Co by vás mělo potkat na cestách za kybernetickou bezpečností

Milan Habrcetl, Security account manager, Cisco Systems
ISSS Hradec Králové, 3.4.2017
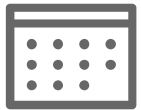
Effective Security

simple | open | automated

The Results Speak for Themselves

~6,5 hours
Median time to detection
with Cisco security

>100 days
Industry median time to detection

Difference between a paperweight and a NGFW?

Threat Intelligence

120TB Security Intelligence	**150,000** Micro-applications	**13B** Web Requests	**5B** Daily Email Connections
1.6M Deployed Devices	**93B** Daily Email Messages	**150M** Deployed Endpoints	**1,000** Applications
19.7B Threats Blocked	**35%** Enterprise Email	**3-5 min** Updates	**4.5B** Daily Email Blocks
1.1M Sandbox Reports	**75,000** FireAMP Updates	**6,000** New Clam AV Sigs	**14M** Deployed Access Gateway

Cisco Security Intelligence
Global Visibility
Global Footprint

Deployed Security Devices
Daily Threats Blocked
Daily Malware
Sandbox Reports

NSS Labs Aug 2016 Breach Detection System Results (Cisco Firepower + AMP)

| Product	Detected < 1 min	Detected < 3 min	Detected < 5 min	Detected < 10 min	Detected < 30 min	Detected < 1440 min
Check Point Software 13500	44.4%	75.9%	86.6%	97.4%	97.9%	99.4%
Cisco Firepower 8120	67.0%	91.8%	96.3%	96.6%	97.1%	100.0%
FireEye NX 10450 and EX 8420	0.6%	2.9%	6.5%	15.2%	85.8%	96.8%
Fortinet FortiGate 500D	48.9%	88.7%	91.0%	95.6%	98.5%	99.4%
Fortinet FortiSandbox-3000D	46.2%	84.2%	88.4%	91.3%	93.1%	99.0%
Lastline Enterprise	5.5%	31.3%	47.8%	85.0%	96.9%	100.0%
Palo Alto Networks 5020 – Inline Mode	7.3%	17.9%	27.6%	43.1%	76.4%	98.9%
Palo Alto Networks 5020 – Tap Mode	6.5%	17.1%	27.0%	42.5%	75.4%	90.1%
Trend Micro Deep Discovery 4000	3.6%	26.7%	66.2%	90.1%	94.0%	99.8%

Figure 5 — Breach Detection over Time (II)

Competitive Threat Intelligence Comparison

	TALOS	Palo Alto Networks (AutoFocus)	Check Point (ThreatCloud)	Fortinet (FortiGuard)
Unique Malware Samples/Daily	1.5M per day	10s of Thousands per day	10s of Thousands per day	10s of Thousands per day
Email Messages Analyzed/Daily	93B per day (86% are SPAM)	none	Not reported	6M SPAM Signatures/day
Total Threats Blocked Daily	19.6B per day	Not reported: Likely 1000s	700K per day	Not Reported
Categorized Web Blocks	4.3B per day	Millions per day	Not reported	35M per day
Threat Data Processed	120TB/day - 3.6PB per month (CWS)	Not reported	Not reported	31TB/Day/900TB per month
Contributing Users/Sensors	150M (AC/AMP)/1.6M (IPS)	1000s	1000s of Gateways	Not Reported
Cost	Free with Product	$35K per Seat	Free with Product	FortiGuard Subscription

CISCO

Our Integrated Approach is Unique
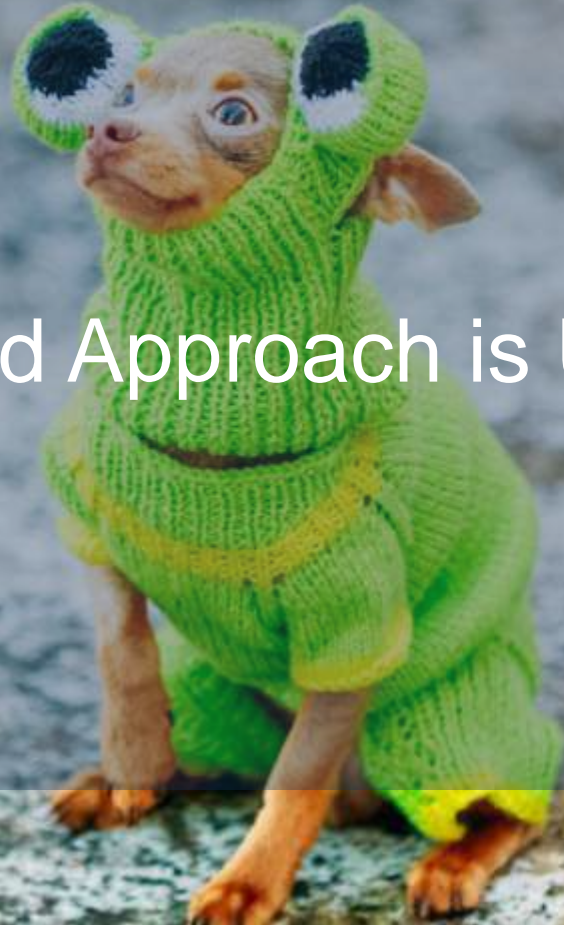
Our Architecture is Game-Changing

Cisco Security is Leapfrogging the Market

Simple, Effective, Integrated & Open Security

CISCO

Thank you.