FORESCOUT

FORESCOUT

The Platform for IT-OT Device Visibility and Control

Ricardo Hernandez
Sales Manager Spain & Portugal

New Technologies & New Responsibilities

2023

Device Growth

"By 2023, the average CIO will be responsible for more than 3x endpoints the manage in 2018."

–Gartner

2021

Responsibility Growth

"By 2021, 70% of OT security will be managed directly by the CIO or CISO, up from 35% today."

–Gartner

What We Hear in the Market

76%

Of industrial sec ops indicate that a cyber-attack is "very or extremely high"

(World Economic Forum)

4 out of 10

ICS security practitioners lack sufficient visibility into their ICS networks

(SANS Institute)

69%

Consider the current threat to their ICS systems to be high or severe/critical

(SANS institute)

100%

Of organizations have IoT technologies, using an avg. of 4.7 different technologies

(Forrester)

44%

Consider that adding devices to the network is the top ICS threat

(SANS Institute)

The 6 Challenges and Risks

Unplanned Operational Downtime

Revenue Growth

IT-OT Relationship Puzzle

Increasing Cyber Threats

Limited Resources/Increasing Workloads

High-Effort Compliance Fulfillment

Common Challenges. Different Perspectives.

IT		OT
From OT devices	**Threats**	From unpermitted devices
Brand, revenue, confidentiality	**Impact**	Productivity, human safety, operations
Cost of audit	**Compliance**	Operations implementation
Connected devices	**Visibility**	Location, behavior, state, performance
Insecure points of entry	**IoT**	Monitoring, predictive maintenance
Device context	**Automation**	Safety concerns
Distributed operations	**Remote Sites**	Costly to monitor
Device impersonation	**Rogue Devices**	Banned, prohibited devices
Security tools, network infrastructure	**Heterogeneity**	Vendors, protocols, legacy, proprietary
Lack of skills	**Resources**	Lack of tech, IT knowledge and skills

Too Much Data, Not Enough Resources

Cybersecurity

- **Blind** to devices in OT networks
- **Unable** to detect vulnerability
- **Complex** system integrations
- **Slow** threat response time

Networking / Infrastructure

- **No** mapping
- **No** segmentation
- **Unable** to monitor packet flows
- **Limited** device compliance

Operations

- **No** real-time asset inventories
- **Inaccurate** tracking firmware and model information
- **Incomplete** vendor and contractor activities
- **Costly** site visits

IT-OT Challenges

The Cost of Doing Nothing

Average cost per hour of unplanned downtime is $260,000*

Impact $$$$$ Frequency: Yearly	Impact $$$ Frequency: Weekly	Impact $ Frequency: Daily

**Multiple sources: Internal Calculation on Contingency Planning Research & Schneider Electric, ATS Survey, Aberdeen Group*

Cybersecurity	Networking / Infrastructure	Operations
Undesired Access and Flows	Connectivity Issues with Field Devices	Unstable Process Values
Stuxnet, Havex, Ukraine Blackout	Routing and/or Gateway Issues	Incorrect Process Measurements
Firewall Misconfigurations	Data Sent in Noncompliant Format	Misconfigured Devices / No Compliance
Intruders Sending Corrupt Commands	Use of Insecure Protocols	Failure and Downtime (short term)

Forescout Provides

Complete real-time IT-OT network visibility

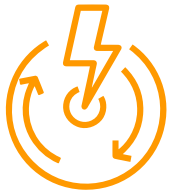
Scalable threat detection and resiliency

Simplified device and regulatory compliance

Continuous process improvement

We provide customers with:

Improved productivity and processes



Faster mitigation of threats

Lower risk profile, leaner operations, stronger brand reputation and higher profits

Why it Matters

Deeper visibility into OT and ICS environments

End-to-end IT-OT risk awareness and compliance

Dynamic network segmentation across the entire enterprise

Automated rapid detection & incident response

Expanded capabilities and advanced features to secure IT and OT and industrial environments.

What if you could…

01 Rapidly implement and manage detailed inventories of all networks and devices?

02 Better detect and remediate both known and unknown cyber threats?

03 Easily manage compliance tasks and network audits centrally?

04 Assure that any vulnerabilities, device changes or behavior alerts are captured?

05 Quickly prioritize vulnerabilities and threat alerts?

Proven Customer References

Manufacturing / Discrete Automation

Food & Beverage

Water Management

Chemicals

Oil & Gas / Process Automation

Pharmaceutical / Life Sciences

Building Automation Systems (BAS)

Electric Power Generation

Electric Power Transmission

Electric Power Distribution

Maritime / Marine

Defense & Aerospace

The Forescout OT-IT Solution

Asset Inventory & Device Visibility

Detailed asset maps ideal for situational awareness

Device & Industry Compliance

- Network assessment
- Network monitoring

Incident Response

Detection of known and unknown cyberattacks and identification of ICS-specific threat indicators

IT

Heterogeneous OT Systems

Immediate Value. Continuous Benefits

Network Profile

Improved productivity and processes

Available in hours

Automated blueprints

Network issues

Vulnerabilities

Suspicious behaviors & protocols

Analysis & Tuning

Faster mitigation of threats

Available in days

Dashboard tuning

Process & network learning

Identification of threats

Specific checks & customization

Monitoring & Integration

Lower risk profile, leaner operations, stronger reputation & higher profits

Always on

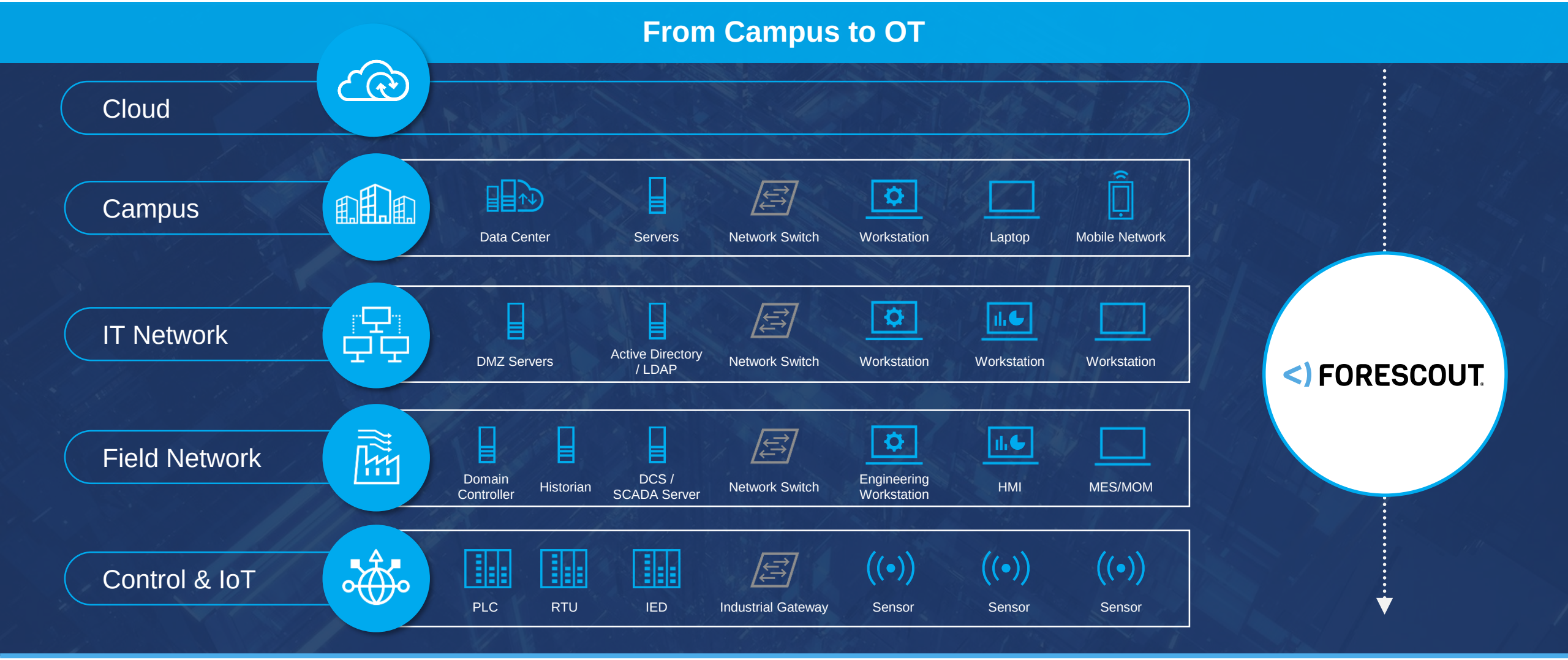
Raise alerts

Changes & anomalies

Continuous reporting

Enterprise workflow integration

The Only Integrated IT-OT Solution



We help organizations like yours to:

Achieve Cyber Resiliency

Achieve complete visibility into your IT and OT network

Detect, analyze and respond to cyber threats and operational issues

Implement automated prescriptive and predictive maintenance

Prevent unexpected downtime to lower operational costs

Forescout provides asset owners with full visibility into their network to detect operational and cyber threats before they affect service, safety and the bottom line.

Thank You