ForeScout

Comply to Connect Strengthening the Weakest Link

NATO NIAS 2017

Ellen Sundra

ForeScout VP Systems Engineering

IT Security Challenges

KrebsonSecurity

620 GB DDOS Attack

Attackers used unsecure routers, DVRs and cameras

YAHOO!

Half a Billion U

Disabled the ar
machines

Eddie Bauer

350 Stores

US and Canada stores breached. Used internal computer systems that are connected to PoS systems

Top 10

vulnerabilities exploited are more than a year old

Source: HP Security Research. Cyber Security 2016; page 32

Reference acronym glossary at end of presentation.

Impact of Inadequate Visibility and Automation

Industry Stats:

- **80%** of successful attacks leverage well-known vulnerabilities – *Gartner Security and Risk Management Summit*
- **99%** of exploits will continue to be from known vulnerabilities up to one year through 2020 - *Gartner*
- **Top 10** exploited vulnerabilities are more than a year old - *HP Security Research.*
- **66%** of networks will experience an Internet of Things based breach by 2018 – *IDC*
- **80%** of all endpoints connected endpoints to the network will not support agent based technologies by 2020 Gartner

Business / Mission impact:

- Reputational damage which could impact funding.
- Breach remediation averages $4 Million per incident – *Ponemon Institute, June 2016*
- Critical citizen services become unavailable, unreliable
- Loss of grant funding or punitive damages due to non-compliance with Federal & State requirements

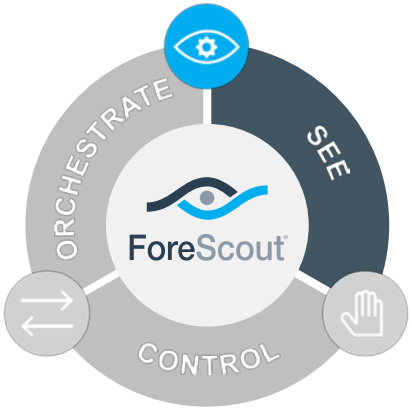
C2C Background

- US-DOD's formal continuous monitoring strategy evolving from NIST 800-53 and SANS 20 critical security controls
- Comply-to-Connect (C2C) is a comprehensive cybersecurity framework of tools and technologies designed to increase cybersecurity efficiency
- 4M+ DOD endpoints under management to date
- Primary objective to enable real-time cyber hygiene situational awareness and enforcement
- Automation of manual processes through third-party toolset integration leveraging an open architecture

Capability Gaps

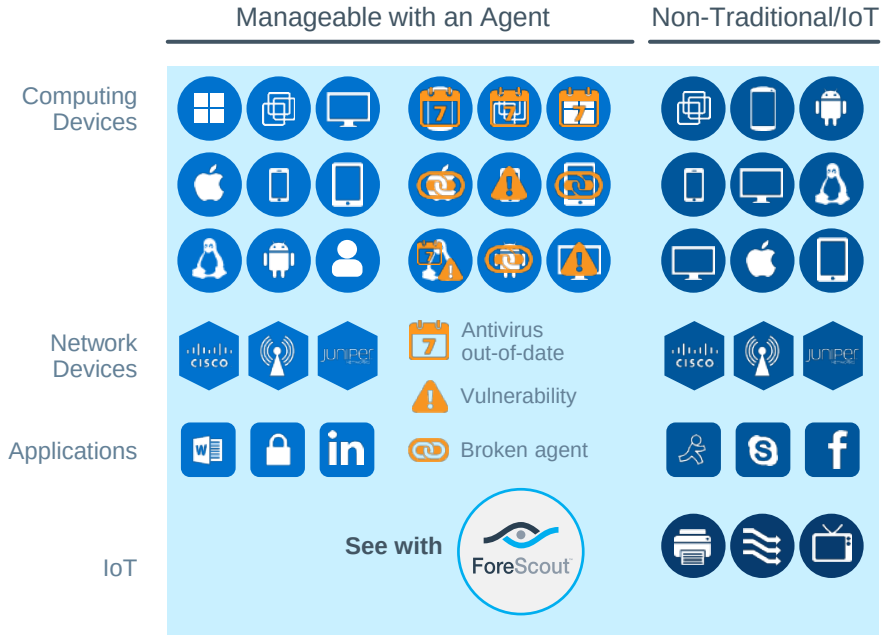
- Agent based security tools and point in time vulnerability scanning tools have inherent visibility gaps
- Lack of compliance enforcement and network access control for pre/post connect
- Need for continuous monitoring and control of ALL IP enabled endpoints in agentless manor
- Existing endpoint security tools relying on manual process to deploy agent or scan

Visibility is Essential



AGENTLESS

CONTINUOUS



Who are you?

Who owns the device?

What type of device?

Where/how are you connecting?

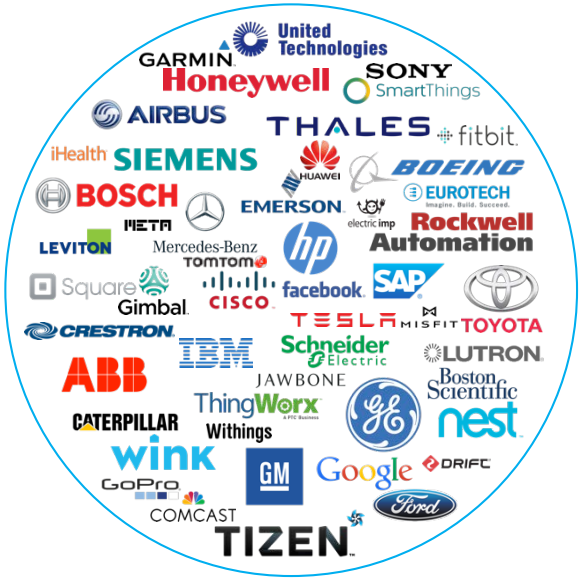
What is the device hygiene?

Reference Acronym Glossary at the end of presentation

Exponential IoT Growth

PC's & Mobile Devices

IoT Devices



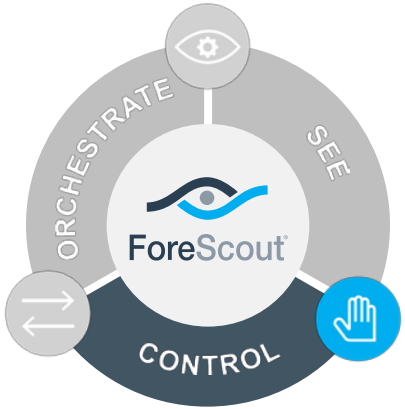
Took **25 years** *to get to* **10 Billion devices***

Will take only **5 years** *to get to* **30 Billion devices***

Source: Gartner IoT, PC and Mobile device forecast 2015

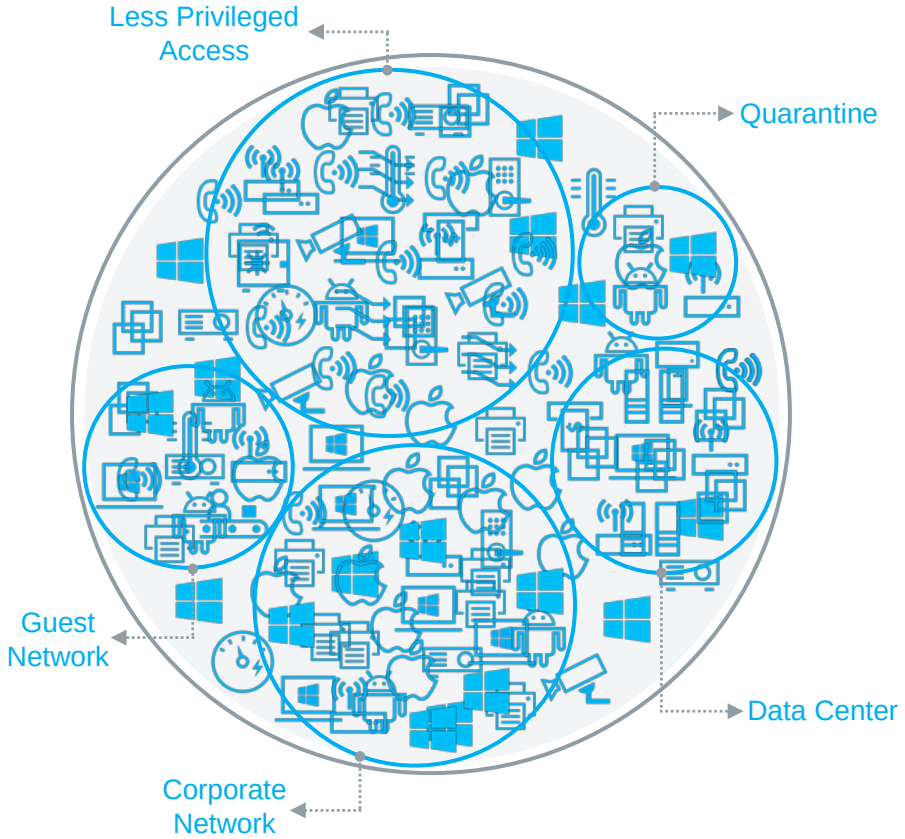
Reference acronym glossary at end of presentation

Automation requires Confidence



POLICY-DRIVEN

AUTOMATED



Notify

Comply

Restrict

Reference acronym glossary at end of presentation.

Critical Characteristics of a C2C Framework

- **Full Network-Based Visibility, Discovery and Classification of All Devices –** Full network visibility requires integration with the network to identify all connected devices in an agentless manor. All other approaches leave visibility gaps.
- **Redundant Manageability and Control of Devices –** Complete device control requires the redundancy of simultaneous agentless and agent-based endpoint inspection and control.
- **Orchestration with Mandated Security and Network Management Solutions –** Compliance against DoD security policy requires out-of-the-box, bi-directional integration with DoD-mandated security tools.
- **Continuous Monitoring and Automated Remediation –** Compliance must be continually monitored and maintained for devices that were previously compliant when they initially connected to the network.

Comply-to-Connect Phases

- **Phase 1: Discover and Classify –** Complete real time visibility to discover/classify/locate every connecting device in an agentless manor
- **Phase 2: Authentication and Authorization –** Control network access at the access layer, with or without 802.1x
- **Phase 3: Pre-Connect Compliance –** At connection, control access based on compliance of security policies
- **Phase 4: Post-Connect Compliance –** Continuously monitor each device, control access/maintain compliance and cyber hygiene

C2C Impact and Outcomes

- **Raises Command Cyber Readiness Inspection (CCRI) scores –** Well above 90% and with reduced manpower
- **Satisfies FY17 NDAA mandates –** Delivers comply-to-connect, software license control, SCADA/ICS control
- **SecDec Scorecard –** Authoritative data source for the SecDef scorecard and automates reporting from third party tools
- **Reduces manpower –** Software and patch management requirements cut by as much as 75%

ForeScout Capabilities Overview

Enables Complete Network Visibility/Control/Integration

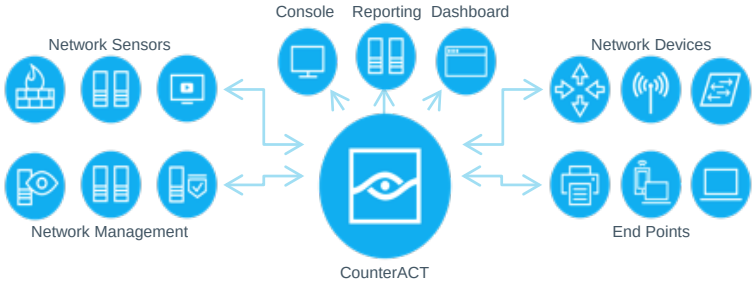
SEE

- Agentless discovery of every IP-based network device
- Categorize devices, users, applications and operating systems
- Continuously monitor every connection

CONTROL

- Notify administrators/users
- Remediate to conform to standards
- Allow, deny or limit network access

ORCHESTRATE



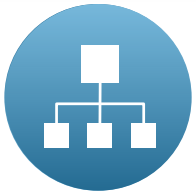
- Share contextual data
- Automate common processes/workflows
- Accelerate system-wide response

How ForeScout is Different

Fast and easy to deploy

- Agentless and non-disruptive
- Scalable, no re-architecting

+



Infrastructure agnostic

- Works with mixed, legacy environment
- Avoid vendor lock-in

+

Flexible and customizable

- Optimized for diversity and BYOD
- Supports open integration standards

ForeScout

Thank You!

Ellen Sundra, VP of Systems Engineering
ForeScout Technologies
Ellen.Sundra@ForeScout.com

ForeScout