FORESCOUT

CYBER SECURITY CHALLENGES FOR OT/ICS/IOT

Dr. Elisa Costante, VP Research at Forescout

Forescout: A Global Security Company

Customers

3100+
Customers in over 80 countries

4M+
Devices in largest deployment

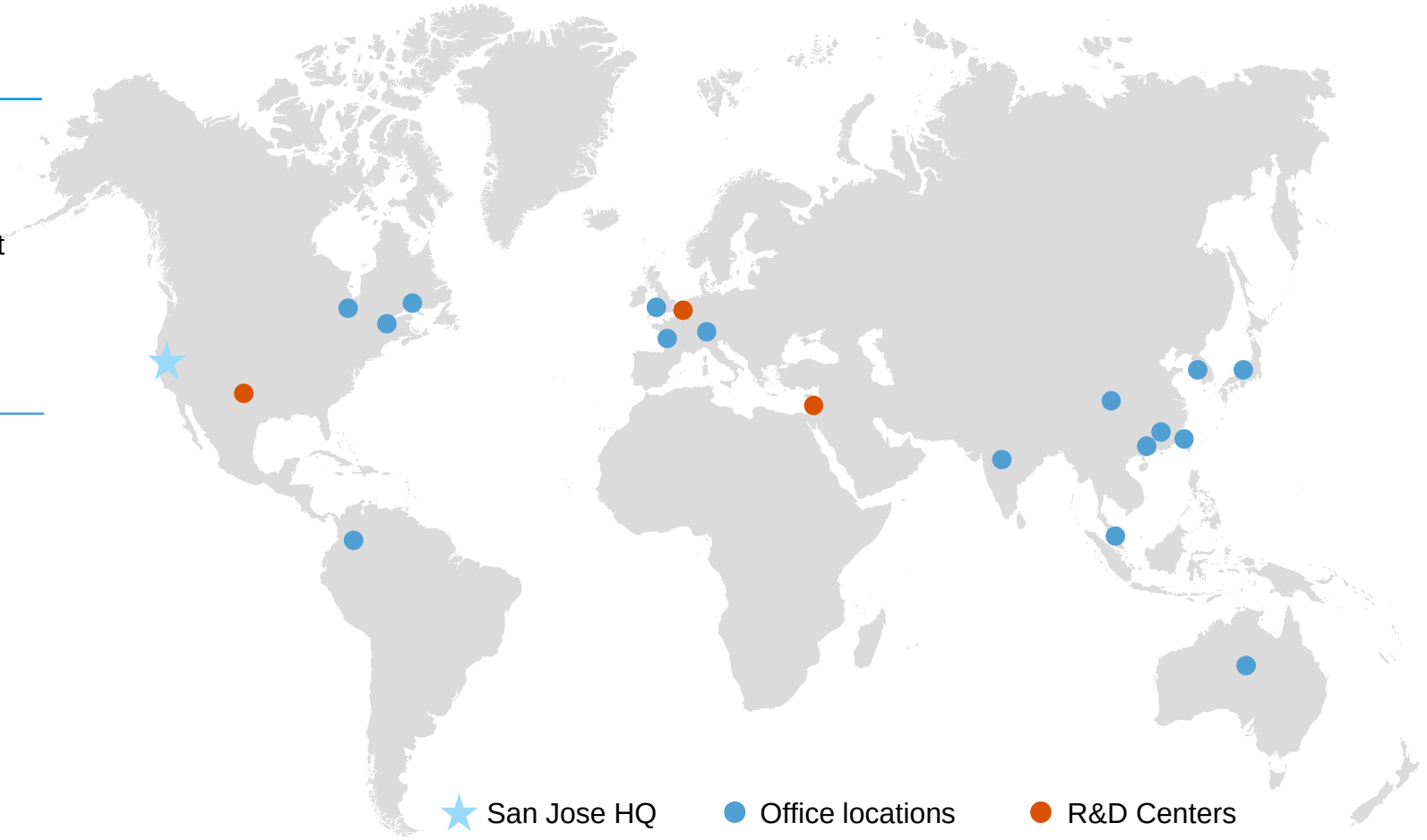
Intelligence

15M+
Unique Device Fingerprints

455M+
Device Datapoints

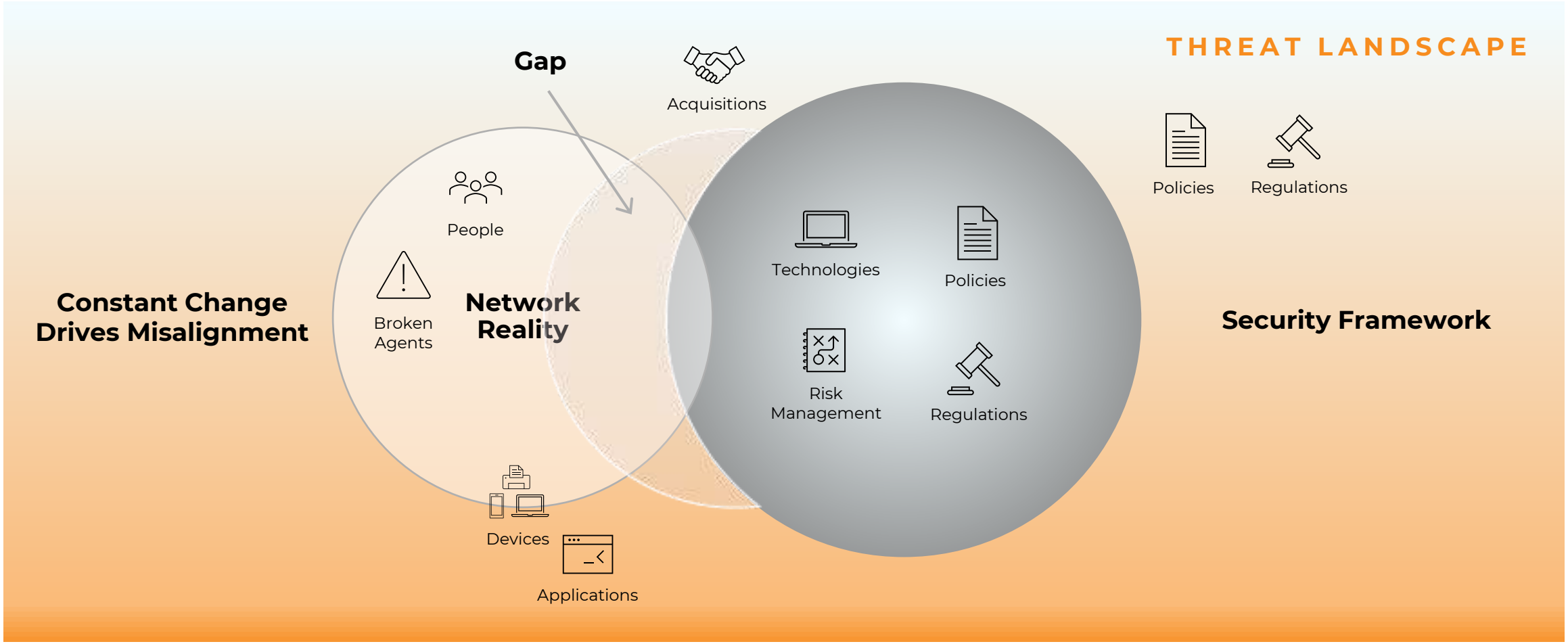
R&D Team

300
Team members (total)

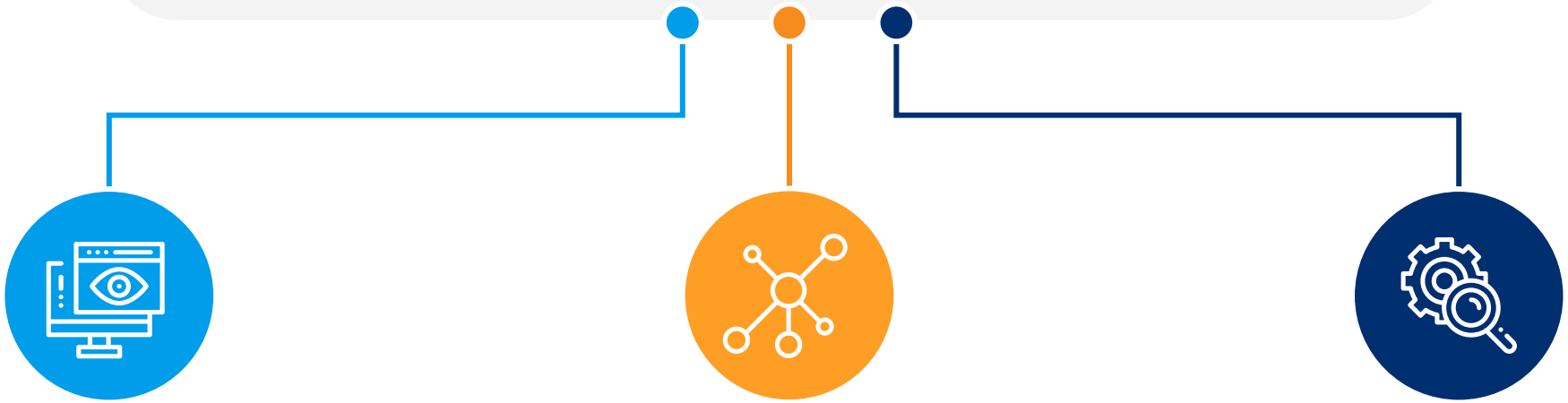


More Connectivity. New Risks.

Landscape


Gap
Acquisitions
THREAT LANDSCAPE
Policies
Regulations
People
Broken Agents
Network Reality
Technologies
Policies
Risk Management
Regulations
Constant Change Drives Misalignment
Security Framework
Devices
Applications

Challenges



Cybersecurity

- Limited to no visibility in OT networks
- Inability to discern if systems are vulnerable
- Too many alerts and logs to manage efficiently
- Complex and clunky integration into SIEM and other enterprise tools
- Slow and expensive threat detection and response time

Infrastructure

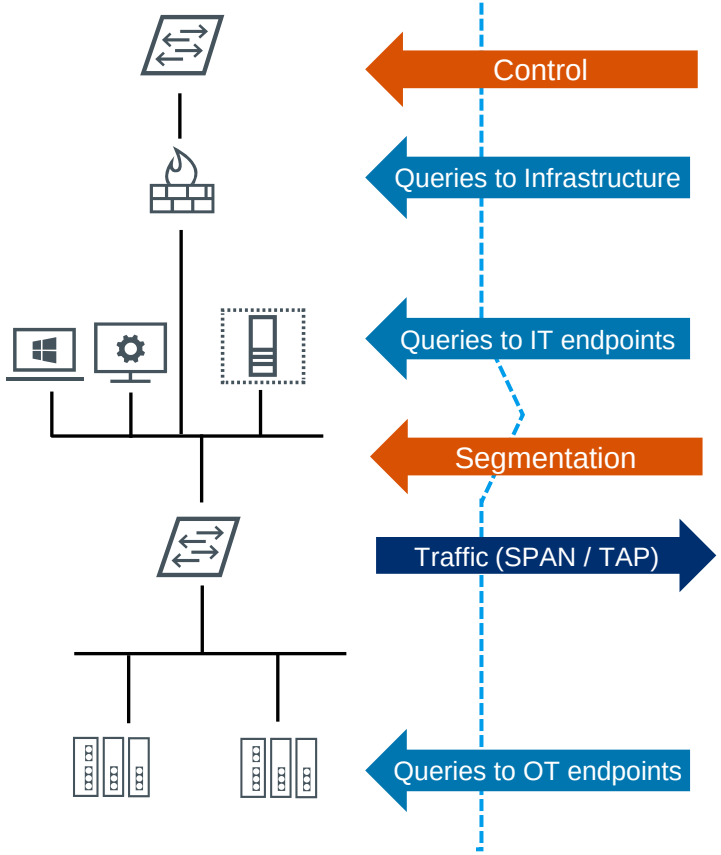
- No network maps and good knowledge of device location in the field/plant environment
- Limited segmentation strategy for OT
- Inability to monitor and understand packet/traffic flows
- Lack of device compliance
- (Is my switch configured correctly?)

Operations

- Unable to monitor and enforce compliance tasks
- No real-time asset inventory
- Inaccurate tracking of device firmware and model information
- Incomplete vendor and contractor activities
- Costly and time-consuming site visits to field

Forescout's Solution

NETWORK



Control

Queries to Infrastructure

Queries to IT endpoints

Segmentation

Traffic (SPAN / TAP)

Queries to OT endpoints

FORESCOUT PLATFORM

Discover | Assess | Govern

Passively Discover & Assess

Passive asset discovery by parsing the various IT and OT protocols seen in the network using patented Deep **Protocol** Behavior **Inspection**. Risk assessment with ICS-specific CVE DB & Threat Indicators

Actively Discover & Assess

Discover asset details and compliance using more **passive** & **active** techniques by **querying infrastructure** and **selected endpoints**

Exchange insights

Share information and automate workflows through integrations with other IT and security products

Assess & Govern Access

Dynamically group, visualize and isolate assets to minimize exposure and breach impact

Enforce & automate policy-based controls to proactively reduce your attack surface and rapidly respond to incidents

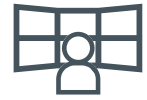
THIRD PARTY ENTERPRISE SYSTEMS

Alerts

Assets

Tickets

Risks, IOCs & CVEs



SIEM /SOC

Asset DB & Ticketing system

LDAP / AD

Vulnerability Assessment Tools

Case studies

Advanced Metering Infrastructure

Key Benefits

- **Enhanced compliance & policy monitoring capabilities**
- **Maximized cyber resiliency**
- **Faster response times with detection & logging**

Challenge

European utility is looking for ways to detect uncompliant and misbehaving smart meters, e.g., with malformed traffic, terminating power delivery or unencrypted commands. A challenge is that part of the traffic is encrypted and more than a million of smart meters will be deployed in the next years.

Solution

Built-in malformed traffic detection for unencrypted DLMS/COSEM traffic & Decryption of encrypted traffic for further deep packet inspection and compliance monitoring

Detection and alerting of unresponsive meters

Logging & Detection of commands that close, disconnect or schedule closure of a meter and further customer-defined commands

Alerting of, for example, Set/Action requests sent unencrypted or too many commands overloading meters

Electric Power Distribution

Key Benefits

- **Extending ICS visibility & maintenance scheduling for substation fleet**
- **Improved threat detection and threat analysis for informed remediation strategy**

Challenge

Our customer needed to find a way to improve their fleet monitoring and security strategy for hundreds of substations without ripping out and replacing their existing infrastructure. They had the goal of monitoring all traffic at 150+ IEC 61850 substations with DNP3 and ICCP servers as well as synchrophasor technology.

Solution

Detected misconfigurations of substation devices

Detected malfunctioning RTU causing loss of process visibility

Detected problem in the US power grid, buffer overflow in PLCs due to grid instability

Detected undesired operations, operators connecting to field devices with Telnet instead of SSH

Electric Power Generation

Key Benefits

- **Improved ICS visibility and faulty equipment detection**
- **Detection of several suspicious operational and cyber behavioral patterns**

Challenge

Our customer needed to implement a non-intrusive cybersecurity solution for multiple 100MW+ generation stations which could integrate seamlessly with Emerson Ovation and Modbus protocols.

Solution

Detected unwanted external DNS lookups to 13 different DNS servers across the globe in 22 different domains

Detected unsupported antivirus software in the system

Detected MODBUS gateway malfunctions

Detected self-configured IP addresses in 4 different nodes which were identified and properly configured

Detected unauthorized use of TELNET inside the control system network for maintenance work

Thank You!