

ATHENS 17<sup>TH</sup> APRIL 2019

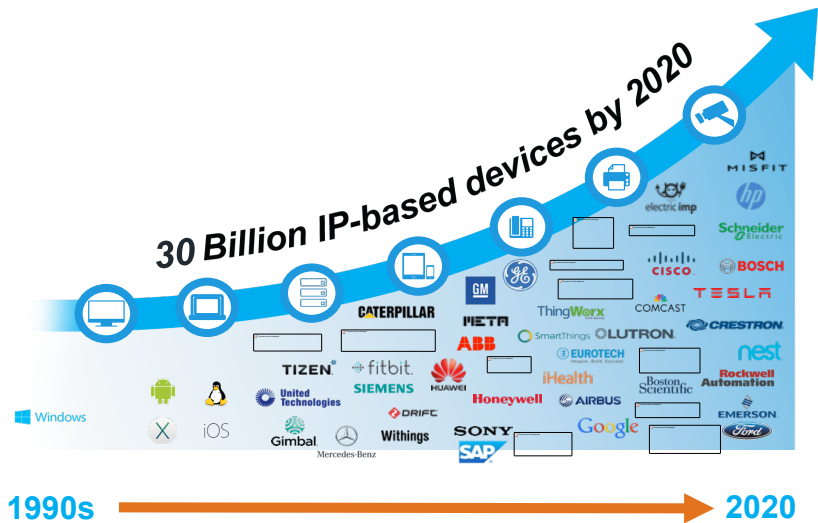
SECURITY IN THE IOT AND OT ERA:  
**DEVICE VISIBILITY  
AND CONTROL**

**Enrico Rossi**  
Regional Sales Manager  
[enrico.rossi@forescout.com](mailto:enrico.rossi@forescout.com)



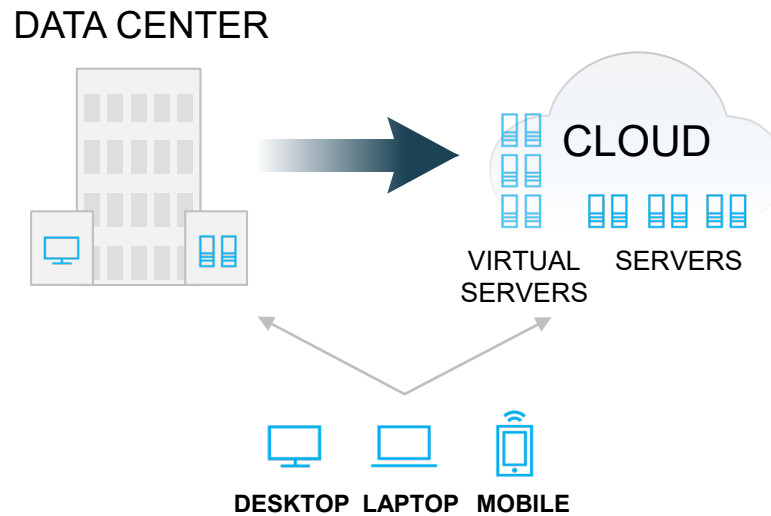
# Three Trends That Make Your Next Breach Inevitable

## Growth of Devices & Platform Diversity



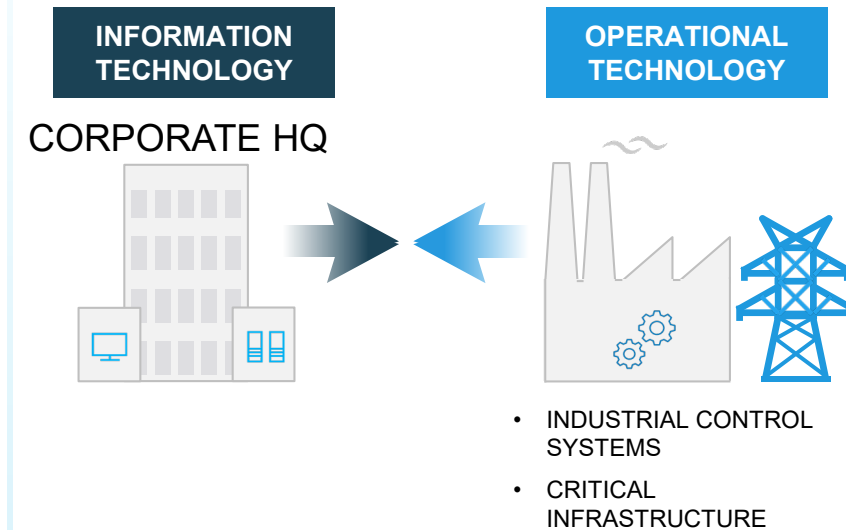
- < Innumerable device-specific operating systems (OS)
- < Cannot get agents onto new devices
- < Cannot write agent-based software for every OS

## Cloud Adoption Creates New Challenges



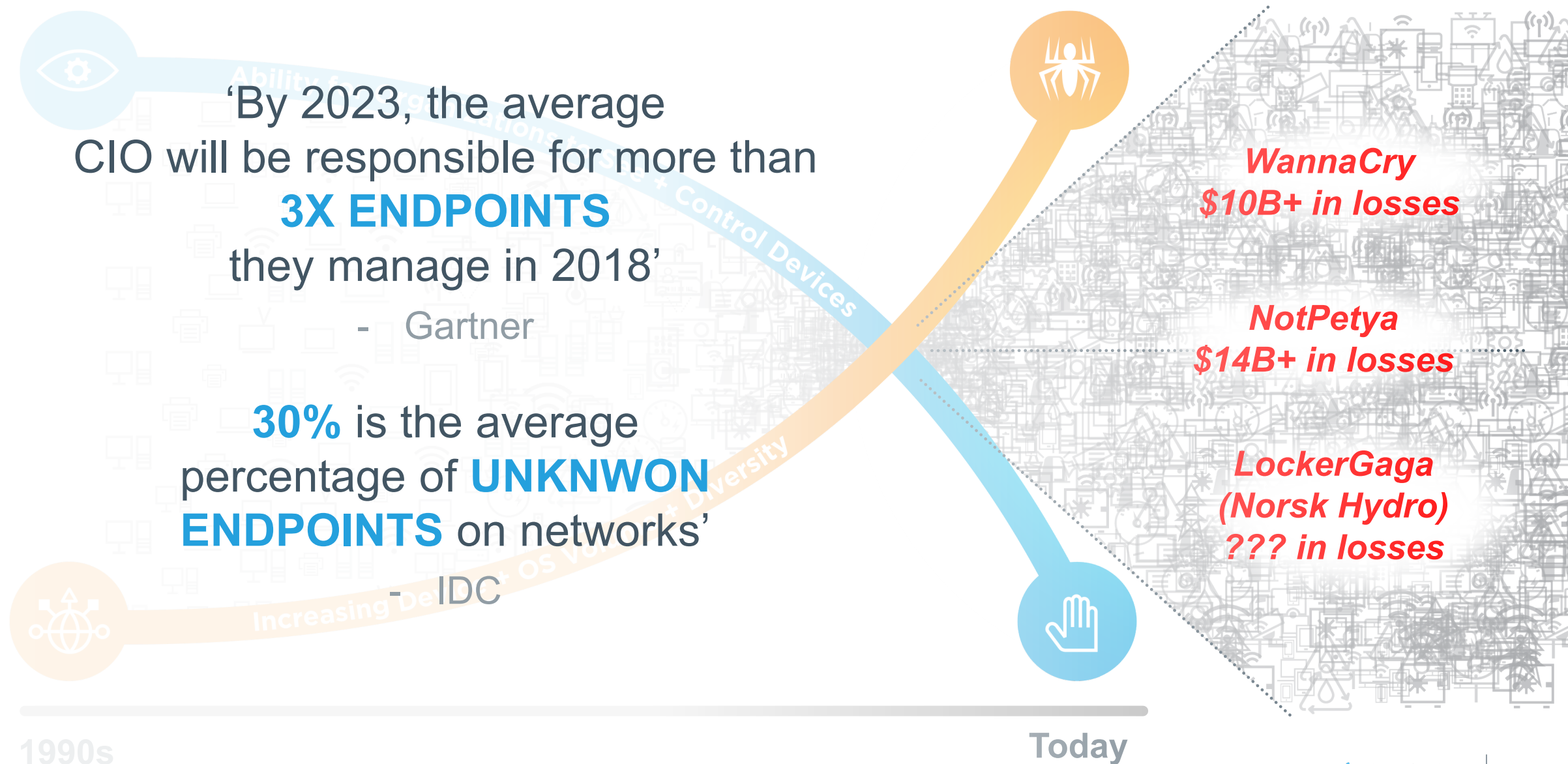
- < Multiple Device Locations and Access Points
- < Heterogeneous Environment with Multiple Vendors
- < De-centralized Management

## OT Convergence With IT Heightens Risk



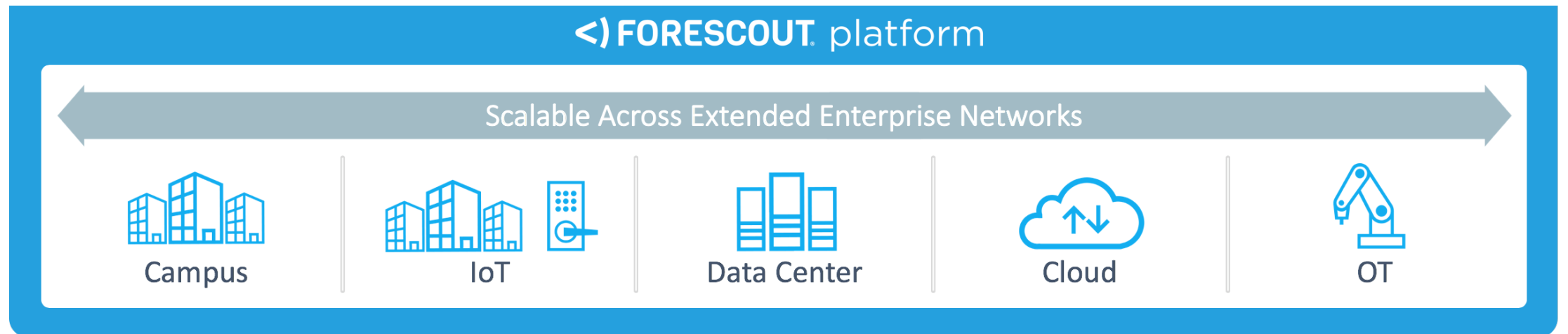
- < OT networks are no longer physically separated
- < Threats moving between cyber & physical dimensions
- < Assets are highly vulnerable & rarely can be patched

# Device Visibility and Control: It's Everyone's Problem, and It's Getting Worse



# Forescout's Mission

## 100% Devices Visibility and Control





DEVICE  
VISIBILITY

# Here's How We Let You See 100% of What's on Your Network

## What We Do

**DISCOVER** all IP-addressable devices at time of connect



Physical



Virtual

**CLASSIFY** every device & categorize appropriately

*IoT*



HuddleCamHD

*BYOD*



HP Elite Tablet  
on Windows 10

*Managed*



Red Hat Linux  
on VMware vSphere

**ASSESS** device posture by



OS



App



Agent



User





DEVICE  
VISIBILITY

# Here's How We Let You See 100% of What's on Your Network

## How We Do It

### Agentless

- <> ✓ No device agents needed
- <> ✓ Intelligently uses passive & active techniques

### Heterogeneous a.k.a. Vendor Agnostic

- <> ✓ Integrate >70 network & security technologies
- <> ✓ Extend beyond campus to IoT, DC, cloud & OT

### Intelligent

- <> ✓ Device Cloud >1K customers contributing to classification
- <> ✓ Comprehensive device taxonomy across IT & OT (Over 100 Protocols in OT Environment)

### Continuous

- <> ✓ Real-time, so no need to schedule scans
- <> ✓ Policy engine constantly evaluates device state to policy

### Adaptive

- <> ✓ Smooth Deployment
- <> ✓ Adaptive Policies (Pre-Connect, Post-Connect etc.)



INCIDENT  
RESPONSE

# You Have to Respond & Remediate Quickly

## ORCHESTRATE

### CMDB/ITSM

servicenow

### SIEM

MICRO  
FOCUS

IBM

splunk>

### VA

RAPID7

Qualys

tenable

### PAM

CYBERARK

### NGFW

paloalto  
NETWORKS

FORTINET

Check Point  
SOFTWARE TECHNOLOGIES LTD.

### NAC

cisco

FORTINET

aruba  
a Hewlett Packard  
Enterprise company

### EDR

Carbon Black. CROWDSTRIKE

### EPP

McAfee

Symantec

### ATD

paloalto  
NETWORKS

FireEye

Check Point  
SOFTWARE TECHNOLOGIES LTD.

### EMM

Microsoft Intune

MobileIron

vmware

IBM

### Micro-segmentation

aws

Microsoft Azure

vmware NSX

cisco

# Forescout – A Trusted Partner

## Visibility

Discover 30% more devices on average

## Orchestration

Increase value of existing investment  
Reduce MTTR with automation

**3300**

Customers in over 80 countries

Across all major industries including  
Government, Financial Healthcare



**FORESCOUT**

**7M+** Device in Device Cloud

**2M+** Devices in a single deployment

**65M** Total Device capacity sold

## Time-to-Value

65 days – average time for visibility roll out

**74**

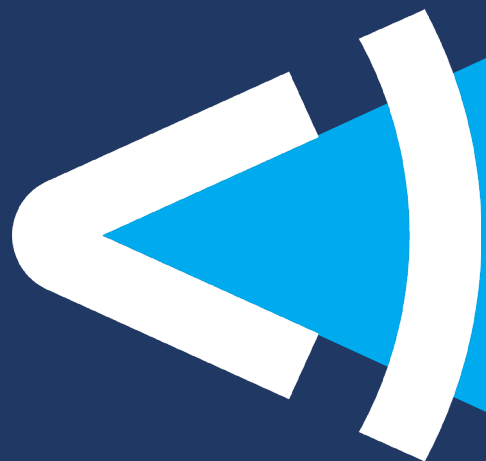
Net Promoter Score  
(above security industry average)





SEE OUR DEMO

17<sup>th</sup> April 2019 h. 15:00 @ D1-A5



THANKS FOR YOUR ATTENTION