


Comply-to-Connect: DoD's Existing Foundation for ICS Cybersecurity



Christina Hoefler -- Global Principal Systems Engineer for OT/ICS Solutions
MOSAICS Industry Day -- 18 May 2021
Security Automation & Orchestration

ForeScout - Actively Defend the Enterprise of Things


by continuously **identifying**, **segmenting** and **enforcing compliance** of *every connected thing*




Customers
3,800 in over 90 countries*
27% of the Global 2000



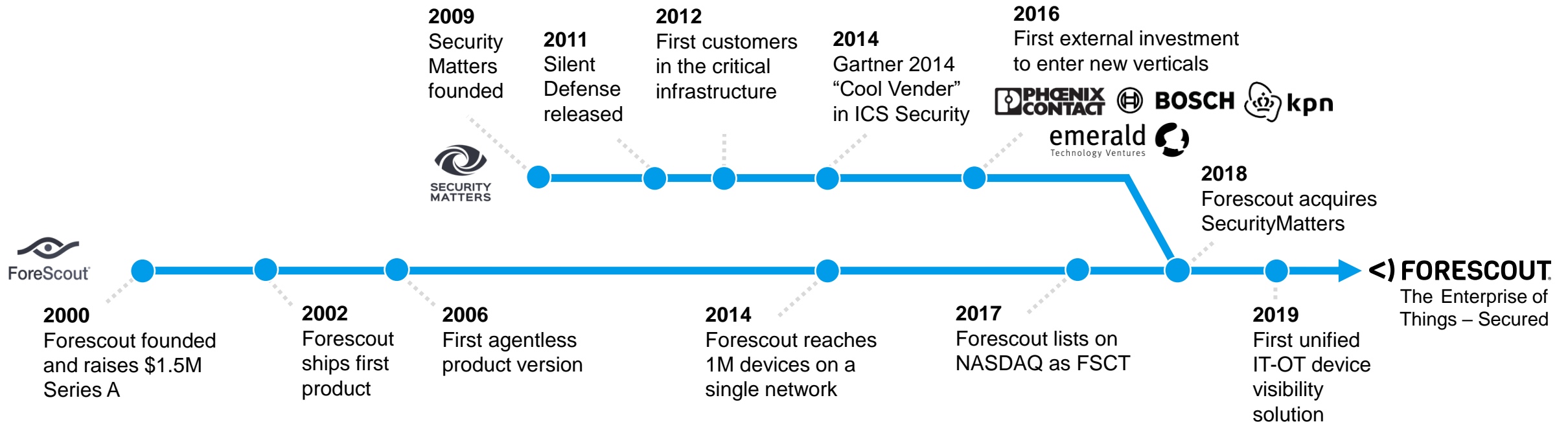
1,000+ Employees
worldwide*



Foundations and Experience in IT, IoT & OT



2 million+ endpoints in a single deployment*

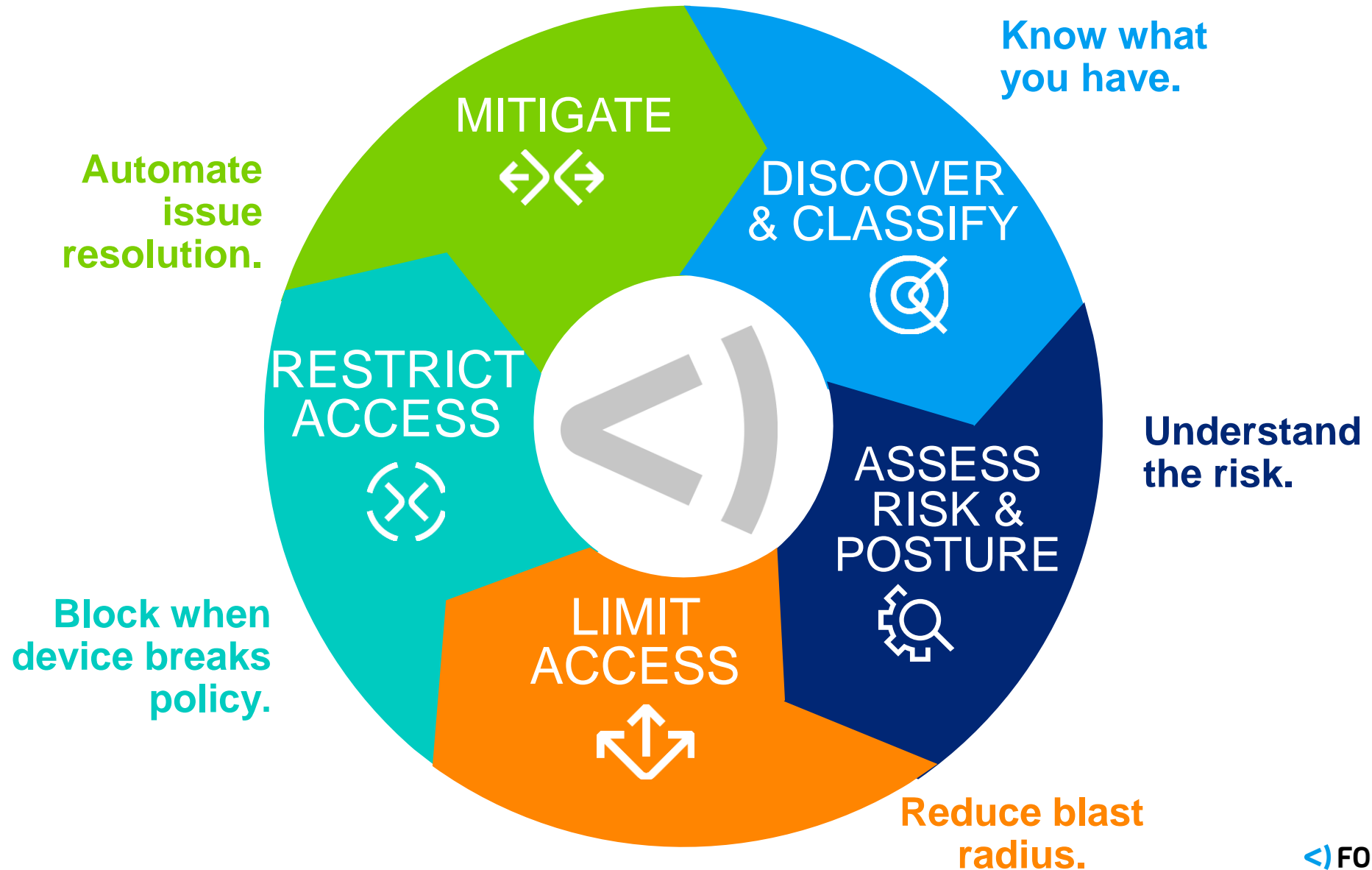


* As of March 31, 2021



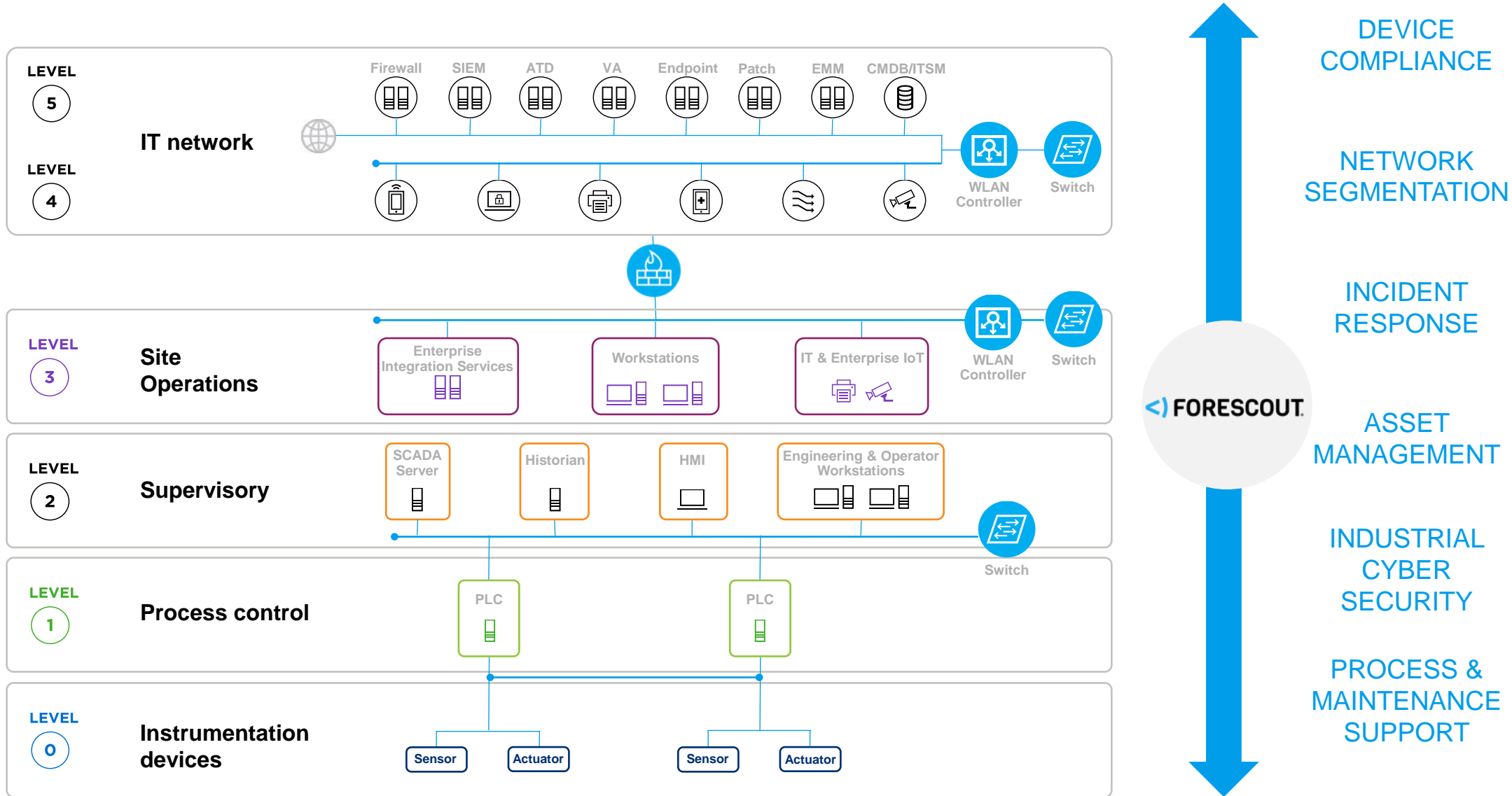
OUR VISION – OUR PLATFORM

Identify and Regulate



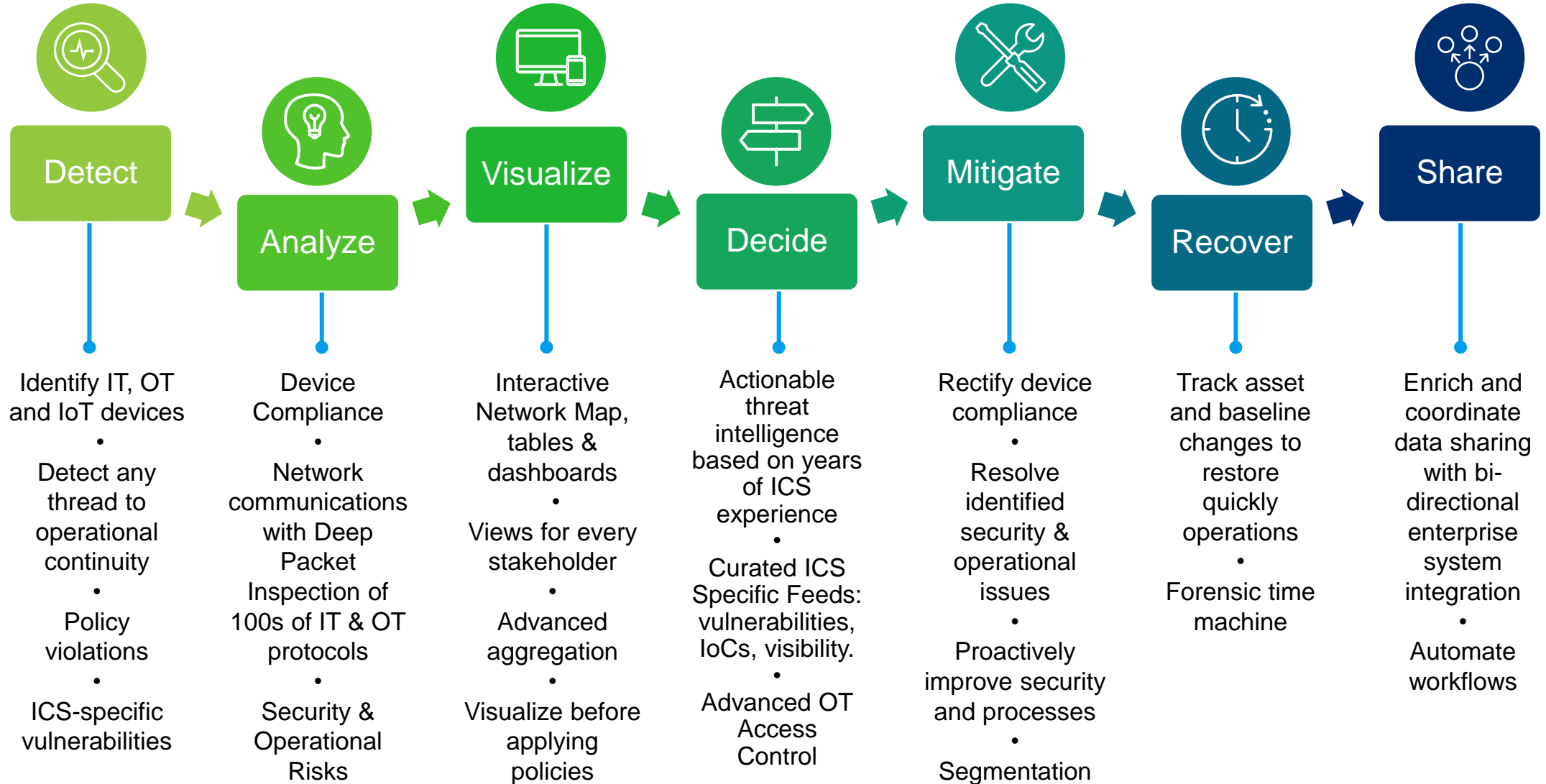


Identify and regulate every connected device



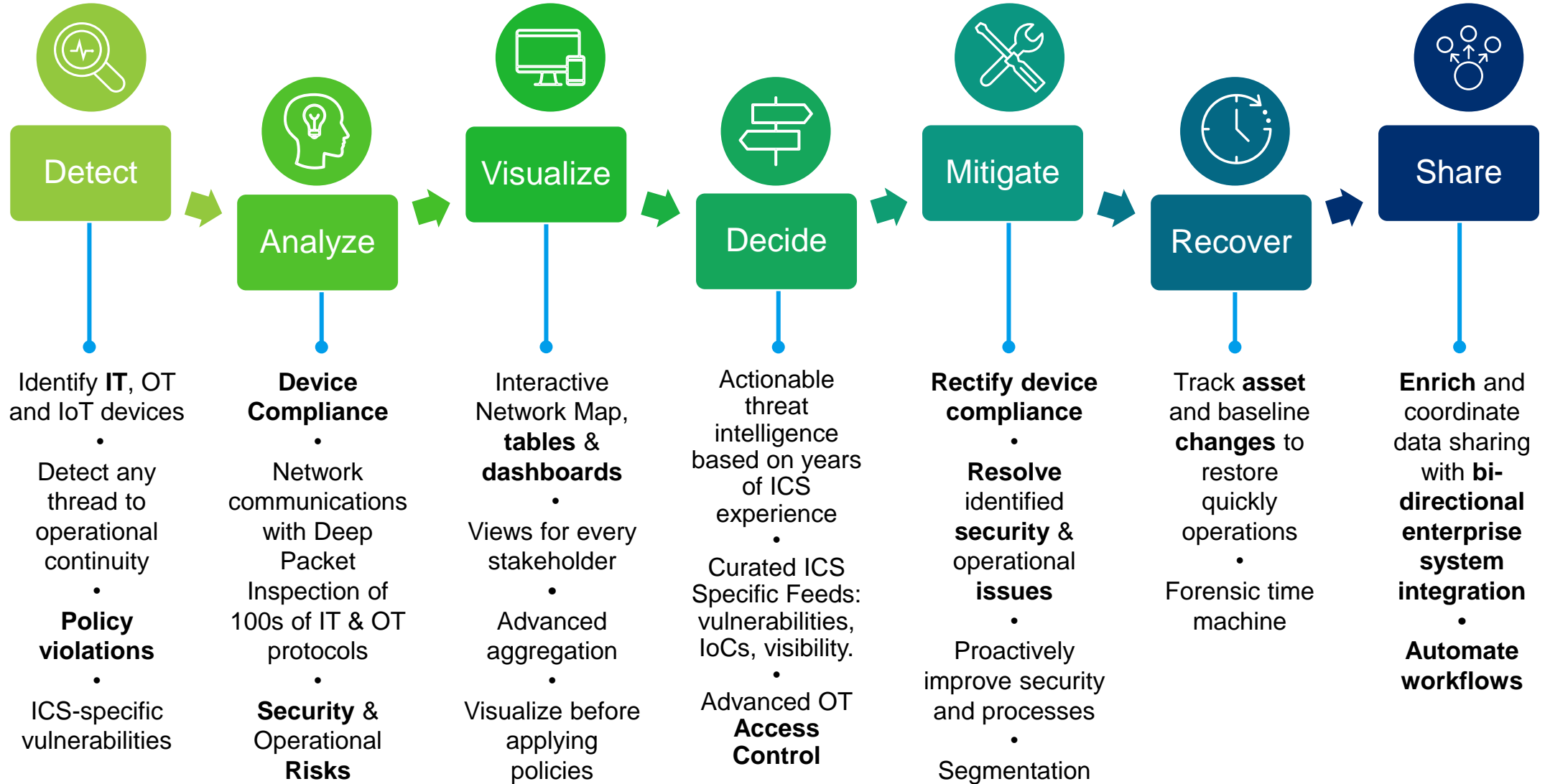


MOSAICS – Operational Cyber Defense with Forescout





MOSAICS – Operational Cyber Defense with Forescout



In bold capabilities with current C2C baseline

Forescout OT Deployment Options

OT NETWORK

- Network Traffic e.g. via SPAN
- Network Infrastructure e.g. Switch, Access Point, VPN concentrator, Firewall
- Endpoints e.g. Windows-based client, Linux server, virtual infrastructure

FORESCOUT PLATFORM

Identify & Assess

eyeInspect
Asset details and potential threats are identified **passively** by parsing the various IT and OT protocols seen in the network using patented Deep **Protocol Behavior Inspection**. Build in ICS-specific CVE DB & Threat Indicators

eyeSight
Asset details and policy compliance are identified as assessed using **passive & active** techniques **querying infrastructure** and **selected endpoints**

Integrate

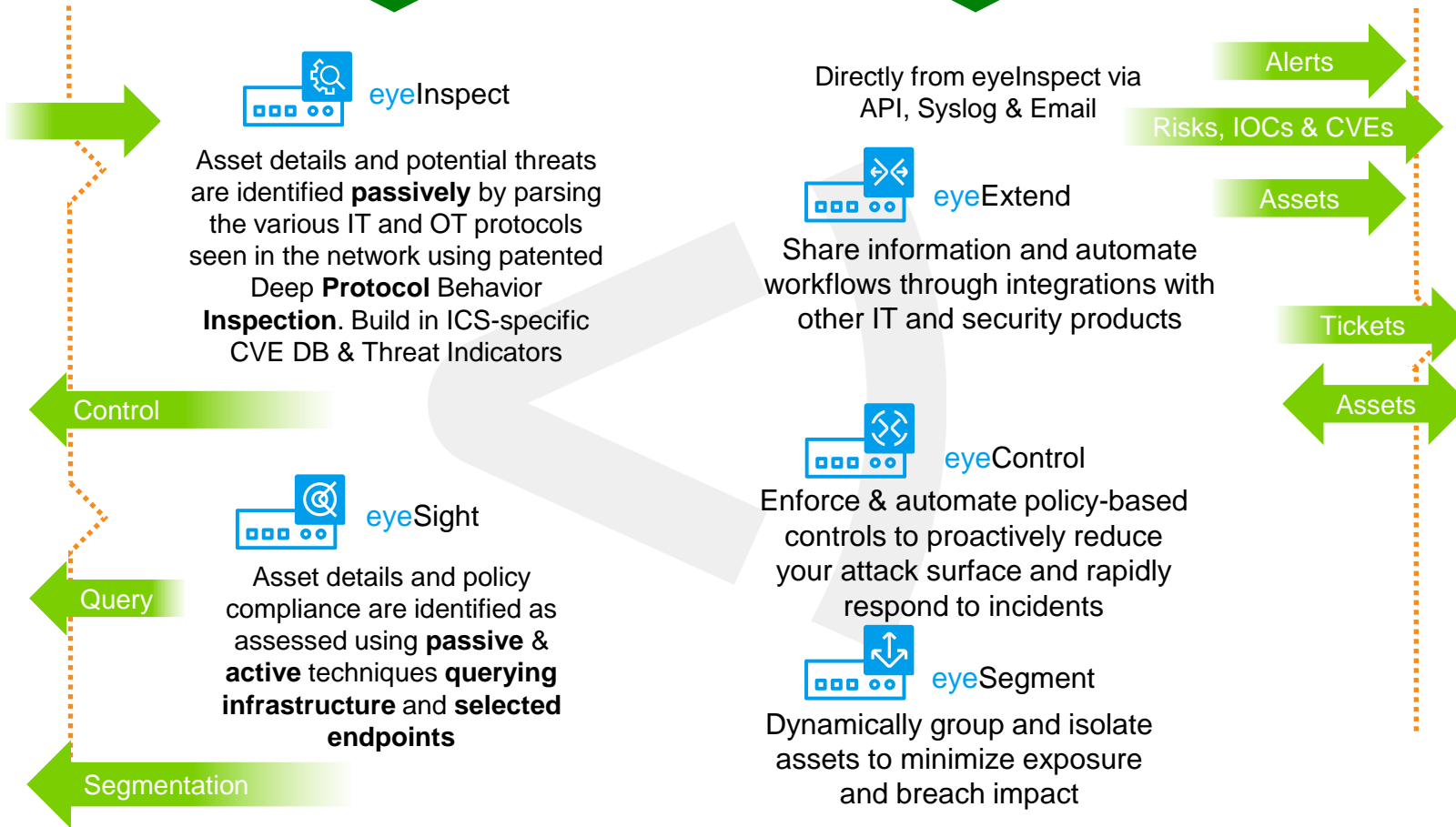
Directly from eyeInspect via API, Syslog & Email
eyeExtend
Share information and automate workflows through integrations with other IT and security products

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

eyeSegment
Dynamically group and isolate assets to minimize exposure and breach impact

THIRD PARTY ENTERPRISE SYSTEMS

- SIEM / SOC
- Asset DB & Ticketing system
- LDAP / AD
- Vulnerability Assessment Tools



Thank You

Christina Hoefler -- Global Principal Systems Engineer for OT/ICS Solutions

MOSAICS Industry Day -- 18 May 2021

Security Automation & Orchestration