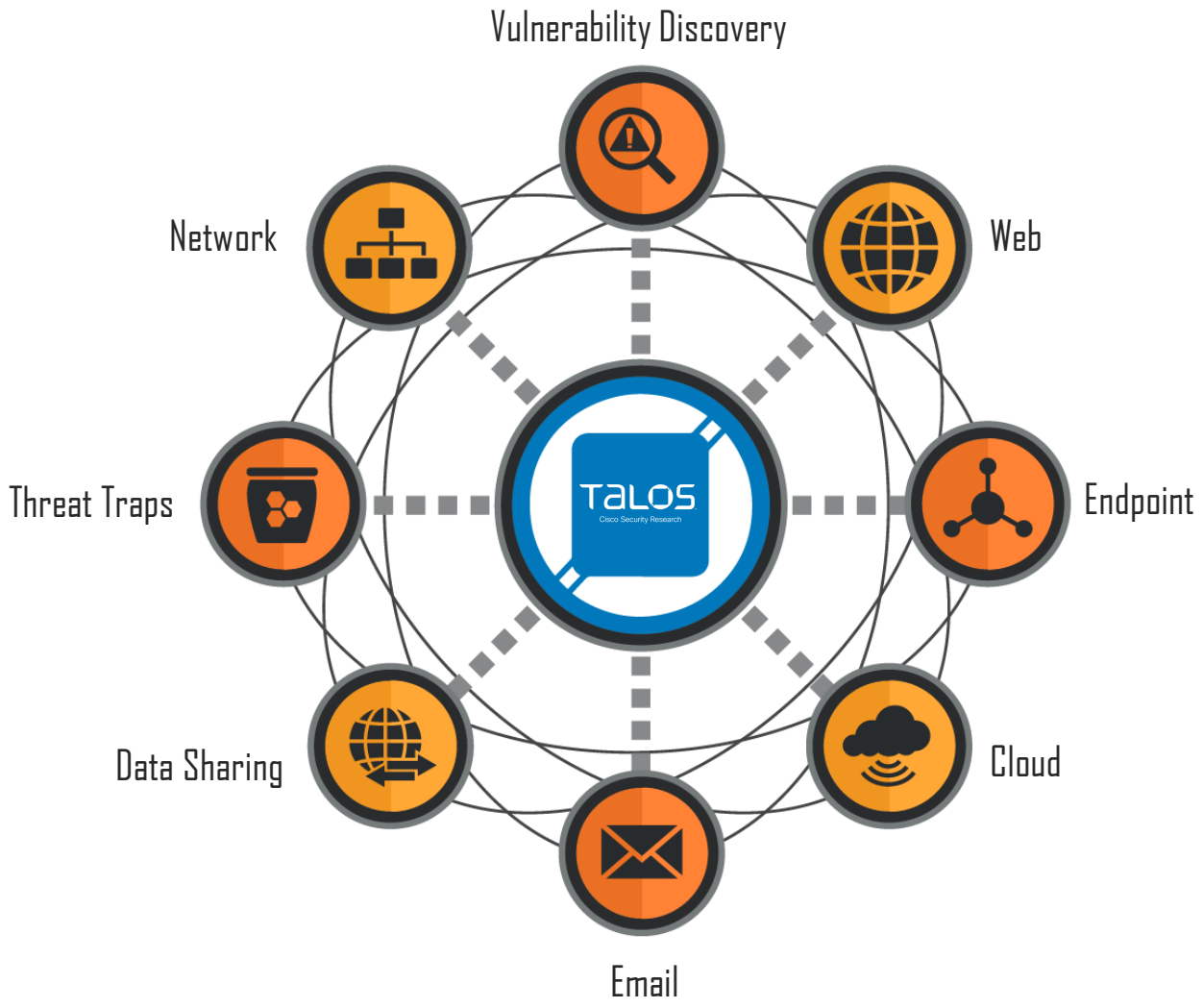
Unmatched Visibility

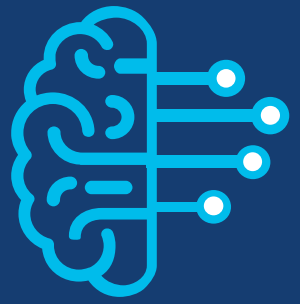
To stop more, you have to see more.

- The most diverse data set
- Community partnerships
- Proactively finding problems

2.2 Trillion Artifacts Seen Daily

1.9 Trillion Email artifacts
175 Billion DNS Entries
47 Billion Web requests
70 Billion Network Flows (includes Cognitive)
189 Million File Artifacts (14M never-before-seen)
100 Million new detection events
500 Million Authentications (per month)





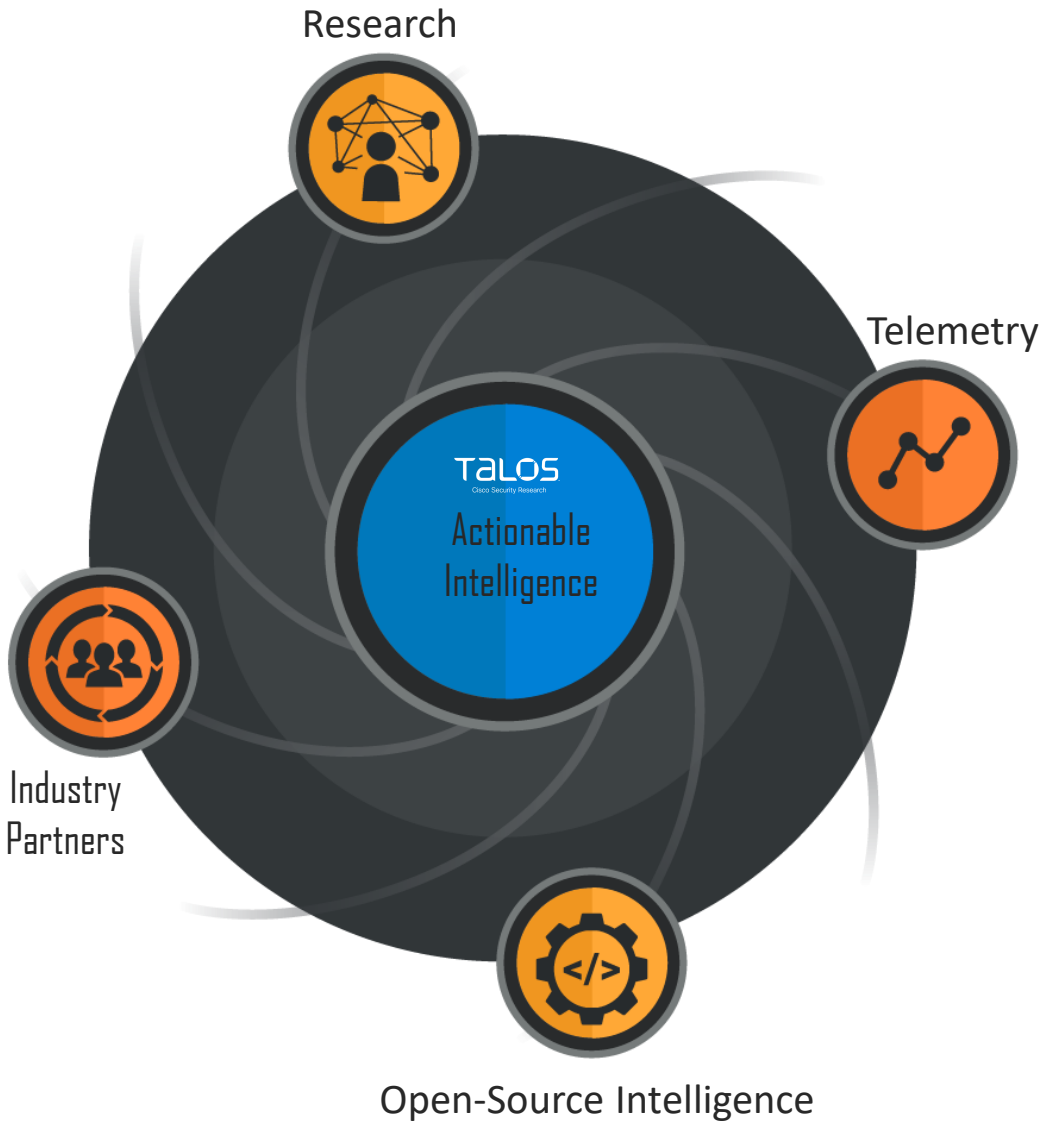
TALOS
Cisco Security Research

Actionable Intelligence

Security controls are best served by data that lets tools respond to immediate threats.

- Rapid coverage
- Distillation and analysis
- Threat Context

It's not detect and forget, it's detect and analyze.



TALOS
Cisco Security Research

Actionable Intelligence

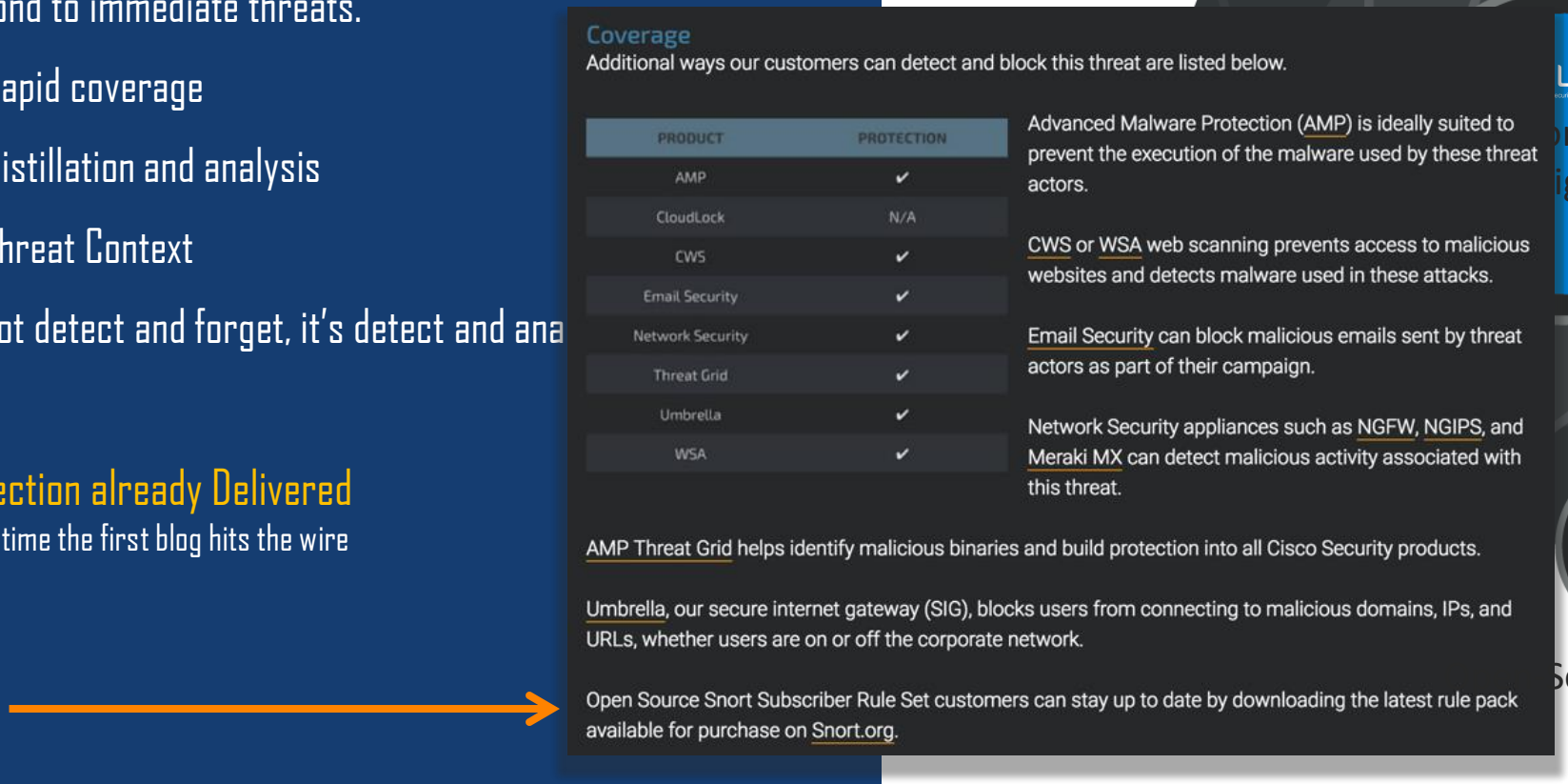
Security controls are best served by data that lets tools respond to immediate threats.

- Rapid coverage
- Distillation and analysis
- Threat Context

It's not detect and forget, it's detect and ana

Protection already Delivered

By the time the first blog hits the wire



Coverage

Additional ways our customers can detect and block this threat are listed below.

PRODUCT	PROTECTION
AMP	✔
CloudLock	N/A
CWS	✔
Email Security	✔
Network Security	✔
Threat Grid	✔
Umbrella	✔
WSA	✔

Advanced Malware Protection (AMP) is ideally suited to prevent the execution of the malware used by these threat actors.

CWS or WSA web scanning prevents access to malicious websites and detects malware used in these attacks.

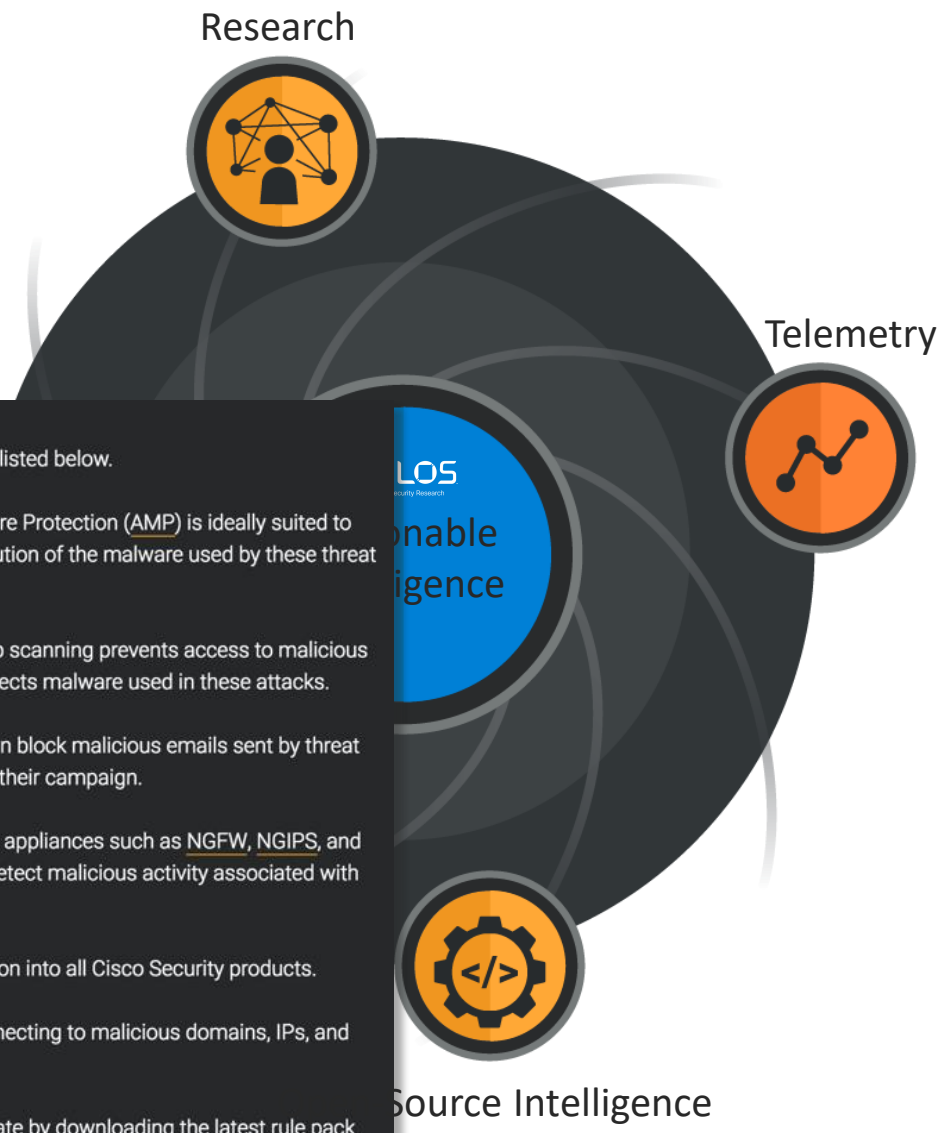
Email Security can block malicious emails sent by threat actors as part of their campaign.

Network Security appliances such as NGFW, NGIPS, and Meraki MX can detect malicious activity associated with this threat.

AMP Threat Grid helps identify malicious binaries and build protection into all Cisco Security products.

Umbrella, our secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs, and URLs, whether users are on or off the corporate network.

Open Source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.



TALOS
Cisco Security Research

Collective Response

The ability to bring rapid protection to close off multiple attack vectors instantaneously is crucial

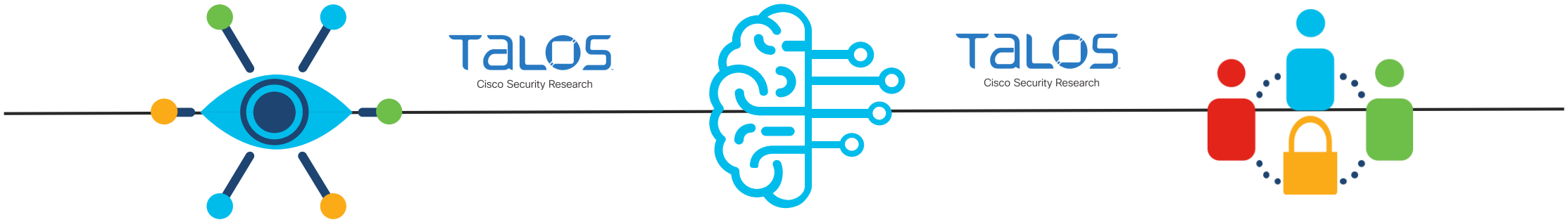
- **Breadth:** See once, protect everywhere
- **Depth:** Response and interdiction drives continuous research
- **Scale:** Delivering portfolio-wide protection, in real-time

10.5 Billion Daily Responses

6.5 Billion rejected emails
1.4 Billion DNS blocks
2.6 Billion URL Blocks
1 Million malicious file blocks
100 Thousand new file convictions
100 Million Vulnerability-Exploit events

Immediate Response + Extended Response + Response Follow-up

Cisco Cybersecurity is ‘Threat Intelligence Focused’



Unmatched Visibility

Actionable Intelligence

Collective Response

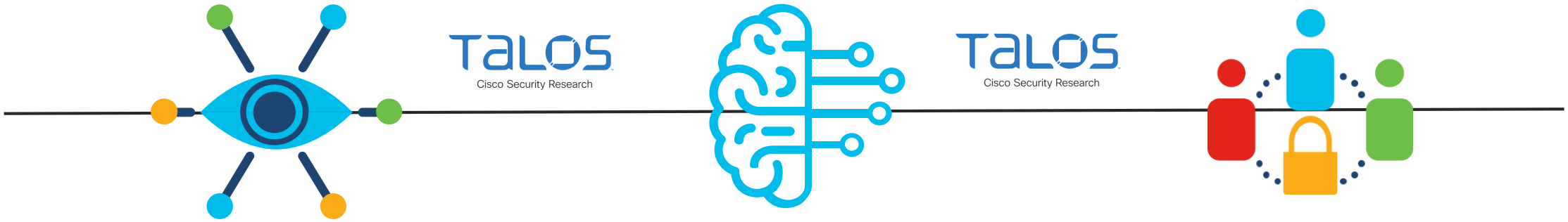
Our Customers are Breached Less

Cisco Finds Attackers the Fastest

We Protect our Customers BEFORE the Attack

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cisco Cybersecurity is ‘Threat Intelligence Focused’



Unmatched Visibility

Our Customers are Breached Less
Versus Other Security Vendors (2019 >100:1)

Actionable Intelligence

Collective Response

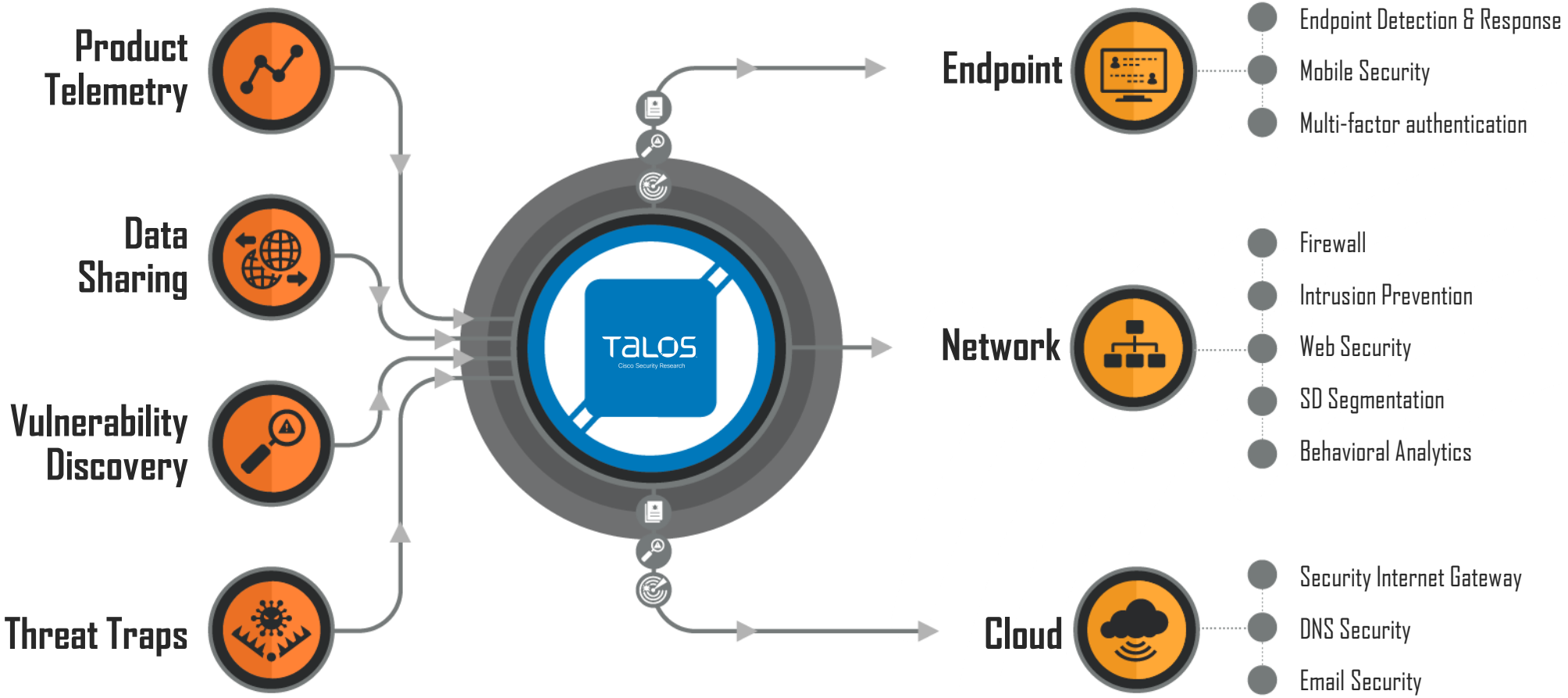
Cisco Finds Attackers the Fastest
Versus the Industry average of ~100 Days.
(AMP <3 hours)

We Protect Customers BEFORE the Attack
In 2018, Cisco Talos eliminated over 365 new vulnerabilities
from the market BEFORE a day0 attack could be weaponized

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

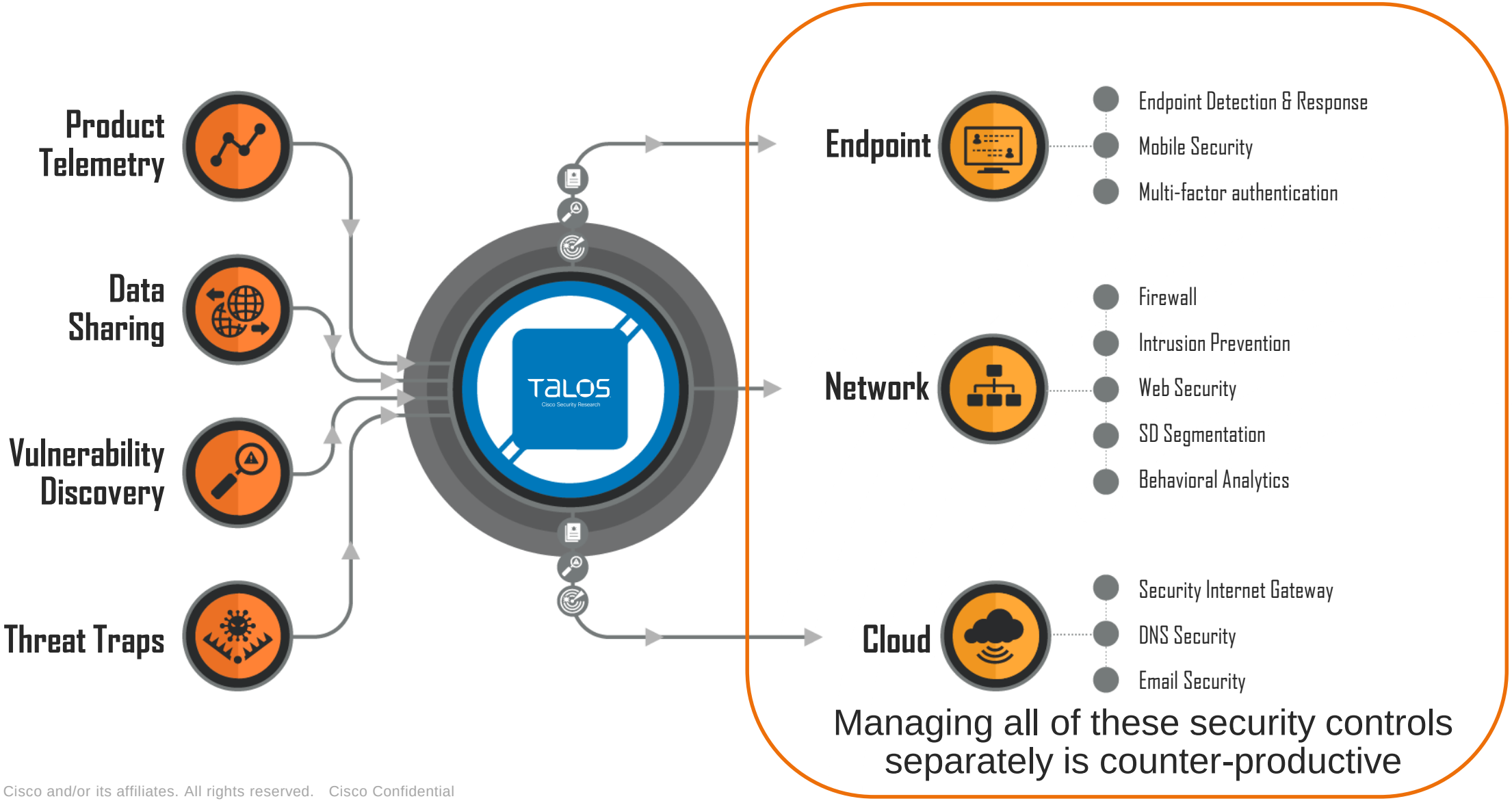
[1]2018 Collective Incident Response Data

From Unknown to Understood



© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Security that works together is top priority for our customers



© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Why is this important?
Nothing is 100% and layers have gaps

[redacted]

Sep 6, 2019, 10:29 AM

to me

This message has been deleted. Restore message

Good Morning,

Please see the attached file!!!
Don't hesitate to ask me any questions.

Zip pass 777

Regards,

[redacted]
Hudson Property Management, LLC
[redacted]
www.hudsonpm.com

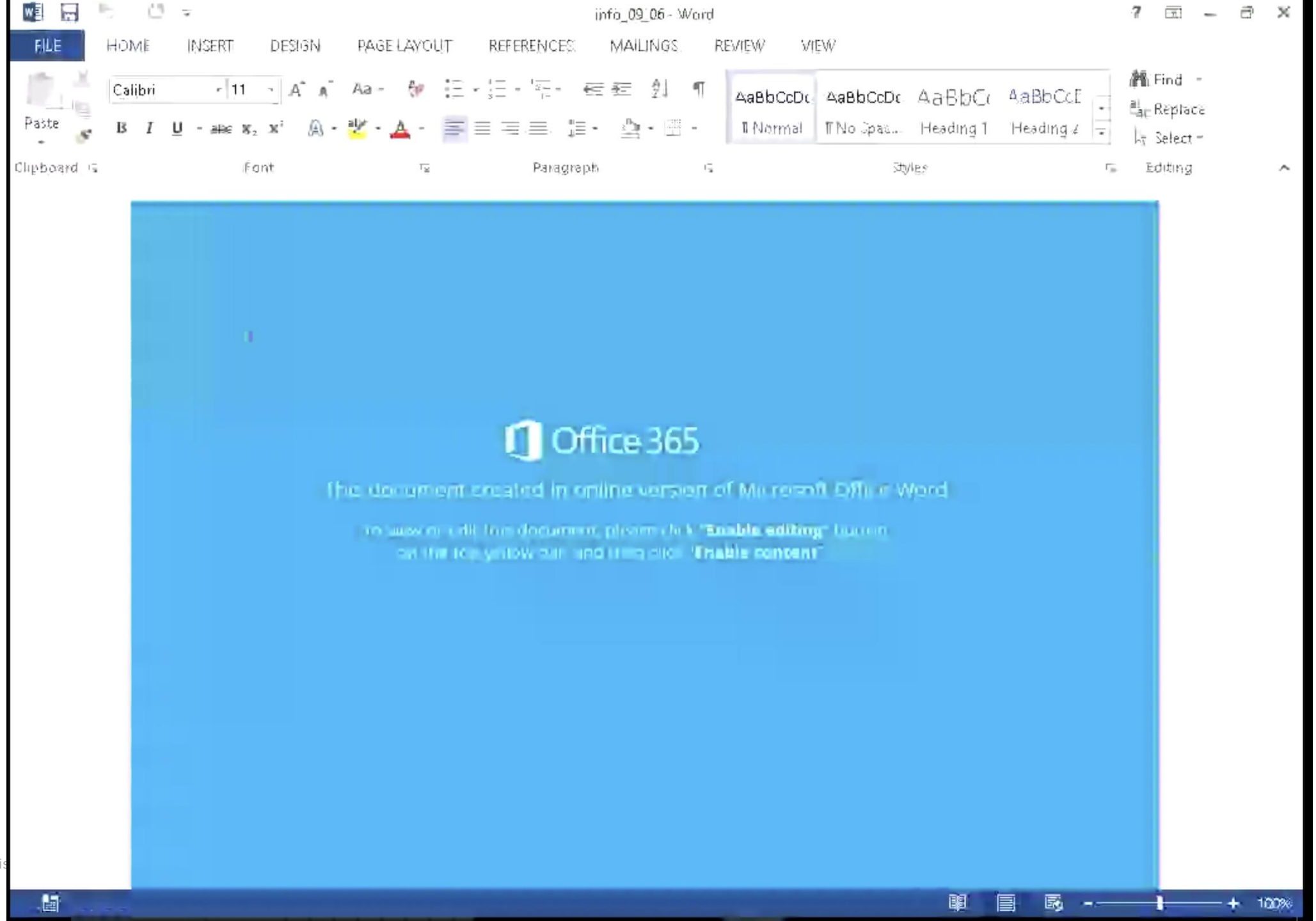
From: [redacted]
Sent: Tue, 22 May 2018 17:18:51 +0000
To: [redacted]
Sub [redacted]

•••

Encrypted attachment warning – Be careful with this attachment. This message contains 1 encrypted attachment that can't be scanned for malicious content. Avoid downloading it unless you know the sender and are confident that this email is legitimate.

Hudson_Property_...

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential


info_09_06 - Word
FILE
HOME
INSERT
DESIGN
PAGE LAYOUT
REFERENCES
MAILINGS
REVIEW
VIEW
Calibri
11
Paste
Clipboard
Font
Paragraph
Styles
Editing
Find
Replace
Select
Normal
No Spac...
Heading 1
Heading 2
Office 365
This document created in online version of Microsoft Office Word
To view or edit this document, please click "Enable editing" button
on the top yellow bar, and then click "Enable content"
100%

© 2019 Cis

‹ Samples

Metrics
Metadata
Indicators
Network
HTTP Traffic
DNS Traffic
TCP/IP Streams
Extracted Domains
Processes
Artifacts
Registry Activity
Consolidated
Created Keys
Modified Keys
Deleted Keys
File Activity

Sample ID	9237a3c468735a9659b528e547b7e705	**Filename**	Hudson_Property_Management.zip
Submitted By	krpatullo	**Magic Type**	Zip archive data, at least v2.0 to extract
OS	Windows 10	**File Type**	zip
Started	9/6/19 10:53:55 am	**First Seen**	9/6/19 10:53:53 am
Ended	9/6/19 11:00:51 am	**Last Seen**	9/6/19 10:53:53 am
Duration	0:06:56	**SHA-256**	5dde0bac3b5872e1079e738...
Sandbox	rcn-work-004	**SHA-1**	f6b86ccb5fbee3c070dfc72a82855b8f033aac6e
Playbook	No Playbook Applied	**MD5**	183a342b2794614f9805f96c196e3b4f
Network Exit Localization	US - Pennsylvania - Philadelphia	**Tags**	
		FP/FN	0 False Positive / 0 False Negative

Behavioral Indicators

Search

Title	Categories	ATT&CK	Tags	Hits	Score
Office Document Launches a Powershell	pattern	defense evasion	dropper, obfuscation, phishing, script	1	100
A Domain Flagged By Cisco Umbrella Downloaded A PE	domain		compound, dns, umbrella	1	95
Document Contains VBA Macro With Random Variables And ActiveX Controls	macros		activex, compound, embedded, macro, obfuscation, vba	4	95
Document Submission Contacted Domain Flagged By Cisco Umbrella	domain		compound, dns, umbrella	1	95
Document Used WMI to Launch Process	pattern	defense evasion	compound, dropper, obfuscation,	1	95

Emotet Overview

Emotet is one of the most widely distributed and actively developed malware families on the crimeware landscape today. It is a highly modular threat with a variety of payloads being delivered. Emotet began purely as a banking trojan, but over the years, has continued to evolve and more recently, has been associated with some larger-scale targeted Ryuk ransomware infections. The primary infection vector remains malicious emails sent as part of widespread spam campaigns. Emotet is commonly delivered via both macro-laden office documents, as well as URL-based spam messages that lead to an eventual infection. These campaigns change and evolve daily, and the supporting infrastructure also changes on a near constant basis. It's not uncommon to see Emotet reuse of some of the command and control (C2) servers over more extended periods.

The goal of Emotet, as is the case with crimeware-based threats, is monetary. Attackers use Emotet to deliver modular payloads it can use to monetize infections. Those payloads can include threats like banking trojans, stealers, self-propagation, email harvesters and ransomware. The modules the attackers deploy are likely chosen based on the way they can best monetize infected systems and the environments in which those systems reside.

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Defend Across All Attack Vectors

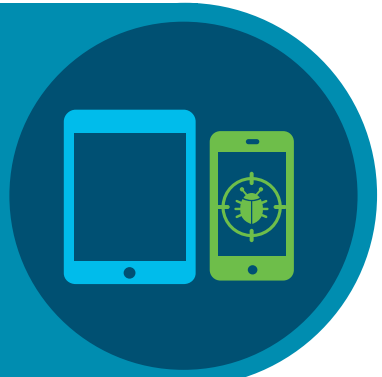
- Blocks users from connecting to malicious web sites
- Stops hackers from controlling and spreading ransomware

Cisco Umbrella

- Blocks users from receiving phishing attack emails and the harmful attachments that cause ransomware

Cisco Cloud Email Security with Advanced Malware Protection

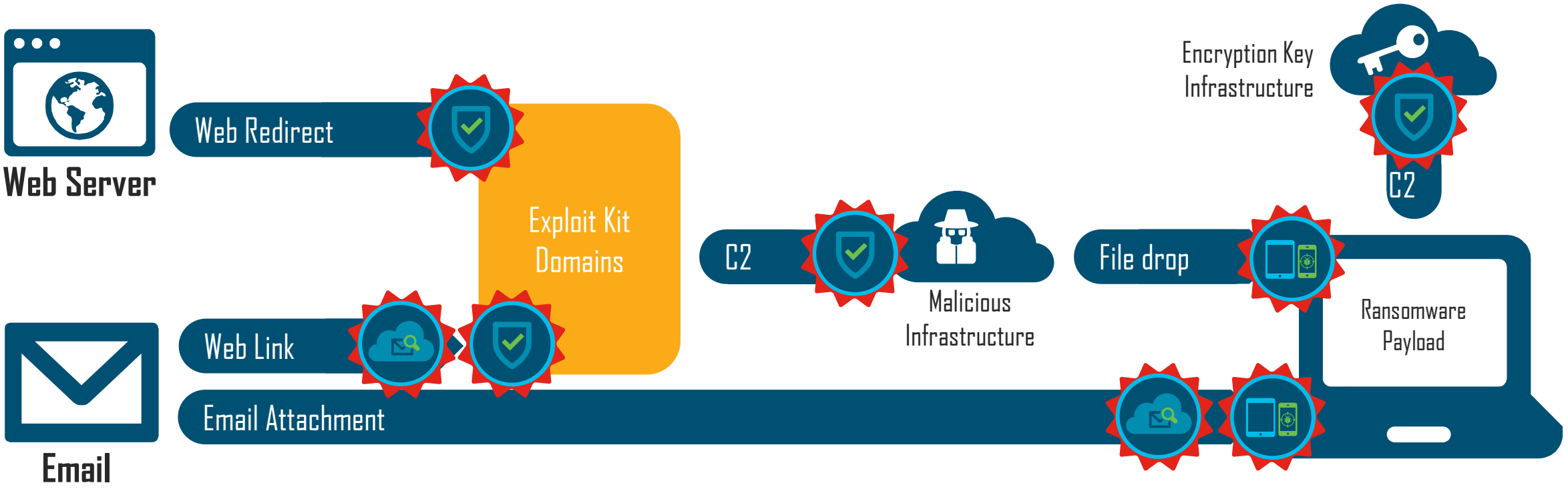
- Quarantines malicious files on endpoints to prevent infection
- Prevents the lateral movement of ransomware across your network



Cisco Advanced Malware Protection for Endpoints

isco and/or its affiliates. All rights reserved. Cisco Confidential

Break the Ransomware Chain



Cisco Ransomware Defense

- Stopped by Cisco Umbrella
- Stopped by Cisco Cloud Email Security with AMP
- Stopped by Cisco AMP for Endpoints

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Beyond Quick Prevention

Visibility

See and control what's on your network

Segmentation

Limit the lateral spread of ransomware

Response Planning

Prepare now

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

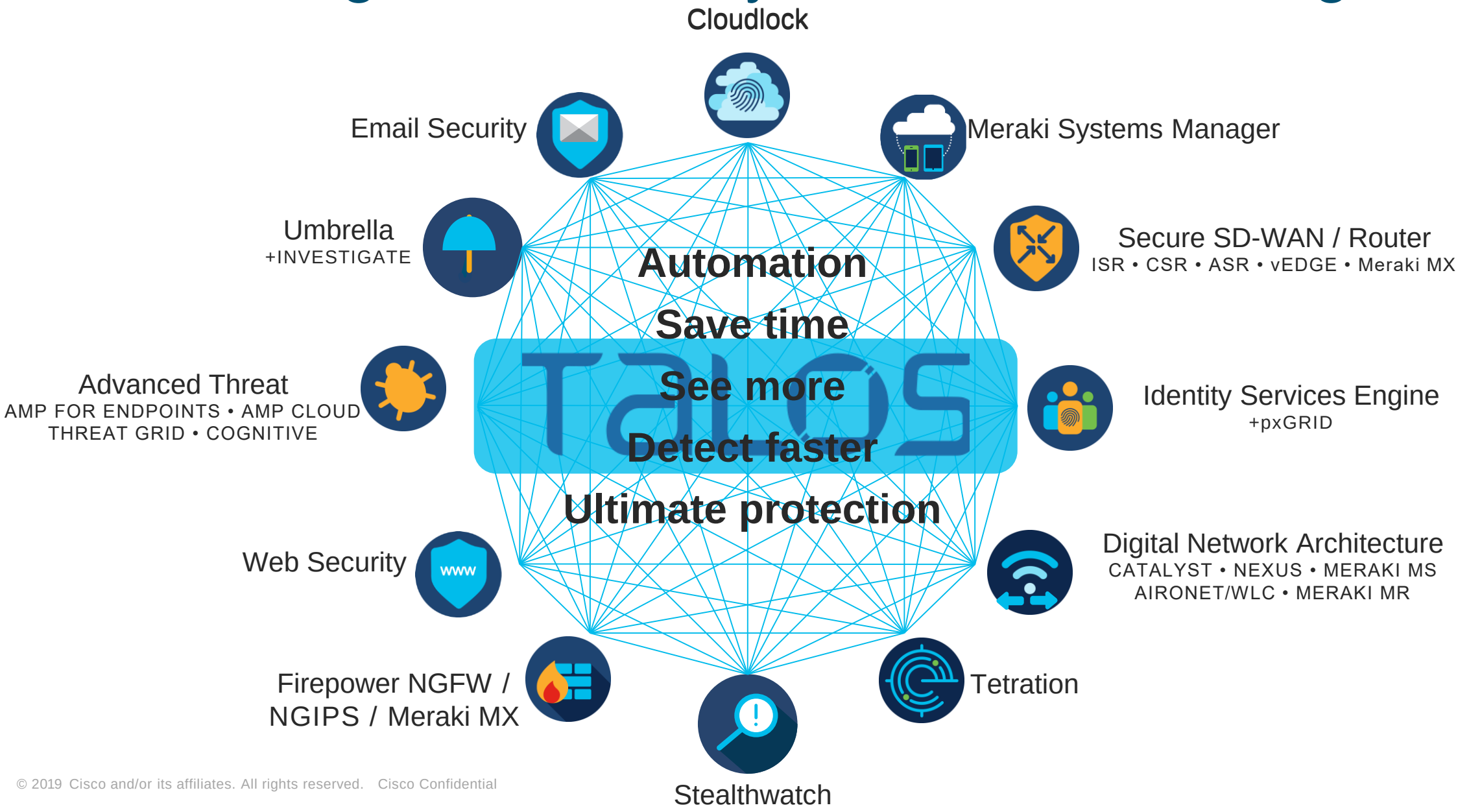
Cisco Ransomware Defense

Advanced Prevention

- Next Generation Firewall
- Next Generation IPS
- Web Security with AMP
- Stealthwatch
- Identity Services Engine
- TrustSec
- AMP Threat Grid
- Cisco Security Services

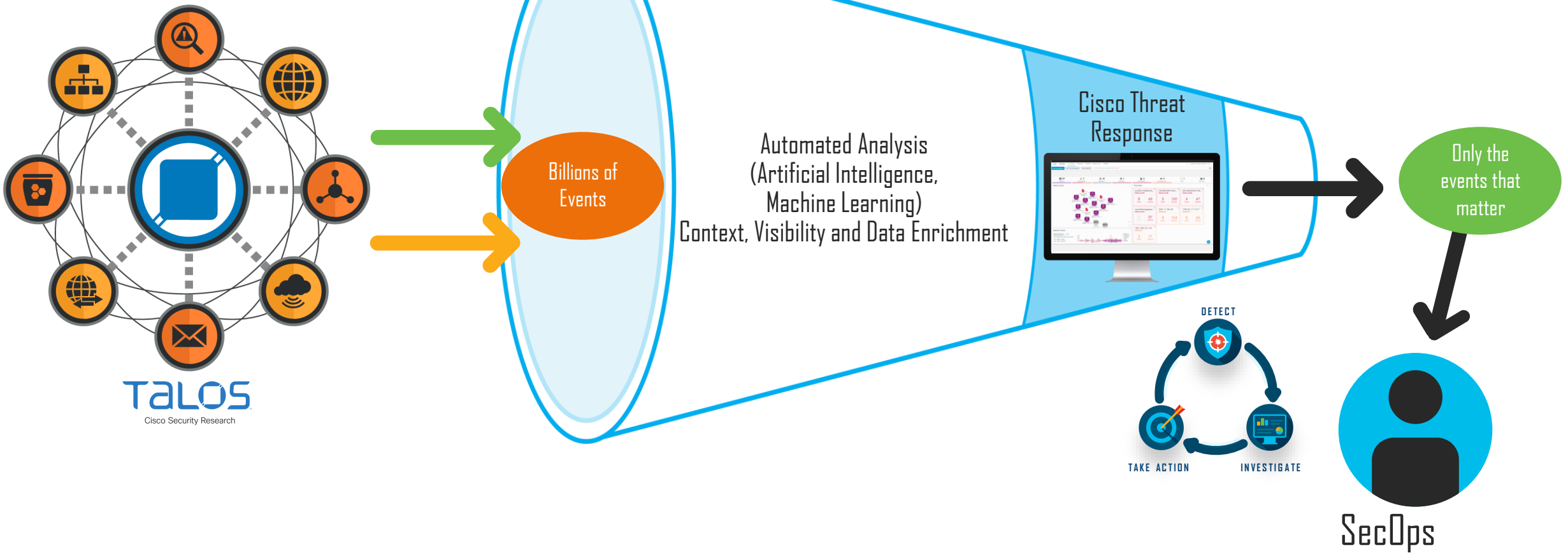
© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cisco's Integrated Security Portfolio Works Together



© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Applied Threat Intelligence Through Integration and Automation



© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cisco Threat Response

Key pillar of our integrated architecture for faster defense

Automates & orchestrates across all Cisco security products using a single UI [1]

Focused on automating security operations functions – detection, investigation, and remediation

Included free as part of Cisco's security product licenses

[1] Product UI tools will be transparent within CTR UI – pivots are invisible and deep linked

© 2019 Cisco and/or its affiliates. All r dential

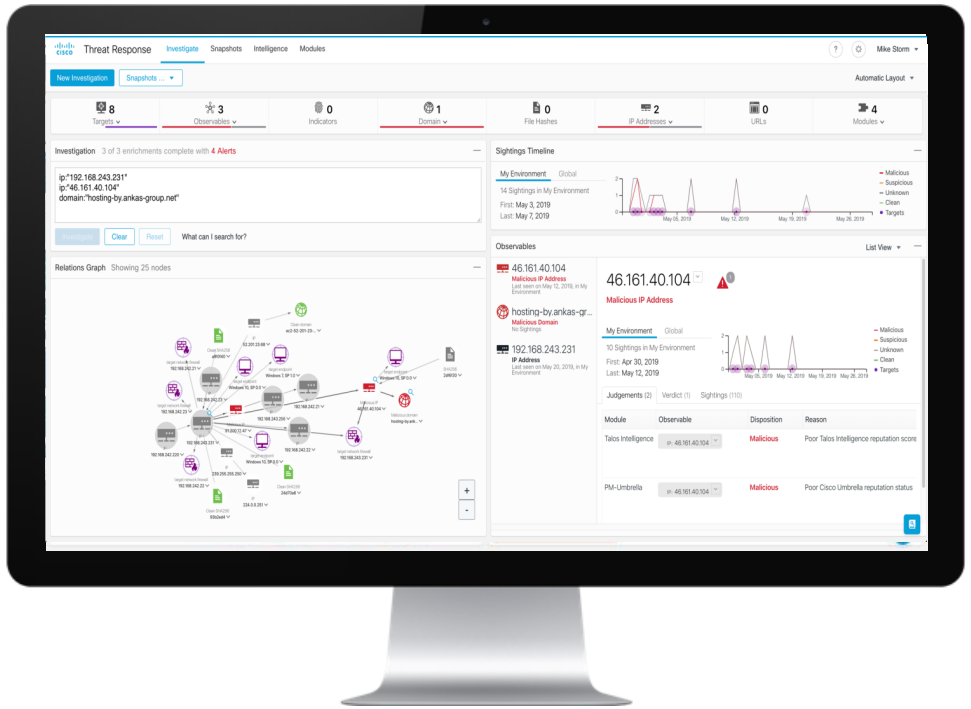
Cisco Threat Response

Would you like to improve your cybersecurity posture...
while efficiently and effectively managing risks?

Would you like to shorten time-consuming investigations...
while focusing your staff on higher-value activities?

Would you like to manage fewer security vendors...
while dramatically improving your cybersecurity capabilities?

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential



Demo

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

CISCO