ForeScout

Improve Attack Responses Through Real-Time Network Visibility

Chris Sherry

Regional Director, UKI & Northern Europe

1. **Visibility Challenges**

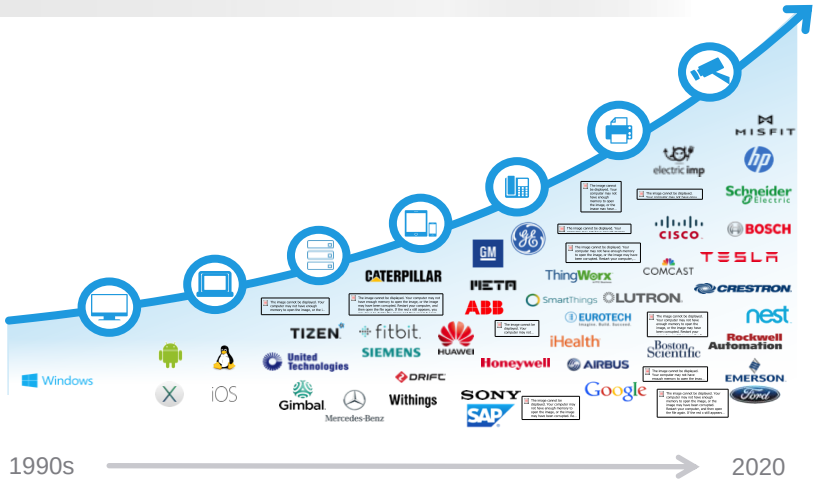
2. Network Visibility

3. Use Cases

Confluence of Macro Trends Creating Visibility Challenges

Growth of Devices and Platform Diversity

- 28Bn IP-based devices by 2020

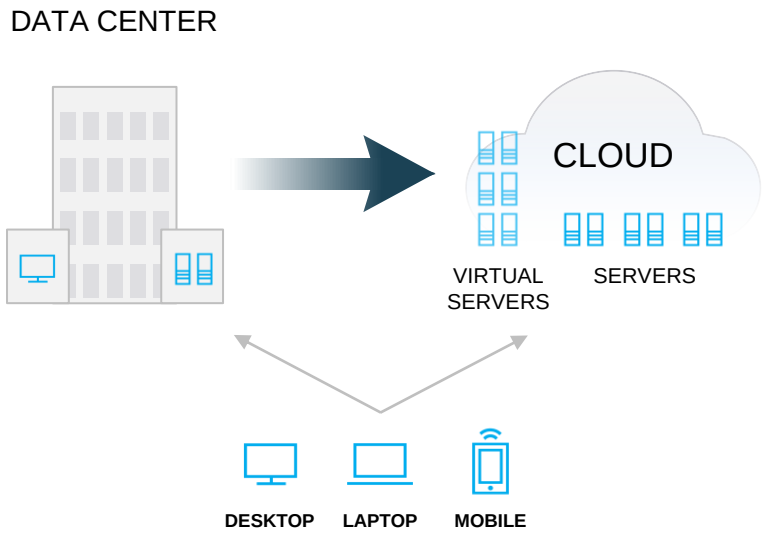


› Innumerable device-specific operating systems (OS)

› Cannot get agents onto new devices

› Cannot write agent-based software for every OS

Cloud Adoption Creates New Challenges

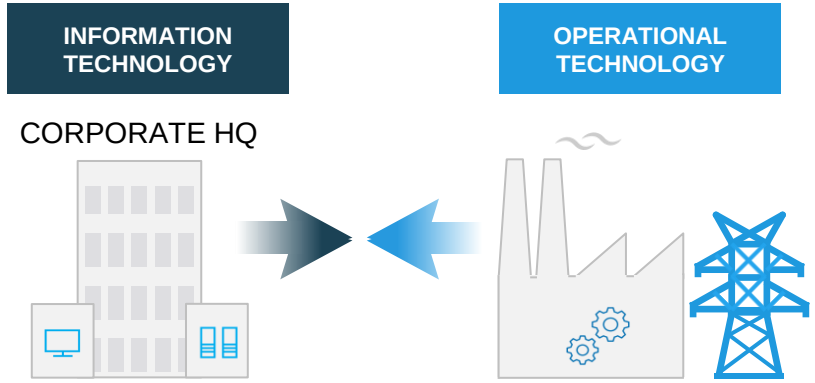


› Multiple Device Locations and Access Points

› Heterogeneous Environment with Multiple Vendors

› De-centralized Management

IT and OT Convergence

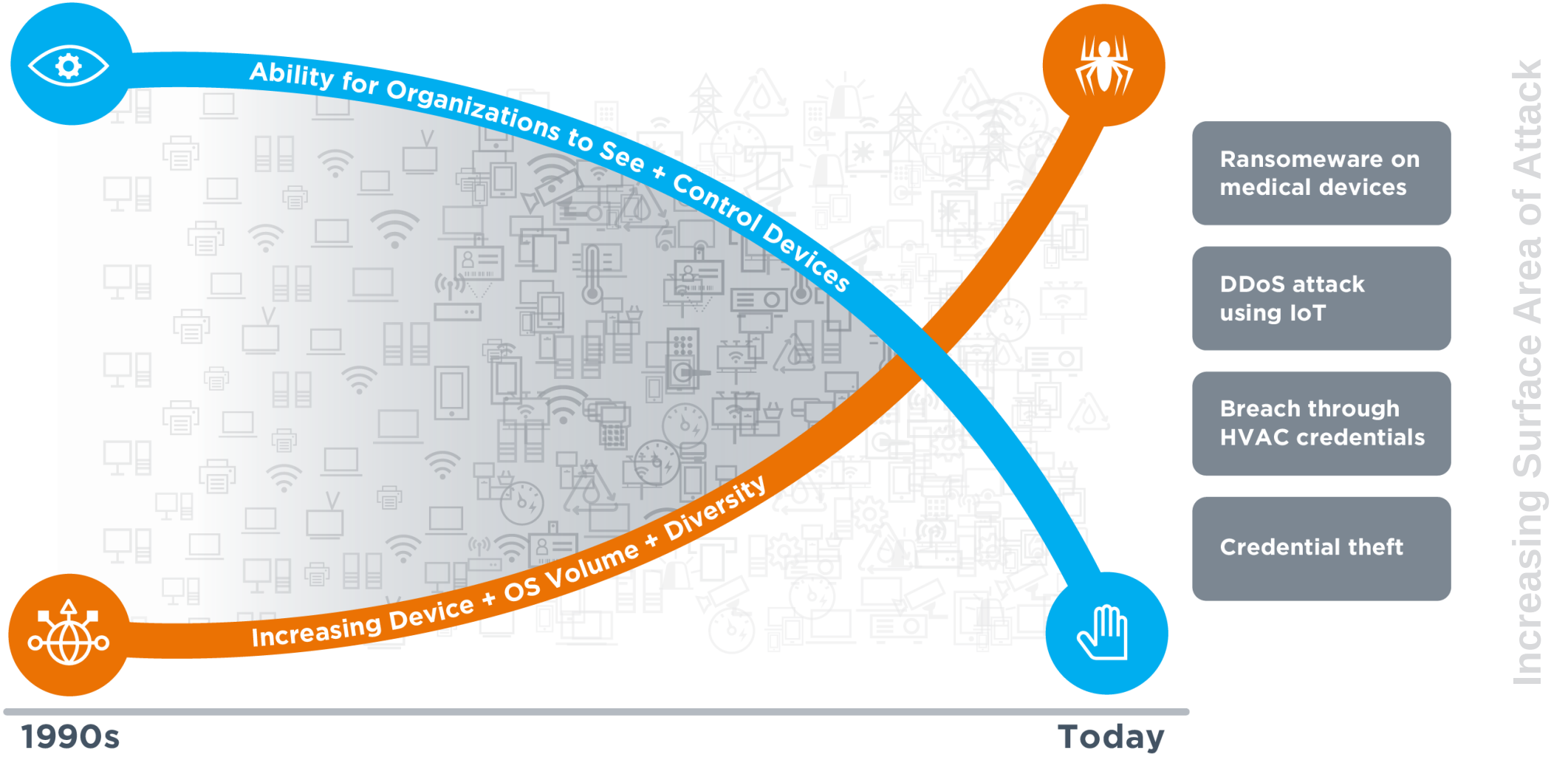


› OT networks are no longer physically separated

› Threats moving between cyber and physical dimensions

› Assets are highly vulnerable and rarely can be patched

Visibility & Control Gap Vulnerability



True Protection Against the Threat

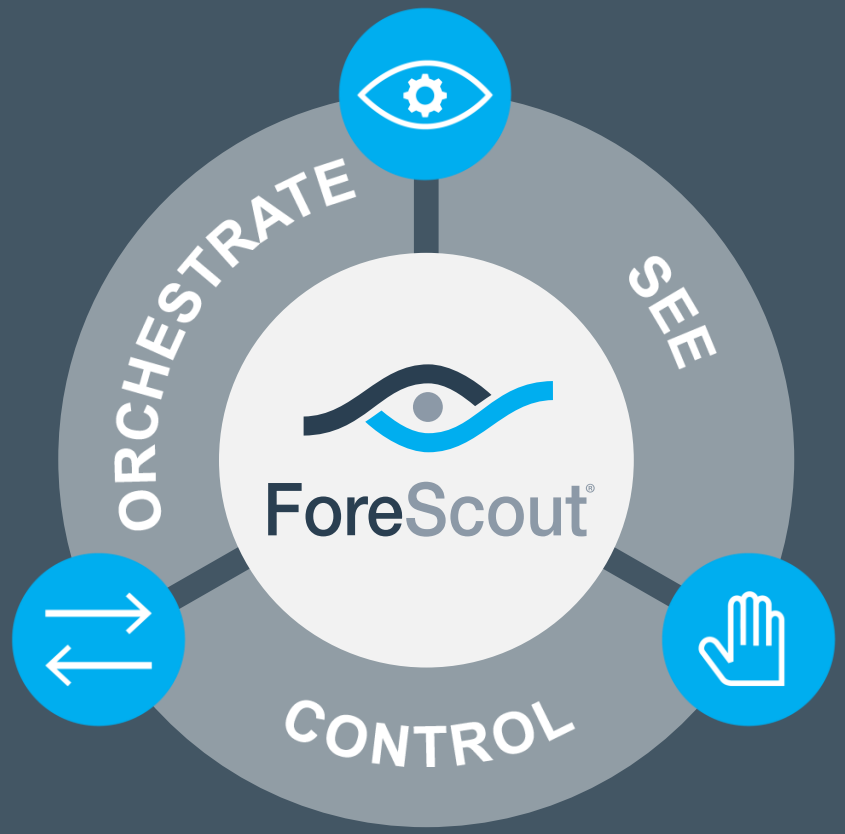
“If you really want to protect your network, you really have to know your network: you have to know your devices and the things on your network”

Rob Joyce
Chief of Tailored Access Operations NSA

1. Security Challenges

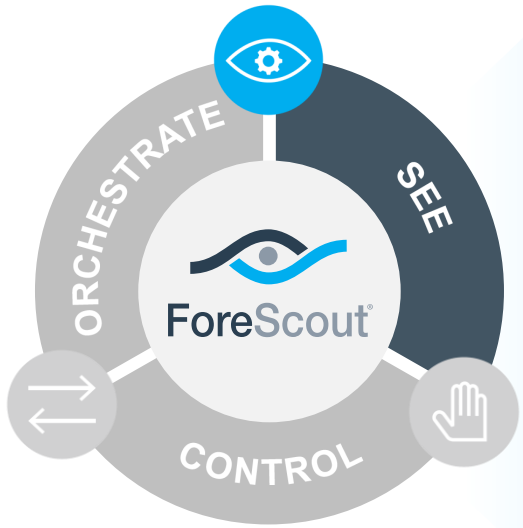
2. Network Visibility

3. Use Cases



ForeScout Platform

See: Discover, Classify, and Assess Devices on the Network



DISCOVER all IP-addressable devices at time of connect

- Connection type
- Hardware info
- MAC and IP address
- Certificate
- Name

- Encryption agents
- Firewall status
- Configuration
- Wired, wireless, and VPN
- Rogue devices

- File name, dates, and sizes
- Services and processes installed or running
- Installed
- Running

CLASSIFY devices into categories using a rich set of data

BYOD | IoT | Corporate Managed

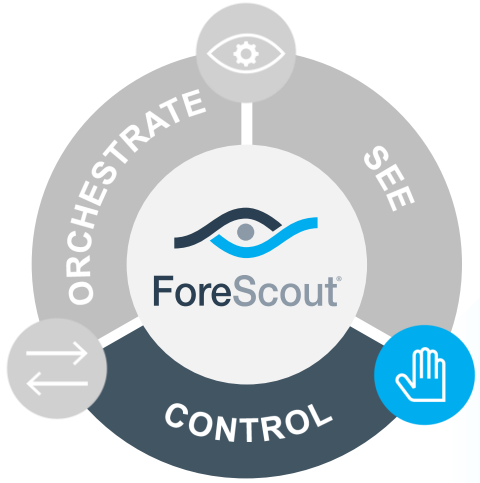
ASSESS device security posture to take action

Personal laptop

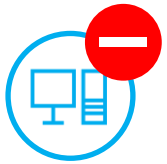
Security camera

Corporate Managed Desktop

Control: Implement Policies and Take Action



Security camera



Windows PC

NOTIFY

- Open trouble ticket
- Send email notification
- SNMP Traps
- Start application
- Run script to install application
- Auditable end-user acknowledgement
- HTTP browser hijack
- Trigger endpoint management system

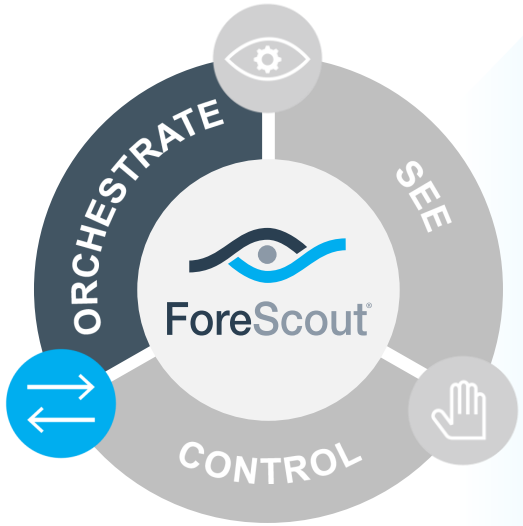
COMPLY

- Deploy a virtual firewall
- Reassign the device to a VLAN
- Update access lists
- DNS hijack (captive portal)
- Move device to a guest network

RESTRICT

- Move device to quarantine VLAN
- Block access with 802.1x
- Alter login credentials to block access
- Block access with device authentication
- Turn off switch port (802.1X, SNMP)
- Wi-Fi port block
- Terminate applications
- Disable peripheral device

Orchestrate: Enhance Value of Existing Security Solutions



+EXTENDED MODULES

EMM
vmware airwatch · MobileIron · IBM

VA
Qualys. · RAPID7 · tenable

NGFW
Check Point SOFTWARE TECHNOLOGIES LTD. · paloalto NETWORKS

SIEM
MICRO FOCUS · IBM · splunk>

EPP / EDR
FireEye · McAfee · Symantec.

ATD
Check Point SOFTWARE TECHNOLOGIES LTD. · paloalto NETWORKS · FireEye

ITSM
servicenow

PAM
CYBERARK

COMPLIANCE
Advanced Compliance (SCAP)

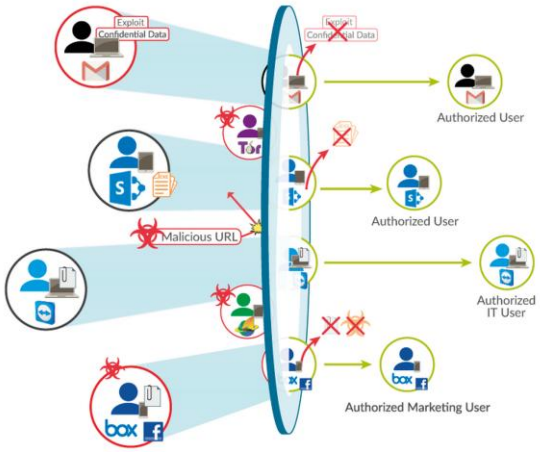
CMT
IBM

+BASE MODULES

SDN
vmware NSX

CLOUD
amazon web services

ForeScout Integration with NGFWs



- ✓ Implement dynamic network segmentation based on real-time device intelligence from ForeScout
- ✓ Share user and device insight from ForeScout CounterACT® to enforce identity aware access policies within Check Point NGFW
- ✓ Reduce your attack surface, prevent unauthorized access to sensitive resources & minimize the impact of data breaches

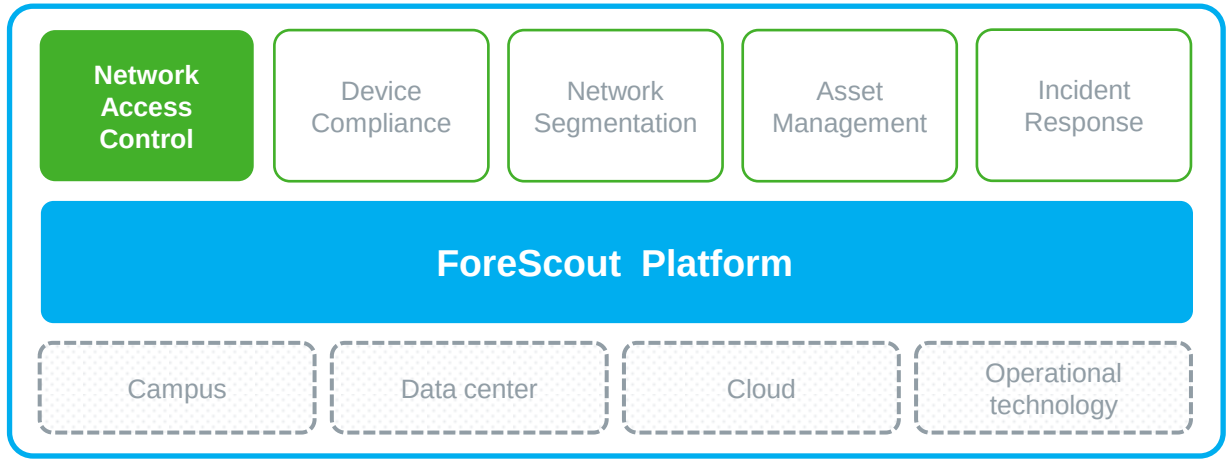
Reference Acronym Glossary at the end of presentation

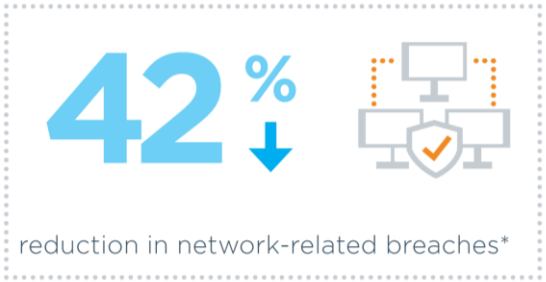
1. Security Challenges

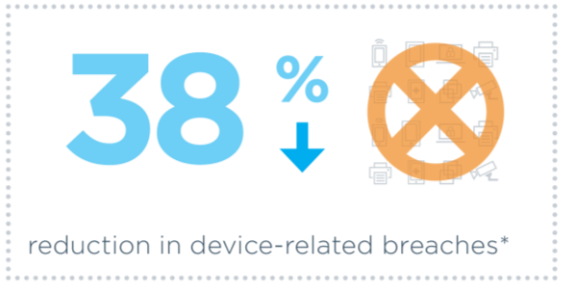
2. Network Visibility

3. Use Cases

Use Case #1– Network Access Control







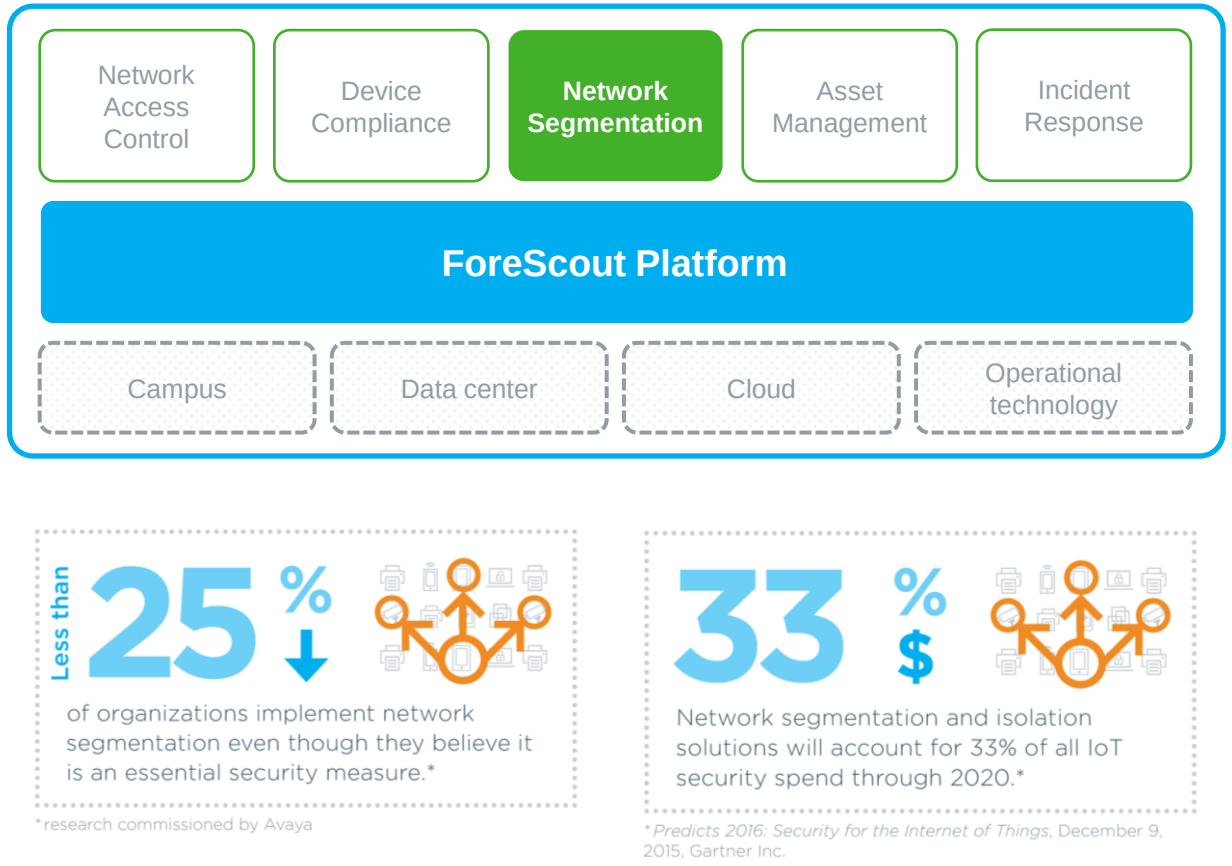
Key Use Cases:

- Control access to confidential data based on device and user profiles
- Prevent infected or noncompliant devices from spreading malware
- Automatically enforce actions for identified situations without human involvement

ForeScout can do network access control either with 802.1x or without 802.1x. Many network devices are not ready to do 802.1x. so having a non-.1x solution is critical.

- IT Central Station Review

Use Case #2 – Network Segmentation



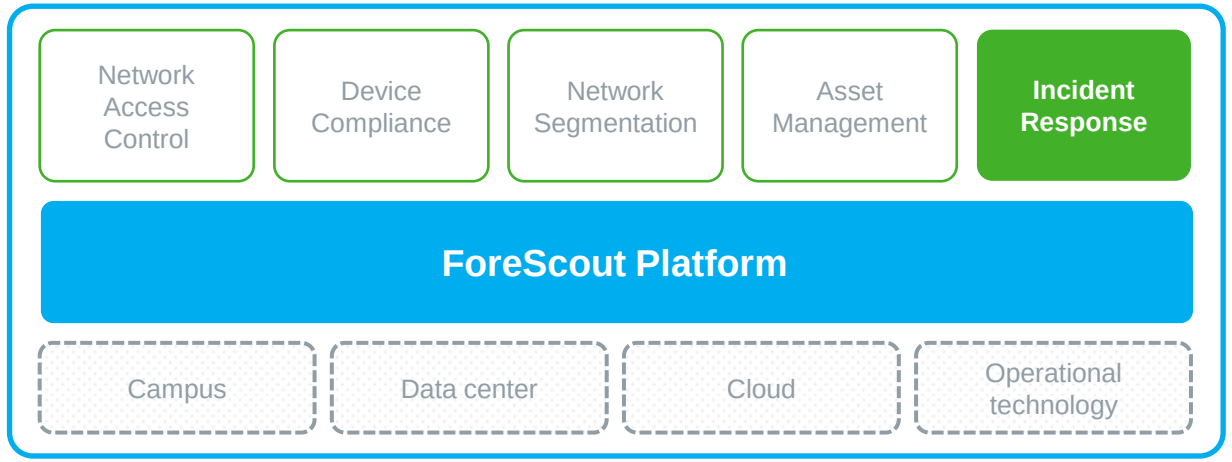
Key Use Cases:

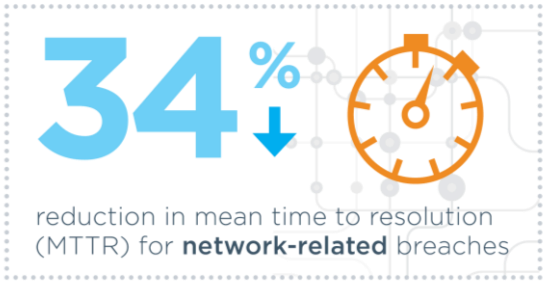
- Gain visibility into what devices are talking to each other
- Dynamically assign segments as the network and/or devices change
- Prevent select devices from communicating to other devices in different areas of the network across the extended enterprise

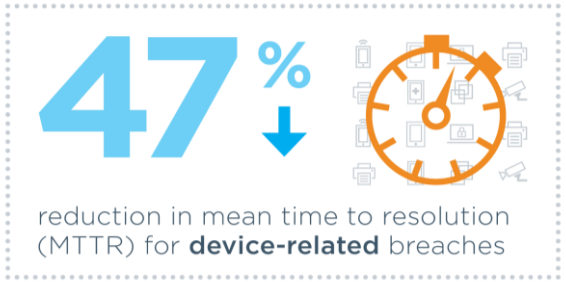
ForeScout provides Immediate relocation of network devices to segregated "Vendor" network based on autonomous analysis.

- IT Central Station Product Review, 2017

Solution #5 – Incident Response







Key Use Cases:

- Remediate mis-configured, vulnerable & non-compliant virtual & physical devices
- Hunt for vulnerabilities, IOCs & other attributes provided by leading threat detection, VA & SIEM vendors
- Automate mundane IT tasks natively or in concert with leading ITSM & security orchestration vendors

300 hours to less than 18 hours per month reduction in user downtime and system restoration time.

- Hillsborough Community College 2017

Our Product Vision

THE DEFACTO STANDARD FOR DEVICE VISIBILITY & CONTROL ACROSS THE ENTERPRISE

Campus

- Network
- Laptops / Desktops
- Mobile
- Users
- IoT Devices

Data Center

- Badging
- Servers
- Virtual Servers
- Security

Cloud

- Private Cloud
- Public Cloud
- amazon web services
- vmware
- Microsoft Azure

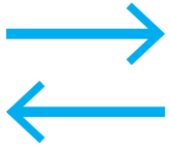
Operational Technology

- Physical Security
- Building Automation
- Physical Equipment
- Controller Systems

Why Customers Choose ForeScout

1. Visibility
   - ✓ Continuous monitoring
   - ✓ Agentless deployment

2. Time-to-Value
   - ✓ Rapid installation
   - ✓ Existing IT systems



3. Orchestration
   - ✓ Fragmentation reduction
   - ✓ Automated response

Thank You