ForeScout

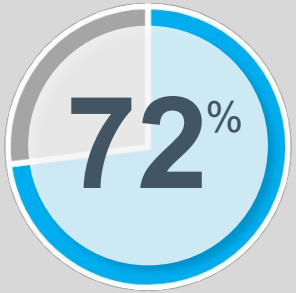
Transforming Security Through Visibility

Jargal.B

September 2017

Cybersecurity Trends

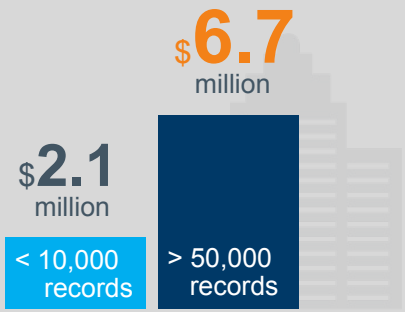
No Immunity



72% of the G2K companies surveyed had 5 or more security incidents in the last 12 months.

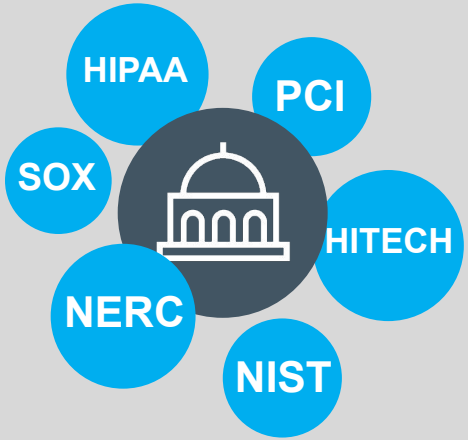
Source: Continuous Monitoring and Threat Mitigation with Next Generation NAC, Frost & Sullivan

Average annual cost of security incidents



Source: 2016 Cost of Data Breach Study: Global Analysis, Ponemon Institute

Regulatory mandates



Reference acronym glossary at end of presentation

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

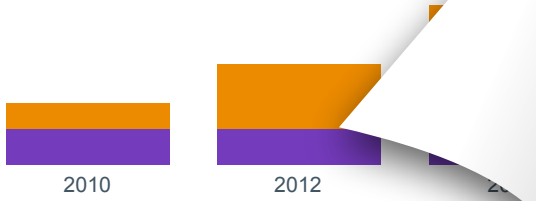
vulnerabilities exploited are more than a year old

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

Reference acronym glossary at end of presentation.

IT Security Landscape

Less than 10% of new devices connecting to t
corporate environment will be manageable th
traditional methods



66%

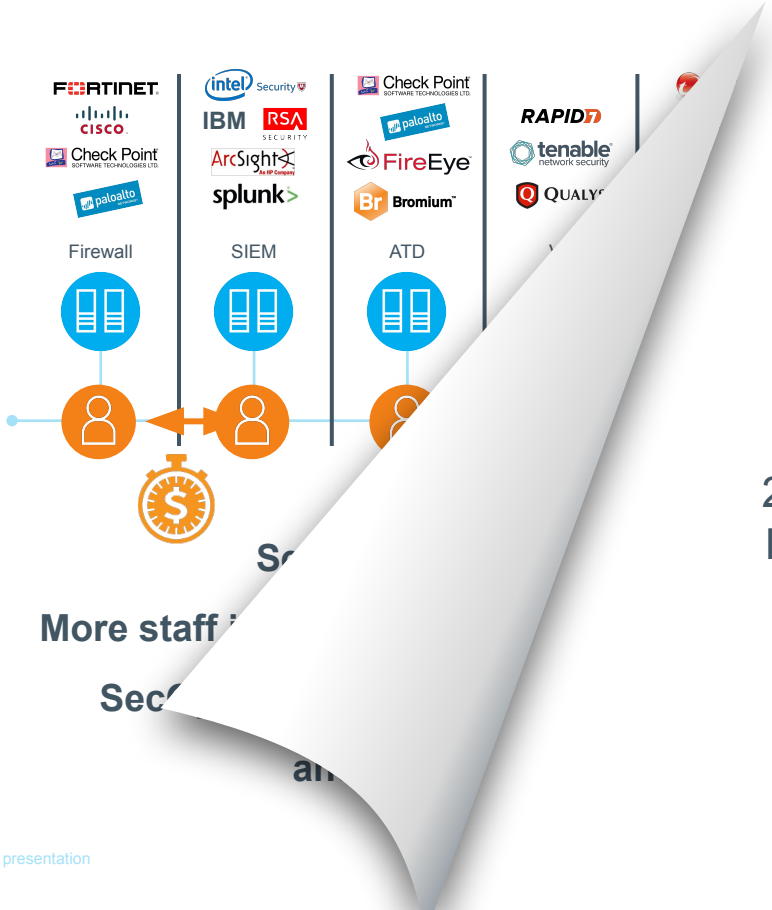
of all networks will have an IoT security breach by 2018

IDC

Source: Gartner, BI Intelligence, Verizon, ForeScout

Reference acronym glossary at end of presentation.

IT Security Landscape

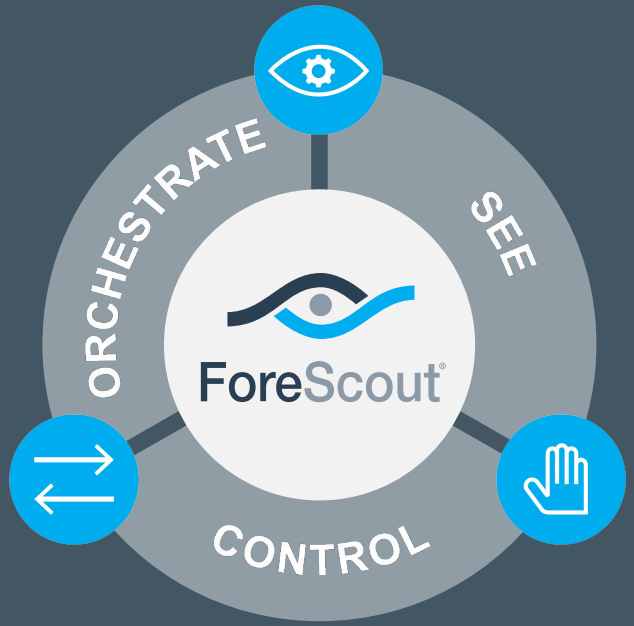


85%

of IT device management activities will be automated by 2021 due to exponential growth in IT devices; increase from the less than 5% today.

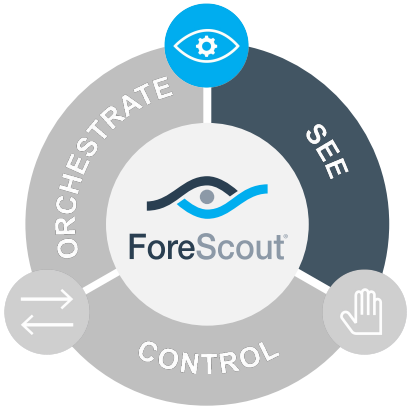
Gartner

Reference Acronym Glossary at the end of presentation



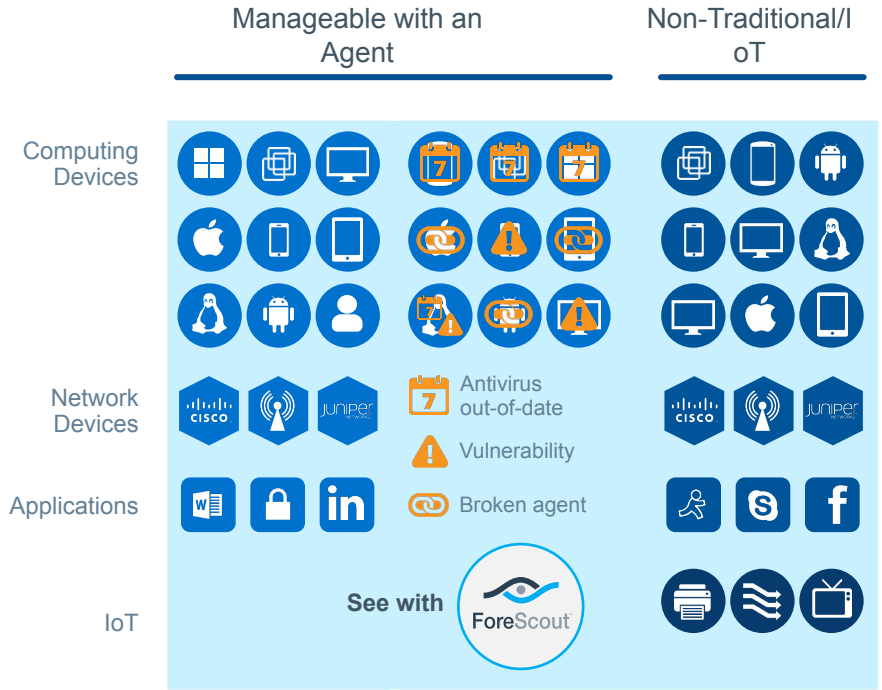
ForeScout Solution

See



AGENTLESS

CONTINUOUS



Who are you?

Who owns the device?

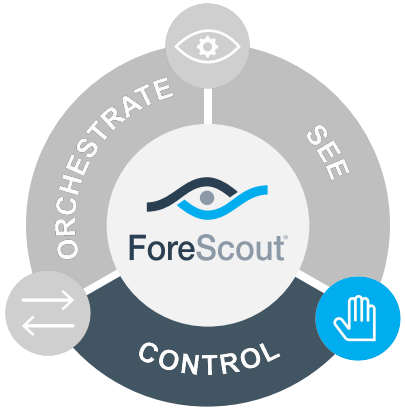
What type of device?

Where/how are you connecting?

What is the device hygiene?

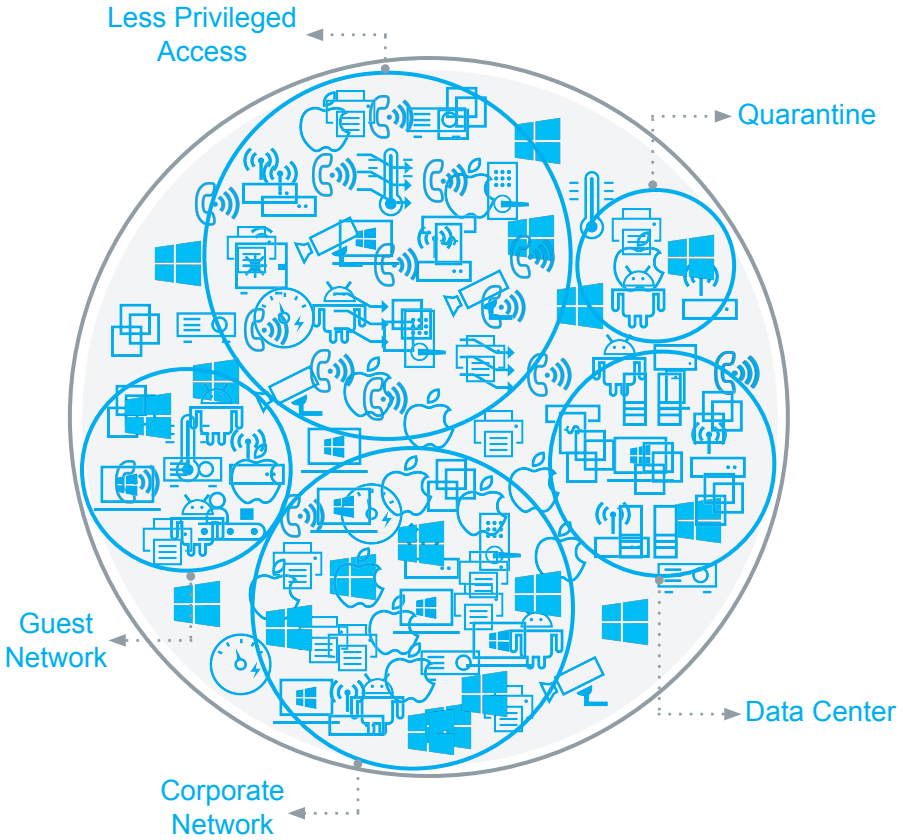
Reference Acronym Glossary at the end of presentation

Control



POLICY-DRIVEN

AUTOMATED



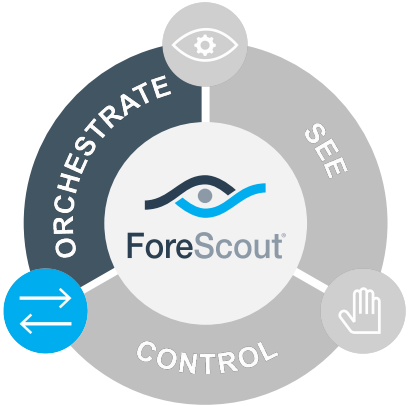
Notify

Comply

Restrict

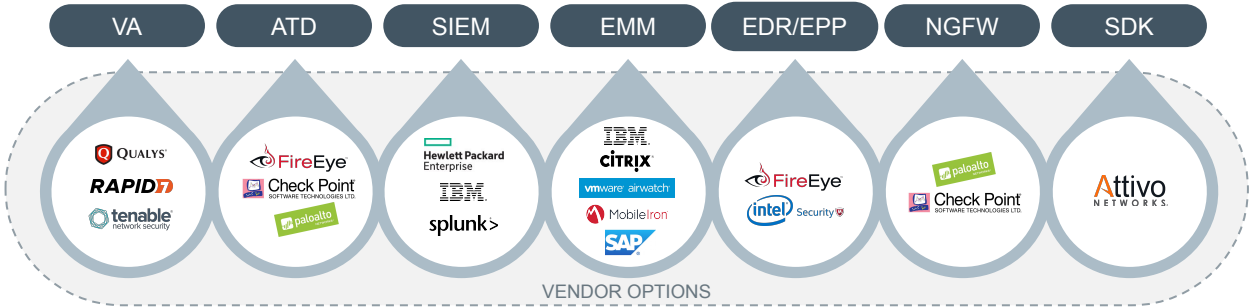
Reference acronym glossary at end of presentation.

Orchestrate

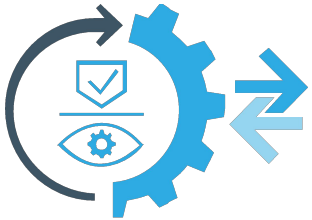


BREAK DOWN SILOS

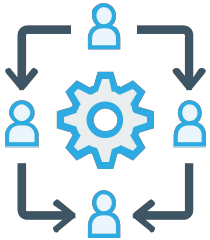
MAXIMIZE EXISITING INVESTMENTS



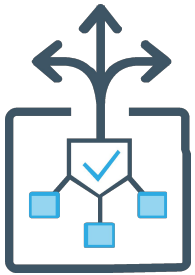
Share Contextual Insights



Automate Workflows

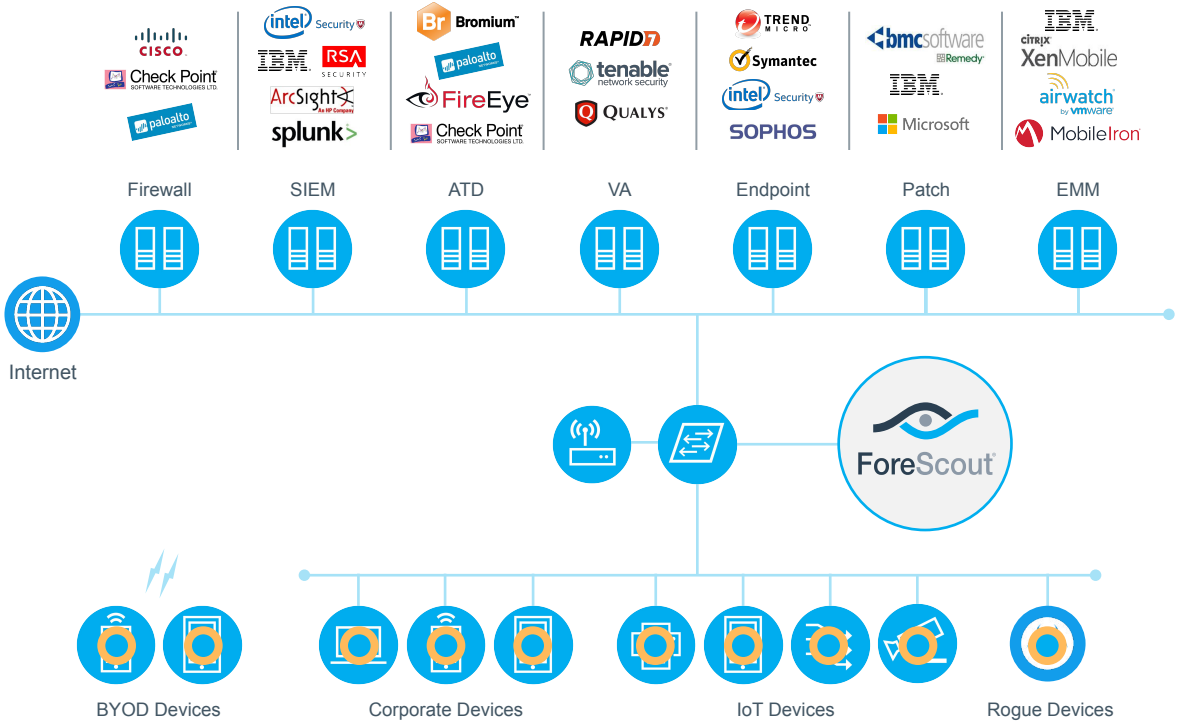


Automate Response Actions



Reference Acronym Glossary at the end of presentation

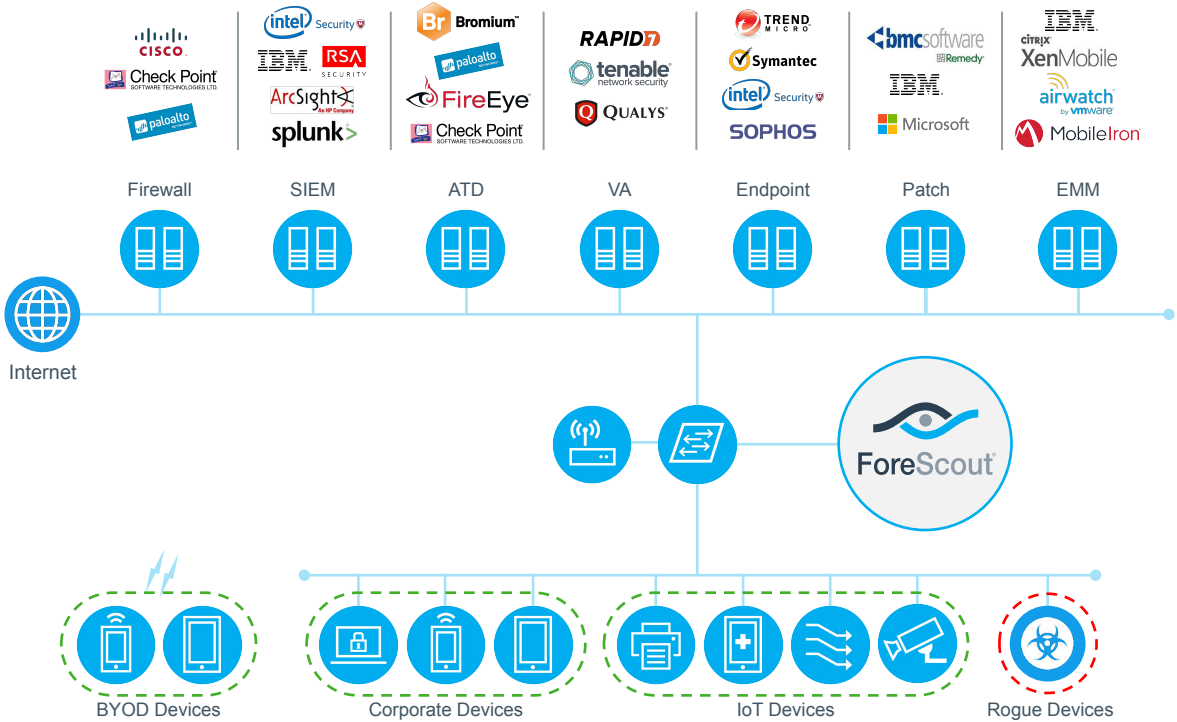
IT Security – With ForeScout



1. See corporate, BYOD, IoT, rogue devices.
2. Control network access based on user, device, policy
3. Trigger update and patches on managed endpoints
4. Detect transient devices and trigger real-time vulnerability scans
5. Automate enrollment for guests and BYOD including mobile devices
6. Rapidly respond to incidents, without human intervention

Reference acronym glossary at end of presentation

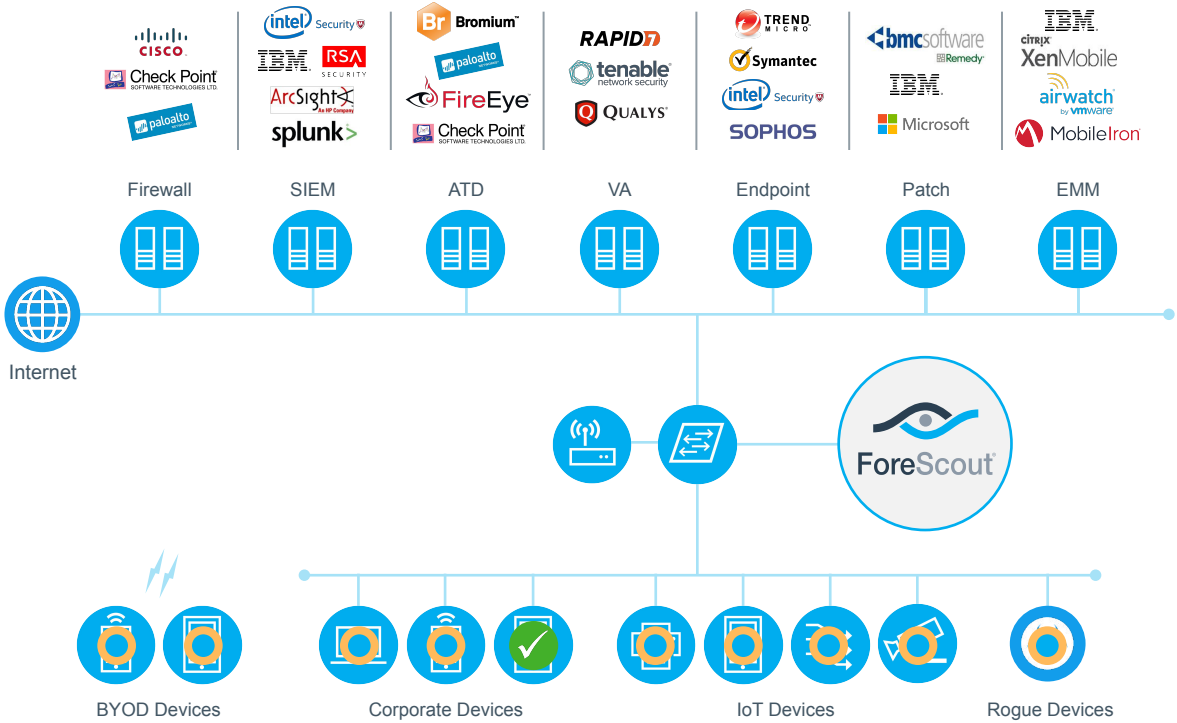
IT Security – With ForeScout



1. See corporate, BYOD, IoT, rogue devices.
2. Control network access based on user, device, policy
3. Trigger update and patches on managed endpoints
4. Detect transient devices and trigger real-time vulnerability scans
5. Automate enrollment for guests and BYOD including mobile devices
6. Rapidly respond to incidents, without human intervention

Reference acronym glossary at end of presentation

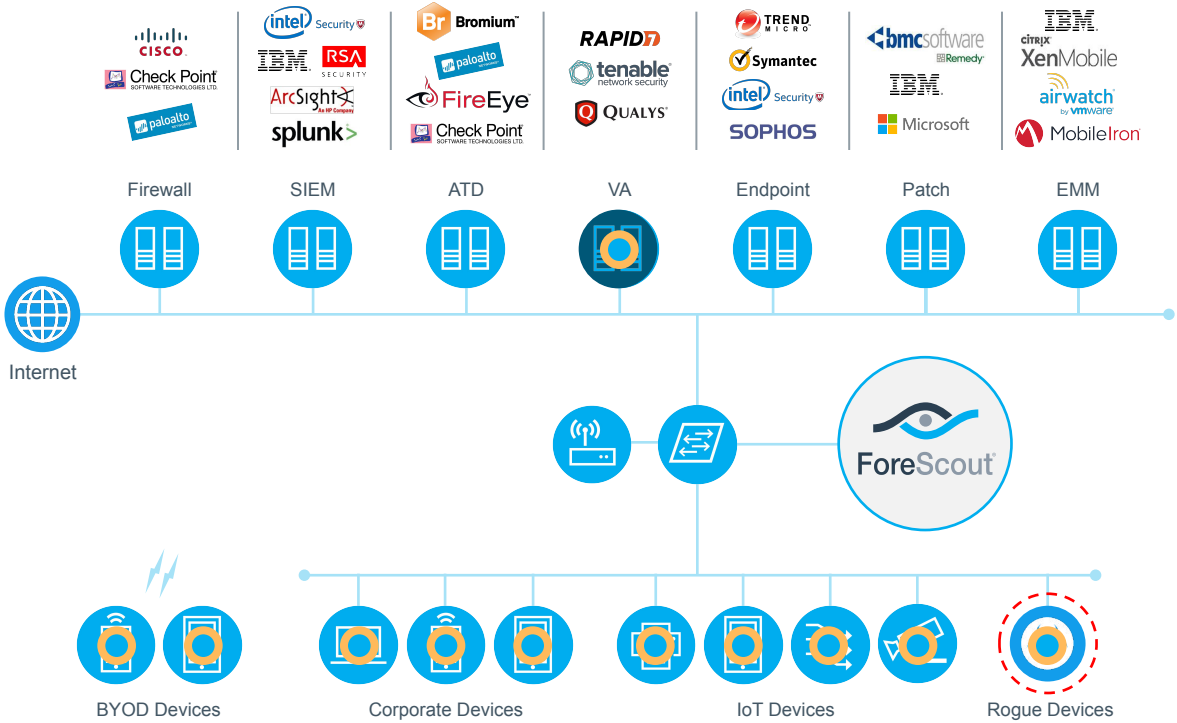
IT Security – With ForeScout



1. See corporate, BYOD, IoT, rogue devices.
2. Control network access based on user, device, policy
3. Trigger updates and patches on managed endpoints
4. Detect transient devices and trigger real-time vulnerability scans
5. Automate enrollment for guests and BYOD including mobile devices
6. Rapidly respond to incidents, without human intervention

Reference acronym glossary at end of presentation

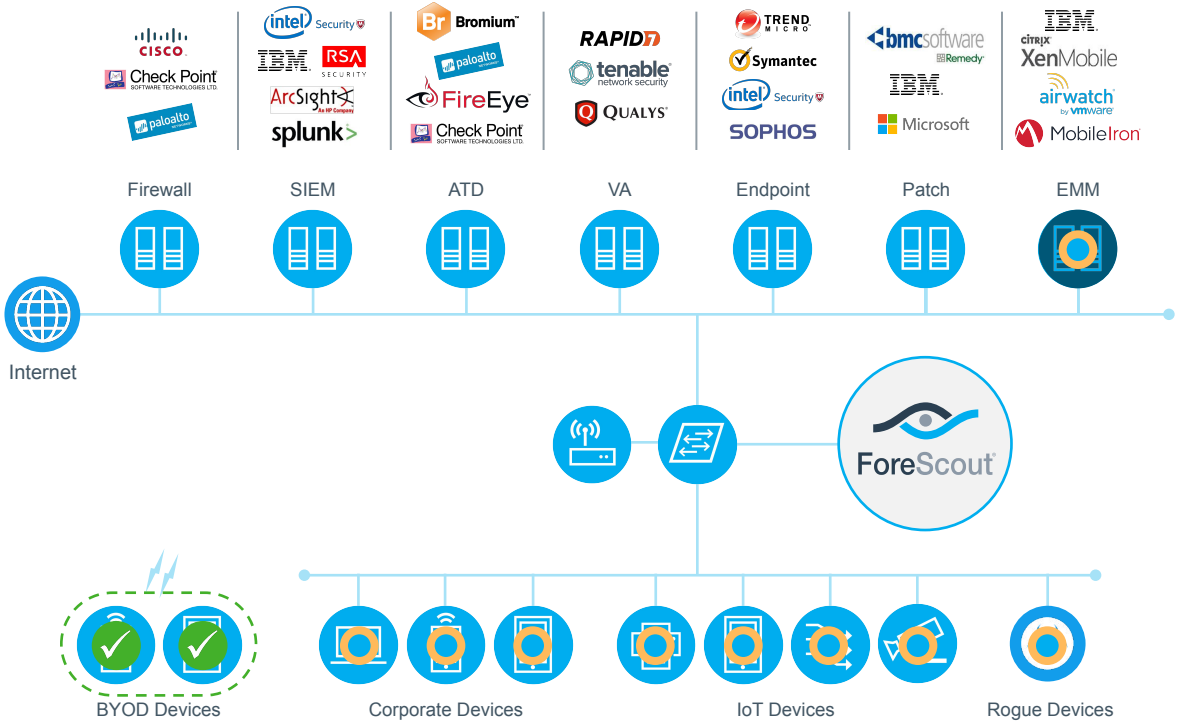
IT Security – With ForeScout



1. See corporate, BYOD, IoT, rogue devices.
2. Control network access based on user, device, policy
3. Trigger updates and patches on managed endpoints
4. Detect transient devices and trigger real-time vulnerability scans
5. Automate enrollment for guests and BYOD including mobile devices
6. Rapidly respond to incidents, without human intervention

Reference acronym glossary at end of presentation

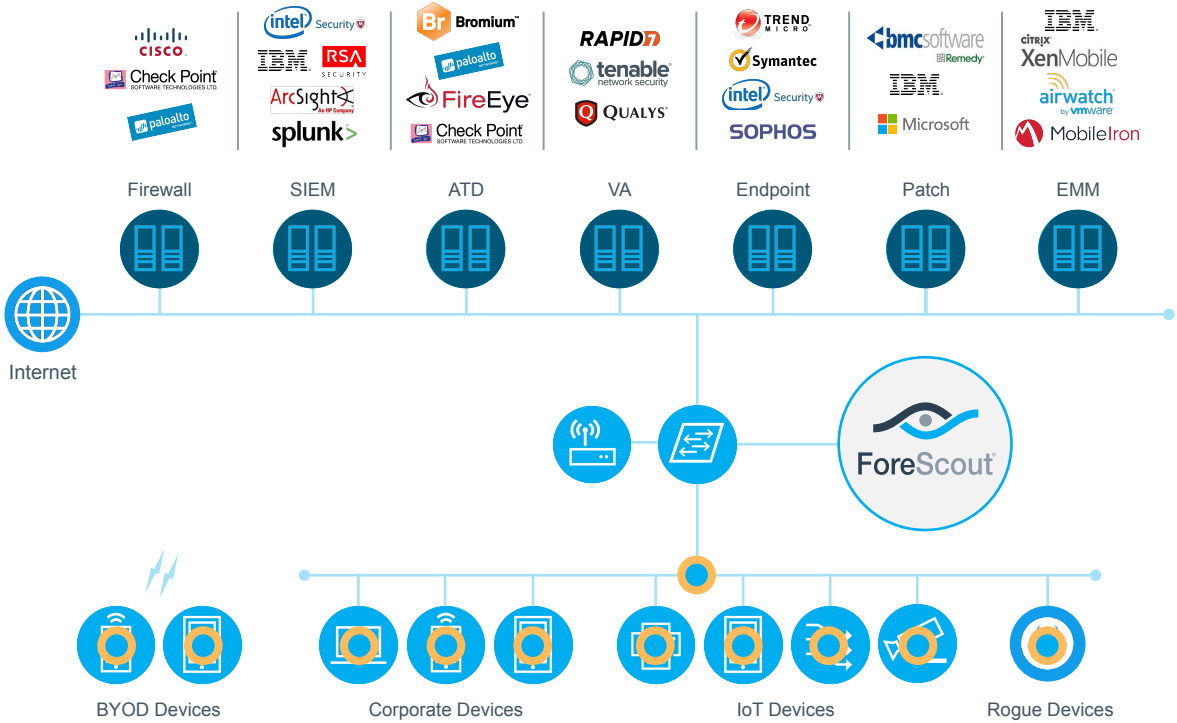
IT Security – With ForeScout



1. See corporate, BYOD, IoT, rogue devices.
2. Control network access based on user, device, policy
3. Trigger updates and patches on managed endpoints
4. Detect transient devices and trigger real-time vulnerability scans
5. Automate enrollment for guests and BYOD including mobile devices
6. Rapidly respond to incidents, without human intervention

Reference acronym glossary at end of presentation

IT Security – With ForeScout



1. See corporate, BYOD, IoT, rogue devices.
2. Control network access based on user, device, policy
3. Trigger updates and patches on managed endpoints
4. Detect transient devices and trigger real-time vulnerability scans
5. Automate enrollment for guests and BYOD including mobile devices
6. Rapidly respond to incidents, without human intervention

Reference acronym glossary at end of presentation

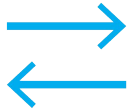
ForeScout

Technical Competitive Overview – Cisco ISE

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

2016 Awards and Recognition

Gartner

Gartner IoT Security Market Guide
Gartner, 2016

JPMorgan Chase & Co.

JP Morgan Chase Hall of Fame Innovation Award for Transformative Security Technology
JPMC, 2016

Forbes 2016 THE Cloud100

Cloud100 World's Best Cloud Companies
Forbes, 2016

500 Technology Fast 500 NORTH AMERICA

Deloitte's Fastest Growing Companies in North America
Deloitte, 2016

SR Silicon

20 Fastest Growing Security Companies
The Silicon Valley Review, 2016

Gartner

Gartner NAC Market Guide
Gartner, 2016

SC MAGAZINE

Excellence Award for Threat Solutions
SC Magazine, 2016

CRN

Computer Reseller News Top Security Company
CRN, 2016

Inc. 5000

Inc. 5000
Fastest Growing Companies
Inc. 5000, 2016

nanalyze

9 Hot Cybersecurity Startups
Nanalyze, 2016

Reference acronym glossary at end of presentation

Thank you!

Acronym Glossary

AAA	Authentication, Authorization and Accounting
ACL	Access Control List
ACS	Access Control Server [Cisco]
API	Application Programming Interface
ARP	Address Resolution Protocol
ATD	Advanced Threat Detection
ATP	Advanced Threat Prevention
AWS	Amazon Web Services
BYOD	Bring Your Own Device
CA	Certificate Authority
CASB	Cloud Access Security Broker
C&C	Command and Control
CCE	Common Configuration Enumeration
CEF	Cisco Express Forwarding
CIS	Center for Internet Security, Inc.
CMDB	Configuration Management Database
CoA	Change of Authorization
CPPM	ClearPass Policy Manager
CPU	Central Processing Unit
CSC	Critical Security Controls
CVE	Common Vulnerabilities and Exposures
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DLP	Data Loss Prevention
DNS	Domain Name Server
EDR	Endpoint Detection and Response
EMM	Enterprise Mobility Management
EPP	Endpoint Protection Platform
FERC	Federal Energy Regulatory Commission
FW	Firewall
GCP	Google Cloud Platform
GUI	Graphical User Interface

HIP	Host Information Policy [Palo Alto Networks]
HIPAA	Health Insurance Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health
HPS	Host Property Scanner
IaaS	Infrastructure as a Service
ID	Identification
IDaaS	Identity as a Service
IM	Instant Messaging
IOC	Indicators of Compromise
iOS	iPhone Operating System [Apple]
IoT	Internet of Things
IP	Internet Protocol
ISE	Identity Services Engine [Cisco]
IT	Information Technology
ITAM	Information Technology Access Management
ITSM	Information Technology Service Management
MAB	Mac Authentication Bypass
MTP	Mobile Threat Prevention [FireEye]
MTTD	Mean Time to Detection
MTTR	Mean Time to Resolution
NA	Not Applicable
NAC	Network Access Control
NAT	Network Address Translation
NERC	North American Electric Reliability Corp.
NetBIOS	Network Basic Input/Output System
NGFW	Next-Generation Firewall
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
Nmap	Network Mapper

OVAL	Open Vulnerability and Assessment Language
OS	Operating System
OT	Operational Technology
P2P	Peer-to-Peer
PAM	Privileged Access Management
PAN OS 7.x	Palo Alto Networks Operating System 7.x
PC	Personal Computer
PCI	Payment Card Industry
PKI	Public Key Infrastructure
pxGrid	Platform Exchange Grid [Cisco]
RADIUS	Remote Authentication Dial-In User Service
Reauth	Reauthorization
RTU	Remote Terminal Unit
SANS	System Administration, Networking, and Security Institute
SaaS	Software as a Service
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Compliance Automation Protocol
SCCM	System Center Configuration Manager
SDN	Software Defined Network
SGT	Security Group Tags [Cisco]
SGT	Security Group Tags [Cisco]
SIEM	Security Information and Event Management
SNMP	Simple Network Management Protocol
SOX	Sarbanes-Oxley
SQL	Structured Query Language
SSID	Service Set Identifier
SSO	Single Sign On
STIG	Security Technical Implementation Guide

SYSLOG	System Log
TACACS	Terminal Access Controller Access Control System
TAM	Threat Assessment Manager [FireEye]
TAP	Threat Analytics Platform [FireEye]
TCO	Total Cost of Ownership
TIP	Threat Intelligence Platform
UBA	User Behavior Analytics
USB	Universal Serial Bus
VA	Vulnerability Assessment
vFW	Virtual Firewall
UBA	User Behavior Analytics [Splunk]
USB	Universal Serial Bus
VDI	Virtual Desktop Infrastructure
VM	Virtual Machine
VPN	Virtual Private Network
WAF	Web Application Firewall
WAP	Wireless Application Protocol
XCCDF	The Extensible Configuration Checklist Description Format
XML	Extensible Markup Language

ForeScout