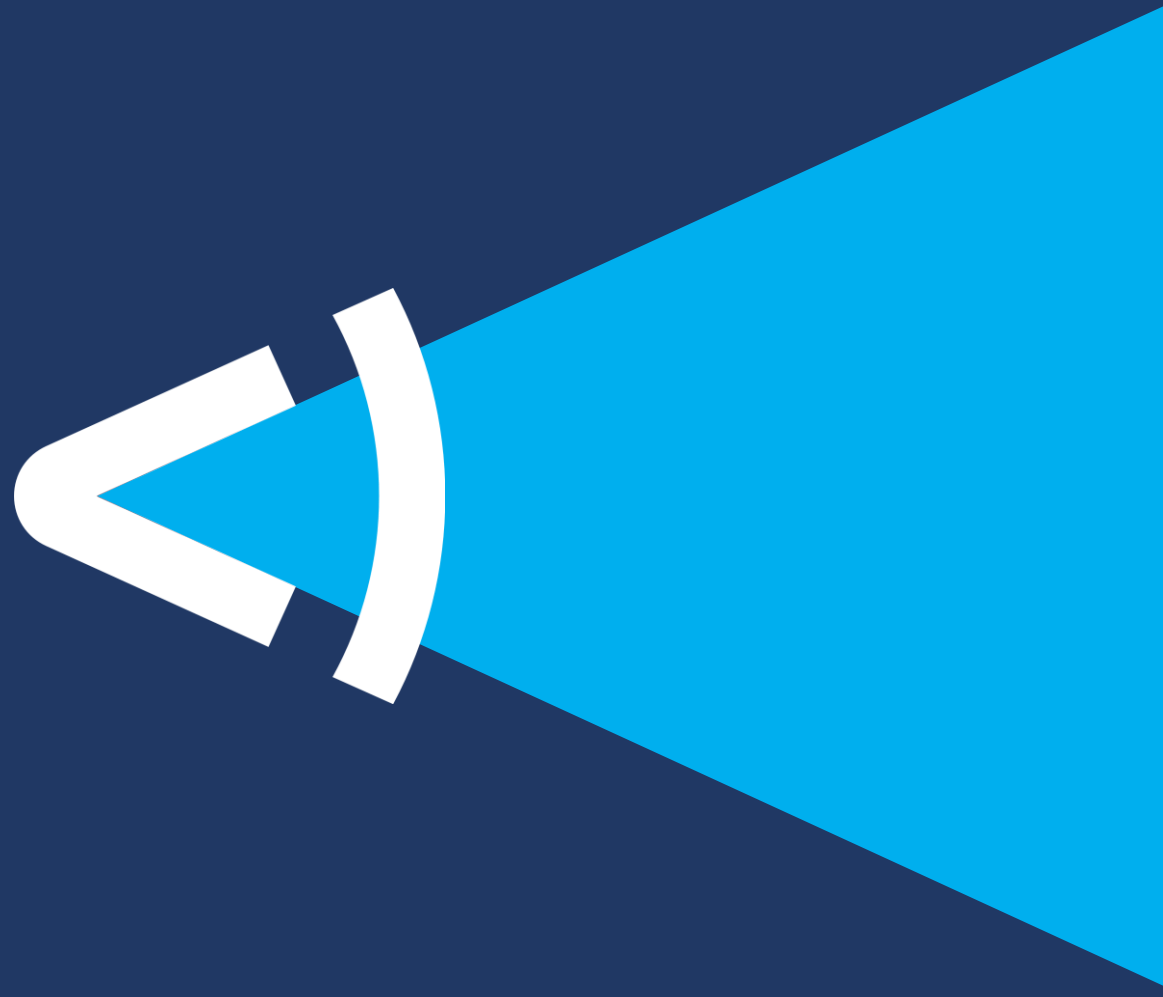
FORESCOUT

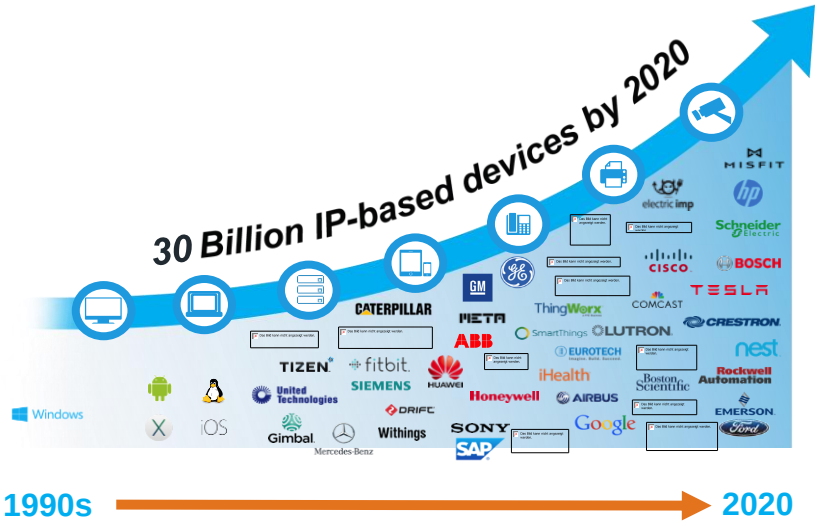
DEVICE VISIBILITY AND CONTROL



Daniel Kuenzli
Systems Engineer DACH

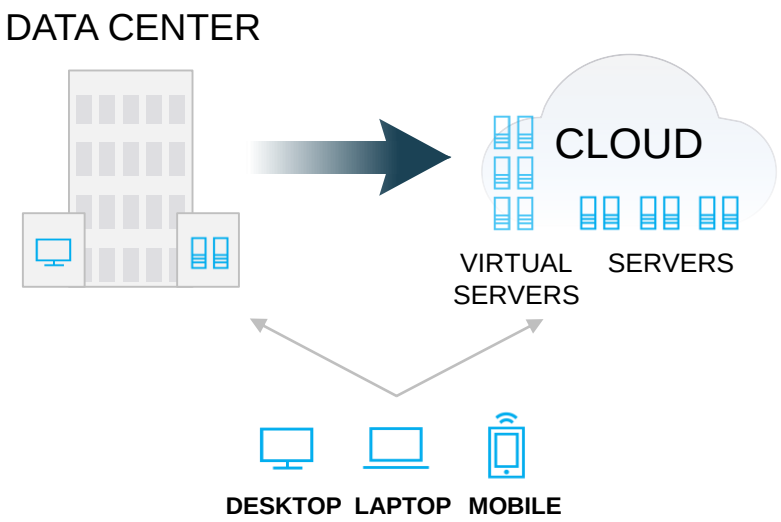
Three Trends That Make Your Next Breach Inevitable

Growth of Devices & Platform Diversity



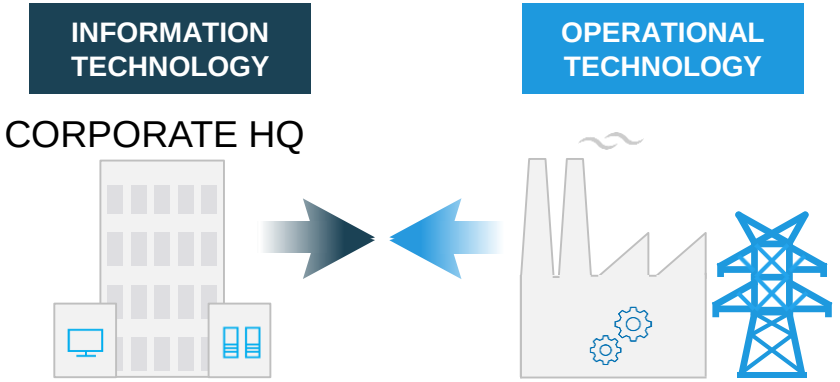
- Innumerable device-specific operating systems (OS)
- Cannot get agents onto new devices
- Cannot write agent-based software for every OS

Cloud Adoption Creates New Challenges



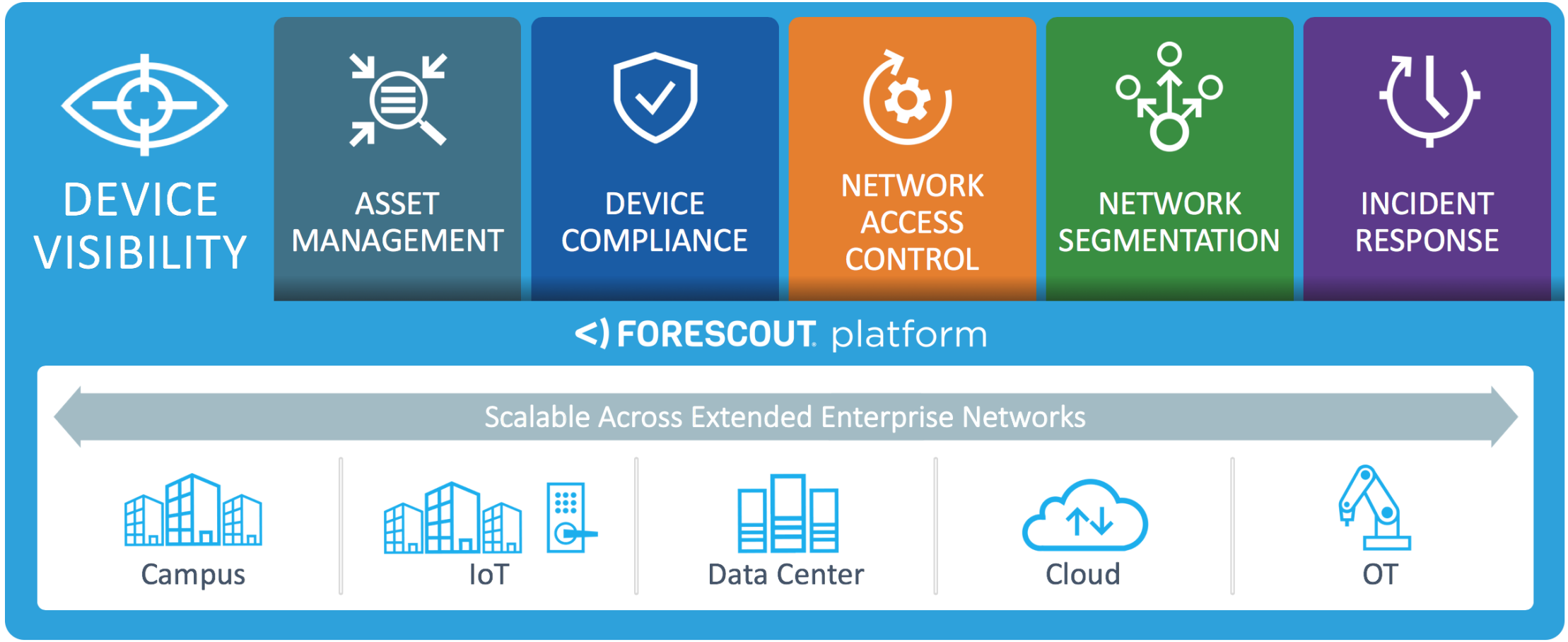
- Multiple Device Locations and Access Points
- Heterogeneous Environment with Multiple Vendors
- De-centralized Management

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

Forescout's Mission: 100% Device Visibility and Control



DEVICE VISIBILITY

Device Visibility: You Can't Secure What You Can't SeeTM

Forescout gives you the ability to continuously discover, classify & assess every IP-connected device that touches the extended enterprise network in real time!

Business Challenges:

- Enterprises, on average, have **~30% more devices connected** than expected
- Even when enterprises know about devices connecting, they often **don't know what they are** & whether they should be there
- IT & regulatory device **audits** are challenging & **often fail**

Technical Challenges:

- Agents are not supported and/or not deployed on all devices
- Little to no device attribute information to classify & assess connected devices
- No single source of truth that is current for all connected devices

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

How We Do It

Agentless

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

Heterogeneous

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

Intelligent

- ✓ Device Cloud ~1000 customers contributing/7M devices
- ✓ Comprehensive device taxonomy across IT & OT

Continuous

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

With Asset Management, You Can Accurately Secure Connected Things

ASSET MANAGEMENT

Challenges:

- Most asset management systems are **populated by human** beings and keeping the data up to date is challenging
- Many asset management systems **do not store data** from unmanaged machines such as IoT & OT
- Work around from customers is to hire **expensive consultants** to manually take inventory

Natively

- **Automate** the inventorying of IP-connected assets across IT & OT networks

Pinpoint the real-time location of all IP-connected things

Continuously and accurately assess all IP-connected devices

Extend/Automate

- **True-up** enterprise CMDBs with complete device inventory & context

Inform UEM tools about BYOD devices connecting to the enterprise network

CMDB

servicenow

UEM

IBM MobileIron vmware

DEVICE COMPLIANCE

With Device Compliance, You Can Evaluate & Reach Compliance

Challenges:

- **Limited and out-of-date data** on machine posture versus corporate policies
- Point in time VM systems **miss ongoing changes** in device posture
- **Lack of compliance enforcement** for non-traditional devices (e.g. massive MAC whitelists)

Natively

- **Automatically** install or repair a broken agent
- **Report** on patch status for Microsoft Windows & Apple OSX endpoints
- **Pinpoint** where compliant and non-compliant device are located in seconds
- **Scan** specific devices for SCAP compliance

Extend/Automate

- **Trigger** best-of-breed Vulnerability Management vendors to scan and update devices that are missed by scheduled scans.
- **Inform** agent-based platforms of outdated agents & signature files then auto-remediate as necessary

Vulnerability Management

RAPID7 Qualys. tenable

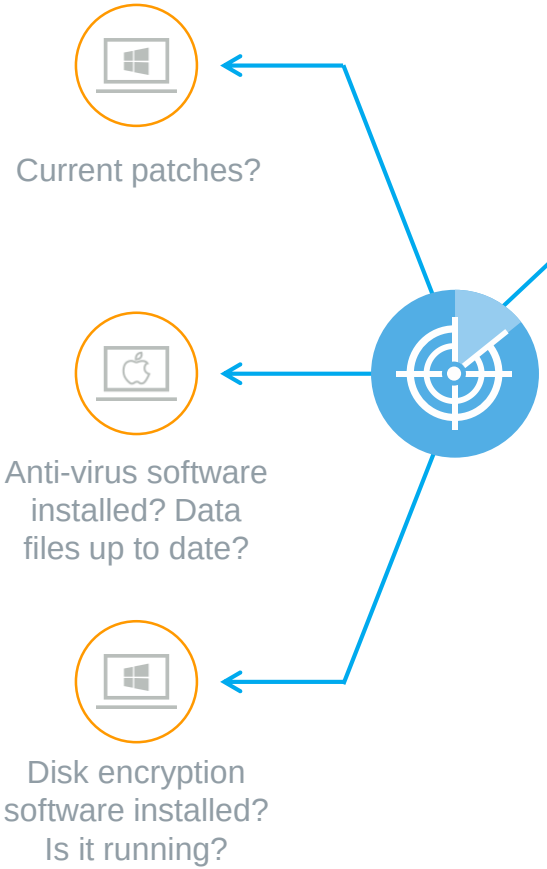
UEM/EPP/EDR/PAM

IBM Microsoft Intune MobileIron vmware Carbon Black. CROWDSTRIKE Symantec. McAfee CYBERARK

Automated Compliance with Forescout

CONTINUOUS COMPLIANCE ASSESSMENT AND ENFORCEMENT

- Verify hosts and their behaviors meet company compliance requirements
- Hosts can be examined for policy compliance before network access granted
- Actions to manage non-compliant hosts can include notification, user based remediation, restricted access, automated remediation



Posture Compliance Examples

3rd Party Reported Behavior	Device Type	Personal Firewall
Anti-Malware	Disk Encryption	Password
Anti-Spyware	Files	Patched
Anti-Virus	IOCs	Registry Keys
Applications	Ownership	Services
USB	Operating System	And more….

Active Virus Shield PC Ziggy

BitDefender Kaspersky F-Secure Microsoft

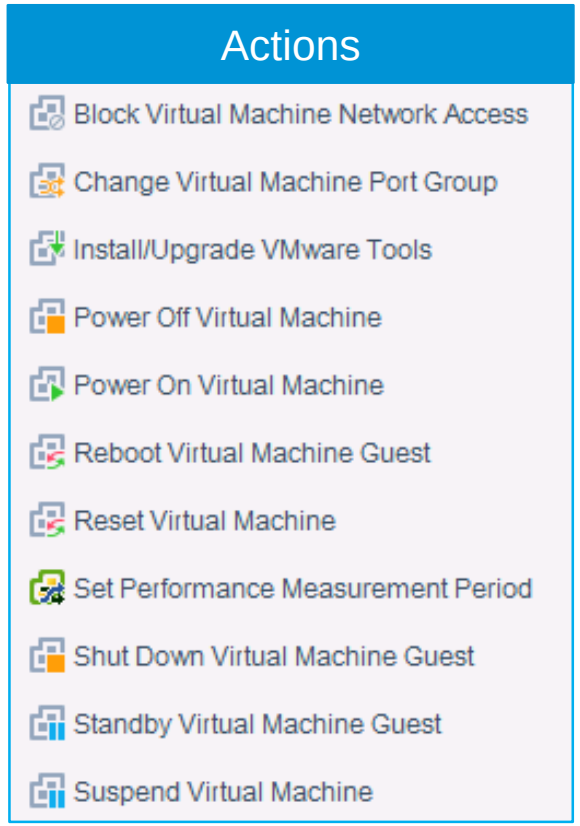
Sophos McAfee K7 Computing Trend Micro

G Data LANDesk Panda Symantec

Comodo Hauri

Data Center Compliance Assessment

- Fetch ESXi host and VM properties from vCenter®
- Use policy-based approach to check compliance based on VMware hardening guidelines
- Take remediation actions to mitigate risk from non-compliant machines



Host compliance policies supported by CounterACT® in Campus environment also apply to VMs running Windows, macOS and Linux

With Network Access Control, You Can Control Access Simply & Easily

NETWORK ACCESS CONTROL

Challenges:

- **Takes years to deploy** so limited value
- **Costly** network upgrades typically required
- **Lack of heterogeneous** network infrastructure support
- **Dependency** on agents (802.1x) limits device visibility

Natively

- **Interoperate** with over 70 infrastructure devices avoids network upgrades
- 802.1x is **optional**
- **Isolate** non-compliant or infected devices without changing configuration of network infrastructure
- **Continuously** monitor device hygiene & take action when necessary
- **Automatically** assess & onboard guest wireless devices

Extend/Automate

- **Co-exist** with agent-based 802.1x solutions

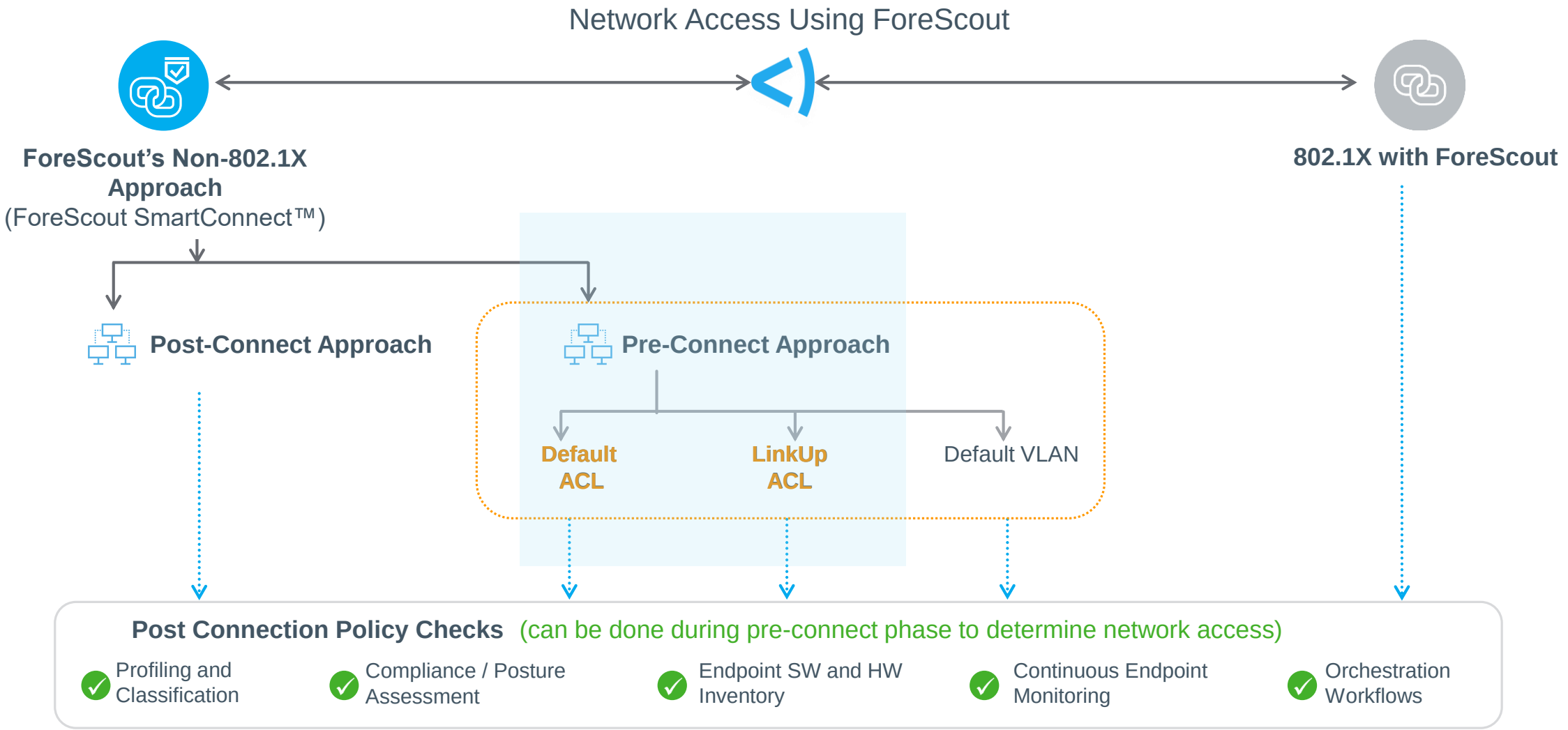
NAC

aruba a Hewlett Packard Enterprise company

cisco

FORTINET

Non-802.1X Wired Pre-Connect Options



NETWORK SEGMENTATION

With Network Segmentation, You Can Confidently Segment Your Network

Challenges:

- Little to no automation exists to update the numerous policies **as devices change and move**
- Most network are big and flat and have very little in terms of inter-company ability to **stop bad actors once they get in**
- Segmentation **policy sprawl due to multiple segmentation solutions** serving different parts of the enterprise network
- **Limited insight** into traffic patterns between devices

Natively

Automatically **create** traditional & virtual ACLs to extend segmentation to any device

Dynamically **assign** entities to zones based on device type, application, user & location

Extend/Automate

Provide full device & user contextual information to industry leading NGFW vendors to enable dynamic segmentation

Share context with leading virtual infrastructure, cloud & micro- segmentation platforms

NGFW

Check Point SOFTWARE TECHNOLOGIES LTD. | paloalto NETWORKS | FORTINET

Micro-segmentation

aws | Microsoft Azure | vmware NSX

INCIDENT RESPONSE

With Incident Response, You Can Respond & Remediate Quickly

Challenges:

- Potentially never **containing the incident** due to new devices connecting and the lack of complete visibility
- Most IR teams are not prepared for **IoT or OT incidents**
- **Lengthy mean-time-to-response** allows extensive lateral spread of attacks
- Inability to **correctly prioritize alerts** and assess threat criticality of incidents

Natively

- **Identify** high risk devices that haven't been contained or remediated
- **Execute** predefined remediation for non-compliant devices at time of connect to reduce MTTR
- **Search** for potentially vulnerable devices
- **View** a single dashboard showing overall device health across the entire enterprise

Extend/Automate

- **Hunt** for vulnerabilities, IoCs & other attributes provided by leading threat detection, vulnerability management & SIEM vendors
- **Execute** 'response' actions as requested by leading SOAR vendors

ATD / EDR

FireEye, paloalto NETWORKS, Carbon Black., CROWDSTRIKE

SIEM / ITSM

IBM, splunk>, servicenow

Our Product Vision

THE STANDARD FOR **DEVICE VISIBILITY AND CONTROL** ACROSS THE EXTENDED ENTERPRISE

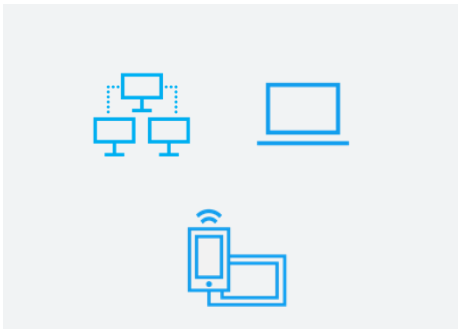
Campus

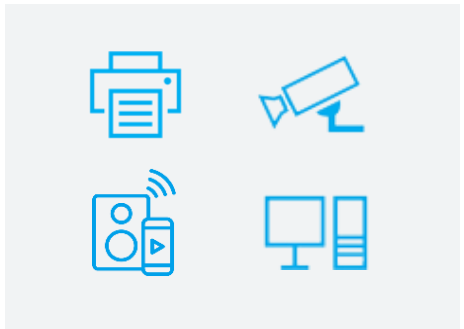
IoT

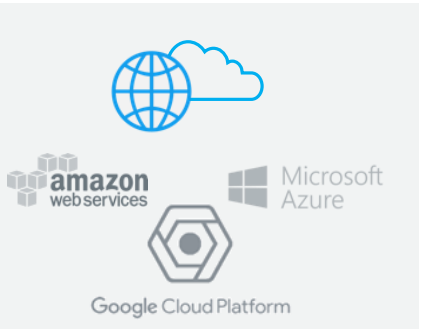
Data Center

Cloud

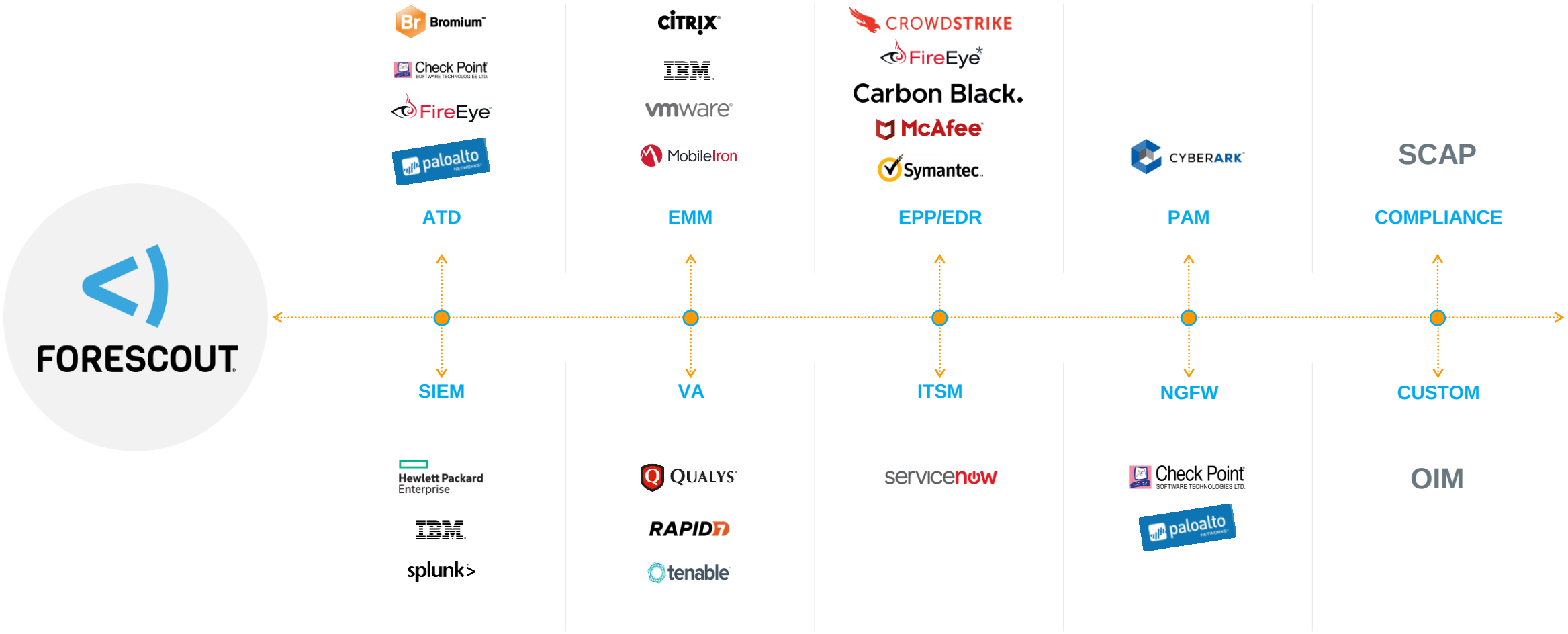
Operational Technology







ForeScout Extended Modules Ecosystem



Forescout Industrial Cyber Resilience

Device Visibility

See in real-time what your ICS network devices are doing

Detection

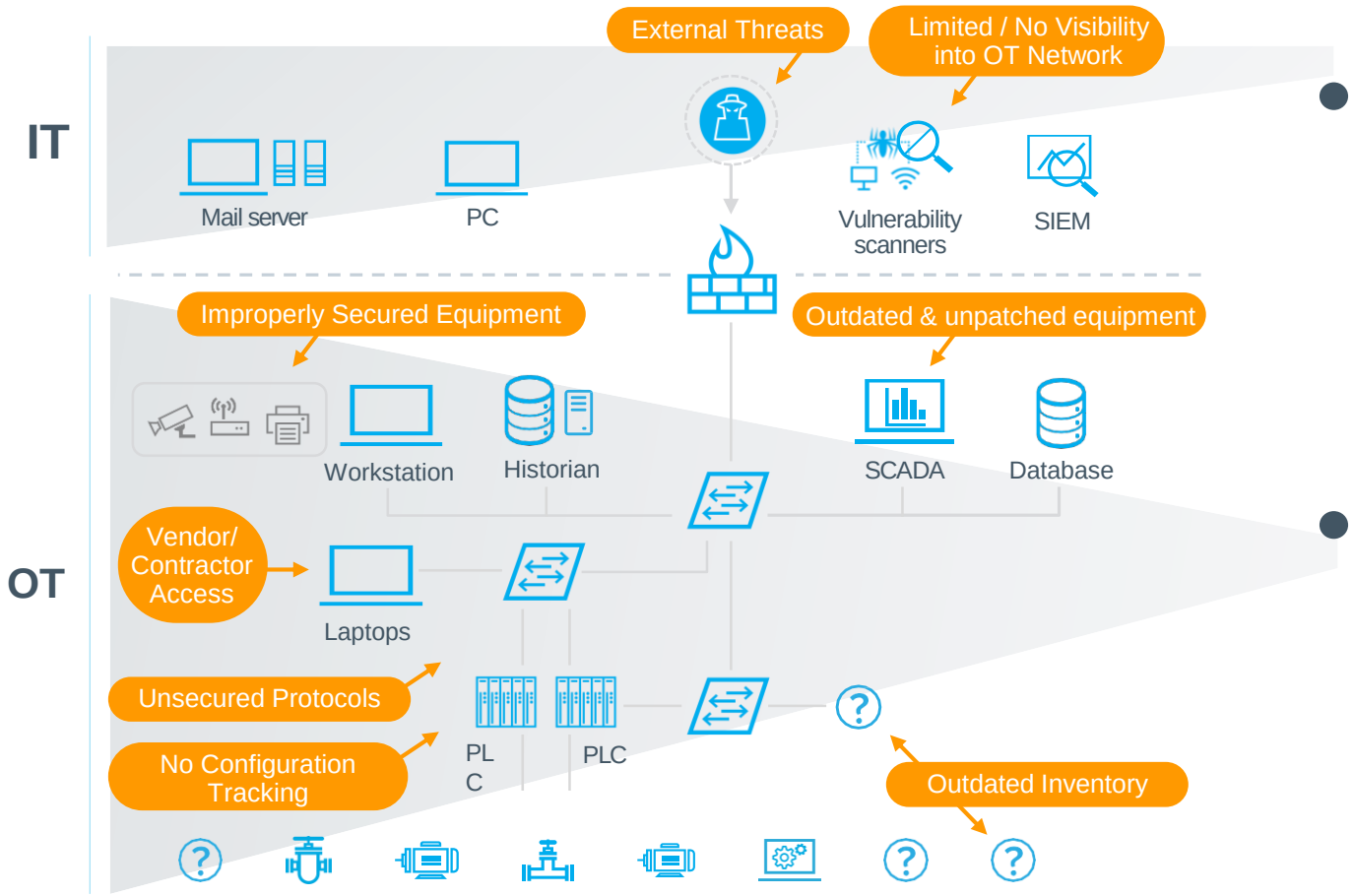
Catch known and unknown threats at their earliest stages

Control

Know what's going on at all times and easily share that data with the organization

We provide instant visibility into your network and detection of all cyber threats to your industrial environment.

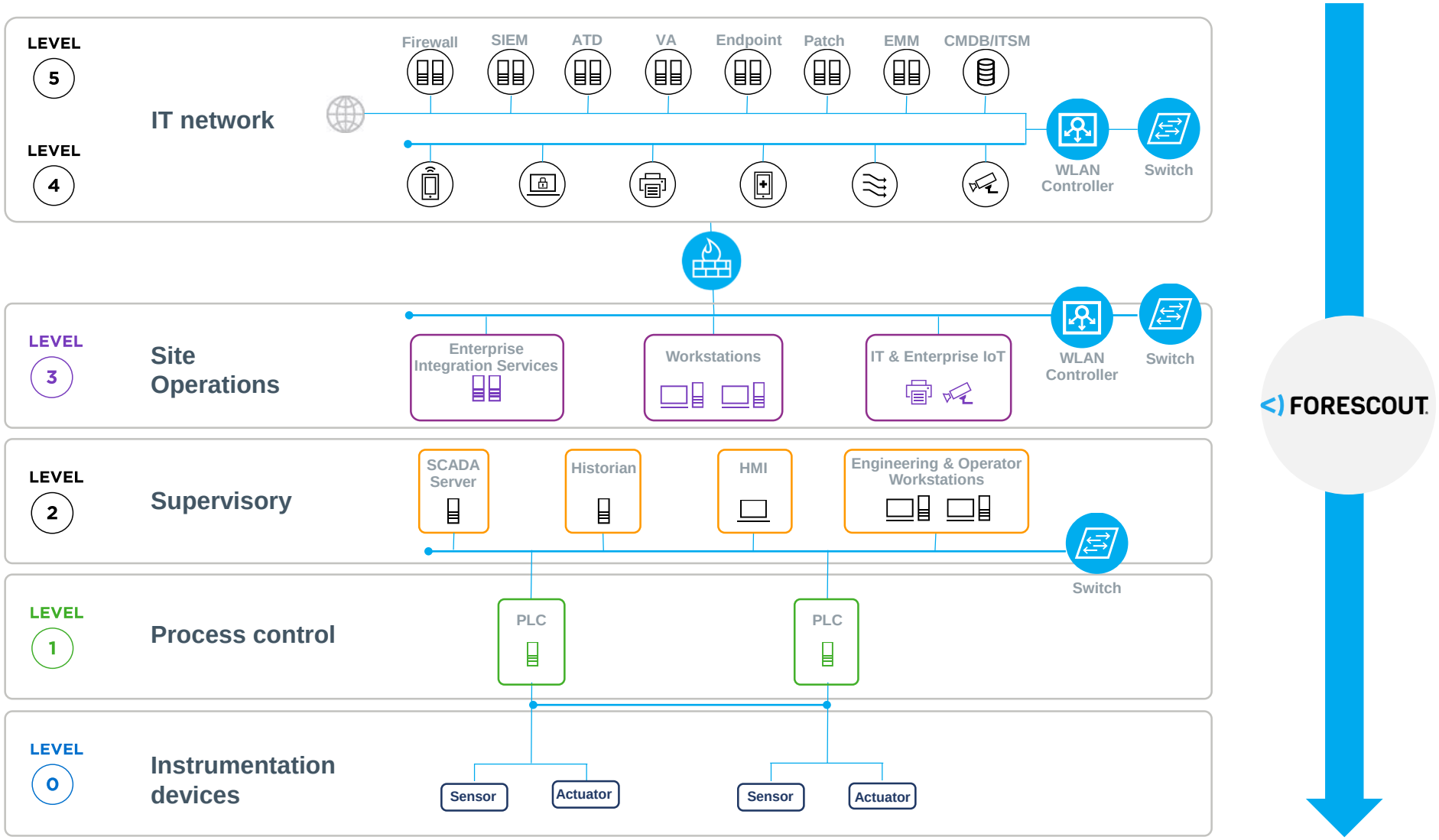
ForeScout + SecurityMatters is the Answer to the IT/OT Integration Challenges



- **Limitations of dedicated IT Solutions**
  - Limited visibility into OT assets
  - IT security tools can't operate in OT environments
    - *Active methods – Disrupt operations*
    - *OT equipment can't accept agents*
  - No ability to be "selectively active" to ensure reliability and safety of critical assets
- **Limitations of OT centric solutions**
  - Limited visibility of device posture into workstations, IoT, and IT devices in OT environments
  - No visibility to poor patch hygiene for Windows assets
  - Limited ability to classify device types outside of automation equipment
  - Lack of endpoint context such as switch and port

With the convergence of IT and OT, security solutions must be able to address cyber risk across all device types found in an OT environment

Now: Unified IT and OT Device Visibility and Security



Example OT Device Vendors

HMI

- ICONICS — Make the Invisible Visible™
- RSView32
- WinCC Professional
- Wonderware

DCS

- ABB
- EMERSON
- Foxboro by Schneider Electric
- Honeywell
- YOKOGAWA

PLC

- GE
- MITSUBISHI ELECTRIC
- OMRON
- Rockwell Automation
- Schneider Electric
- SIEMENS

Example Protocols in OT (Proprietary)

Proprietary OT Systems / Protocols

- ADE (Phoenix Contact)
- ADS/AMS (Beckhoff)
- BSAP & BSAP IP (Bristol Babcock)
- CDP (Cisco)
- Centum DCS (Yokogawa)
- CIP extensions (Rockwell/AB)
- Citect (Schneider Electric)
- CodeSys (Wago, ABB, and others)
- COMEX (Schneider Electric Foxboro)
- CSLib (ABB 800xA)
- CSP (Rockwell/AB)
- CygNet SCADA (CygNet)
- DeltaV (Emerson)
- DMS (ABB AC 800 F)
- Experion (Honeywell)
- Fast Message Protocol (SEL)
- FOX (Honeywell Niagara / Tridium)
- ISaGRAF IXL (Yokogawa ProSafe and others)
- LonTalk (LonWorks)
- Melsoft (Mitsubishi Electric)
- MMS (ABB AC 800 M)
- Modbus/TCP Unity (Schneider Electric)
- OASyS (Schneider Electric)
- Ovation (Emerson)
- PN800 (ABB Harmony)
- S7COMM+/OMS+ (Siemens)
- SPLUS (ABB Symphony Plus)
- SRTP (GE)
- Step7 (Siemens)
- Telnet extensions (SEL)
- Triconex Tristation (Schneider Electric)
- Vnet/IP (Yokogawa),

Example Protocols in OT (Standard)

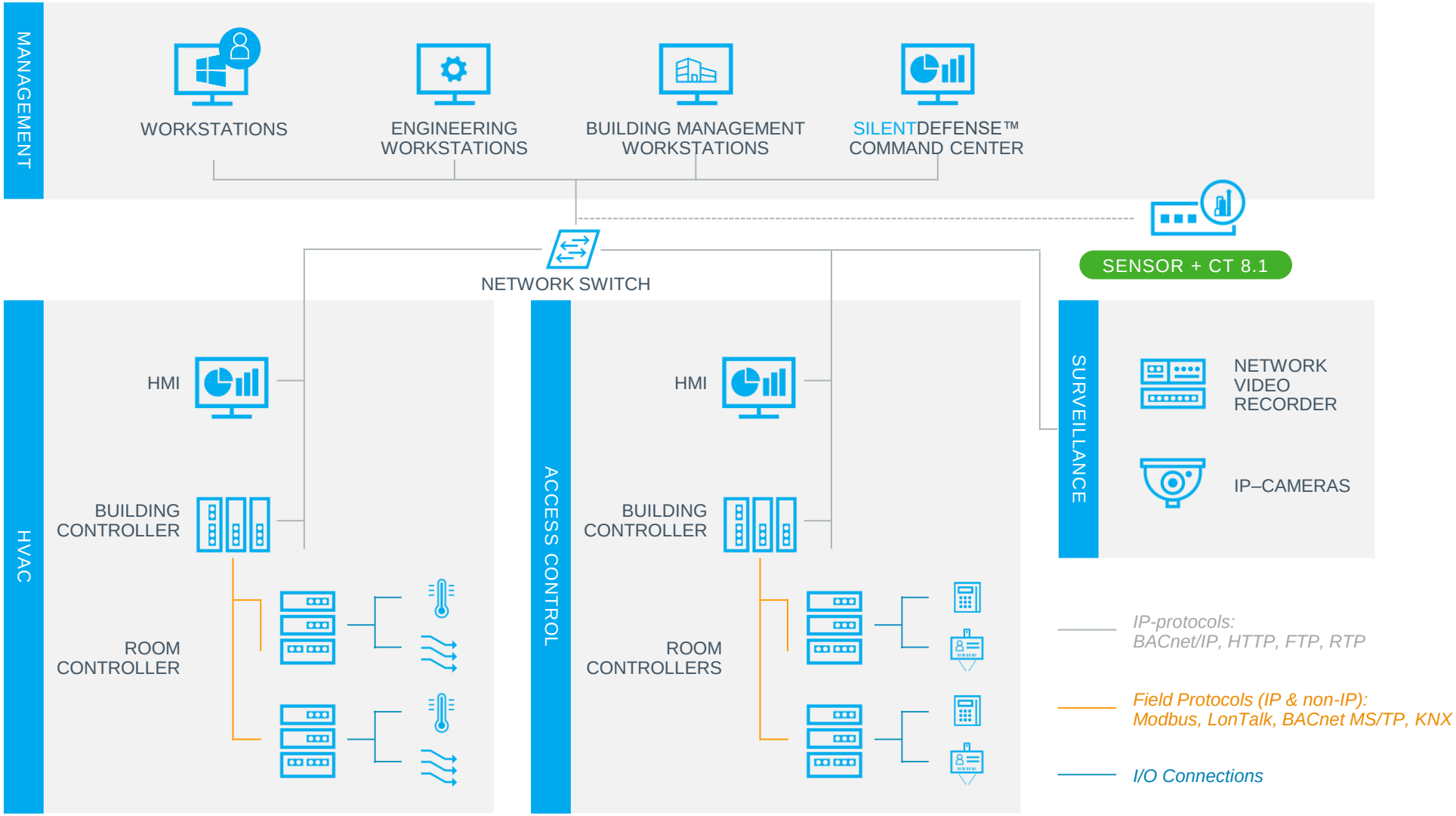
Standard OT Protocols

- BACnet
- CC-Link (Field, FieldBasic Control)
- DNP3
- EtherCAT
- EtherNet/IP + CIP
- Foundation Fieldbus HSE
- IEC 60870-5-104
- ICCP TASE.2
- IEC 61850 (MMS, GOOSE, SV)
- IEEE C37.118 (Synchrophasor)
- Modbus ASCII
- Modbus RTU
- Modbus/TCP, OPC-DA
- OPC-AE
- PROFINET (RPC, RTC, RTA, DCPand PTCP) SLMP

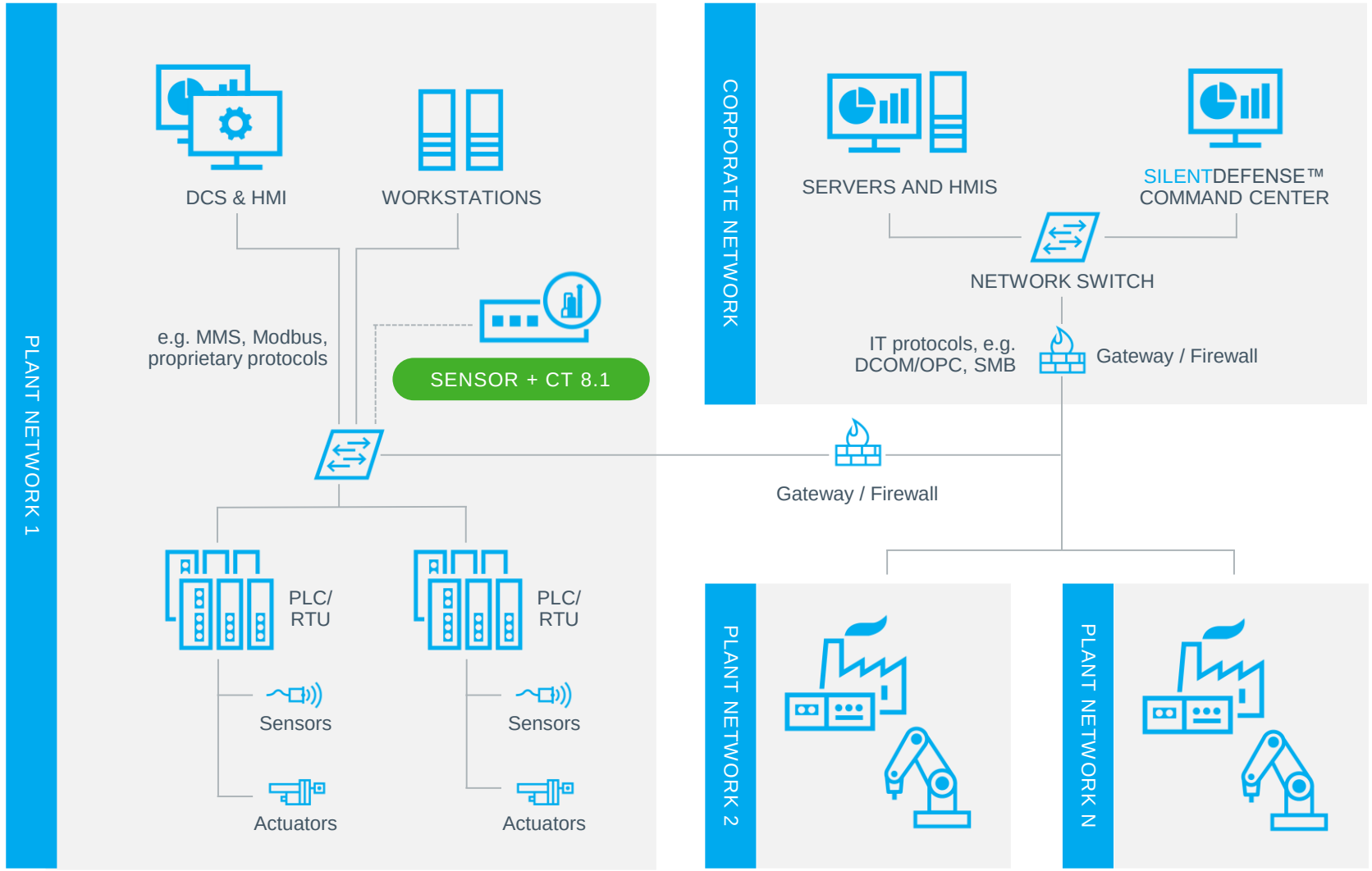
IT Protocols

- AFP
- BGP
- DHCP
- DNS
- DTP
- FTP
- HTTP
- IMAP
- Kerberos
- LDAP
- LDP
- LLDP
- MS-SQL
- MQTT
- NMF
- NTP
- NetBIOS
- OpenRDA
- Oracle TNS
- POP3
- PVSS
- Radius
- RDP
- RFB/VNC
- RPC/DCOM
- RTCP
- RTP
- RTSP
- SMB /CIFS
- SMTP
- SNMP
- SSDP
- SSH
- SSL
- STP
- SunRPC
- Telnet
- TFTP

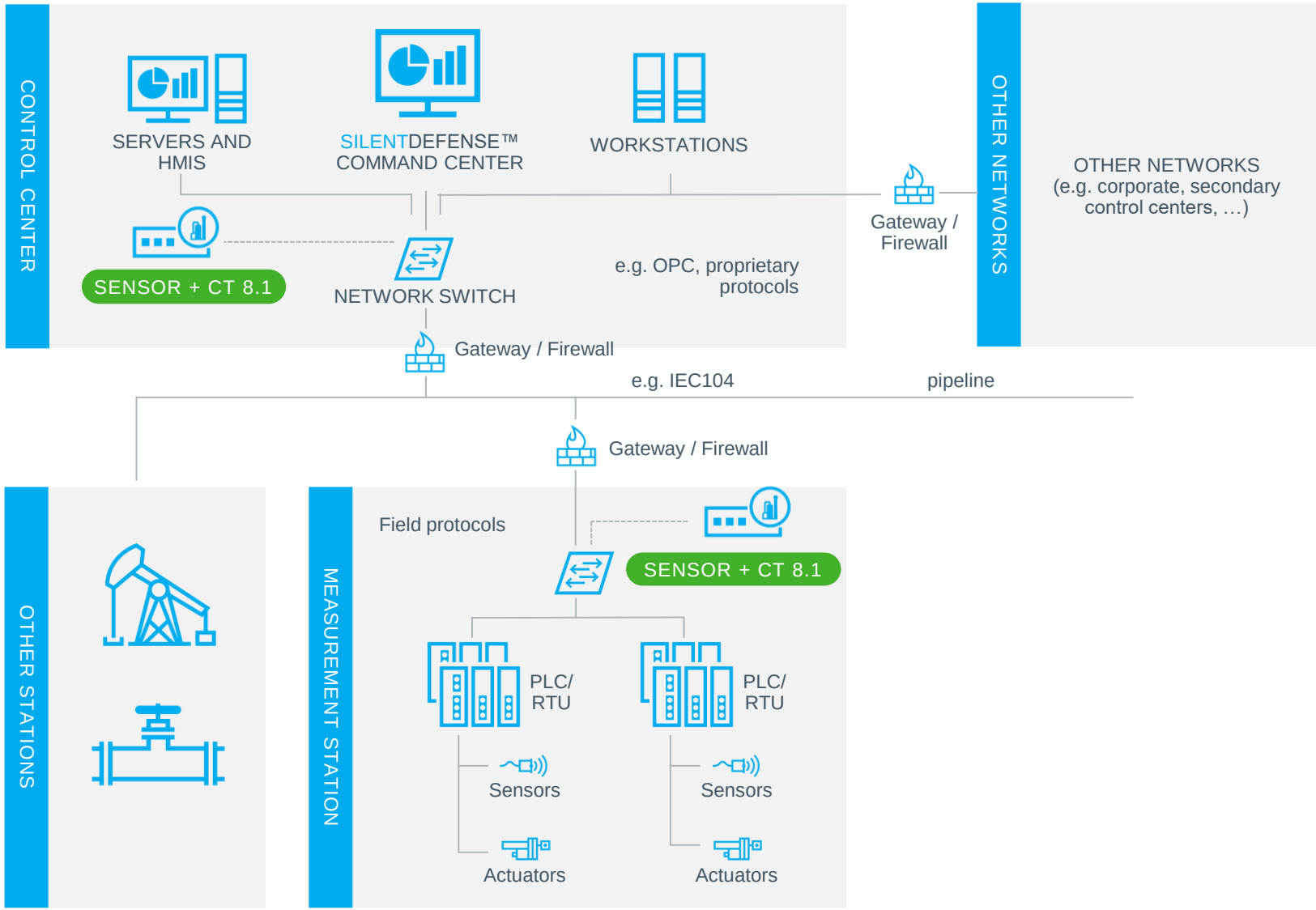
Building Automation



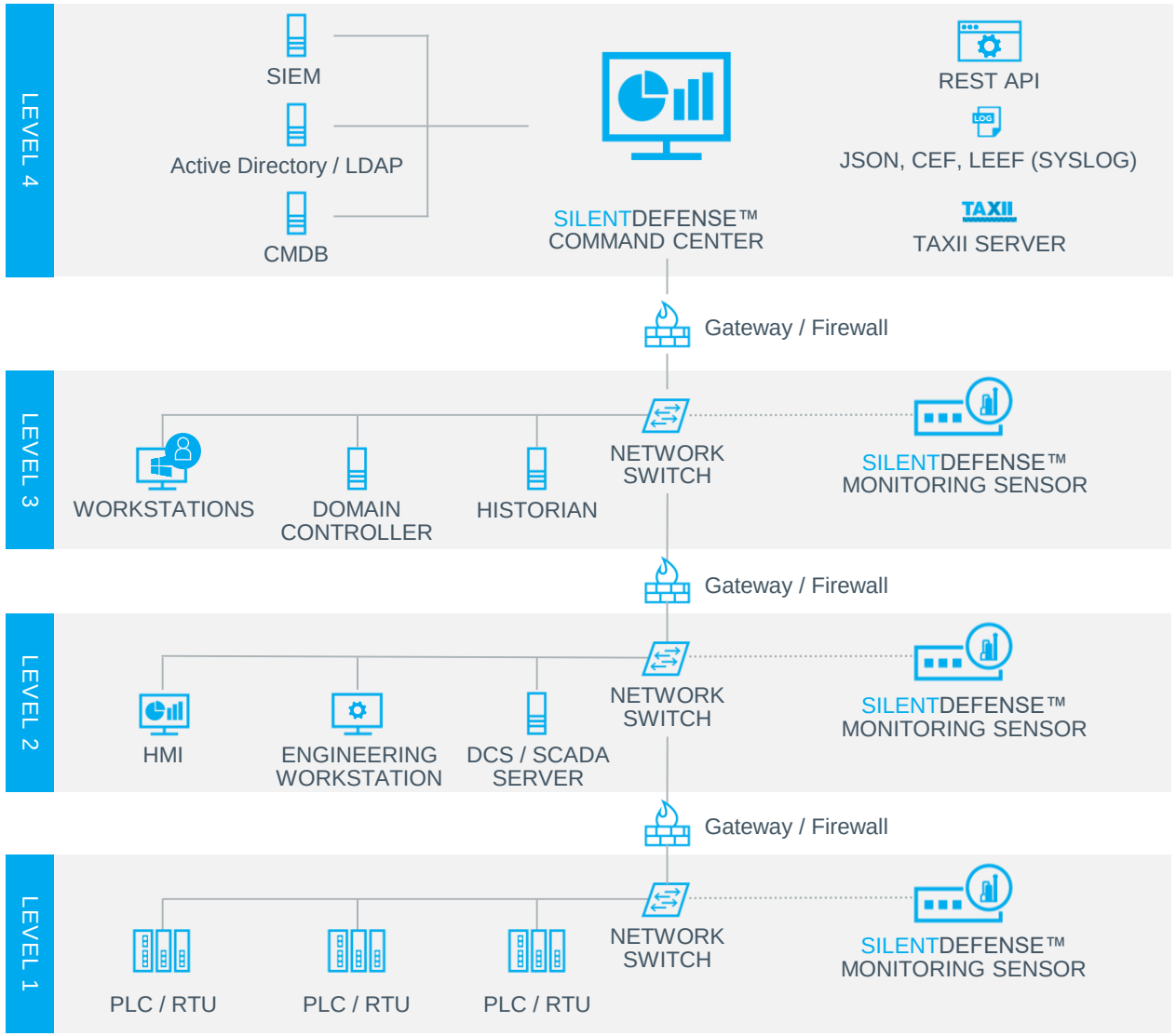
Plant / Manufacturing (DCS)



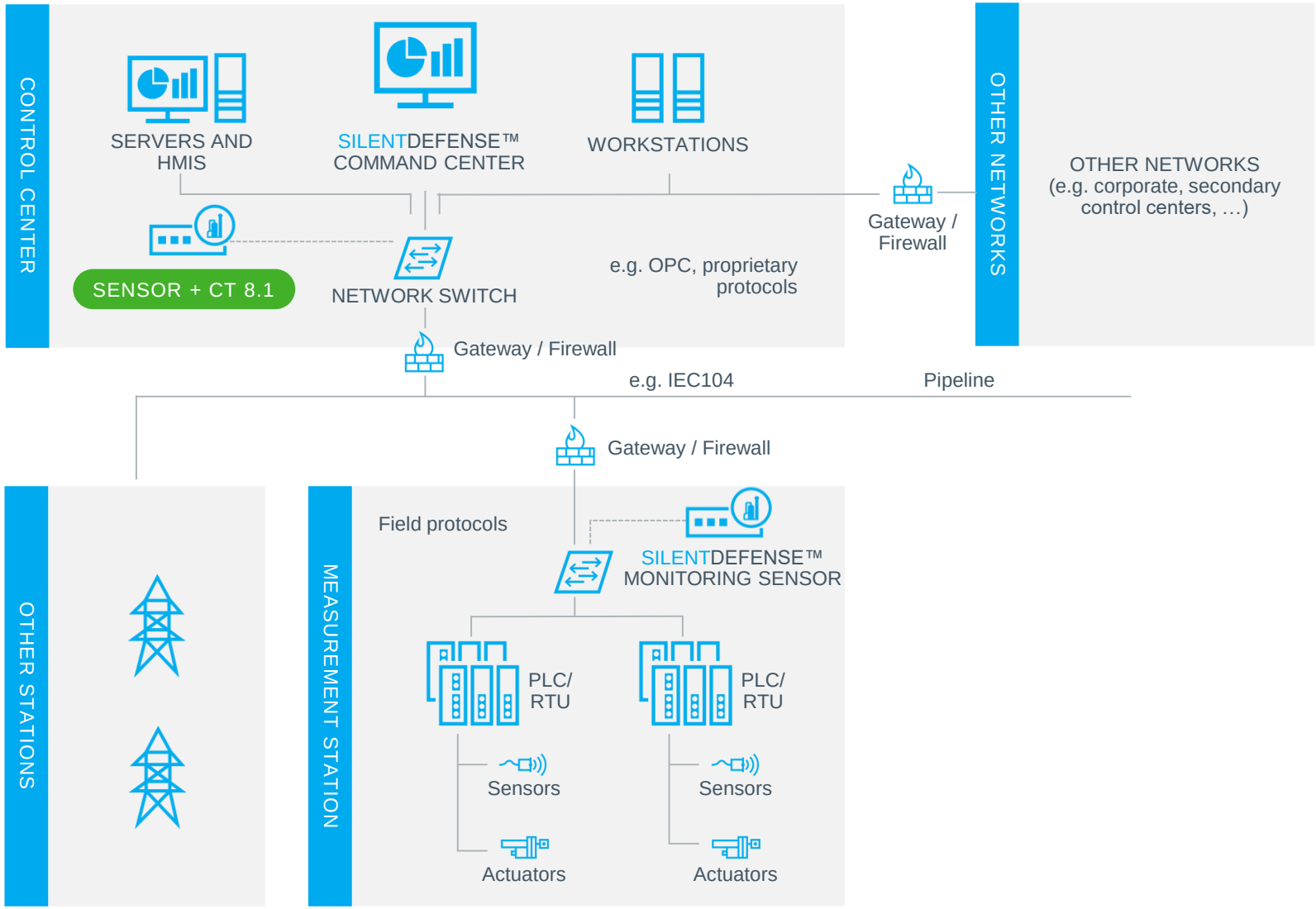
Oil & Gas Pipeline



Industrial Automation



Electric Power



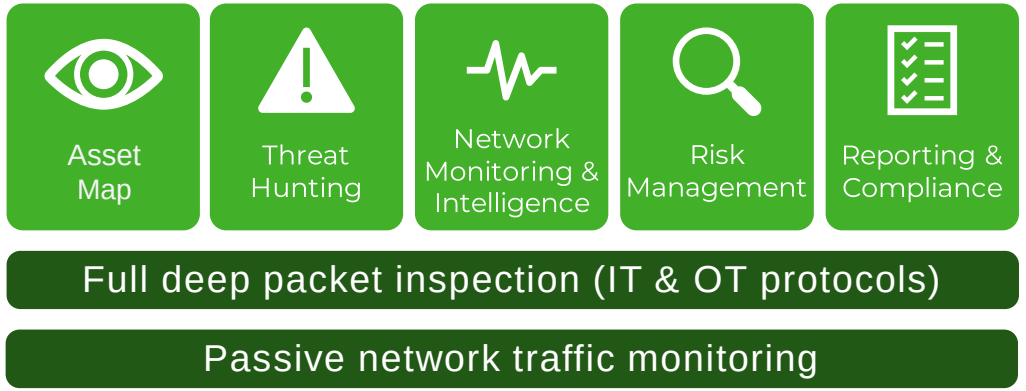
FORESCOUT 8.1: Unified Device Visibility and Control Platform

OT Premium Offering

ForeScout CounterACT®

Existing Integration

SecurityMatters SilentDefense™



Easy Deployment

- Easy to use
  - 802.1X not mandatory
  - Non-intrusive, audit-only mode
  - No agents needed (dissolvable or persistent agent can be used)
  - Simple policy management
- Fast and easy to deploy
  - All-in-one appliance
  - Out-of-band deployment
  - No infrastructure changes or network upgrades
  - Rapid time to value – unprecedented visibility in hours or days
  - Physical or virtual appliances
  - Policies can be initially built in a monitor only mode, no control actions
- Ideal for multi-vendor, heterogeneous network environments

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)

Next Steps