Con ultra velocità alla protezione completa!



September 2018

Ciro Pizzo, Consulting Systems Engineer Cybersecurity – CISCO Systems, EMEAR/Switzerland LinkedIn: https://www.linkedin.com/in/ciro-pizzo-security/

Agenda

ıılıılı cısco

- Threat Landscape
- Cisco Cybersecurity Architecture
- What works best for Ticino
- LIVE DEMO
- Visit us at the booth for more demo and interaction!

How Hackers Make Money

Cryptojacking % per transaction

>\$50

DDoS as a Service ~\$7/hour

DDoS

11 1.1 1.1 CISCO

Medical Record

4022 5201 2244

Credit Card Data

\$0.25-\$60

Ransomware >\$250 per host Mobile Malware \$150

Spam \$50/500K emails

Malware Development \$ to be contracted (commercial malware)

Exploits \$100k-\$300K

Facebook Account \$1 for an account with 15 friends

S



Cisco Cybersecurity Stack

Cloud Security & Security from the Cloud Platform Based Threat-Focused Visibility Driven

> Complete Solution

Before

During

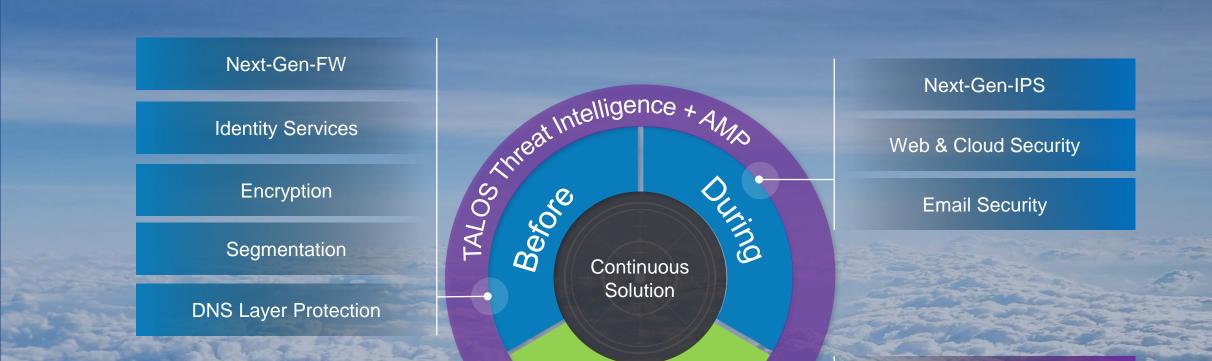
After

Pervasive

Continuous

Always On

ululu cisco



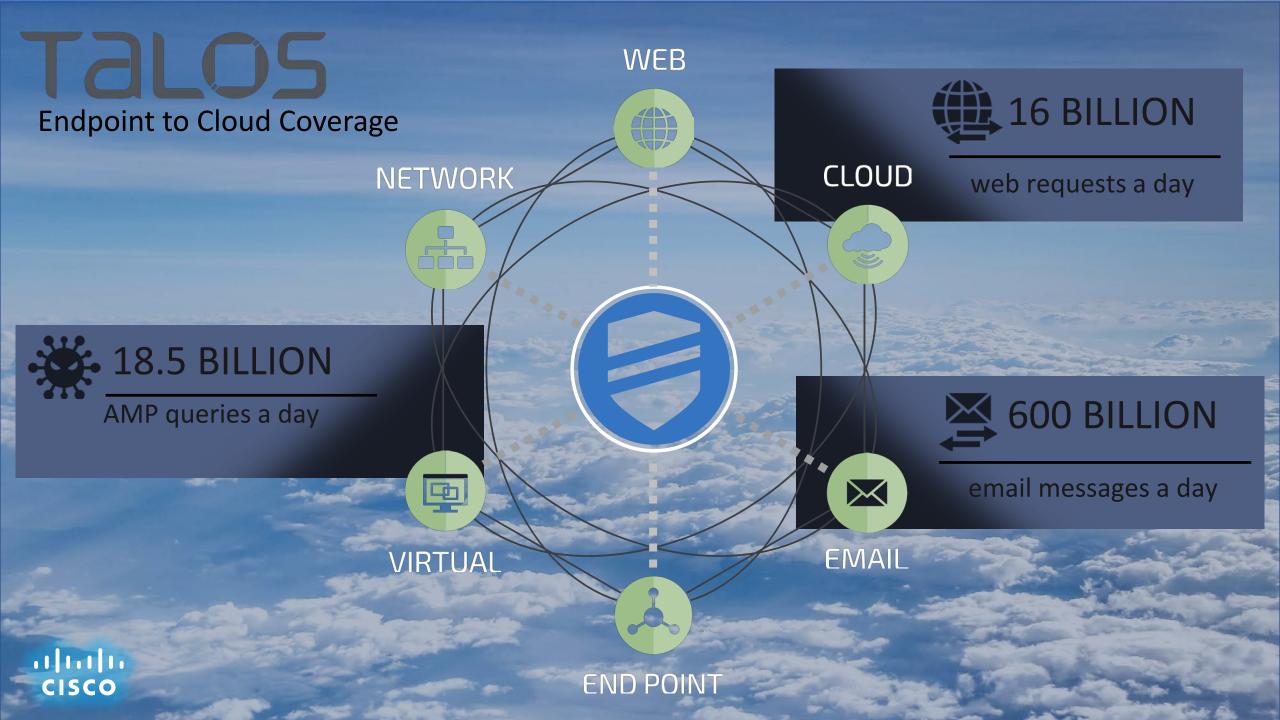
After

Advanced Malware Protection

Network Security Analytics

DNS Intelligence

ıı|ıı|ıı cısco



What might work best for Ticino?

From my experience, but don't nail me on this one ©

Easiest security solution you'll ever deploy

1 Signup

2 Point your DNS

3 Done in 10 minutes!

Umbrella

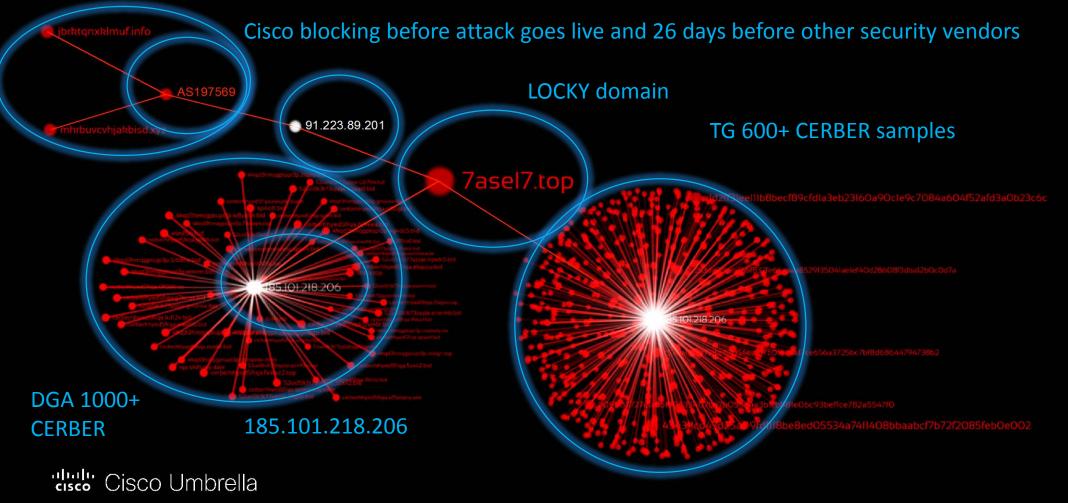
Start blocking in minutes

X

OPEN

 (\mathbf{X})

Visualizing attacker infrastructure



NGFW & NGIPS with Cisco Firepower



FMC – Firepower Management Center

Unified Central Manager for NGFW, NGIPS, AMP for Endpoint correlated alerts, ISE correlation & mitigation, deepest level of Threat Analytics and SIEM Integration



Speed Impact Assessment and Response

Attack Impact Level

Attac	k Im	pact l	_eve	2			<u> </u>	Priority ×	Impact ×	Inline × Result	Source IP ×	Source × Country	Destination × IP	Destination × Country
					4		<u>2016-06-28 09:54:13</u>	<u>high</u>	2	$\mathbf{\Psi}$	10.200.1.17		10.200.1.32	
					Т.		<u>2016-06-28 09:53:11</u>	<u>high</u>	3	$\mathbf{\Psi}$	192.168.1.7		74.125.228.53	USA USA
					4		2016-06-28 09:52:43	<u>high</u>	4	$\mathbf{\Psi}$	72.21.91.109	USA	old the state of t	
					4		2016-06-28 09:52:13	<u>high</u>	2	$\mathbf{\Psi}$	10.200.1.17		10.200.1.196	
					1		<u>2016-06-28 09:52:06</u>	<u>high</u>	2	$\mathbf{\Psi}$	10.200.1.17		<u>10.200.1.124</u>	
Application × Protocol	<u>Client</u> ×	Web × Application	<u>10C</u> ×	Application Risk	1		2016-06-28 09:51:22	<u>high</u>	2	4	10.200.1.17		olimitati <u>10.200.1.41</u>	
	DNS			Very Low	4		2016-06-28 09:51:16	<u>high</u>	2	$\mathbf{+}$	10.200.1.17		10.200.1.162	
	SSL client	Gmail		Medium	4		<u>2016-06-28 09:48:51</u>	<u>high</u>	4	$\mathbf{+}$	10.0.202.63		10.0.68.120	
	Chrome	Web Browsing			+		2016-06-28 09:48:51	<u>high</u>	4	¥	10.0.30.124		10.0.30.91	
-		Web browsing		<u>Medium</u>	4		2016-06-28 09:48:44	<u>high</u>	3	4	255.255.255.255		10.112.10.86	
DNS	DNS			Very Low	+		2016-06-28 09:48:40	<u>high</u>	3	¥	192.168.1.7		<u>74.125.26.106</u>	USA USA
DNS	DNS			Very Low	1		<u>2016-06-28 09:47:24</u>	<u>high</u>	2	$\mathbf{\Psi}$	10.0.247.133		<u>ग</u> <u>10.0.121.57</u>	
DNS	DNS			Very Low	1		2016-06-28 09:47:24	<u>high</u>	3	4	<u> 10.131.12.106</u>		🗐 <u>10.0.68.66</u>	
DNS	DNS			Very Low	4		2016-06-28 09:47:24	<u>high</u>	2	$\mathbf{\Psi}$	10.0.247.133		olimitati 🗐 🧃 🗐	
<u> </u>	Firefox	Web Browsing		Medium	4		2016-06-28 09:47:24	<u>high</u>	3	$\mathbf{\Psi}$	10.0.228.118		olimitati 🗐 🗐 🗐	
	Firefox	Web Browsing		Medium	4		<u>2016-06-28 09:46:34</u>	<u>high</u>	4	$\mathbf{\Psi}$	10.0.57.137		10.110.10.31	
	Firefox	Web Browsing		Medium	4		2016-06-28 09:46:34	<u>high</u>	4	$\mathbf{+}$	172.16.0.15		olimitati 10.0.95.22	
HTTPS	SSL client	Google		Medium	4		2016-06-28 09:45:09	<u>high</u>	3	4	10.200.1.244		209.87.214.208	USA
	Firefox	Web Browsing	Triggered	<u>Medium</u>		Mediu	um Zone B	Z	one A		and a set	-		
П НТТР	Firefox	Web Browsing		Medium		Mediu	<u>Im</u> Zone B	<u>Z</u>	one A	201		and the	-	100
	Firefox	Web Browsing	Triggered	Medium		<u>Mediı</u>	<u>Im</u> Zone B	Z	one A			12.25	1 Dans	A second
	Firefox	Web Browsing		Medium		Mediu	<u>Im</u> Zone B	<u>Z</u>	one A	-		Surger .	Street, all	The state
	Eirefox	Web Browsing		<u>Medium</u>		<u>Mediı</u>	<u>Im</u> Zone B	<u>Z</u>	one A			Carlos and	and the state of t	- martin
□ <u>http</u>	Firefox	Web Browsing	-	Medium		<u>Mediu</u>	um Zone B	<u>Z</u>	one A			and the	a stand	

FMC – Visibility & Risk top apps, user, threats & customize

Overview Analysis Policies Devices Objects

Dashboards • Reporting Summary .

 Traffic by Application Risk 	- ×
Risk	▼ Total Bytes (KB)
Very Low	1,030,206.07
Medium	517,297.76
<u>High</u>	281,700.20
Low	102,730.37
Very High	2,141.11

Last updated 32 minutes ago

v Total Bytes (KB)
1,289,430.68
398,977.41
227,632.65
10,053.20
7,981.56

Last updated 32 minutes ago

Traffic by Application Category

Category	Total Bytes (KB)
network protocols/services	786,020.53
web browser	288,162.46
network utilities	140,635.26
web services provider	43,392.29
security management	40,335.72
VPN/tunnel	23,582.47
search engine	17,929.67
email	16,147.03
collaboration	10,515.36
business	9,003.41

Top Operating Systems Seen	
OS Name	▼ Count
Linux	942
Windows	595
Android	420
Chromium	149
Mac OSX	64
+1 👚 <u>iOS</u>	62
-1 🖡 <u>AIX</u>	58
-1 🌡 AIX 5L	58
FreeBSD	7
Blackberry	4
Last updated 32 minutes ago	0
Connections by URL Reputation	-
Reputation	Total Connections
Well known	25,100
Benign sites	1,344
Benign sites with security risks	925
+1 * Suspicious sites	10
-1 👃 <u>High risk</u>	9
Last updated 32 minutes ago	

Risky Applications with Low Business Relevance

Application	Total Connections
+1 會 🗔 Bingbot	78
-1 👃 🥅 Facebook	73
Livestream	67
Ident	39
VouTube	24

System Help v Global \ demo_user_56 v

Application	Total Bytes (KB
Internet Explorer	193,623.72
Firefox	23,855.56
Chrome	16,042.23
SMTP	6,996.66
Thunderbird	6,763.24
Mobile Safari	4,996.91
NetBIOS-ns	2,924.40
C Kerberos	2,755.88
NetBIOS-dgm	2,169.05
Libwww-Perl	1,759.16
Safari	864.43
+1 👚 IMAP	790.28
-1 🖡 🗔 <u>BITS</u>	786.93
FireAMP SSL	770.62
PS3 web browser	625.58

 Top Web Applications Seen 	-
Application	Total Bytes (KB
IPsec	21,984.83
Google	17,691.71
ENIP ENIP	13,541.74
Wikipedia Edit	9,951.87
Cisco	2,693.71
CloudFront	1,792.27
+1 1 People.com	1,591.79
-1 👃 🔲 CNN.com	1,417.10
+1 1 50AP	1,378.13

Last login on Tuesday, 2018-06-12 at 18:21:14 PM from 198.18.133.222

FMC – auto generated IoCs for both: User and machine

Overview Analysis Policies	Devices Objects			😒 System Help 🕶 Glob	al \ demo_user_56 +
Dashboards • Reporting Su	ummary 🔻				
Network × Threats × In	trusion Events × Status × Ge	olocation × QoS × +		Show th	e Last 🚺 day 🛟 🚺
					Add Widgets
Indications of Compromise by Host	st - X	Intrusion Events	- ×	Connections by Security Intelligence Category	*
Indications of Compromise by Hos	st – A	Intrusion Events		Connections by Security Intelligence Category	
IP Address	▼ Count	Last 1 day	Total	Security Intelligence Category	Total Connections
<u>10.110.10.21</u>	3 🗸		3,048,742	DNS_Intelligence-Attackers	4,653
<u>10.110.10.145</u>	3 🗸		of o to fin the	Network Intelligence-Spam	3,295
10.112.11.152	3 🗸	0 Incharacteristic	896,744	Network_Intelligence-Attackers	3,039
172.16.1.128	3 🗸	1 u der bie dentim blift im sieffinden u Be. ein tanbertan interiert	44,282	DNS Intelligence-Open_relay	2,265
172.16.10.104	3 🗸			<u>Network_Intelligence-Tor_exit_node</u>	2,202
<u>10.0.1.2</u>	2 🗸	Contraction of the second seco	465,738	Network_Intelligence-CnC	1,646
10.0.1.5	2 🗸	3 at party of the set	1.655.442	Network Intelligence-Suspicious	1,068
10.0.1.35	2 🗸	4		Network_Intelligence-Malware	1,036
10.0.1.38	2 🛩	and the second s	129,408	DNS Intelligence-Suspicious	1,017
10.0.1.77	2 🛩	All All and a second and a second and a second as a	3,191,614	Network_Intelligence-Bogon	948
Last updated 24 minutes ago	٩, ١			Last updated 24 minutes ago	
 Traffic by Security Intelligence Ca 	stegory – X			Indications of Compromise by User	- ×
Security Intelligence Categ	gory Total Bytes (KB)			Vser	Count
Network_Intelligence-CnC	18,849.05			RAGUEL BUCHHOLZ (DCLOUD-SOC\xbuch, LDAP)	6 🛩
Network Intelligence-Tor exit n	13,250.09			ANNETTE WHITTAKER (DCLOUD-SOC\jwhit, LDAF) 5 ~
Network_Intelligence-Malware	5,391.59			DALIA LEMUS (DCLOUD-SOC\ilemu, LDAP)	5 🗸
Network_Intelligence-Suspicious	3,570.41			CHARISSE YANCY (DCLOUD-SOC\zyanc, LDAP)	5 🛩
Network Intelligence-Attackers	3,422.87			CATARINA HELLMAN (DCLOUD-SOC\vhell, LDAP)	5 🛩
Network_Intelligence-Spam	1,85 <mark>8.03</mark>			CAROLINE DEHAVEN (DCLOUD-SOC\zdeha, LDAP)	5 ~
Network Intelligence-Bogon	1,619.42			CAMMY BARNARD (DCLOUD-SOC\mbarn, LDAP)	5 🛩
URL_Intelligence-Attackers	908. <mark>62</mark>			BEATA WOLFF (DCLOUD-SOC\xwolf, LDAP)	5 🛩
+1 1 DNS_Intelligence-CnC	649. <mark>42</mark>			ASA COBBS (DCLOUD-SOC\vcobb, LDAP)	5 🗸
-1 🗸 URL Intelligence-Phishing	647. <mark>22</mark>			AMIE POULOS (DCLOUD-SOC\gpoul, LDAP)	5 🛩
Last updated 24 minutes ago				Last updated 34 minutes ago	Q

FMC – tracking malware with File Trajectory

Network File Trajectory for 21eb9c87...0398e24f



Meraki Fully Cloud Managed Network & Security

Cisco Meraki: Bringing the cloud to enterprise networks





Meraki MR Wireless LAN



Meraki MS Ethernet Switches



Meraki MX Security Appliances



Meraki SM Mobile Device Management

Why customers choose the Cisco Meraki MX

Oakland

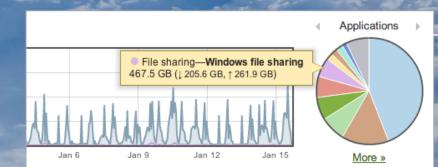


Site-to-site VPN

eleworker - Hilsenbec eleworker - Daghan Z

Connection status for Meraki Corp - appliance





Intuitive centralized management

- No training, no command line
- Templates to configure at-scale
- Packet capture, built-in tools and diagnostics

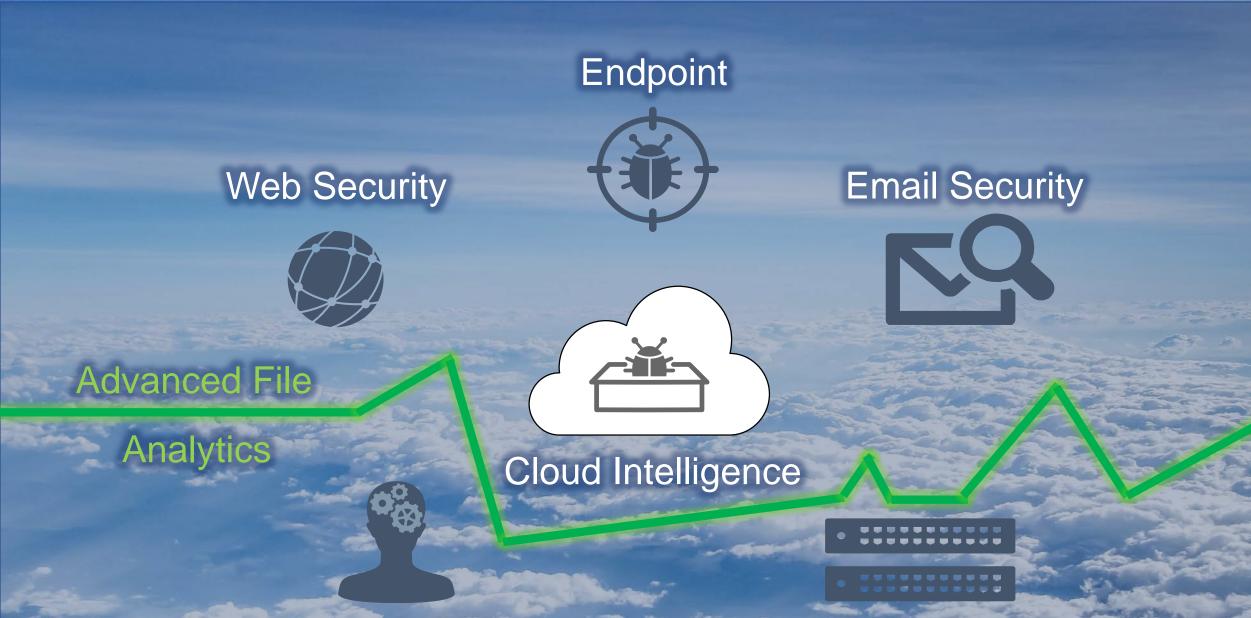
Designed for distributed enterprises

- Single pane of glass visibility
- Zero-touch provisioning
- Seamless updates from the cloud
- Site-to-site IPSec VPN in 3 clicks

Industry-leading visibility

- Fingerprints users, applications, and devices
- Network-wide monitoring and alerts
 - Full stack: APs, switches, Security, MDM

Advanced Malware Protection with Cisco AMP Everywhere



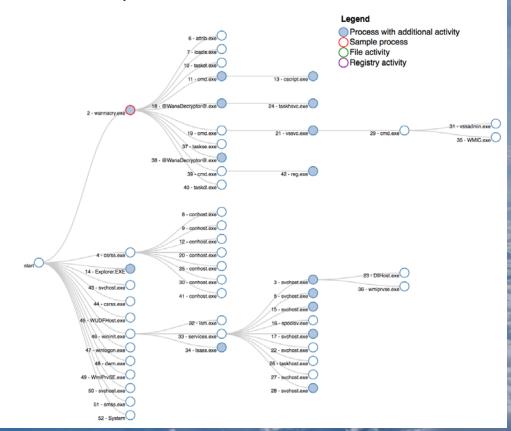
Cognitive Analytics

Firewall & IPS

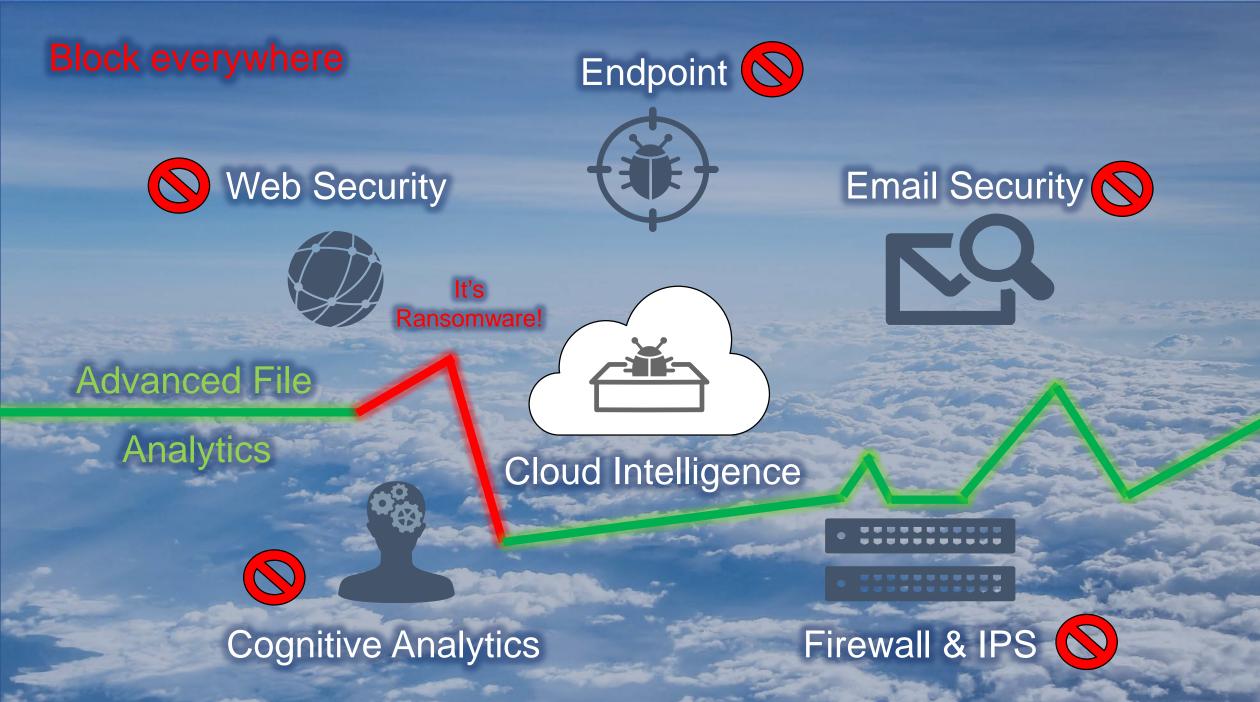
	Title 🖘	Categories	Tags	Hits 🖛	Score -
+	Ransomware Backup Deletion Detected	malware	ransomware, malware, compound	3	100*
+	Wanacryptor Ransomware Detected	malware	ransomware	1	100*
+	Artifact Flagged as Known Trojan by Antivirus	malware	trojan, RAT	2	95*
+	Large Amount of High Entropy Artifacts Written	malware	malware	1	95*
+	Shadow Copy Deletion Detected	weakening	crypto, file, system	2	100
+	Artifact Flagged Malicious by Antivirus Service	forensics	file, antivirus	4	95
+	Process Modified Desktop Wallpaper	attribute	process, scareware, registry, ransom	2	95
+	WMIC Used to Delete Shadow Copy	weakening	system, system modification	1	95
+	BCDEdit Used to Ignore Boot Failures	weakening	system, system modification	1	90
+	Process Created a File in a Recycle Bin Folder	persistence	recycler, file, process	59	90
+	Process Created an Executable in a Recycle Bin Folder	persistence	recycler, executable, file, process	1	90

	ID va	Path 🖏	Source 🕞	Size 🖡	Imports VA	Exports VA	AV Sigs $\forall \texttt{A}$
+	1	wannacry.exe	submitted	3514368	114	0	2
+	2	🛔 1636-wmiprvse.exe	memory	357888	190	0	0
+	3	🛔 1308-@WanaDecryptor@.exe	memory	245760	200	0	2
+	4	A 1980-@WanaDecryptor@.exe	memory	245760	200	0	2
+	5	A 1564-taskse.exe	memory	20480	22	0	0
+	6	🎝 1580-wannacry.exe	memory	3514368	114	0	1
+	7	536-WmiPrvSE.exe	memory	439296	193	0	0
+	8	1400-conhost.exe	memory	338432	200	0	0
+	9	A 1960-taskhsvc.exe	memory	3098624	200	0	0
+	10	A 1524-vssvc.exe	memory	1600512	200	0	0
+	11	⊖ \@Please_Read_Me@.txt	disk	933	0	0	0
+	12	⊖ \@WanaDecryptor@.exe	disk	245760	200	0	3
+	13	☐ \Users\Administrator\AppData\Local\@Ple ase_Read_Me@.txt	disk	933	0	0	0

Process Tree for Sample 72e42c51b430a9773587d712679f493f



PROPERTY AND

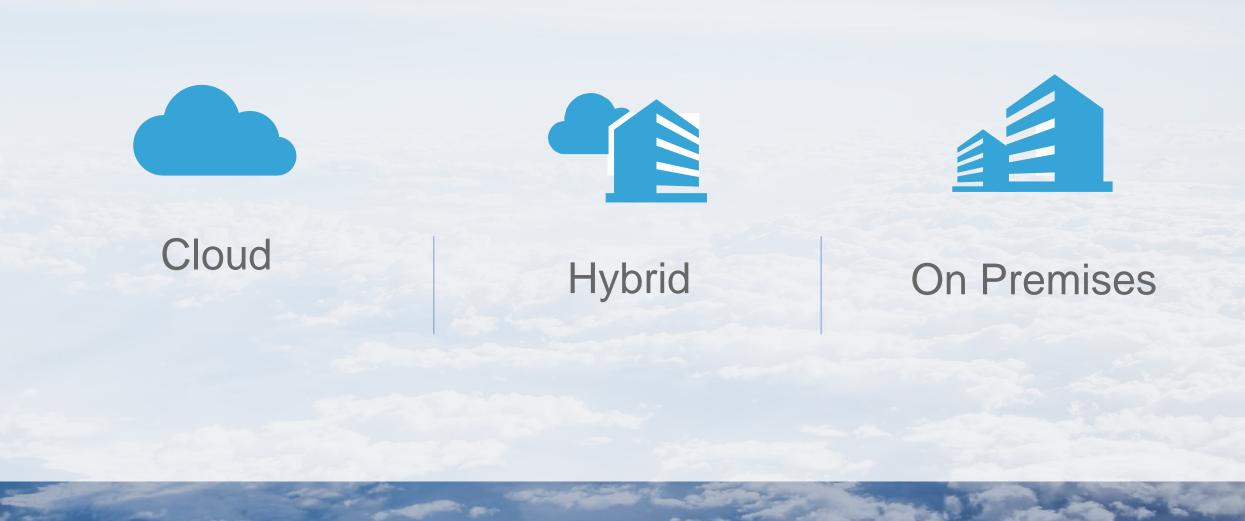


and the second second

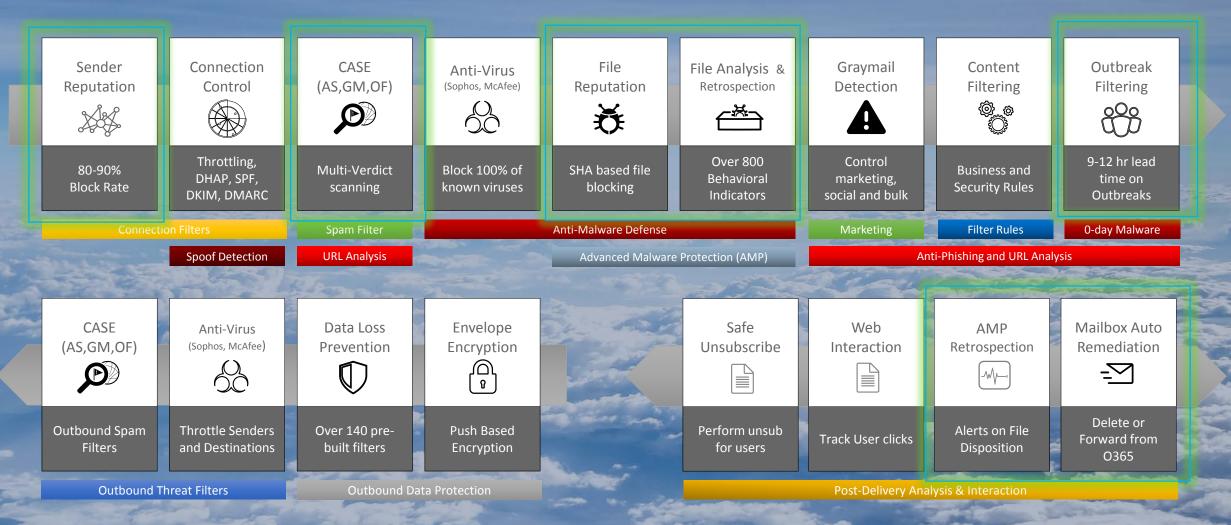
Mitigate O365 migration risks with Cisco Email Security

Email is still the #1 threat vector

Deploy the configuration that works best for you



Inbound Security & Outbound Control



Easy to deploy with O365 and CES activation team

Firejumper Academy – for the Partner SE



Firejumper Academy – for the Partner SE





Security as a Business Enabler

n|n|n cisco