



ASMGi



FORESCOUT®

The Evolution Of Cyber Warfare

Defending against persistent and ever-evolving threats

WEBINAR presented by ASMGi and ForeScout

June 20, 2019

The Evolution Of Cyber Warfare – Today's Presenters

Steve Roesing

*President, CEO,
ASMGi*



Tamer Baker

*Principal Systems Engineer of Americas,
ForeScout Technologies, Inc.*





ASMGi is

... a full-stack technology provider headquartered in Cleveland, Ohio.

- IT Services
- GRC / Security Services
- SDLC Services
- Strategic Technology Partners

I am excited about today's webinar for 3 Reasons ...

1. Forescout is a great partner!

2. Content is incredibly relevant and timely

3. Synergies in thinking and approach



Holistic Security is all about ...

1. Identify risks in terms the business understands
2. Leverage frameworks to evaluate yourself and prioritize mitigation strategy
3. Architect an ecosystem = Orchestration & Automation

Risk Assessment with Financial Quantification

NEXT LEVEL OF CYBER RISK MATURITY

Risk Assessment

CIS Controls Help Facilitate CFO / CEO Discussion

Upgrade
The Story
by Financials

Financial Quantification

Bridges to CFO/CEO/CRO/Legal

Basic CIS Controls

— Reported — Tested

#1 Inventory and Control of Hardware Assets



#2 Inventory and Control of Software Assets



#3 Continuous Vulnerability Management



#4 Controlled Use of Administrative Privileges



#5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers



#6 Maintenance, Monitoring and Analysis of Audit Logs



Foundation Controls

#7 Email and Web Browser Protections



#8 Malware Defenses



#9 Limitation and Control of Network Ports, Protocols and Servers



Cyber Attack

Determination of Cyber Event

\$0 <— \$1.5M —> \$12M

\$800K Security Forensics
\$400K Data Restoration
\$150K Financial Forensics

Replacement or Upgrade of Faulty Controls

\$0 <— \$270K —> \$85M

\$120K Hardware Replacement
\$55K Awareness Training
\$50K Additional Staffing

Data Breach

Review of Legal & Regulatory Action

\$0 <— \$100K —> \$6.5M

\$60K Compliance Prep Work
\$15K Legal Counseling

Notification, Credit Monitoring, Credit Restoration

\$0 <— \$765K —> \$42M

\$400K Credit Restoration

Business Interruption

Loss of Gross Profit

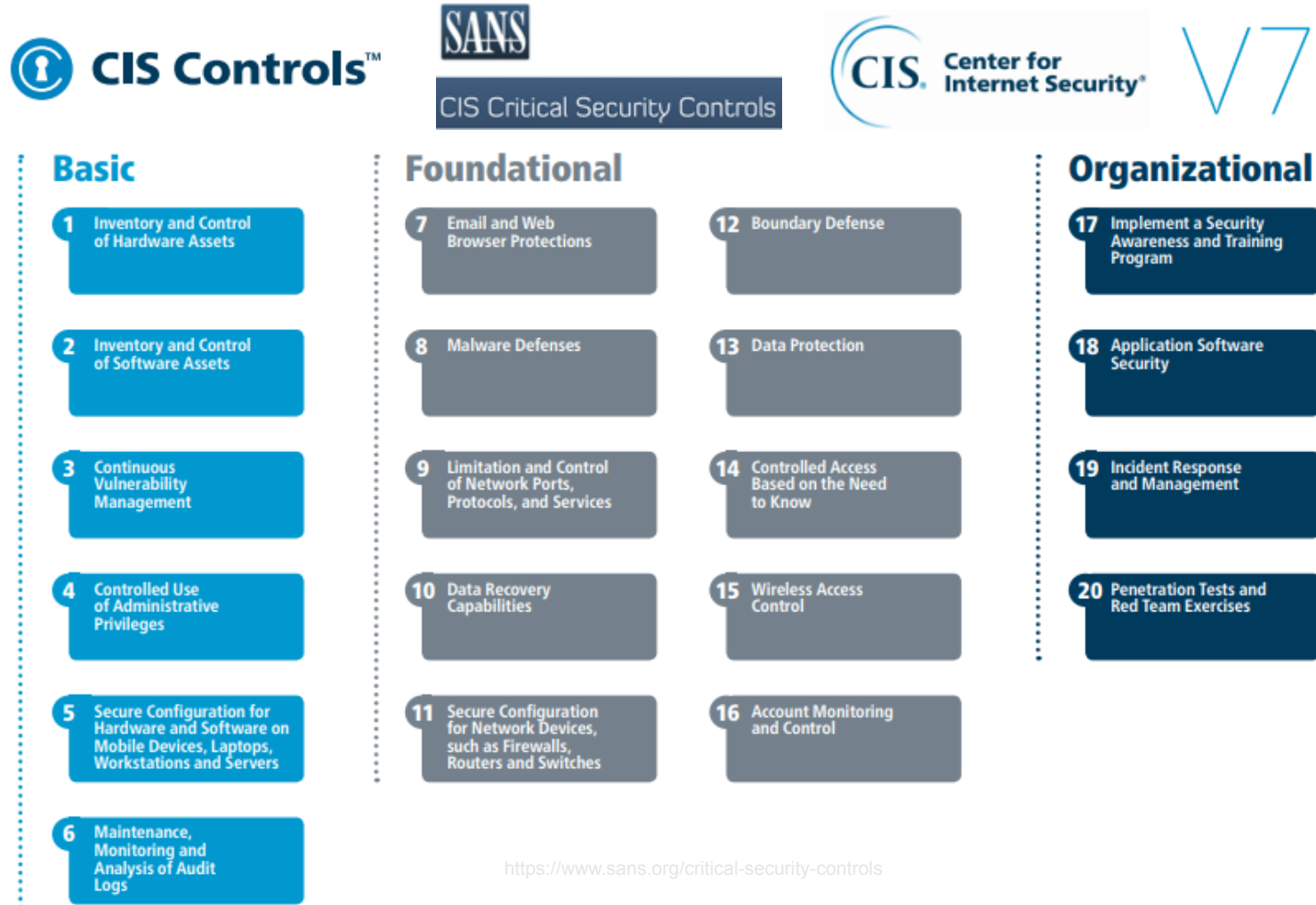
\$0 <— \$850K —> \$105M

\$900K per day Lost Revenue
Analyzed three different portals
Largest expected loss from streaming device

Continuing Costs

\$0 <— \$80K —> \$3.5M

Leverage CIS Controls → What are they



CIS Control 1: Inventory and Control of Hardware Assets

Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

Sub-Controls for CIS Control 1

CIS Control 1: Inventory and Control of Hardware Assets

Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	Implementation Groups		
					1	2	3
1.1	Devices	Identify	Utilize an Active Discovery Tool	Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory.		●	●
1.2	Devices	Identify	Use a Passive Asset Discovery Tool	Utilize a passive discovery tool to identify devices connected to the organization's network and automatically update the organization's hardware asset inventory.			●
1.3	Devices	Identify	Use DHCP Logging to Update Asset Inventory	Use Dynamic Host Configuration Protocol (DHCP) logging on all DHCP servers or IP address management tools to update the organization's hardware asset inventory.		●	●
1.4	Devices	Identify	Maintain Detailed Asset Inventory	Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all assets, whether connected to the organization's network or not.	●	●	●
1.5	Devices	Identify	Maintain Asset Inventory Information	Ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network.		●	●
1.6	Devices	Respond	Address Unauthorized Assets	Ensure that unauthorized assets are either removed from the network, quarantined or the inventory is updated in a timely manner.	●	●	●
1.7	Devices	Protect	Deploy Port Level Access Control	Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.		●	●
1.8	Devices	Protect	Utilize Client Certificates to Authenticate Hardware Assets	Use client certificates to authenticate hardware assets connecting to the organization's trusted network.			●

<https://www>

Saying at ASMGi ...

Action = Results

Upgraded to Saying 2.0 ...

Orchestrated Action = Great Results!

THE EVOLUTION OF CYBER WARFARE...

Defending against persistent and ever-evolving threats

Tamer Baker
Principal Systems Engineer of Americas



A Word About Me

Tamer Baker

Principal Systems Engineer of Americas and Global Public Sector

Responsible for designing customized security solutions for Healthcare, Financial, Education, Commercial and Public Sector customers.

Forescout SE for 5+ years

Forescout customer for several years prior

Specializing in Compliance/Audits/Security Frameworks



A Global Security Leader

- Network Architect and Security Advisor
- 10+ Years Security and Network experience
- Forescout customer for years prior to joining Forescout

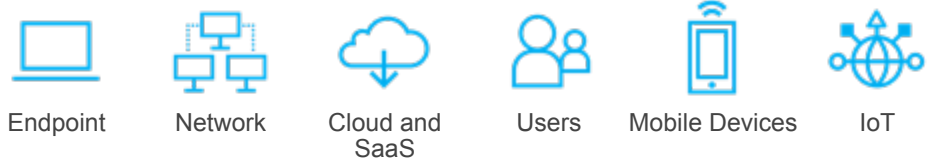
Strong Expertise

- Healthcare
- Government
- Operations
- Military
- Compliance
- Security
- Frameworks
- Audits/Inspections

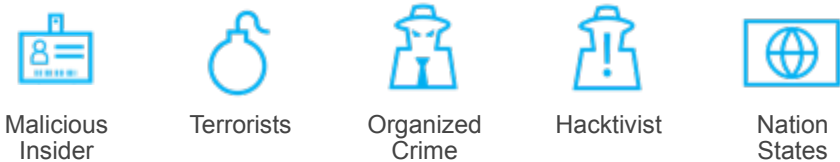


Security Challenges...and lots of motivation for Bad Actors

Expanding Attack Surface



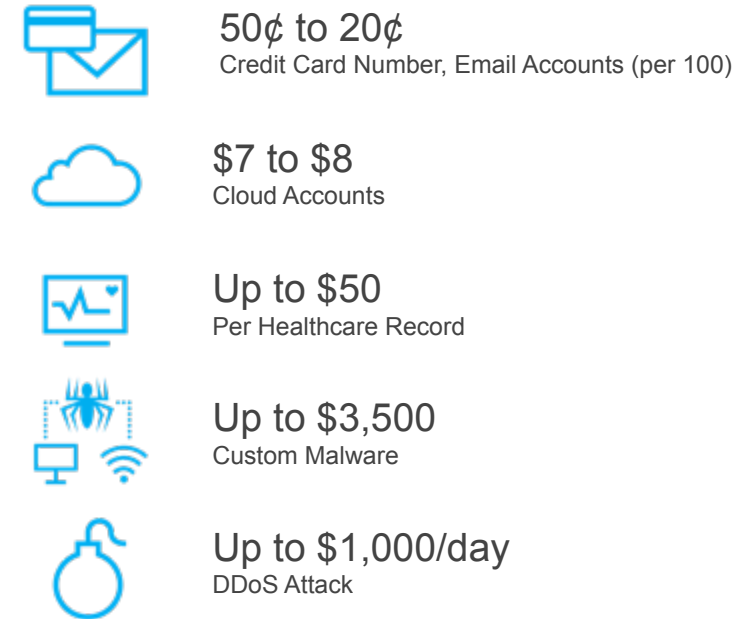
Motivated and Well-Funded Threat Actors



Creative and Sophisticated Attacks



Well-Established Cyber-Crime Economy



Security Challenges

Krebs on Security

620 GB DDoS Attack

Attackers used unsecure routers, DVRs and cameras

YAHOO!

Half a Billion Users

Disabled the antivirus machines with



Eddie Bauer

350 Stores

US and Canada stores breached. Used internal computer systems that are connected to PoS systems

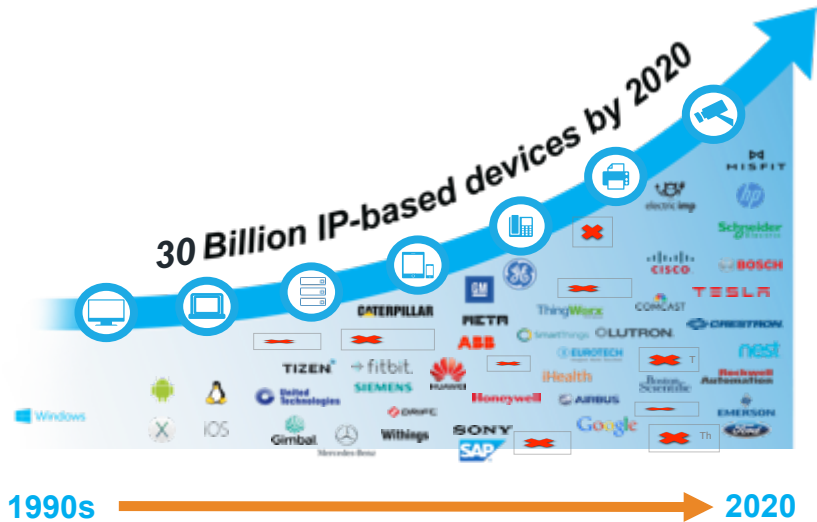
Top 10

vulnerabilities exploited are more than a year old

Source: HP Security Research. Cyber Security 2016; page 32

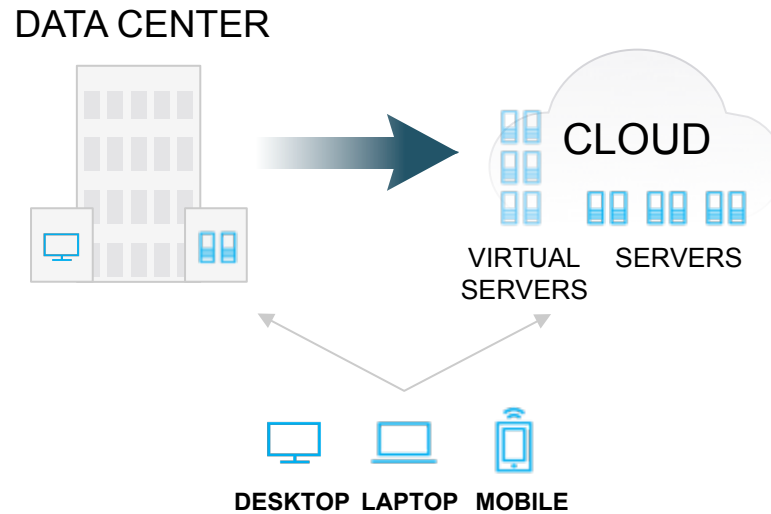
Three Trends That Make Your Next Breach Inevitable

Growth of Devices & Platform Diversity



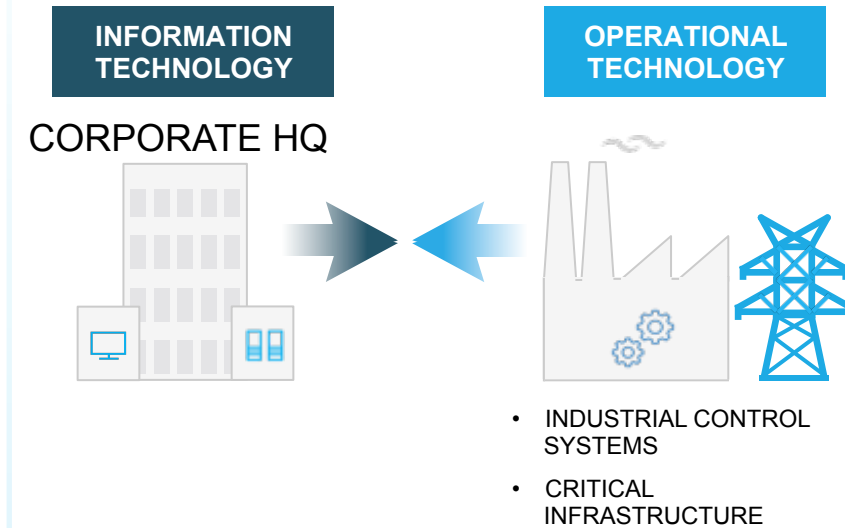
- <| Innumerable device-specific operating systems (OS)
- <| Cannot get agents onto new devices
- <| Cannot write agent-based software for every OS

Cloud Adoption Creates New Challenges



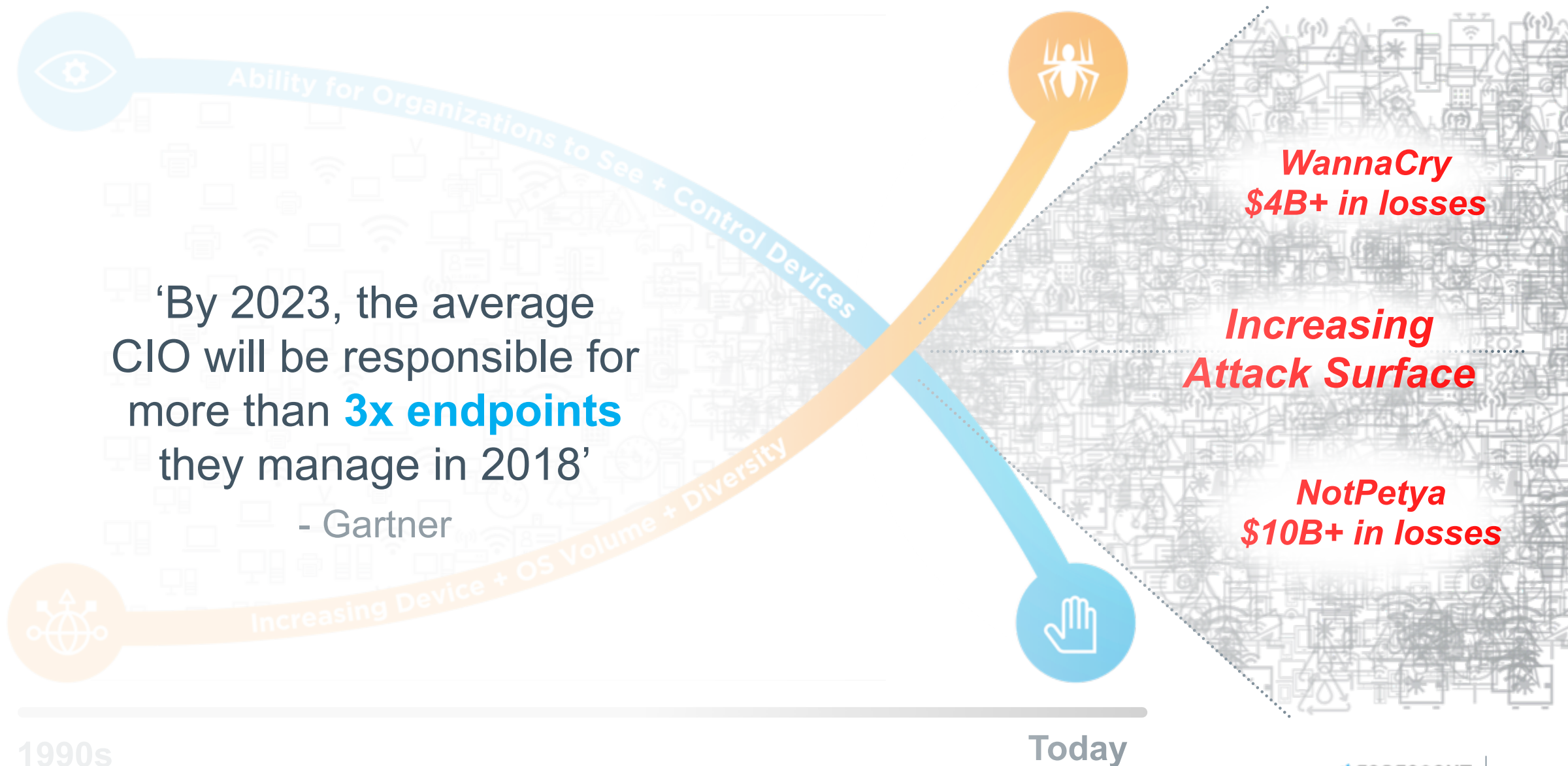
- <| Multiple Device Locations and Access Points
- <| Heterogeneous Environment with Multiple Vendors
- <| De-centralized Management

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



Consequences of Inadequate Visibility

80% of successful attacks leverage well-known vulnerabilities – *Gartner Security and Risk Management Summit*

99% of exploits will continue to be from known vulnerabilities up to one year through 2020 – *Gartner*

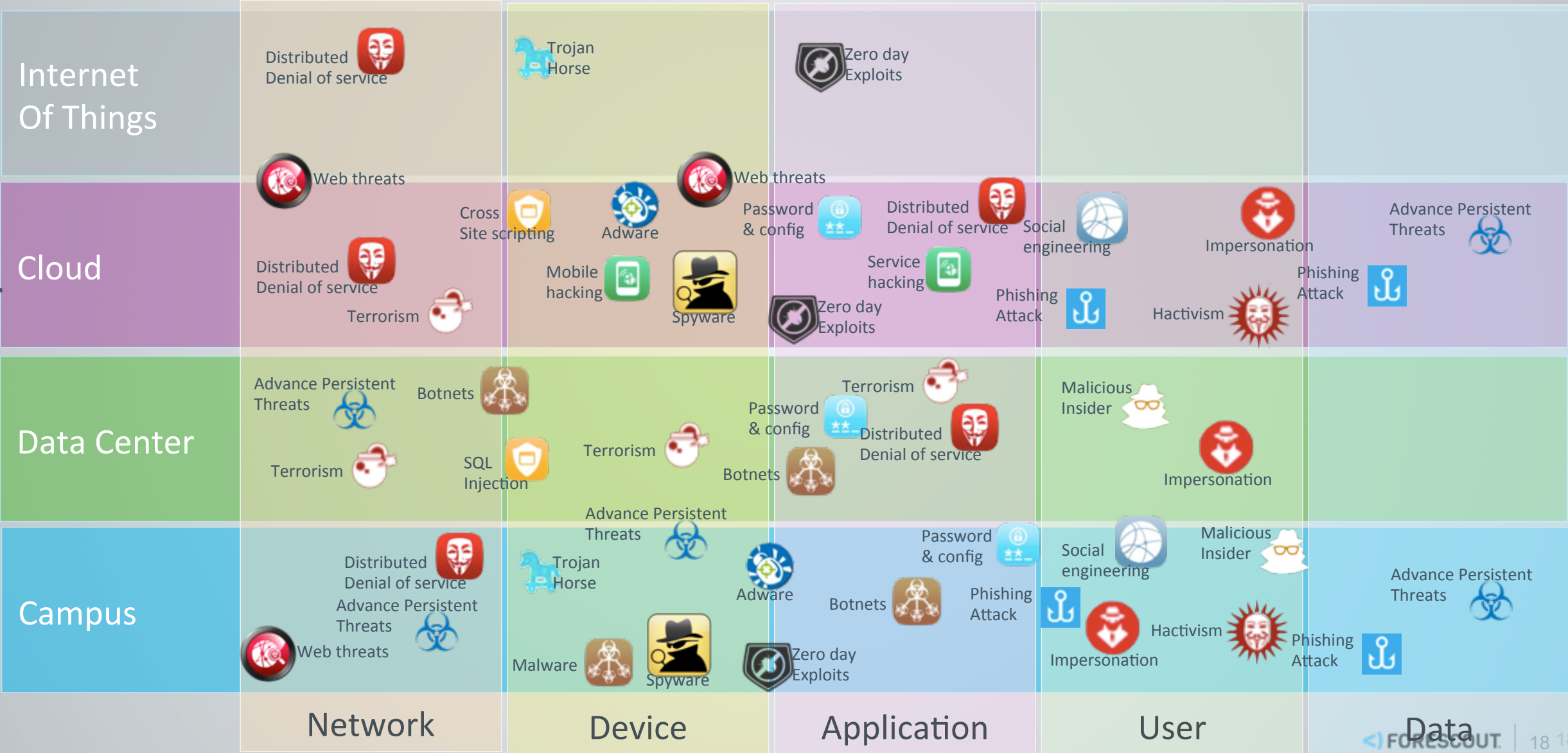
Top 10 exploited vulnerabilities are more than a year old – *HP Security Research.*

66% of networks will experience an Internet of Things based breach by 2018 – *IDC*

80% of all endpoints connected to the network will not support agent based technologies by 2020 *Gartner*

Threat Landscape

Distribution of corporate assets



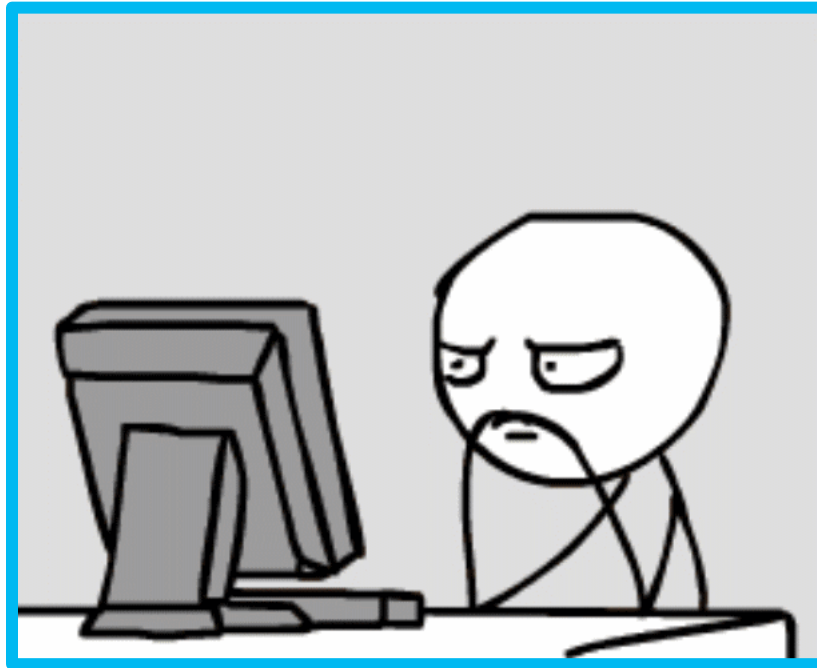
Major Trends in the Security Vendor Landscape

Major trends in the security vendor landscape



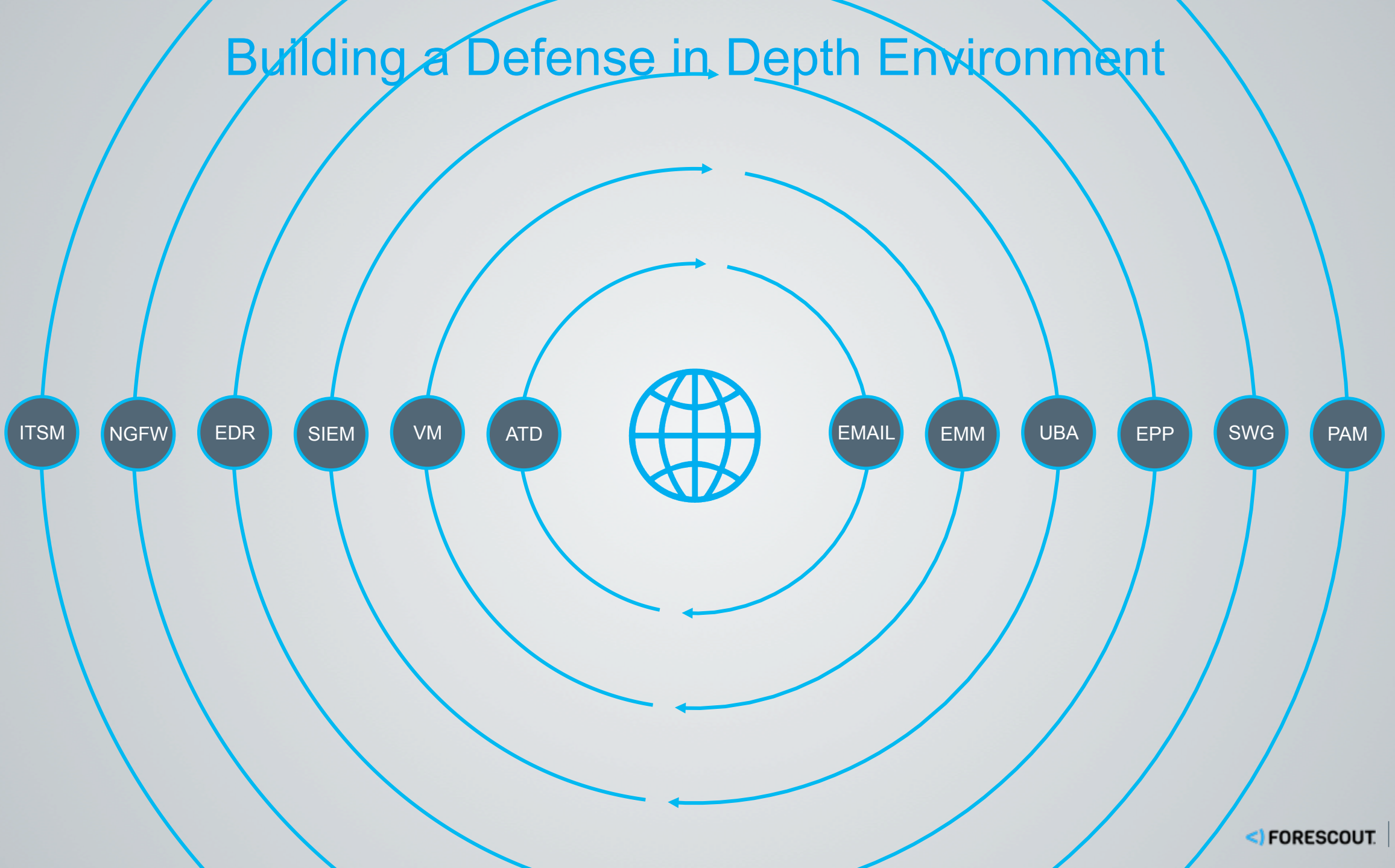
What this means for you and your teams

Baseline
Configurations
VA Scans
Patches
802.1x



Malware
EPP
Inventory
Nothing
Correlates!

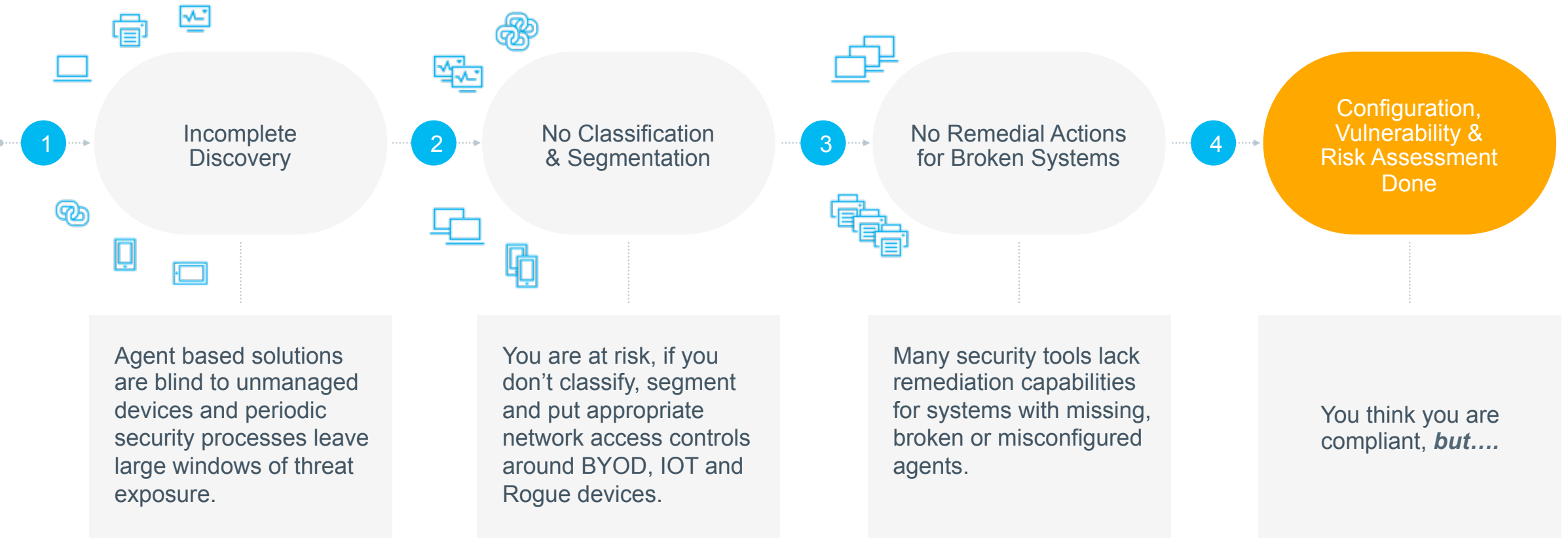
Building a Defense in Depth Environment



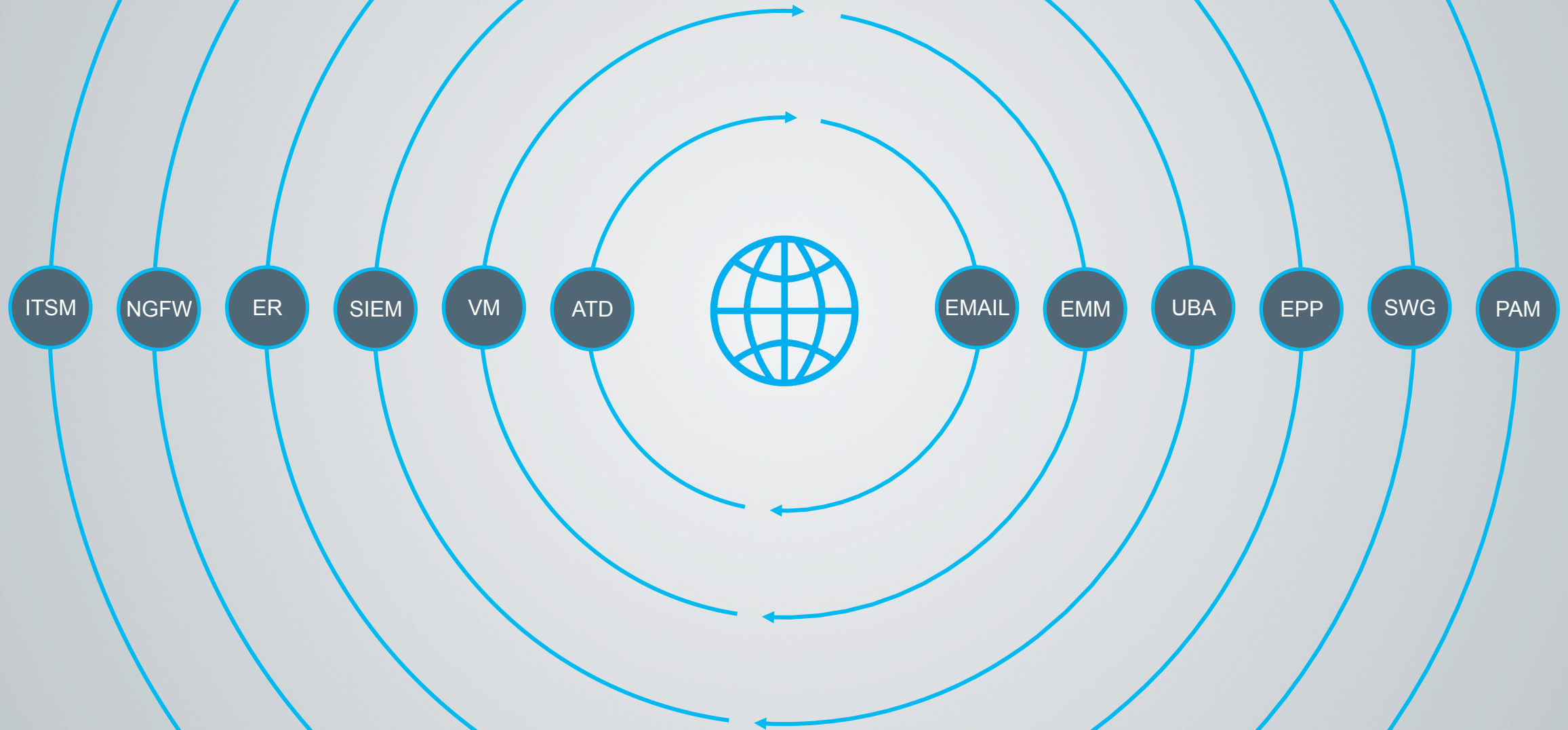


WE THINK WE HAVE IT
COVERED BUT.....

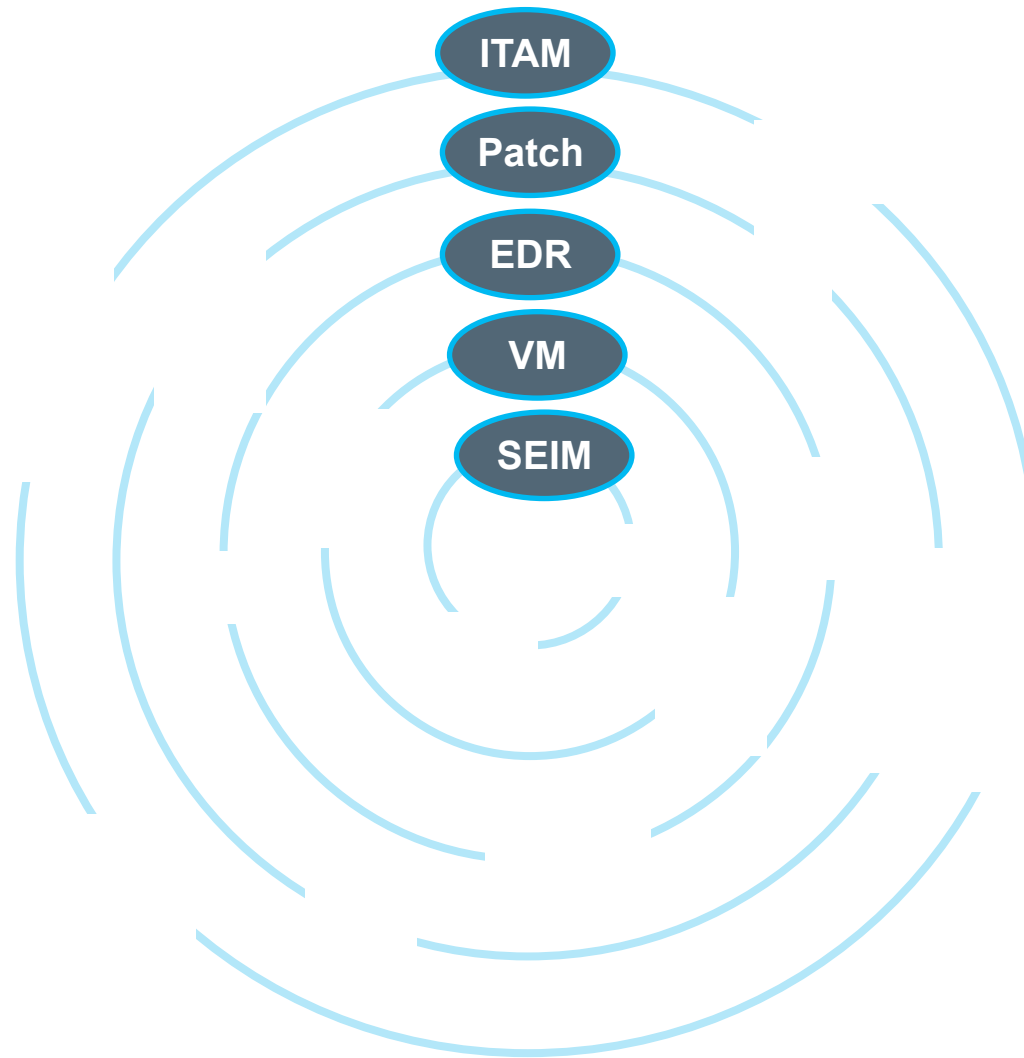
Inadequate Risk Mitigation Leads to Security Breaches



Today's Security Technologies



What happens when you don't have 100% visibility?



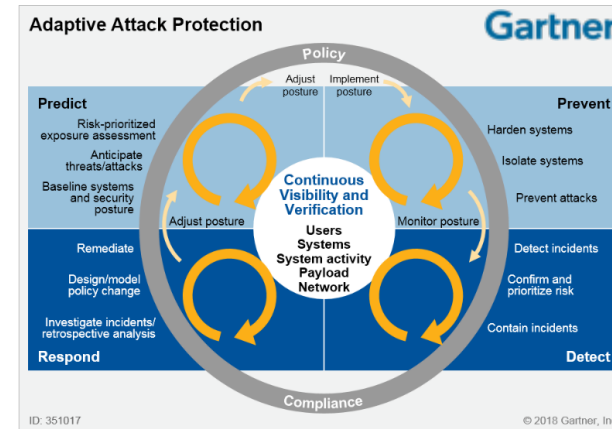


SO...HOW DO WE FIX IT?

Leverage Industry Security Frameworks

Common Themes Across all Frameworks

- <) Know all your connected devices and their security posture, trust nothing
- <) Continuously discover, monitor, assess and prioritize risk
- <) Use analytics, automation, and orchestration to rapidly prevent, detect, prioritize, and respond to threats
- <) Architect security as an integrated, adaptive, programmable system



NIST National Institute of Standards and Technology
U.S. Department of Commerce



Credit: N. Hanacek/NIST



<https://www.sans.org/critical-security-controls>

HITRUST

Health Information Trust Alliance - HITRUST CSF®, a certifiable framework that provides organizations with a comprehensive, flexible and efficient approach to regulatory compliance and risk management. <https://hitrustalliance.net/>

Automated Compliance Management; Leverage Industry Security Frameworks



CIS Critical Security Controls



V7

Basic

1 Inventory and Control of Hardware Assets

2 Inventory and Control of Software Assets

3 Continuous Vulnerability Management

4 Controlled Use of Administrative Privileges

5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7 Email and Web Browser Protections

8 Malware Defenses

9 Limitation and Control of Network Ports, Protocols, and Services

10 Data Recovery Capabilities

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

12 Boundary Defense

13 Data Protection

14 Controlled Access Based on the Need to Know

15 Wireless Access Control

16 Account Monitoring and Control

Organizational

17 Implement a Security Awareness and Training Program

18 Application Software Security

19 Incident Response and Management

20 Penetration Tests and Red Team Exercises

Visibility and Control Across the Extended Enterprise

Leverage the same technology, people and processes across the extended enterprise



Campus



IoT



Data Center



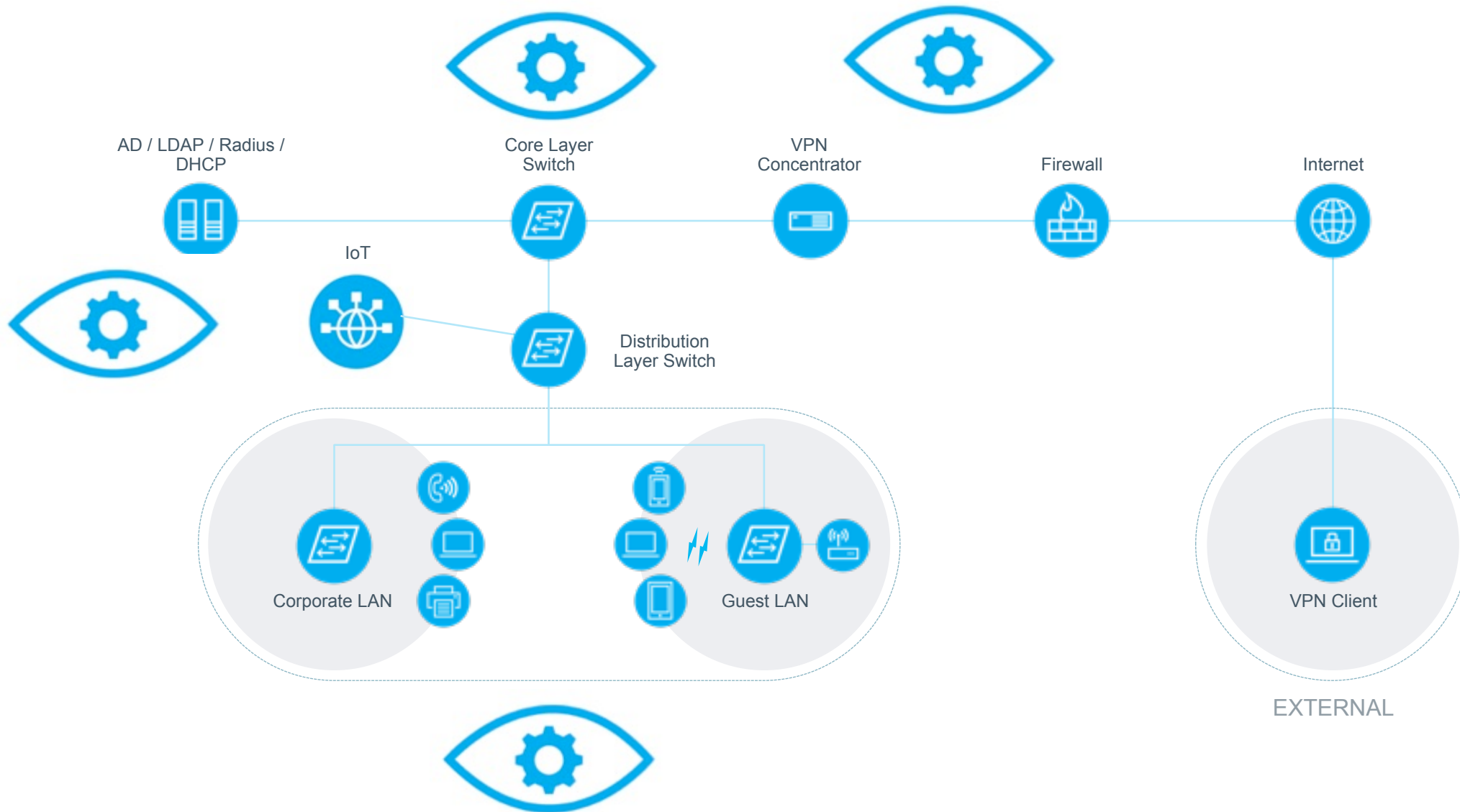
Cloud






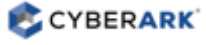















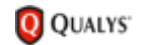


Operational Technology

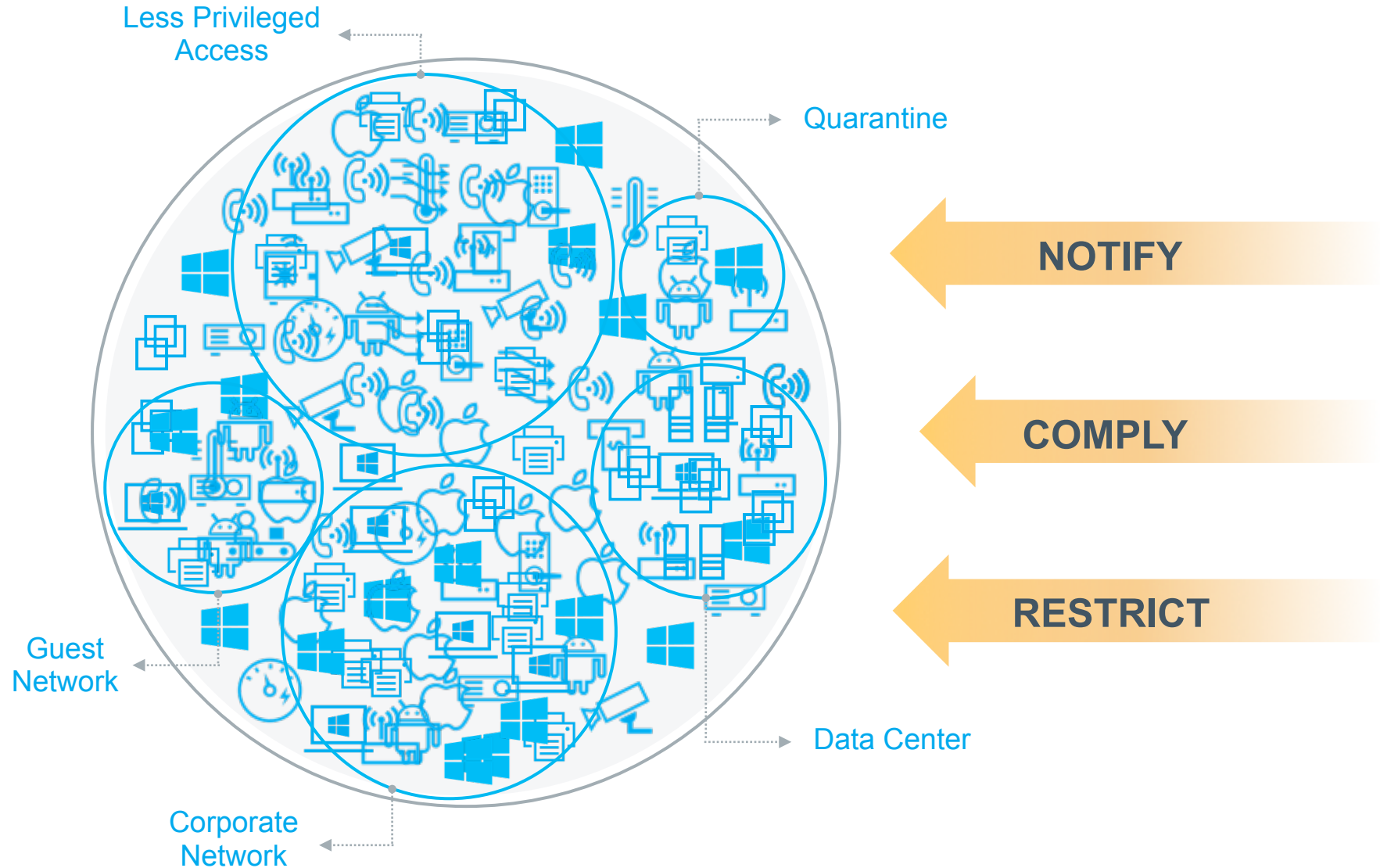


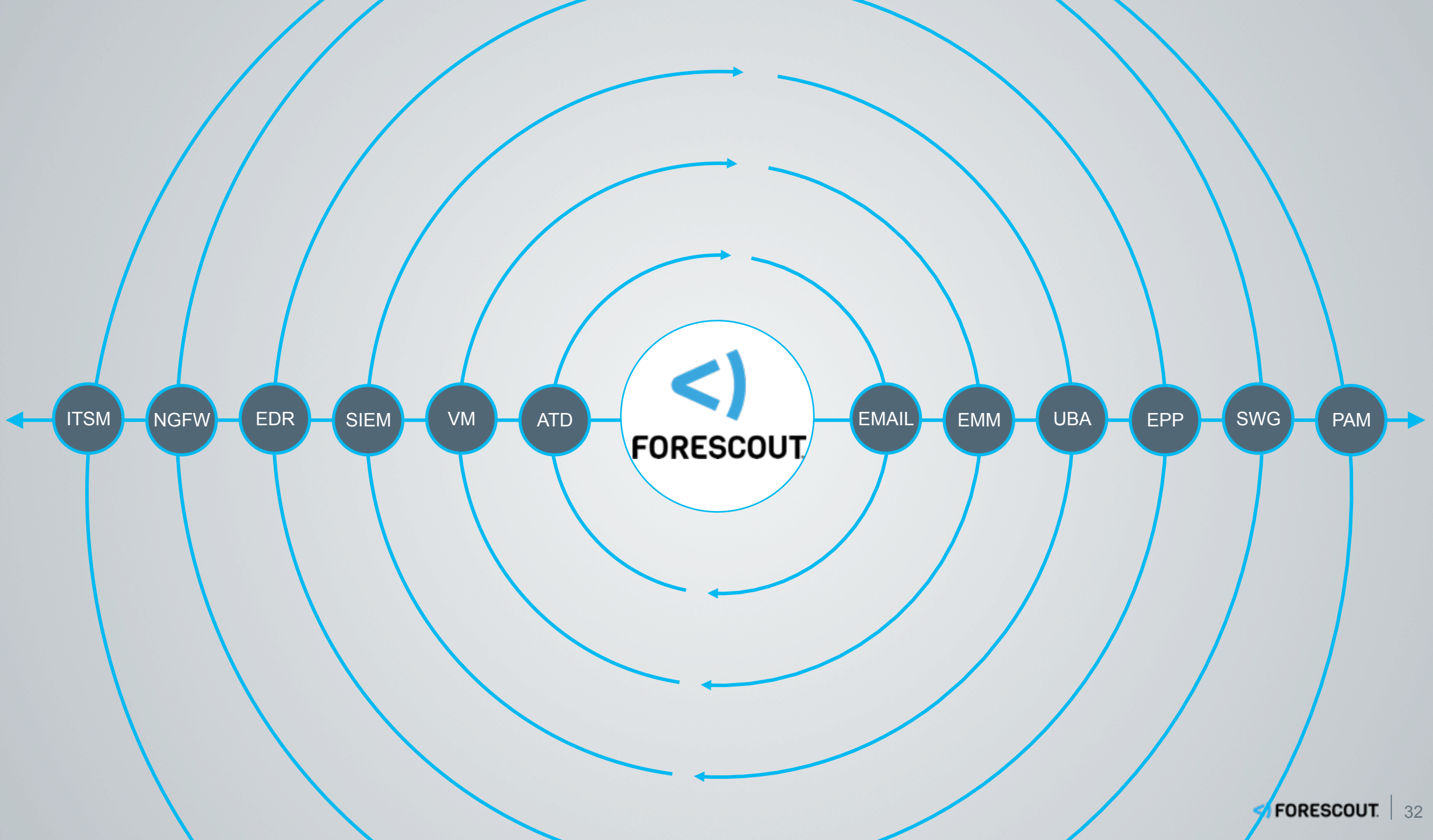
Visibility at the Network Level UPON Connection



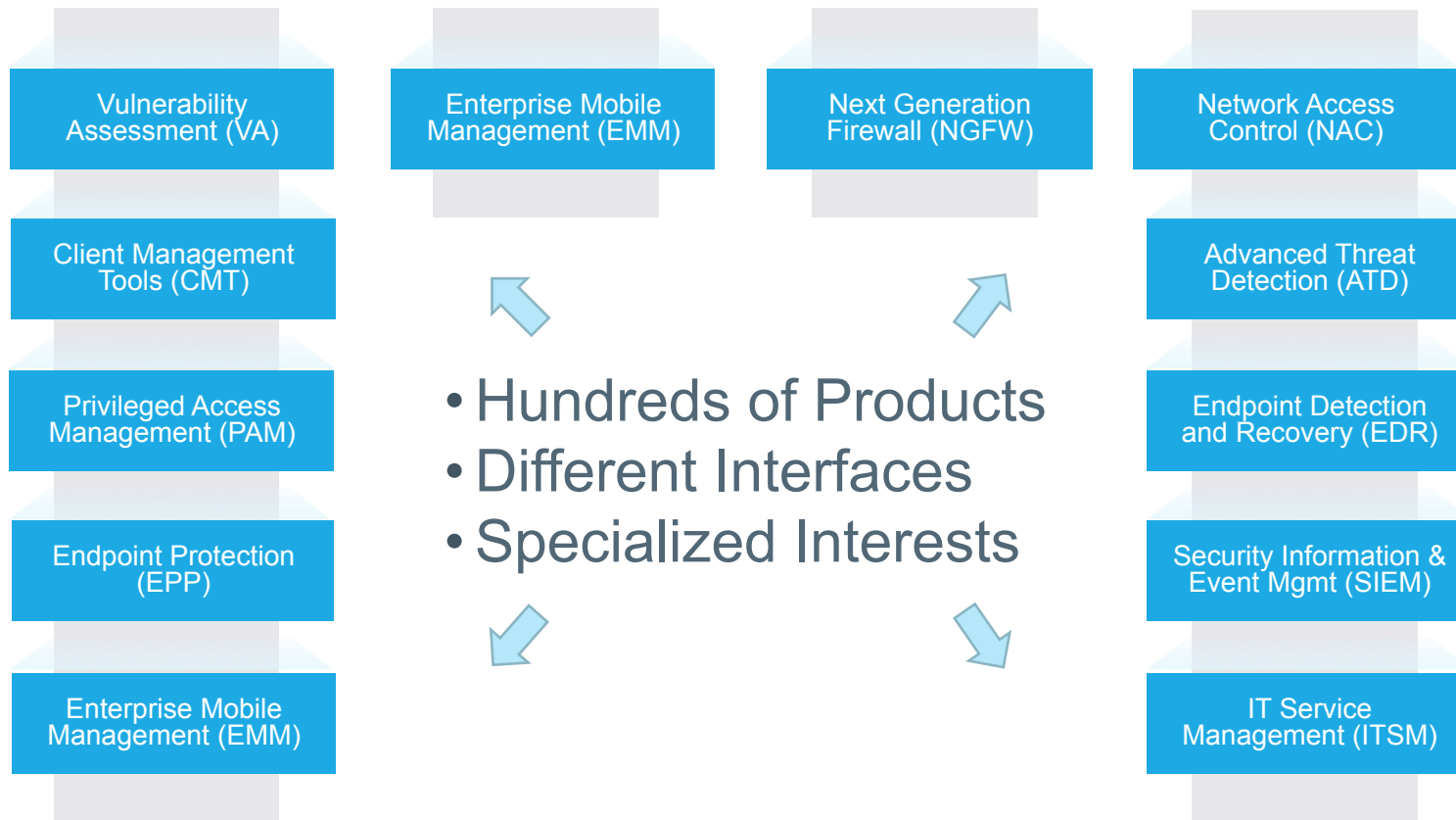
Automate Response

ATD	  
PAM	
EMM	   
EDR/EPP	    
ITSM	
NGFW	 
SIEM	  
VA	  



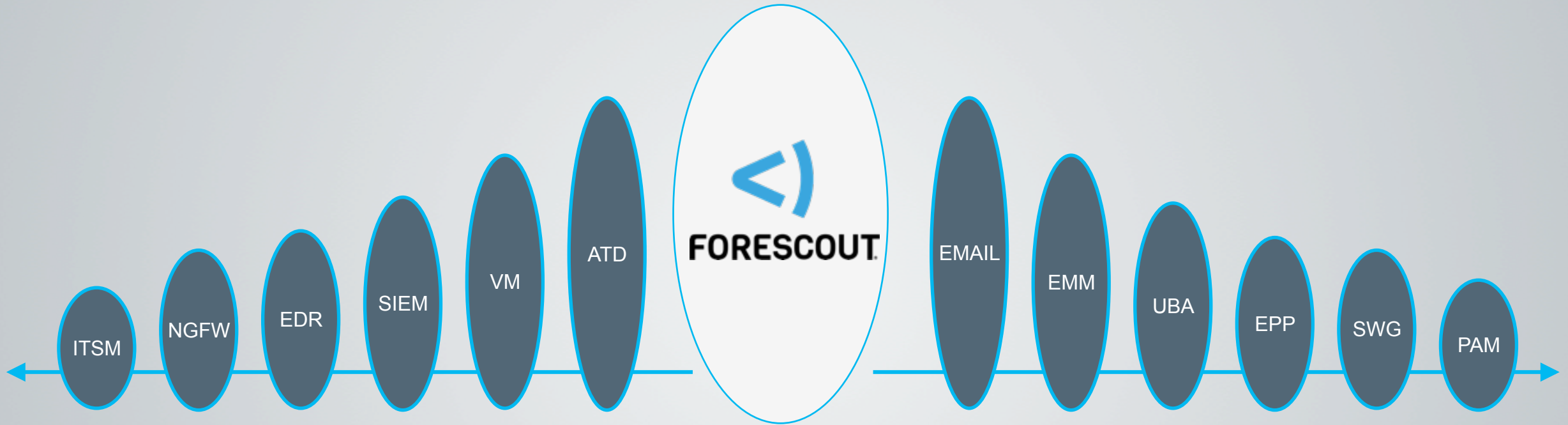


Orchestrate and Automate



Make Your Security Tools Smarter and Work as a Team

Communication between tools build higher walls!



Forescout Vision



Vendor + Vendor =
better security and
maximized investments



Visibility is foundational



Consistent people,
processes and technology
across all vectors



QUESTIONS?

Forescout. The Leader in Device Visibility and Control



ASMGi



FORESCOUT®

Thank You

800 Superior Ave E, Ste 1050
Cleveland, OH 44114

Phone: 216.255.3040
Fax: 216.274.9647

Email: info@asmgi.com

www.asmgi.com