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

- 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

DDoS
as a Service
~$7/hour

Medical Record
>$50

Credit Card Data
$0.25−$60

Ransomware
>$250 per host

Mobile Malware
$150

Malware Development
$ to be contracted
(commercial malware)

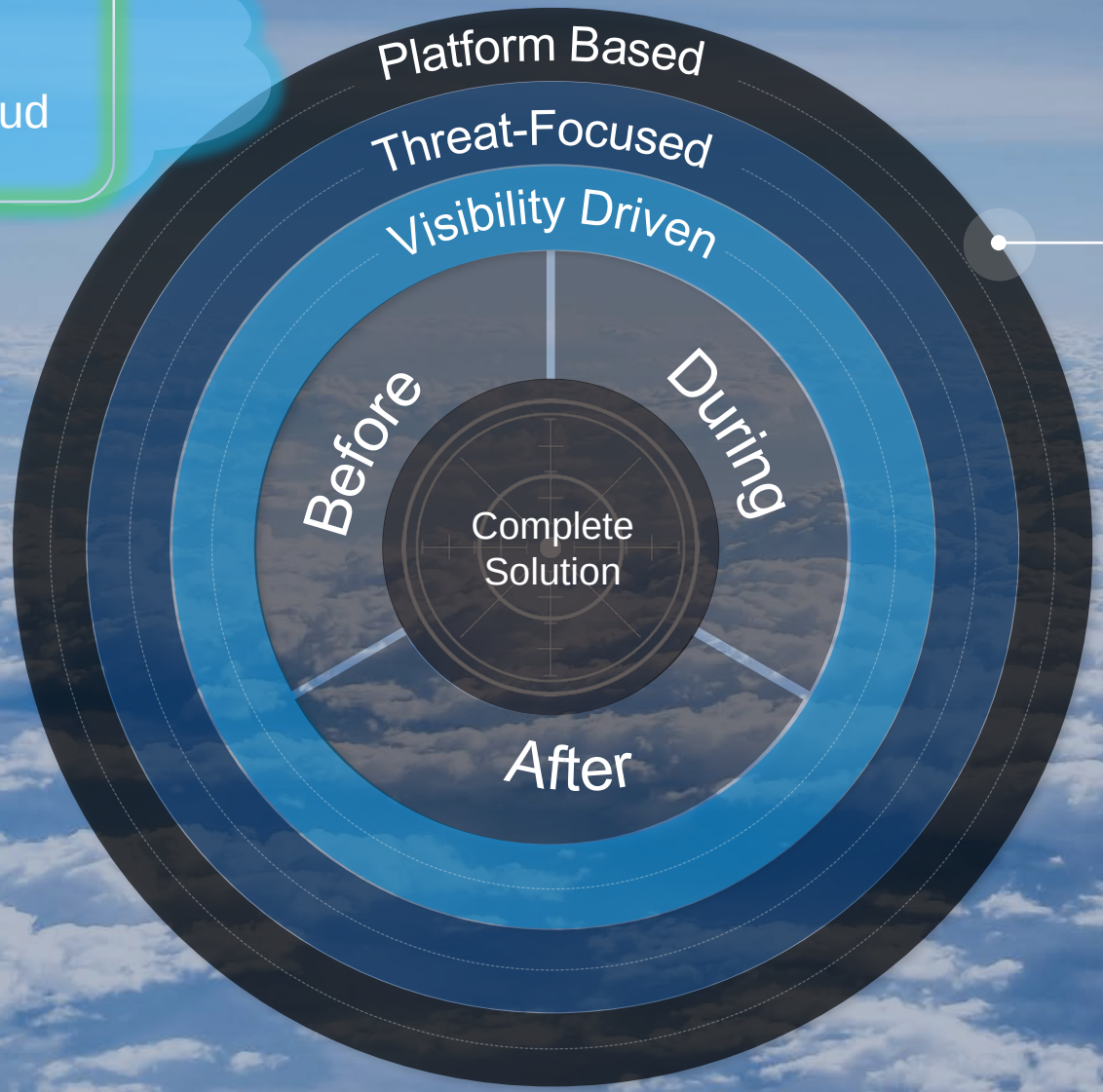
Spam
$50/500K emails

Exploits
$100k-$300K

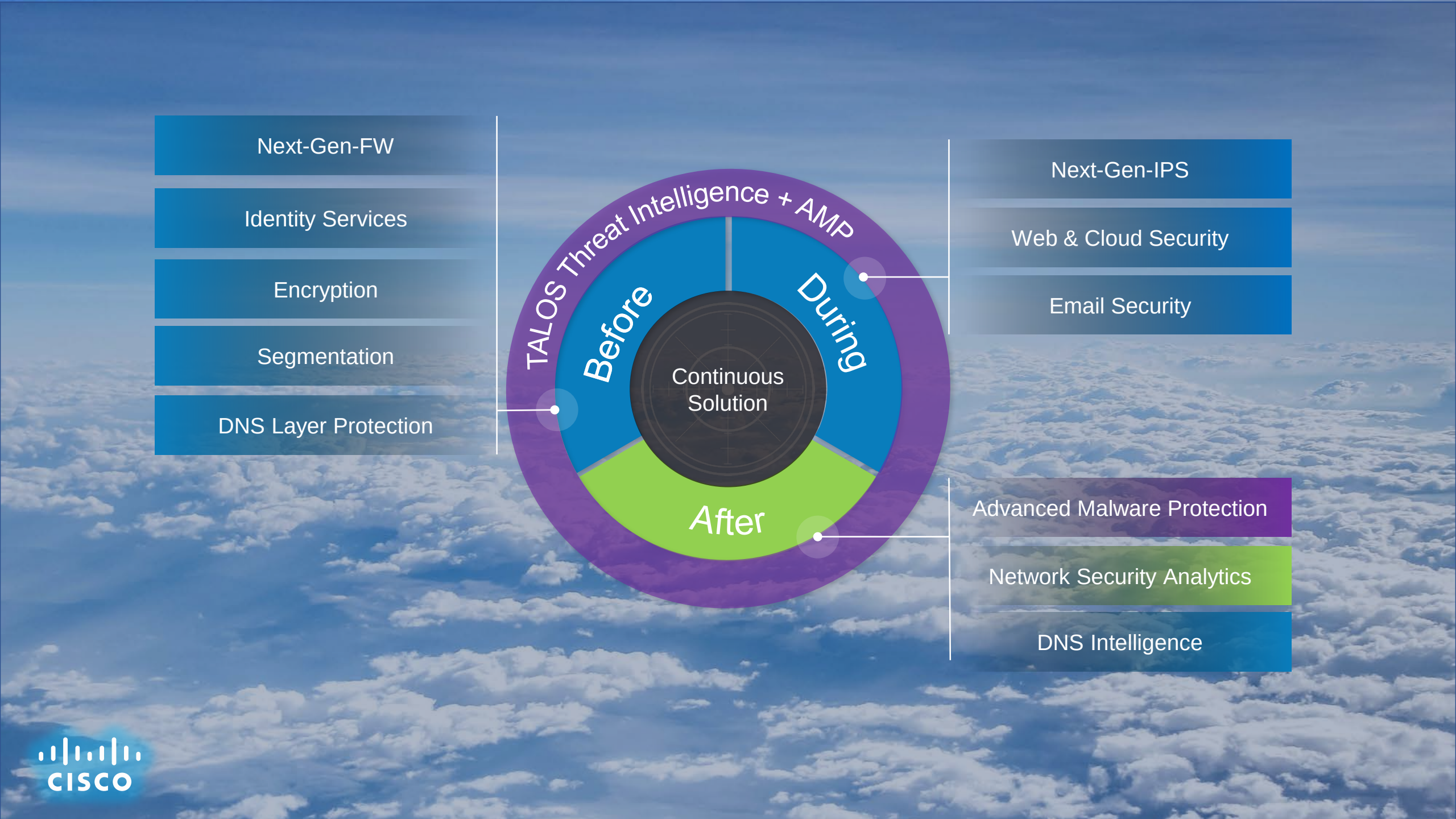
Facebook Account
$1 for an account
with 15 friends

Cisco Cybersecurity Stack

Cloud Security &
Security from the Cloud

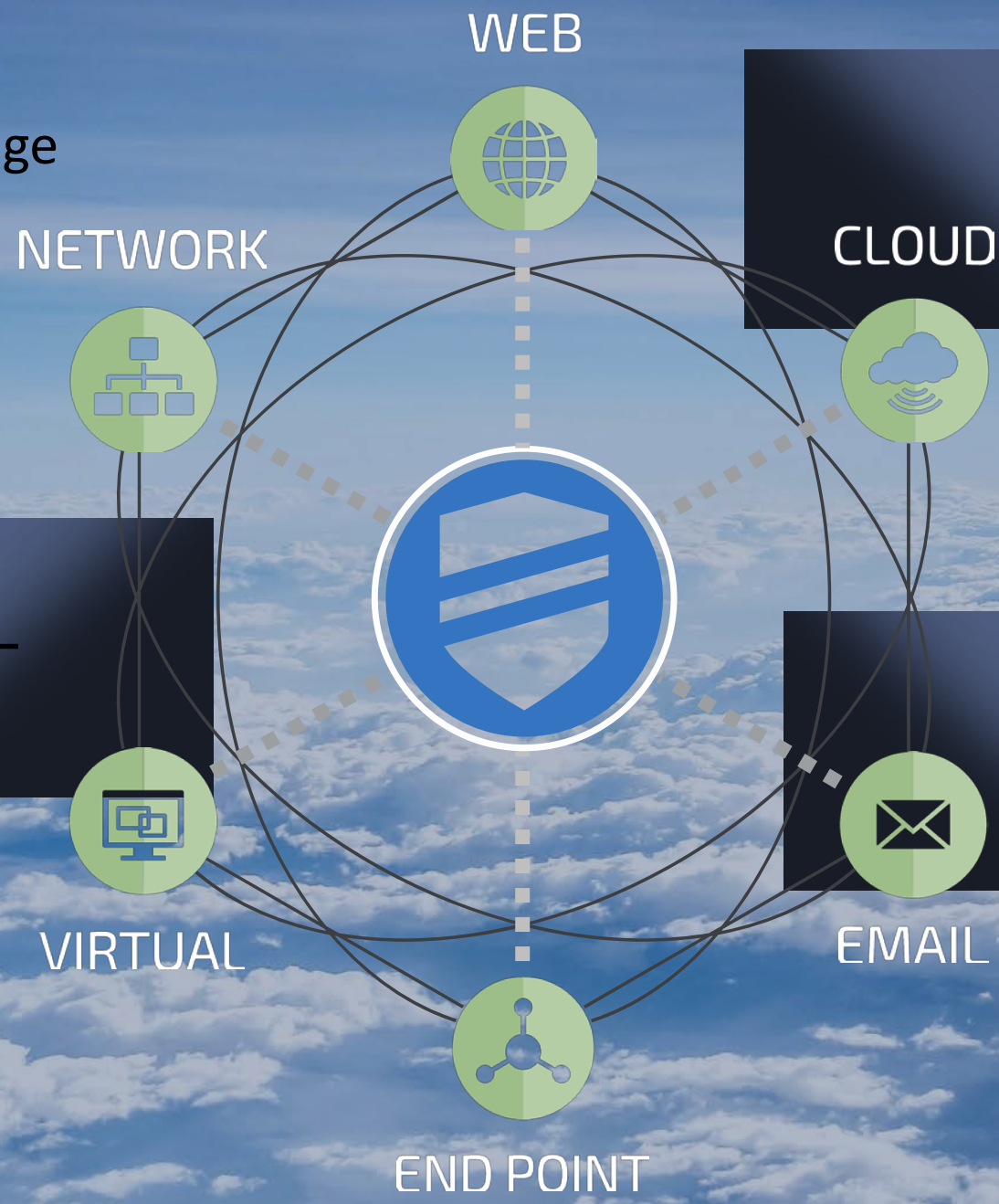


- Pervasive
- Continuous
- Always On


Next-Gen-FW
Identity Services
Encryption
Segmentation
DNS Layer Protection
TALOS Threat Intelligence + AMP
Before
During
After
Continuous Solution
Next-Gen-IPS
Web & Cloud Security
Email Security
Advanced Malware Protection
Network Security Analytics
DNS Intelligence

Talos

Endpoint to Cloud Coverage



16 BILLION

web requests a day

18.5 BILLION

AMP queries a day

600 BILLION

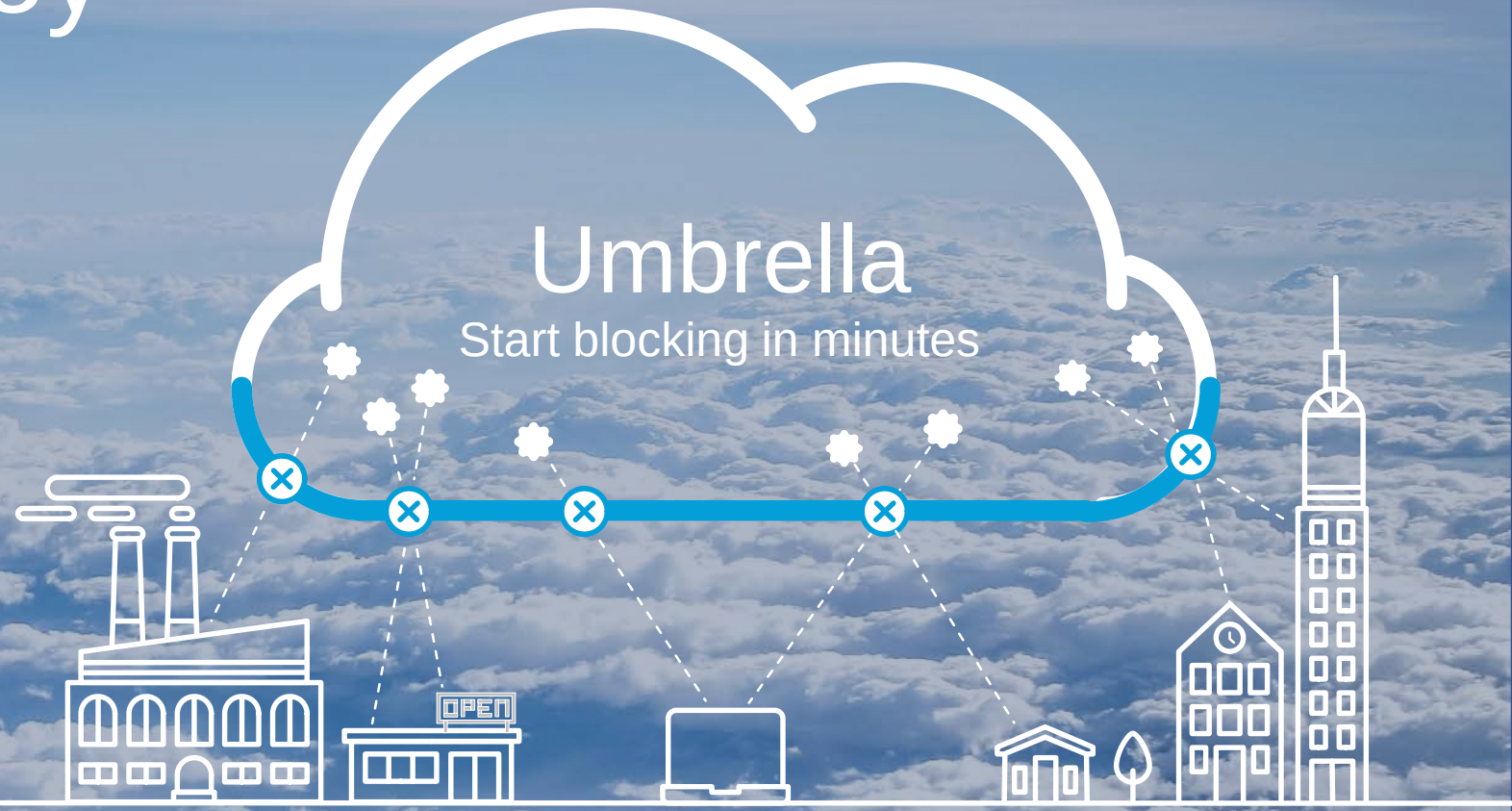
email messages a day

cisco


What might work best for Ticino?
From my experience, but don’t nail me on this one ☺

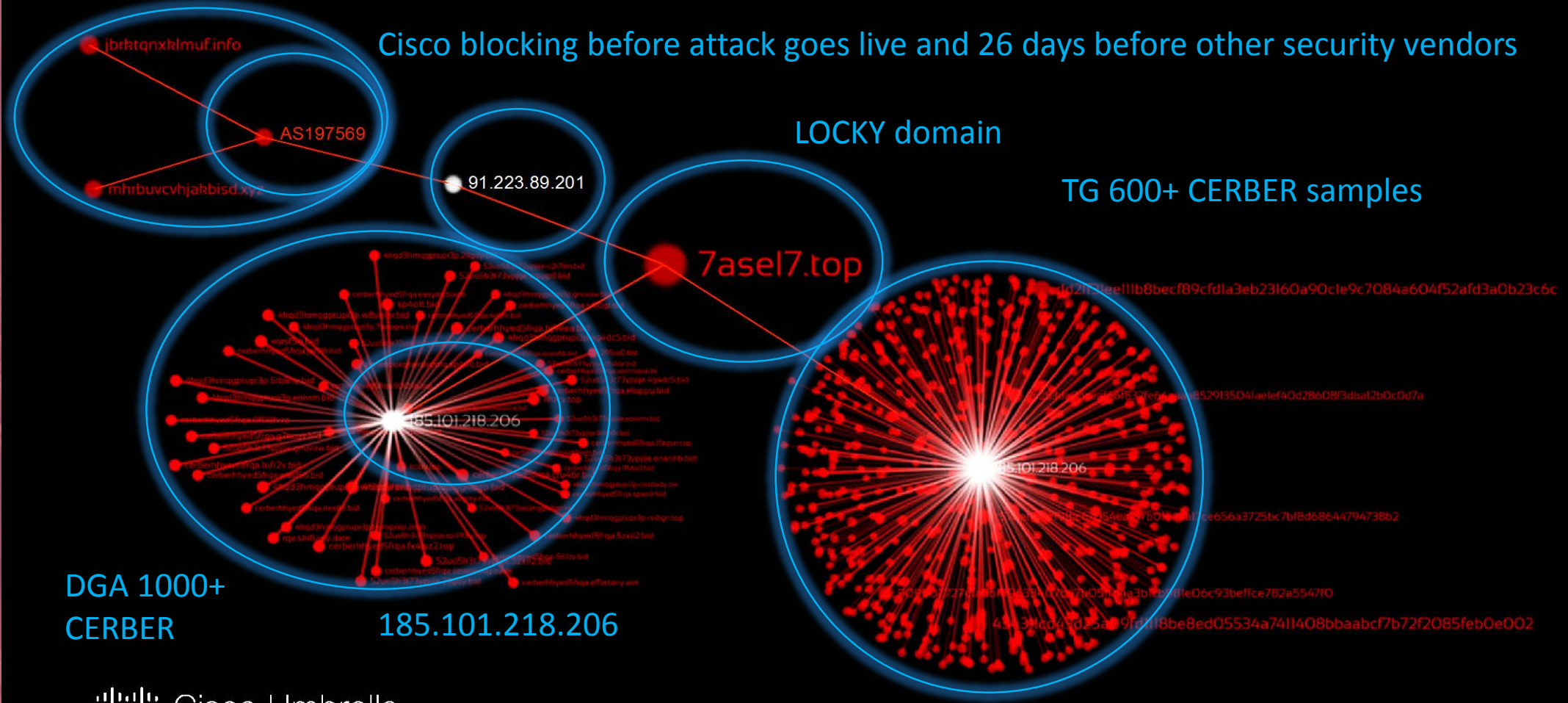
Easiest security solution you'll ever deploy

1. Signup
2. Point your DNS
3. Done in 10 minutes!



Visualizing attacker infrastructure

Cisco blocking before attack goes live and 26 days before other security vendors



LOCKY domain

TG 600+ CERBER samples

DGA 1000+
CERBER

185.101.218.206

Cisco Umbrella

NGFW & NGIPS
with
Cisco Firepower

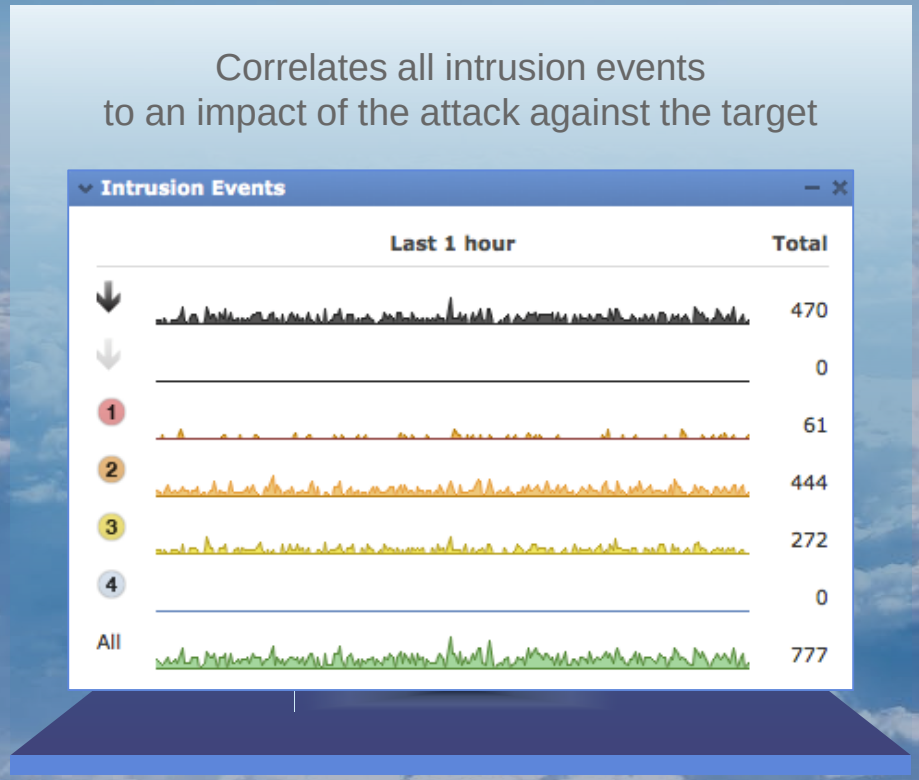
Offering extensive contextual visibility

The more you see, the better you can protect

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

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

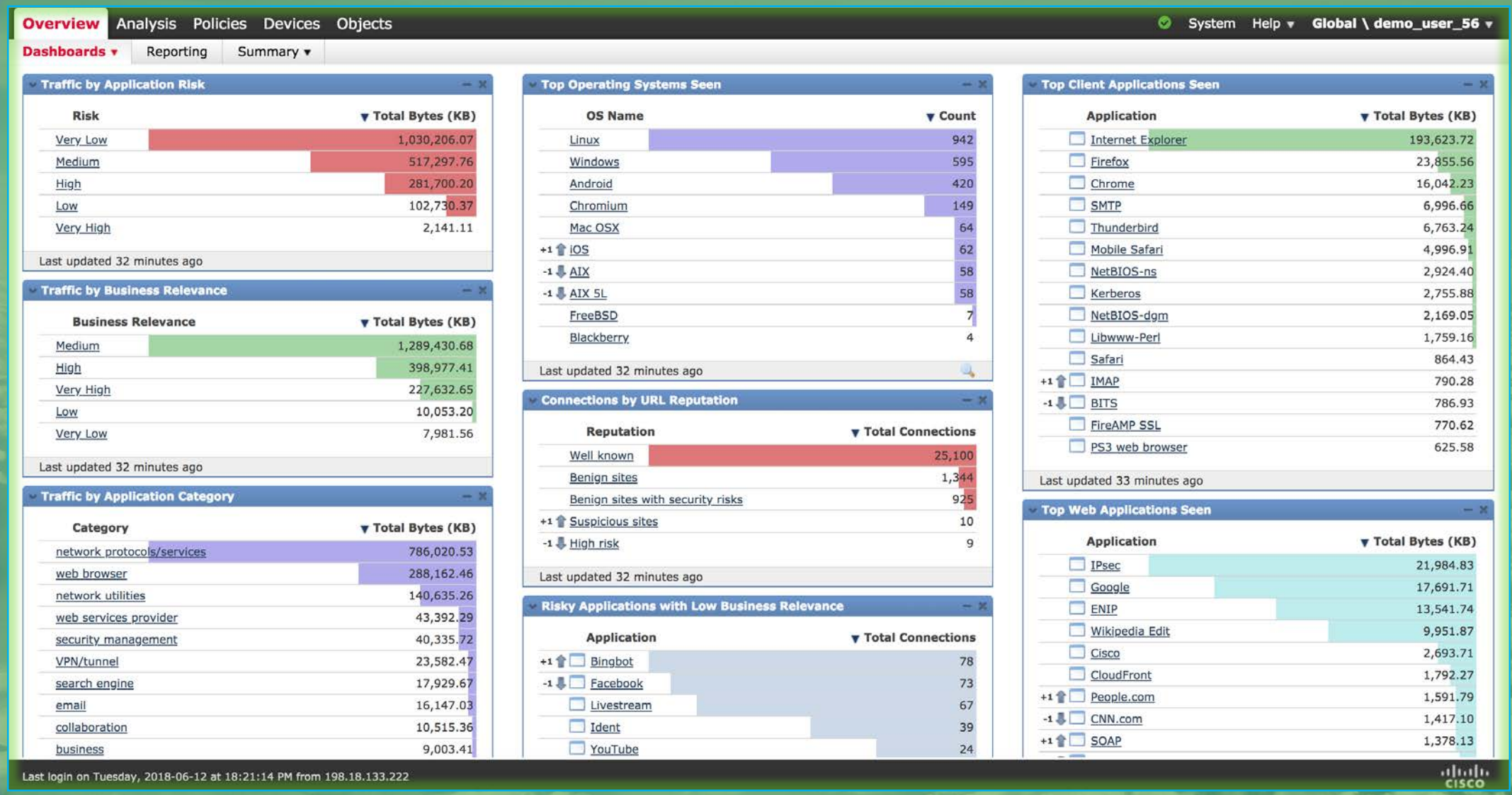
Speed Impact Assessment and Response

Attack Impact Level

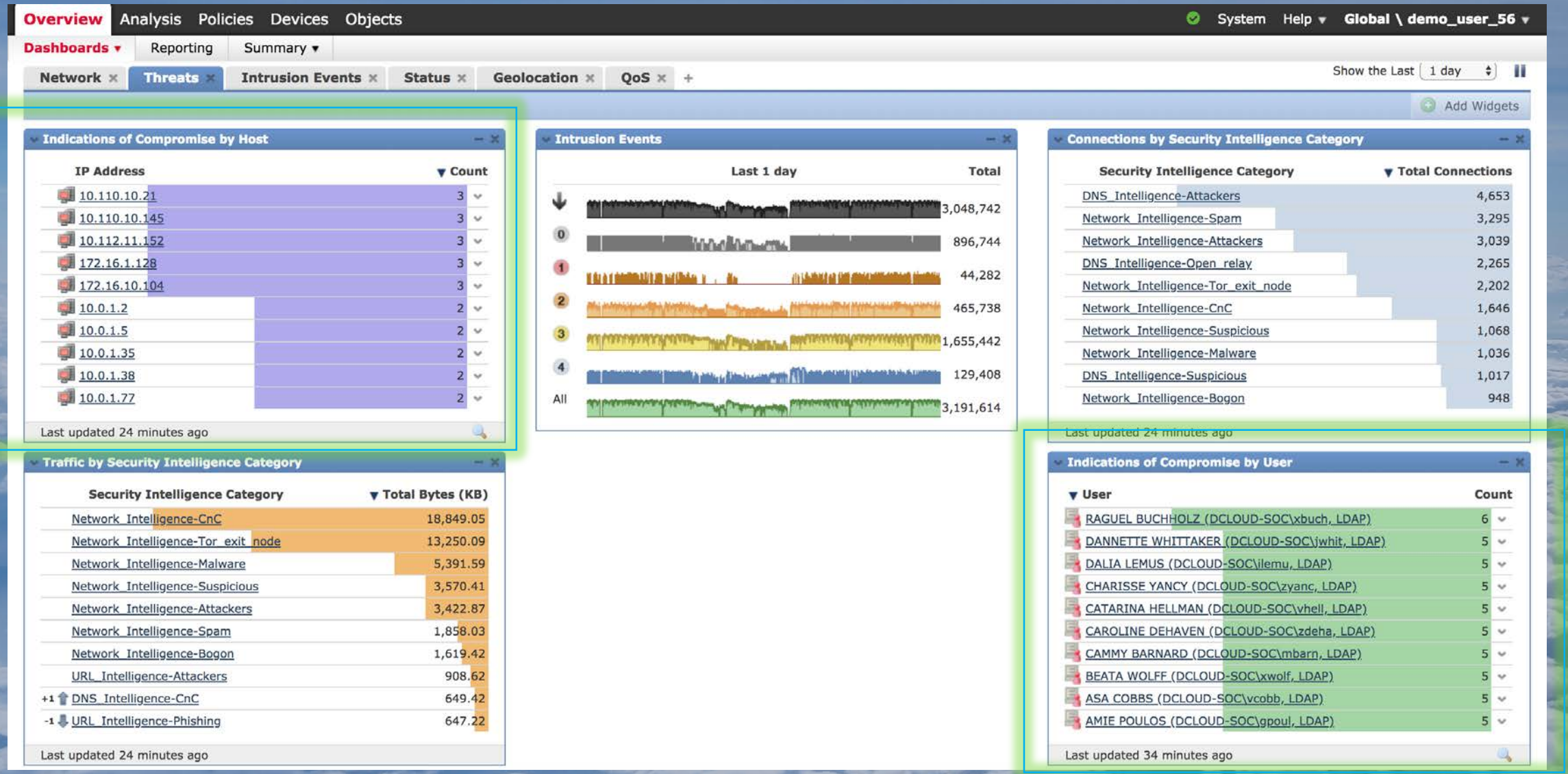
Time	Priority	Impact	Inline Result	Source IP	Source Country	Destination IP	Destination Country
2016-06-28 09:54:13	high	2		10.200.1.17		10.200.1.32	
2016-06-28 09:53:11	high	3		192.168.1.7		74.125.228.53	USA
2016-06-28 09:52:43	high	4		72.21.91.109	USA	192.168.3.7	
2016-06-28 09:52:13	high	2		10.200.1.17		10.200.1.196	
2016-06-28 09:52:06	high	2		10.200.1.17		10.200.1.124	
2016-06-28 09:51:22	high	2		10.200.1.17		10.200.1.41	
2016-06-28 09:51:16	high	2		10.200.1.17		10.200.1.162	
2016-06-28 09:48:51	high	4		10.0.202.63		10.0.68.120	
2016-06-28 09:48:51	high	4		10.0.30.124		10.0.30.91	
2016-06-28 09:48:44	high	3		255.255.255.255		10.112.10.86	
2016-06-28 09:48:40	high	3		192.168.1.7		74.125.26.106	USA
2016-06-28 09:47:24	high	2		10.0.247.133		10.0.121.57	
2016-06-28 09:47:24	high	3		10.131.12.106		10.0.68.66	
2016-06-28 09:47:24	high	2		10.0.247.133		172.16.0.166	
2016-06-28 09:47:24	high	3		10.0.228.118		10.0.57.4	
2016-06-28 09:46:34	high	4		10.0.57.137		10.110.10.31	
2016-06-28 09:46:34	high	4		172.16.0.15		10.0.95.22	
2016-06-28 09:45:09	high	3		10.200.1.244		209.87.214.208	USA

Application Protocol	Client	Web Application	IOC	Application Risk			
DNS	DNS			Very Low			
HTTPS	SSL client	Gmail		Medium			
HTTP	Chrome	Web Browsing		Medium			
DNS	DNS			Very Low			
DNS	DNS			Very Low			
DNS	DNS			Very Low			
DNS	DNS			Very Low			
HTTP	Firefox	Web Browsing		Medium			
HTTP	Firefox	Web Browsing		Medium			
HTTP	Firefox	Web Browsing		Medium			
HTTPS	SSL client	Google		Medium			
HTTP	Firefox	Web Browsing	Triggered	Medium	Medium	Zone B	Zone A
HTTP	Firefox	Web Browsing		Medium	Medium	Zone B	Zone A
HTTP	Firefox	Web Browsing	Triggered	Medium	Medium	Zone B	Zone A
HTTP	Firefox	Web Browsing		Medium	Medium	Zone B	Zone A
HTTP	Firefox	Web Browsing		Medium	Medium	Zone B	Zone A
HTTP	Firefox	Web Browsing		Medium	Medium	Zone B	Zone A

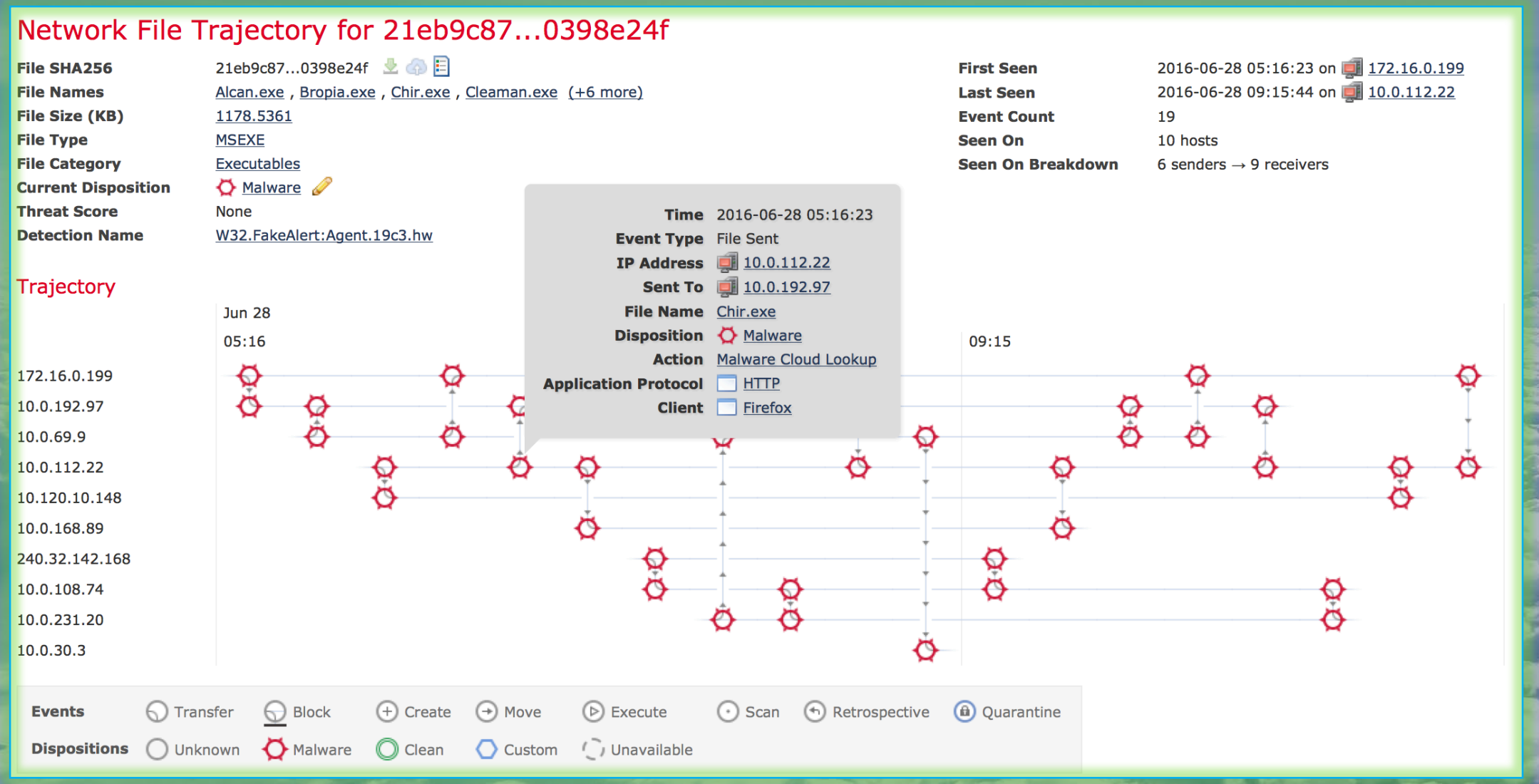
FMC – Visibility & Risk top apps, user, threats & customize



FMC – auto generated IoCs for both: User and machine

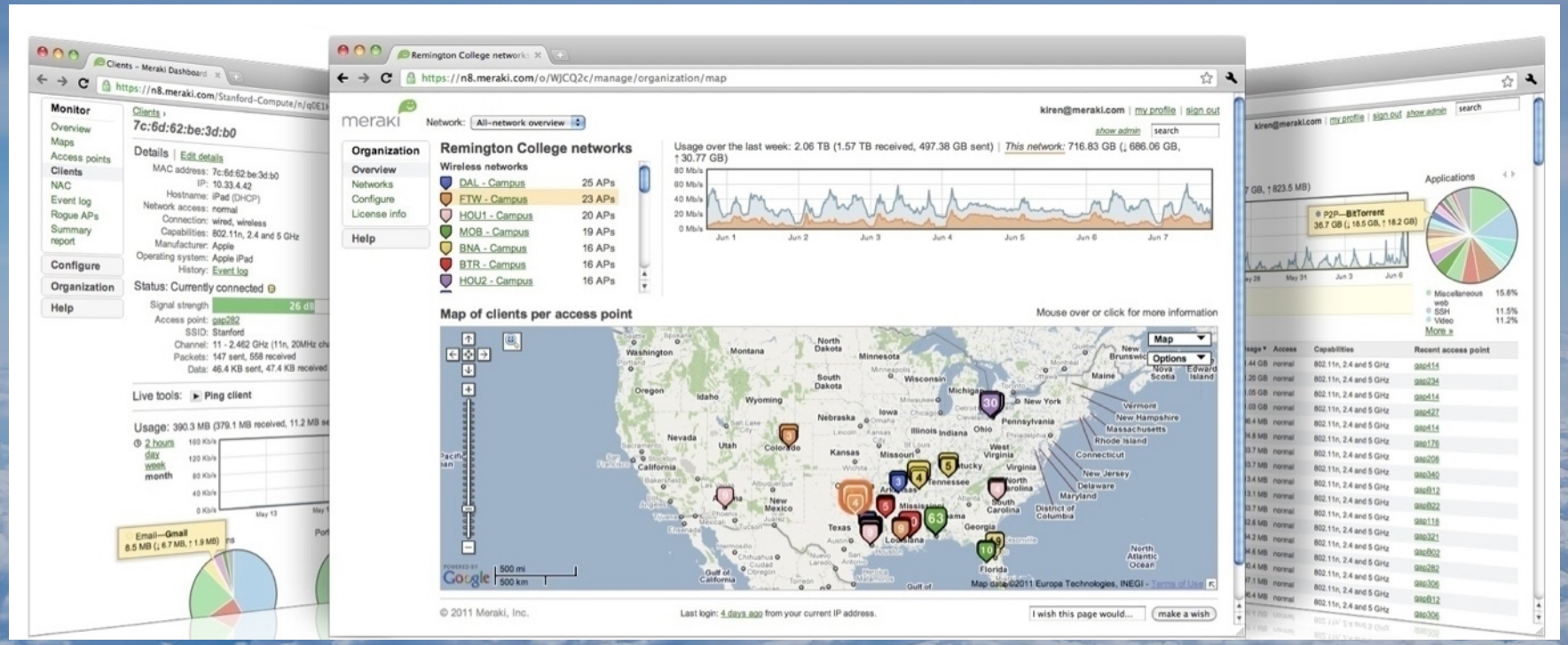


FMC – tracking malware with File Trajectory



Meraki
Fully Cloud Managed
Network & Security

Cisco Meraki: Bringing the cloud to enterprise networks



Meraki MR
Wireless LAN

Meraki MS
Ethernet Switches

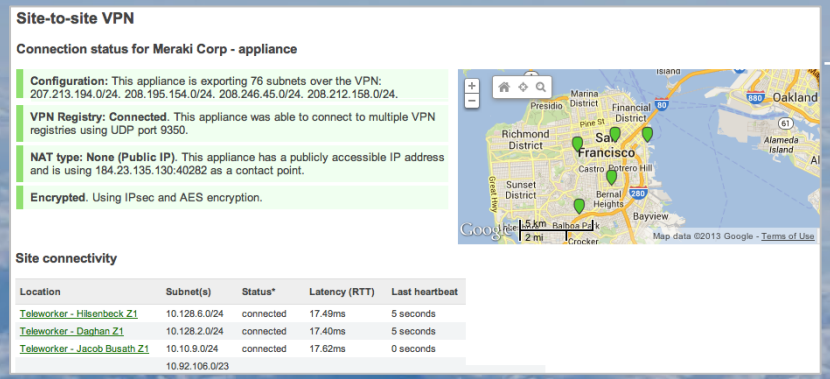
Meraki MX
Security Appliances

Meraki SM
Mobile Device
Management

Why customers choose the Cisco Meraki MX

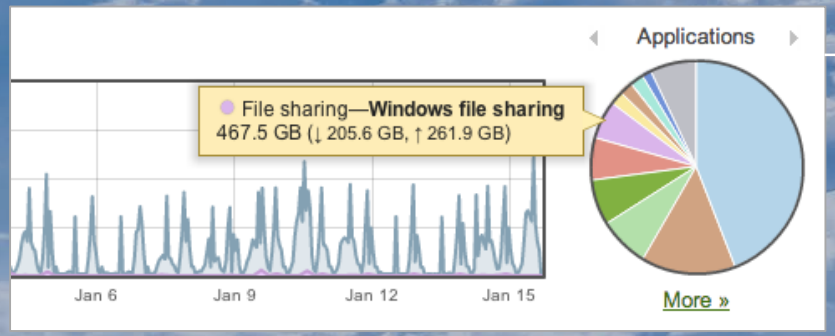
Intuitive centralized management

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



Designed for distributed enterprises

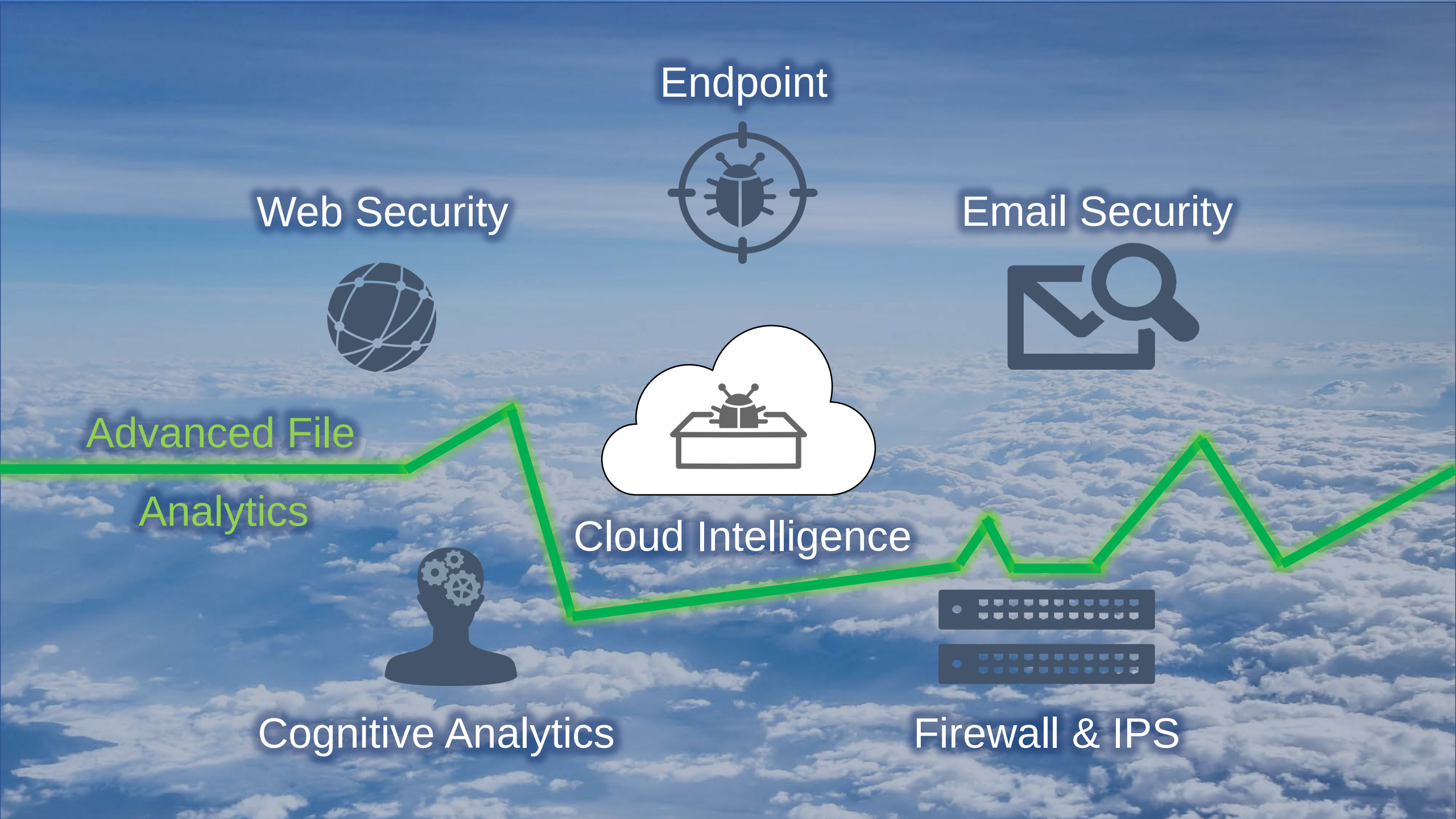
- Single pane of glass visibility
- Zero-touch provisioning
- Seamless updates from the cloud
- Site-to-site IPSec VPN in 3 clicks



Industry-leading visibility

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

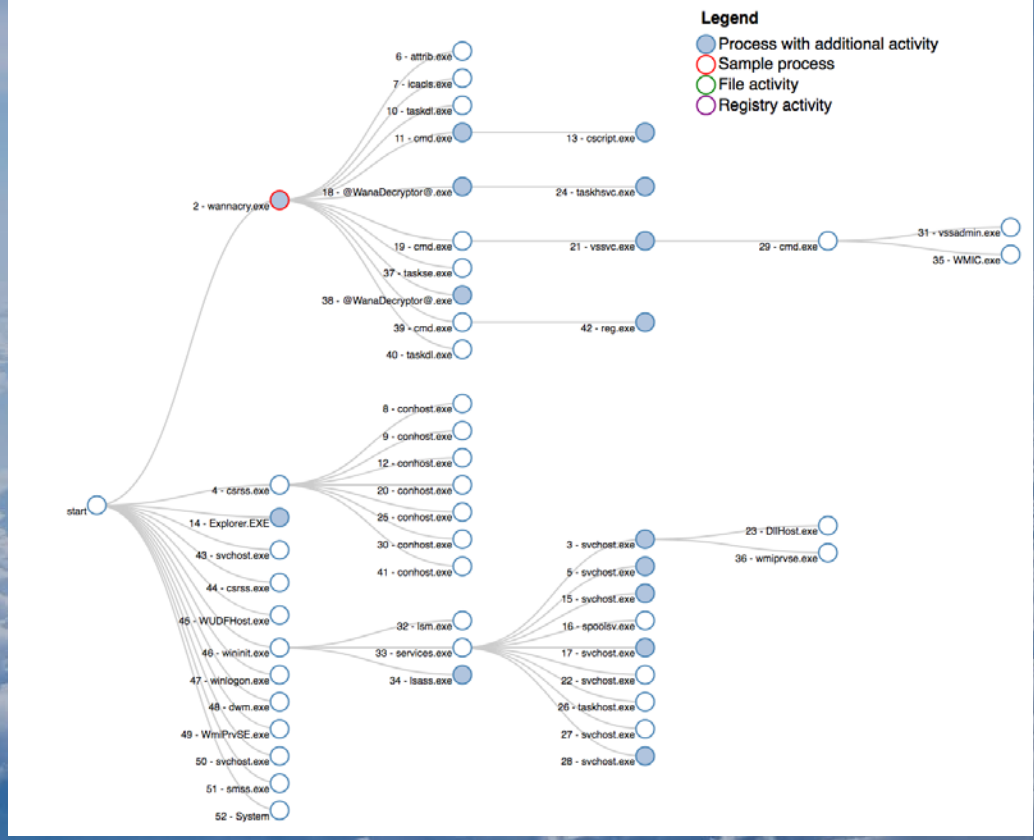
Advanced Malware Protection
with
Cisco AMP Everywhere

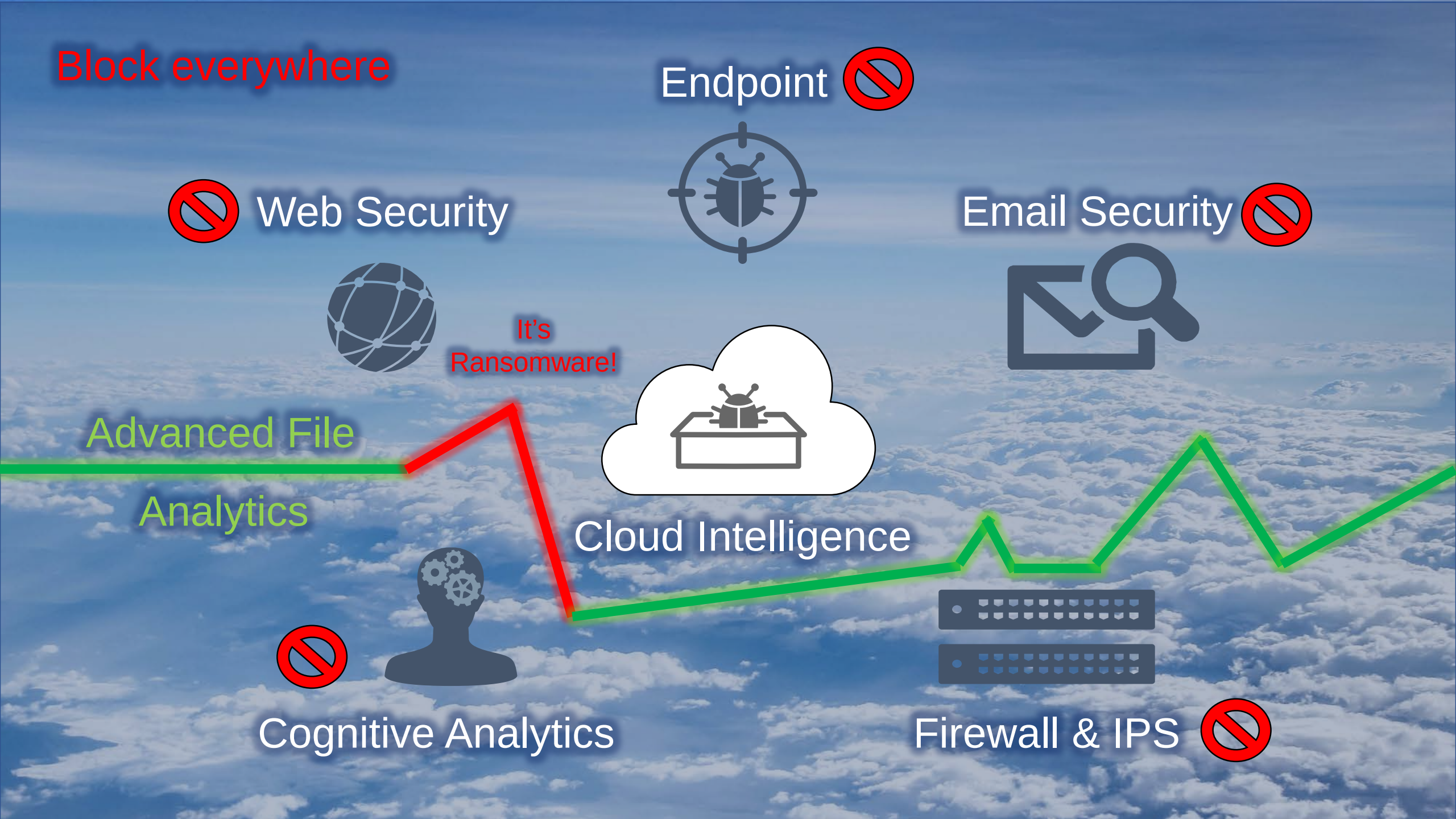

Endpoint
Web Security
Email Security
Advanced File
Analytics
Cloud Intelligence
Cognitive Analytics
Firewall & IPS

	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	Path	Source	Size	Imports	Exports	AV Sigs
+	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	1980-@WanaDecryptor@.exe	memory	245760	200	0	2
+	5	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	1960-taskhsvc.exe	memory	3098624	200	0	0
+	10	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\@Please_Read_Me@.txt	disk	933	0	0	0

Process Tree for Sample 72e42c51b430a9773587d712679f493f




Block everywhere
Endpoint
Web Security
Email Security
It's
Ransomware!
Advanced File
Analytics
Cloud Intelligence
Cognitive Analytics
Firewall & IPS

Mitigate O365 migration risks

with

Cisco Email Security


Email is still the #1 threat vector

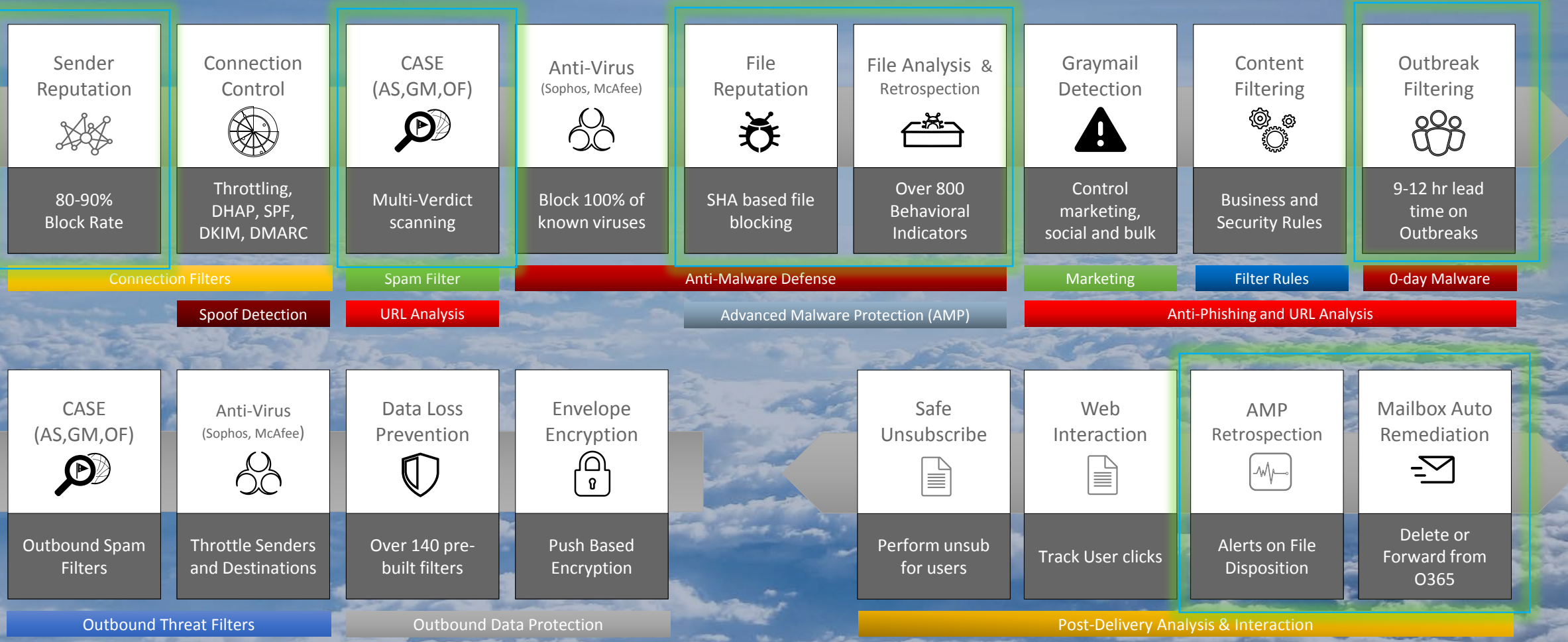
Deploy the configuration that works best for you

Cloud

Hybrid

On Premises

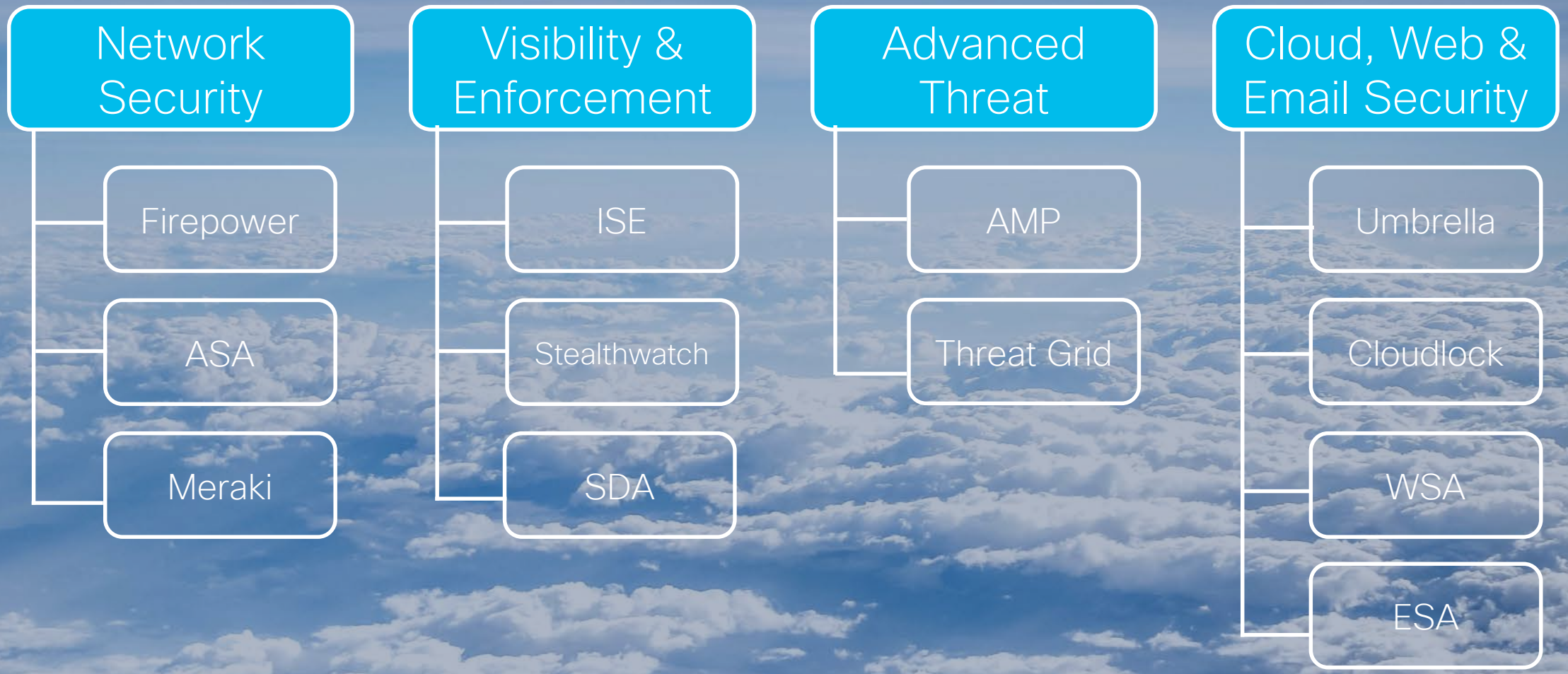
Inbound Security & Outbound Control



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