



Cyber-Security

58. Lunch-Forum der asut

Philipp Müller
March 23rd 2018



Philipp & Security

Wanted to become security expert after ETH studies

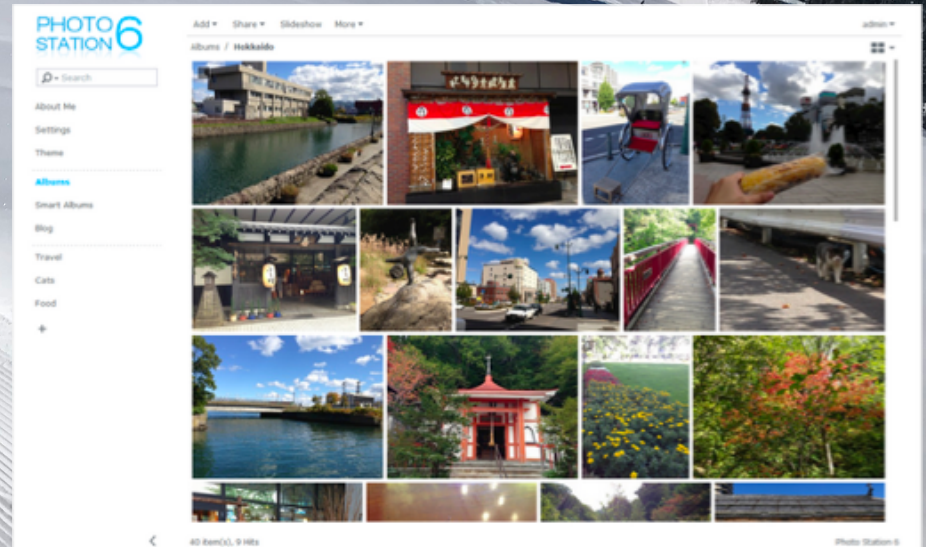
Wanted to launch 1st residential security service

Pre-Sales, IT Infra Ops Director, Sales Mgr

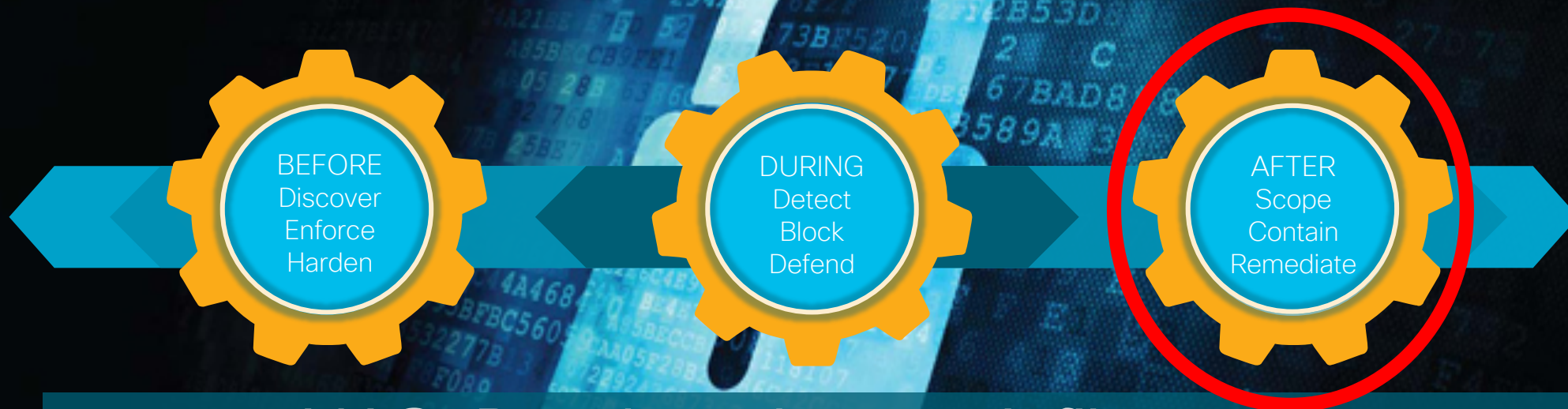




How can this happen?
How can you fix this?







NAS, Dropbox, Laptop infiltrated?

Format everything and setup from scratch?

How to come to a conclusion?






Products & Services / Security /

Advanced Malware Protection (AMP)

Breach prevention. Continuous monitoring of malicious behavior. Rapid malware detection. Malware removal.

AMP in 4 minutes

Compare us with others

-  Free Scan
-  Instant Demo
-  Webcast
-  Contact Us





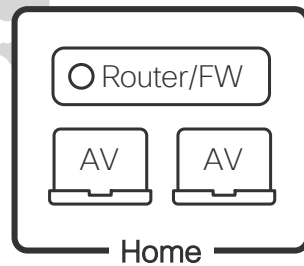
80/20 Rule

Why add Security at the DNS layer?



Malware
C2 Callbacks
Phishing

It all starts with DNS



Benefits

Block malware before it hits

Contains malware if already inside

Used by all devices

Port agnostic

Internet access is faster



IMPORTANT: Employee Communities on Jive is moving to a new platform at the end of Q3. [Learn more to prepare.](#)

More documents by [Justin Hang](#) | Appears in 7 other places.

[Share](#) [Actions](#)

Requesting Umbrella Demo Accounts for Cisco Employees

Like • 38 Comment • 8

Document created by [Justin Hang](#) on May 4, 2016 • Last modified by [Jason Phelps](#) on Aug 31, 2017

Version 34

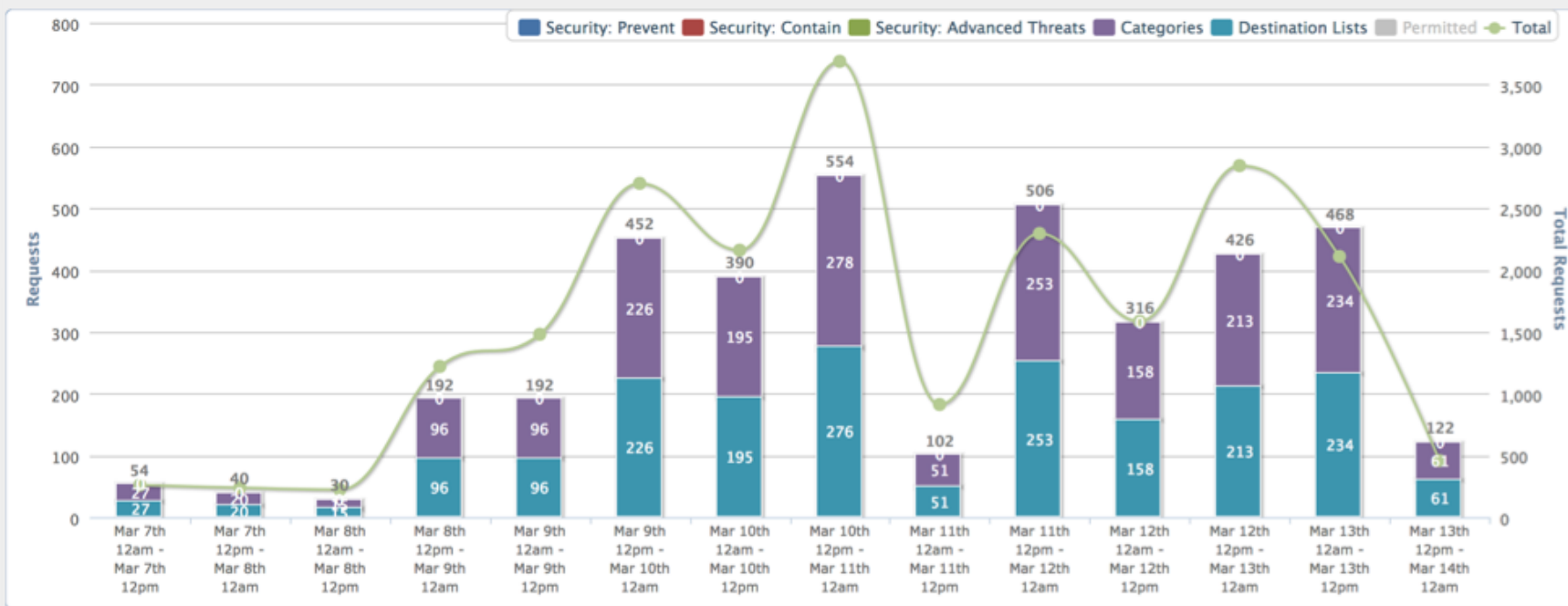




Message Center

Malware: 0 requests blocked in the last 24 hours [View Trend](#) | [View Details](#)

Command and Control: 0 requests blocked in the last 24 hours [View Trend](#) | [View Details](#)



All Requests

18.3K

↑ 110%

8k

All Blocked Requests

2

↑ 100%

4

All Security Events



OpenDNS is now part of Cisco

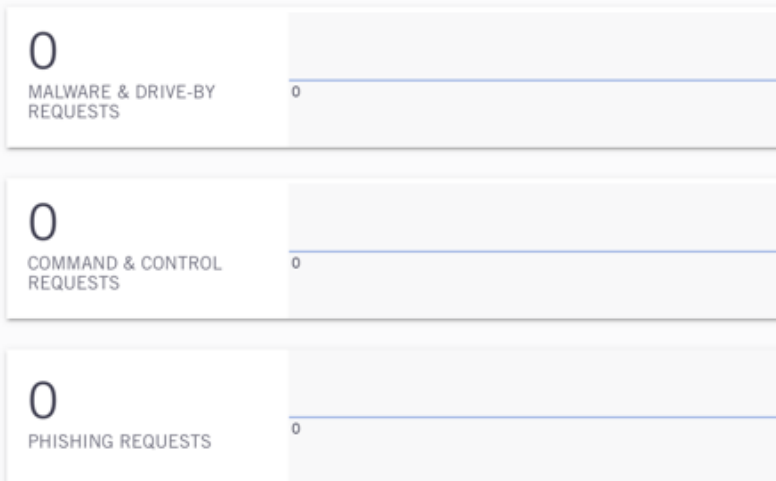


[Sign in to Umbrella](#)

Last 24 Hours Security Report

MAR 12 – MAR 13, 2018

In the last 24 hours, we've protected you from:



Top Security Events

BY DOMAIN		
Domain	Requests	Identities
No data for this period		



Cloud Services



Gain visibility into the cloud services being used across your organization, identify usage patterns, and uncover shadow IT.

All Identities - Last 7 Days (UTC+01:00 [Change time zone](#)) - All Classifications

32

Cloud Services

5

Never Before Seen

1

Total Identity Count

Find a Cloud Service Hide

Service Name:

SHOW SERVICE DETAILS

Filter Cloud Services

Filter by Identity:

Filter by date:

Filter by Classification: SELECT >

RUN REPORT

Name	Classification	Identities	Trend	Requests	Blocked	First Seen	Last Seen
Dropbox	File Sharing, Collaboration	1	– 0	485	0%	Feb. 15, 2018	Mar. 13, 2018
Apple iCloud	Cloud Data Services	1	– 0	304	0%	Feb. 14, 2018	Mar. 13, 2018
Gmail	Communication, Cloud Data Services	1	– 0	156	0%	Feb. 14, 2018	Mar. 13, 2018
Google Docs	Collaboration, Content Sharing	1	– 0	84	0%	Feb. 15, 2018	Mar. 13, 2018
Spotify	Social Media	1	– 0	60	0%	Feb. 15, 2018	Mar. 13, 2018
Cisco Webex	Web Conferencing, Collaboration	1	– 0	54	0%	Feb. 15, 2018	Mar. 13, 2018
Amazon	Cloud Data Services, Storage	1	– 0	47	0%	Feb. 15, 2018	Mar. 12, 2018
Twitter	Social Media, Messaging	1	– 0	43	0%	Feb. 15, 2018	Mar. 13, 2018
Facebook	Social Media, Communication	1	– 0	40	0%	Feb. 15, 2018	Mar. 13, 2018
Google Drive	Storage, File Sharing	1	– 0	37	0%	Feb. 15, 2018	Mar. 13, 2018
LinkedIn	Social Media, Collaboration	1	↑ 1	28	0%	Feb. 16, 2018	Mar. 13, 2018
Box	Content Sharing, File Sharing	1	– 0	20	0%	Feb. 18, 2018	Mar. 13, 2018
Google Analytics	Data & Analytics, Tracking	1	– 0	20	0%	Feb. 15, 2018	Mar. 13, 2018
Chartbeat	Data & Analytics, Tracking	1	– 0	20	0%	Feb. 15, 2018	Mar. 13, 2018

Youtube	Social Media, Content Sharing	1	— 0	15	0%	Feb. 15, 2018	Mar. 13, 2018
Foursquare	Social Media	1	— 0	7	0%	Feb. 16, 2018	Mar. 12, 2018
MS OfficeLive	Collaboration	1	— 0	5	0%	Feb. 19, 2018	Mar. 13, 2018
Evernote	Business Management, Productivity	1	↑ 1	5	0%	Feb. 20, 2018	Mar. 10, 2018
Gigya	CRM & SFA	1	↑ 1	5	0%	Feb. 19, 2018	Mar. 10, 2018
IFTTT	Productivity	1	↑ 1	4	0%	Feb. 15, 2018	Mar. 09, 2018
Instagram	Social Media	1	↑ 1	3	0%	Feb. 15, 2018	Mar. 12, 2018
New Relic	Business Management, Data & Anal...	1	↑ 1	2	0%	Feb. 19, 2018	Mar. 12, 2018
Netflix	Media	1	— 0	2	0%	Feb. 15, 2018	Mar. 09, 2018
Office 365	Content Sharing, Cloud Data Servic...	1	↑ 1	2	0%	Feb. 20, 2018	Mar. 10, 2018
Salesforce	CRM & SFA	1	↑ 1	1	0%	Mar. 10, 2018	Mar. 10, 2018
SumoLogic	IT Services, Data & Analytics	1	↑ 1	1	0%	Mar. 09, 2018	Mar. 09, 2018
OneDrive	Cloud Data Services, Storage	1	↑ 1	1	0%	Mar. 12, 2018	Mar. 12, 2018
Mixpanel	Data & Analytics	1	↑ 1	1	0%	Mar. 10, 2018	Mar. 10, 2018
AddThis	Data & Analytics, Tracking	1	↑ 1	1	0%	Feb. 17, 2018	Mar. 09, 2018
SurveyMonkey	Data & Analytics	1	↑ 1	1	0%	Mar. 13, 2018	Mar. 13, 2018
Cedexis	Tracking	1	↑ 1	1	0%	Feb. 19, 2018	Mar. 09, 2018

With Cisco Umbrella



Discover
3M+
daily new
domain names

Identify
60K+
daily malicious
destinations

Enforce
7M+
malicious destinations
while resolving DNS

91%
of C2 can be blocked
at the DNS layer

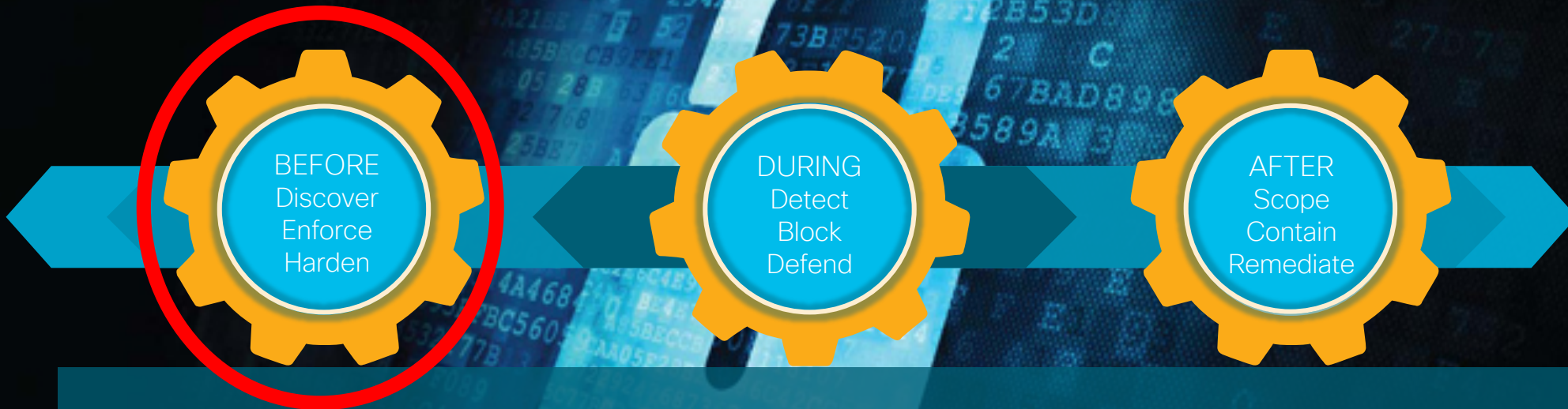
91% of command & control
traffic uses DNS



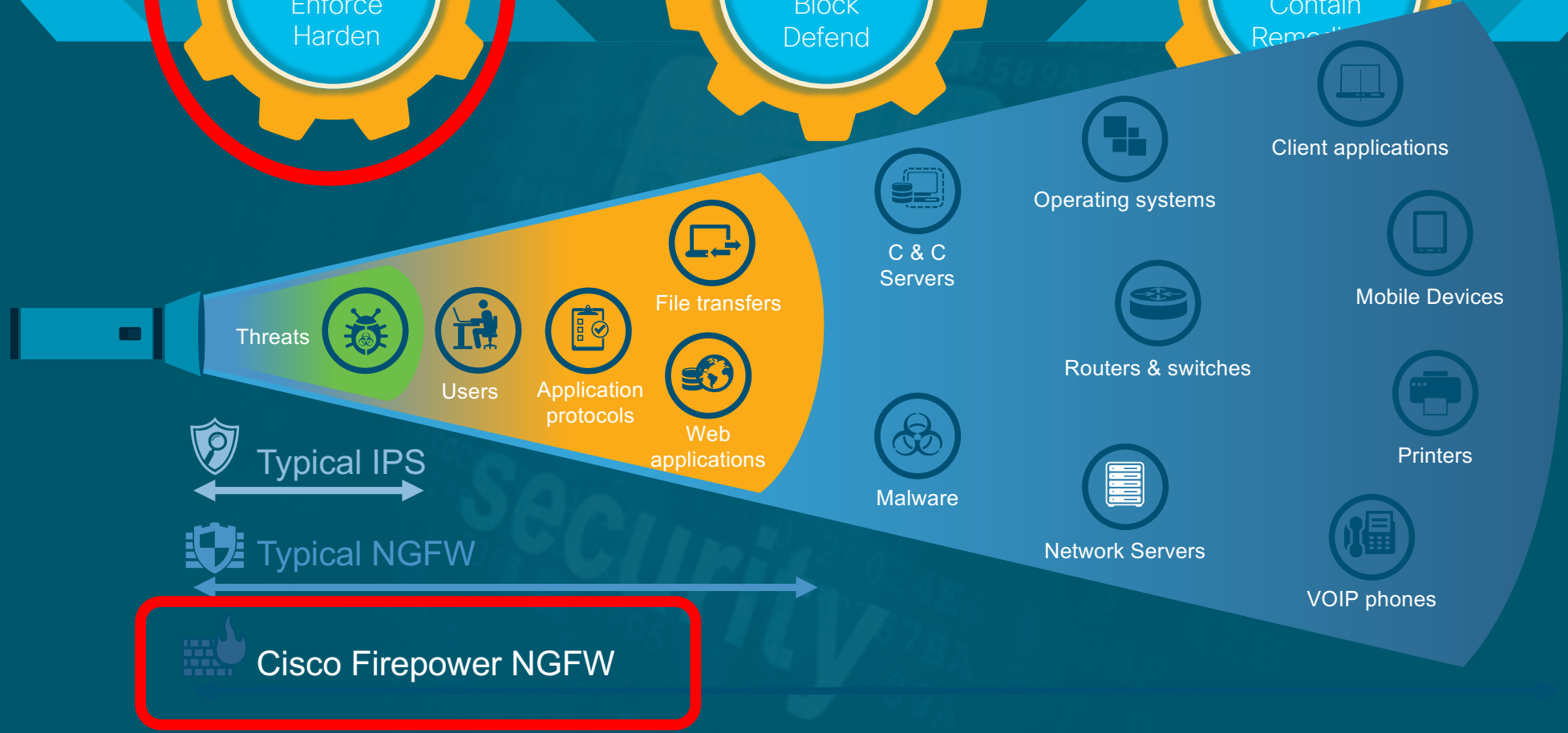
85% of Threats ✓



Chase the remaining 15%



What about files?





Meraki

Your cart
0 Items



[Home](#) [Product Categories](#) ▾ [Licenses](#) [Blog](#) [FAQ and Help](#)

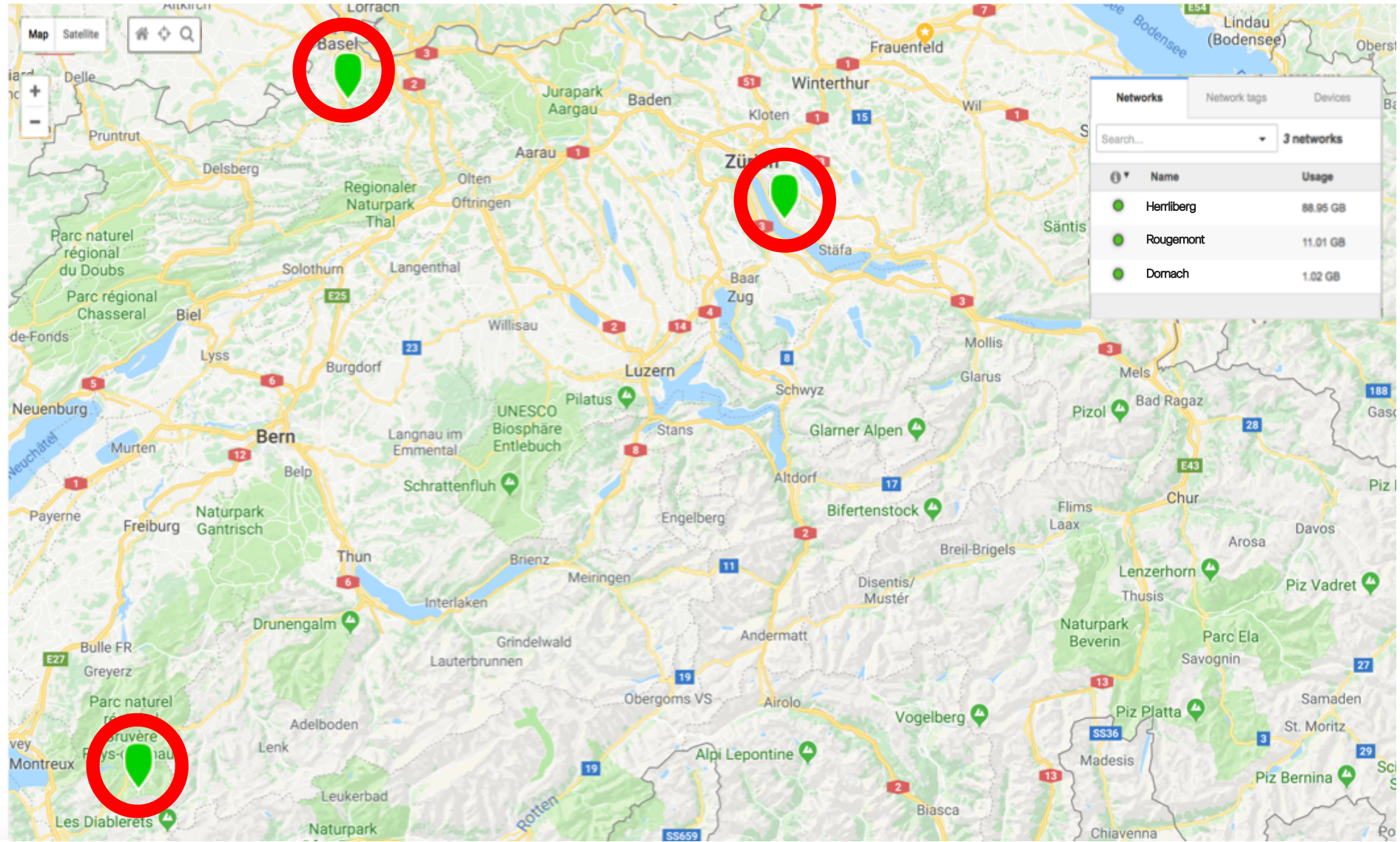
[Login](#)



Welcome to the Cisco employee purchase program for Cisco Meraki gear

You must be a Cisco employee to purchase from the program. To request access, please send an email to epp-registration@meraki.com from your cisco.com or meraki.com address.

- NETWORK
- Herrliberg
- Network-wide
- Security appliance
- Switch
- Wireless
- Organization





Meraki

Your cart
0 Items



[Home](#) [Product Categories](#) [Licenses](#) [Blog](#) [FAQ and Help](#)

[Login](#)

MX64

This MX64 is recommended for a small clinic (approx. 50 users).

Cisco Meraki MX Security Appliances provide quality network infrastructure. Since the MX is 100% cloud managed, management is simple. The M

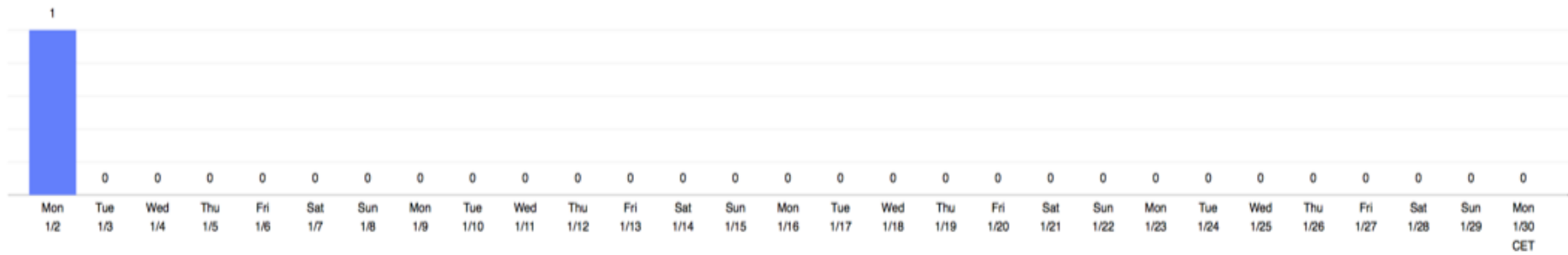
Welcome to the Cisco employee purchase program for Cisco Meraki gear

You must be a Cisco employee to purchase from the program. To request access, please send an email to epp-registration@meraki.com from your cisco.com or meraki.com address.

[Filter ▾](#) 1 matching event

Summary [Events](#)

Events over time



Most affected clients

Client	Network	Last Affected	Events
PHMUELLE-M-R1NT Mac OS X 10.10	Herrliberg	Jan 2 23:40:44	1

Most prevalent threats

Threat	Occurrences
BROWSER-IE Microsoft Internet Explorer create-add range on DOM objects memory corruption attempt	1

Most affected operating systems

OS	Events
Mac OS X 10.10	1

Top sources of threats



- NETWORK
- Herrliberg ▾
- Network-wide
- Security appliance
- Switch
- Wireless
- Organization

DHCP

Main subnet *192.168.1.0/24* ⓘ

Client addressing

Run a DHCP server

Lease time

1 day

DNS nameservers

For DHCP responses

Use OpenDNS

Boot options ⓘ

Boot options disabled

Boot next-server ⓘ

Boot filename ⓘ

Threat protection

Advanced Malware Protection (AMP)

Mode ⓘ

Enabled ▾

Whitelisted URLs ⓘ

There are no whitelisted URLs.

[Add a whitelisted URL](#)

Whitelisted files

There are no whitelisted files.

[Add a whitelisted file](#)

Intrusion detection and prevention

Mode ⓘ

Detection ▾

Ruleset ⓘ

Balanced ▾

Whitelisted rules ⓘ

There are no whitelisted IDS rules.

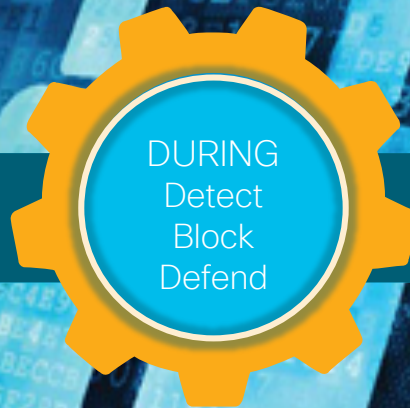
[Whitelist an IDS rule](#)

or [cancel](#)

(Please allow 1-2 minutes for changes to take effect.)



BEFORE
Discover
Enforce
Harden



DURING
Detect
Block
Defend



AFTER
Scope
Contain
Remediate

Umbrella
Malware
Ransomware
C2 Callbacks
Phishing

NGFW:
malicious file
protection





A massive cyberattack knocked out major websites across the internet



Kif Leswing
Oct 21, 2016

Forbes [LOG IN](#)

YOUR READING LIST



Hacked Cameras Were Behind Friday's Massive Web Outage

UNICEF USA *Voice*: For Moms And Babies, A Milestone

The Limit Does Not Exist: Carol Lynn Curchoe Is A STEM Warrior Princess

+7 comments in the last 24 hours

A Physicist Talks God And The Quantum

OCT 21, 2016 @ 04:10 PM 90,673 VIEWS

The Little Black Book of Billion

Hacked Cameras Were Behind Friday's Massive Web Outage



Brian Solomon, FORBES STAFF

Covering technology and the on-demand economy. [FULL BIO](#)



I Know . . .
"Our users ha
the freedom
analyze any r
on their own

Bernard Hakim
Business Intelligence Analyst | Worldline

[worldline](#) [I Know >](#)

[Get the F](#)

Internet users
but mostly in
that some top
loading on Fr

The affected s
Amazon, Twi
Github, and S

It was mostly

Internet of Things Security

TELECOM TV

IoT Security Spending compared to Device Growth

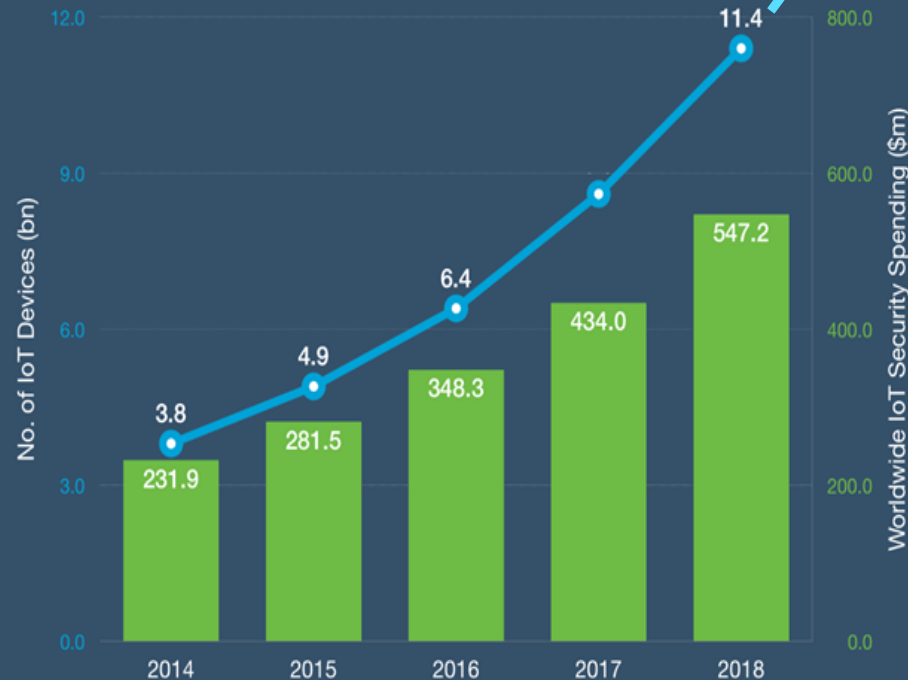
Data: Gartner, various Graphic: TelecomTV

By 2020

25%
of Enterprise attacks
will involve IoT

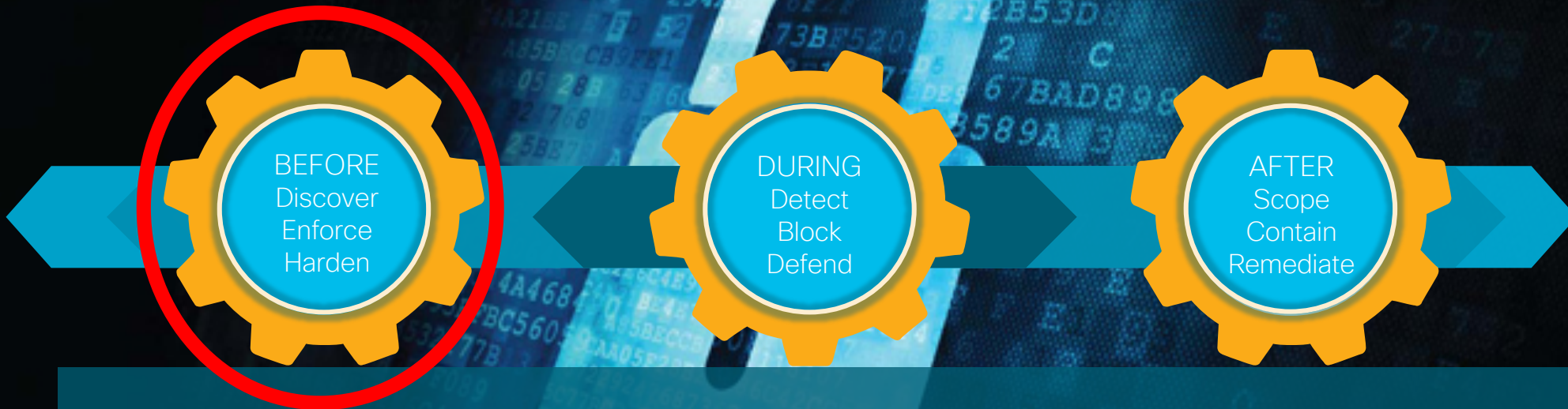
10%
of IT security budgets
allocated to IoT

50%
of IoT implementations
will use Cloud security



50bn Devices

70%
vulnerabilities



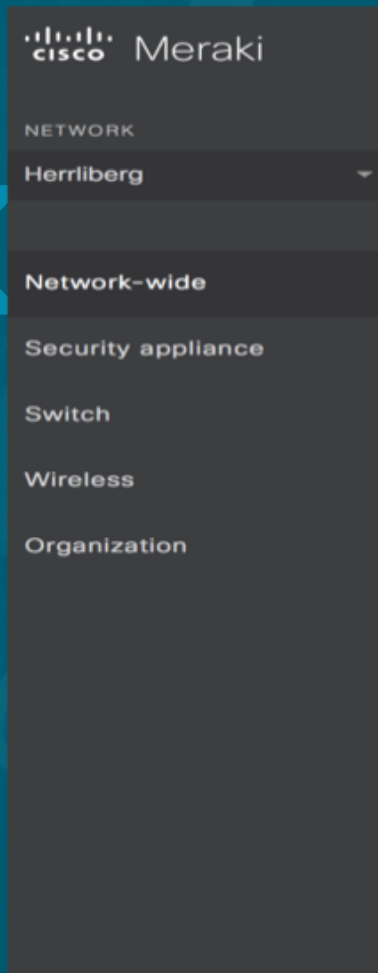
What about IoT security?



The Network sees Everything!

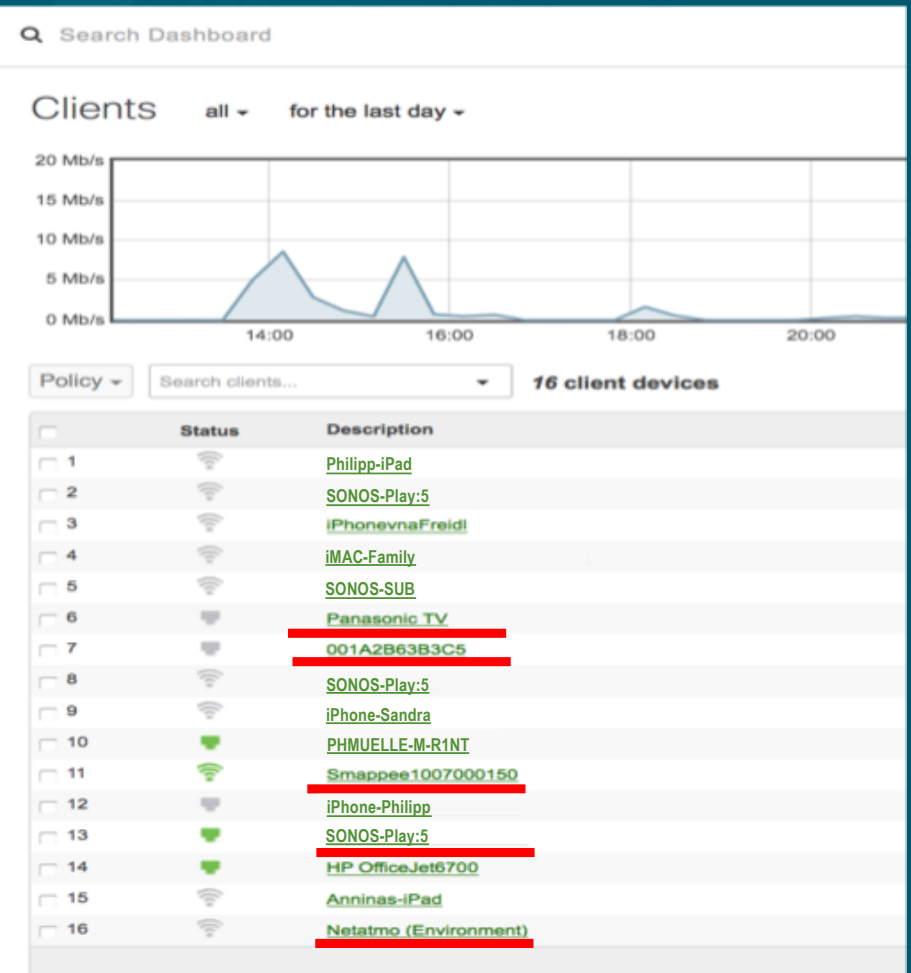


BEFORE
Discover
Enforce
Harden



CISCO Meraki

- NETWORK
- Herrliberg
- Network-wide
- Security appliance
- Switch
- Wireless
- Organization



Search Dashboard

Clients all for the last day

20 Mb/s
15 Mb/s
10 Mb/s
5 Mb/s
0 Mb/s

14:00 16:00 18:00 20:00

Policy Search clients... 16 client devices

	Status	Description
<input type="checkbox"/>	📶	Philipp-iPad
<input type="checkbox"/>	📶	SONOS-Play:5
<input type="checkbox"/>	📶	iPhonevnaFreidl
<input type="checkbox"/>	📶	iMAC-Family
<input type="checkbox"/>	📶	SONOS-SUB
<input type="checkbox"/>	📶	Panasonic TV
<input type="checkbox"/>	📶	001A2B63B3C5
<input type="checkbox"/>	📶	SONOS-Play:5
<input type="checkbox"/>	📶	iPhone-Sandra
<input type="checkbox"/>	📶	PHMUELLE-M-R1NT
<input type="checkbox"/>	📶	Smappee1007000150
<input type="checkbox"/>	📶	iPhone-Philipp
<input type="checkbox"/>	📶	SONOS-Play:5
<input type="checkbox"/>	📶	HP OfficeJet6700
<input type="checkbox"/>	📶	Anninas-iPad
<input type="checkbox"/>	📶	Netatmo (Environment)

Securing IoT



BEFORE
Discover
Enforce
Harden

- 1) Find all devices
- 2) Assign them into the right IoT Segment
- 3) Find the Public Address of Server
- 4) Permit access to that Address and block all the rest



**Strong need
for automating
the
segmentation**

Hospital FACTS:

- 90'000 none IT devices
- vs 25'000 IT devices
- None-IT growing dramatically
- 150'000 “foreign users” access
- 2'100 “foreign” companies



BEFORE
Discover
Enforce
Harden

DNA Center

Secure | https://dcloud-dna-sda-rtp.cisco.com/dna/policy/home?st-host_policy=virtual_network

DESIGN POLICY PROVISION ASSURANCE

Dashboard Virtual Network Policy Administration Contracts Registry

EQ Find Virtual Network +

DEFAULT_VN (24)
INFRA_VN (0)
IoT (2)

Create or Modify Virtual Network by selecting Available Scalable Groups. Reset

Virtual Network Name*
IoT Guest Virtual Network ⓘ

Available Scalable Groups

EQ Find Scalable Group Show Unselected ▾

AC ACI_Ap pServer	AC ACI_We bServer	AP Access Point	AS Airport_ Security...	BY BYOD
BA Baggag e	CO Contract ors	DE Develop ers	DS Develop ment_S...	DO Doctor
EM EMR	FI Finance	GU Guest	NU Nurse	PC PCI_Ser vers
PO	PS	PU	QS	ST

Groups in the Virtual Network

EQ Find Scalable Group

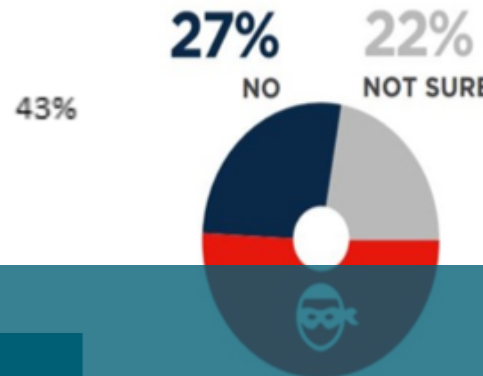
HV HVAC	LI Lights
------------	--------------



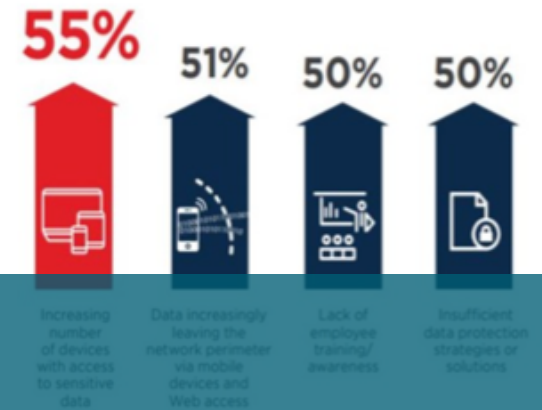
4% 1%

INSIDER THREATS ON THE RISE

Q: Do you think insider attacks have generally become more frequent over the last 12 months?



Q: What do you believe are the main reasons why insider attacks are on the rise?



How to handle internal Threats?

~40 unknown Clients a Year!



Meraki

NETWORK
Rougemont

Network-wide
Security appliance
Switch
Wireless
Organization

4 Mbit/s
0 Mbit/s

Jan 03 Jan 06 Jan 09 Jan 12 Jan 15 Jan 18 Jan 21 Jan 24

Policy Search clients... 26 client devices

	Status	Description	Last seen	Usage *	OS
1	📶	Swisscom Router	Jan 22 09:50	205.62 GB	Other
2	📶	TV-Box-efeca3322b1e0111	Jan 22 09:50	24.89 GB	Other
3	📶	Felix-iPad	Jan 30 08:47	8.94 GB	Apple iPad
4	📶	Caspers-MacBook-Pro	Jan 22 17:23	3.60 GB	Mac OS X 10.12
5	📶	iPhonevonfelix2	Jan 30 08:48	2.37 GB	Apple iPhone
6	📶	iPad-von-Ursula	Jan 30 12:45	2.20 GB	Apple iPad
7	📶	Caspers-iPhone	Jan 22 18:04	771.6 MB	Apple iPhone
8	📶	iPad-von-Merki	Jan 29 17:57	667.1 MB	Apple iPad
9	📶	Leonies-iPhone	Jan 22 18:07	531.7 MB	Apple iPhone
10	📶	Marions-iPhone	Jan 22 18:02	460.4 MB	Apple iPhone
11	📶	DESKTOP-4OC53BN	Jan 29 08:46	329.2 MB	Windows 10
12	📶	android-417d874f896ca1d	Jan 30 12:49	287.5 MB	Android
13	📶	ThinkPad	Jan 17 09:39	222.4 MB	Windows 7/Vista
14	📶	Dell	Jan 22 18:06	156.0 MB	Apple iPad
15	📶	iPad-von-Ursula	Jan 07 16:33	117.1 MB	Apple iPad
16	📶	Samsung-Caroline	Jan 22 18:08	86.0 MB	Apple iPad
17	📶	iPhone-Philipp	Jan 22 17:10	56.5 MB	Mac OS X 10.10
18	📶	Reto-iPad	Jan 22 18:04	48.5 MB	iOS
19	📶	Hanspeter-Merki	Jan 29 18:06	34.2 MB	Apple iPhone
20	📶	HP DeskJet	Jan 22 18:07	20.1 MB	Apple iPhone
21	📶	Access Point Keller	Jan 27 11:02	18.3 MB	Other
22	📶	Christians-iPad	Jan 22 18:07	1.5 MB	Apple iPad
23	📶	Willa-iPhone	Jan 24 08:56	429 KB	Apple iPhone
24	📶	ThinkPad	Jan 17 09:37	165 KB	Windows
25	📶	iPhone-Sandra	Jan 22 09:45	165 KB	Meraki
26	📶	9021:81:07:b0:5f	Jan 16 10:22	None	Other

Segmentation: Guestnet



BEFORE
Discover
Enforce
Harden

Meraki

NETWORK
Herrliberg

Network-wide
Security appliance
Switch
Wireless
Organization

Search Dashboard

Configuration overview

SSIDs Showing 4 of 15 SSIDs. [Show all my SSIDs.](#)

	PhilippNetz	PhilippGuests
Enabled	<input type="checkbox"/> enabled	<input type="checkbox"/> enabled
Name	rename	rename
Access control	edit settings	edit settings
Encryption	WPA2-PSK	Open
Sign-on method	None	Password-protected w
Bandwidth limit	unlimited	unlimited
Client IP assignment	Local LAN	Meraki DHCP
Clients blocked from using LAN	n/a	no
Wired clients are part of Wi-Fi network	no	no
VLAN tag	n/a	n/a
VPN	Disabled	Disabled
Splash page		
Splash page enabled	no	yes
Splash theme	n/a	Modern

Zerotouch



BEFORE
Discover
Enforce
Harden

Welcome to PhilippGuests

Grüezi und herzlich willkommen im PhilippGastnetz. Für freien Internet Zugang bitte das Wifi Passwort eingeben welches beim Telefon im Wohnzimmer oder im Büro gut ersichtlich aufliegt.

You will need to be on the list of authorized users for this network in order to access the Internet.


EMAIL

PASSWORD

Sign In

[I forgot my password](#)

POWERED BY

 Meraki



BEFORE
Discover
Enforce
Harden



DURING
Detect
Block
Defend



AFTER
Scope
Contain
Remediate

Umbrella

Malware
Ransomware
C2 Callbacks
Phishing



NGFW

malicious file
protection



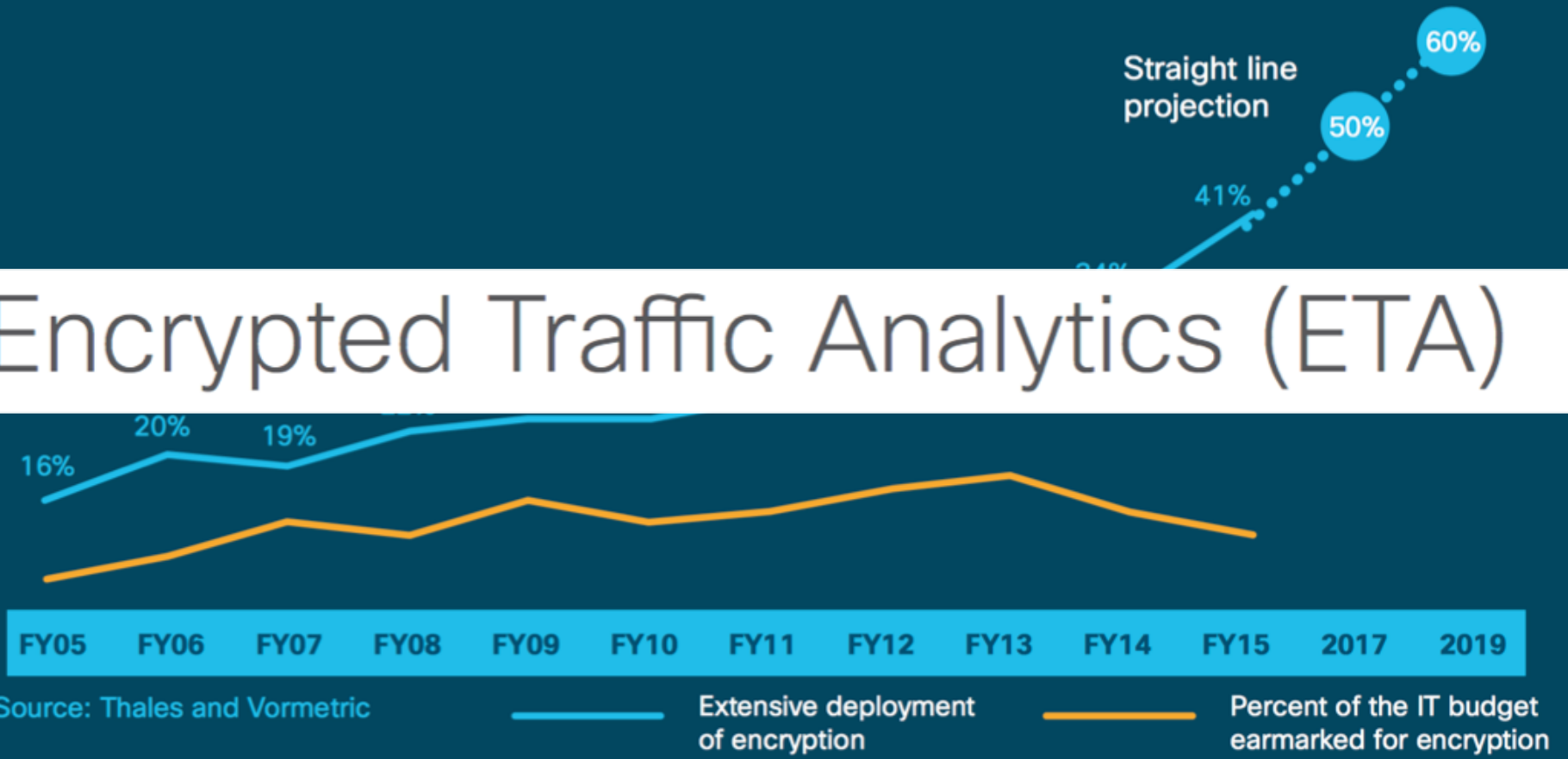
Segmentation TrustSec

IoT Security
Guest Access



Encryption is changing the threat landscape

Encrypted Traffic Analytics (ETA)



Source: Thales and Vormetric

Extensive deployment of encryption
Percent of the IT budget earmarked for encryption




BEFORE
Discover
Enforce
Harden

Security



 **Meraki** CUSTOMERS PRODUCTS SOLUTIONS PARTNERS JOBS



Systems Manager


Cloud Based Enterprise Mobility Management



Security

Cisco Security Connector: Built for iOS 11



 **AMP for Endpoints** 🔔 ? Ciro Pizzo

Dashboard Analysis Outbreak Control **Management** Accounts

Deploy Clarity for iOS (beta)

Group

ios [Download Profile](#)



Umbrella

Malware
Ransomware
C2 Callbacks
Phishing



NGFW

malicious file
protection



**Segmentation
TrustSec**

IoT Security
Guest Access



AMP Everywhere

Files
Endpoint security
Trajectory



Philipp & Security

Cisco Systems, Inc.

NASDAQ: CSCO - 13. März, 11:30 GMT-4

45,64 USD ↑0,09 (0,20 %)

1 Tag

5 Tage

1 Monat

3 Monate

1 Jahr

5 Jahre

Max



Eröffnung	45,78
Hoch	46,16
Tief	45,56

Marktkap.	219,80 Mrd.
KGV	-
Rendite	2,89%



