Safeguard your enterprise by continuously identifying, segmenting and enforcing compliance of every connected thing.
Your enterprise is an Enterprise of Things

Every thing that touches your enterprise exposes you to potential risk. You must see it and secure it. Forescout provides the only solution that actively defends the Enterprise of Things at scale.
WELCOME

Explore Forescout Solutions and learn how Forescout keeps you secure across all your network environments: campus, IoT, data center, cloud and operational technology (OT).

Forescout Solutions include Device Visibility, Asset Management, Device Compliance, Network Access Control, Network Segmentation and Incident Response.

“Hackers could use smart displays to spy on meetings.” – wired.com

“NASA Jet Propulsion Laboratory network was hacked by targeting a Raspberry Pi that wasn’t supposed to be connected to it.” – businessinsider.com

“Nearly 20% of organizations observed at least one Internet of Things (IoT)-based attack in the past three years.” – Gartner

“By 2023, the average CIO will be responsible for more than 3 times the endpoints they managed in 2018.” – Gartner

“65% of acquiring companies experience buyers’ remorse after closing an M&A deal due to cybersecurity concerns.” – Forescout Report

“71% of devices running unsupported Windows operating systems as of January 2020.” – Forescout Report

HOW TO USE THIS GUIDE

This interactive guide includes clickable links. Use them to jump between sections or access supporting resources.

The navigation bar at the top allows you to move between sections.
Forescout Solutions

Gain 100% visibility and classification of all connected physical, virtual and IoT/OT devices.

Manage and secure all IP-connected devices with an accurate, real-time inventory.

Continuously assess devices, monitor them and enforce security policies to maintain compliance.

Control access simply and easily to prevent unauthorized or rogue devices from connecting.

Confidently segment your network to eliminate lateral infiltration risks.

Respond and remediate quickly to reduce risk of business disruption from security incidents/breaches.

Click on an icon to learn more.
Device Visibility

You can’t secure what you can’t see.™

Continuously discover, classify and profile your entire enterprise of things—all IP-connected IT, IoT and OT devices—the instant they enter your network. Gain accurate, real-time visibility of every asset using active and passive methods to drive security and IT management.

The Forescout difference:

- Automatically discover and classify 100% of devices, no agents required
- Assess device security posture on employee-owned, contractor-owned and IoT/OT devices without risking business disruption
- Continuously monitor devices and compliance status as devices come and go from your network

“We started implementation at lunchtime and when I fired up my computer that evening, 97 percent of our environment had already been discovered and classified. Within seven hours, we had detailed visibility of our global environment. That's impressive.”

— Joseph Cardamone, Sr. Information Security Analyst and NA Privacy Officer, Haworth

**Before Forescout**

- A single unknown device is all a breach needs
- Inconsistent and incomplete view across campus, data center, cloud and OT
- Can’t see devices that don't have a software agent
- Audits find up to 60% unknown devices

**After Forescout**

- 100% device visibility
- Single platform discovers & classifies traditional, non-traditional (including IoT/OT) & virtual instances (VMs/cloud workloads)
- Agentless visibility - no software agents required
- Find up to 60% more devices
How it works: Device Visibility

- **A** Poll switches, VPN concentrators, APs and controllers for list of devices that are connected
- **B** Receive SNMP traps from switches and controller
- **C** Receive NetFlow, sFlow, Flexible NetFlow data
- **D** Monitor 802.1x requests to the built-in or external RADIUS server
- **E** Monitor DHCP requests to detect when a new host requests an IP address
- **F** Optionally monitor a network SPAN port for HTTP user-agent, TCP fingerprinting and 60+ protocols
- **G** Query public/private cloud APIs
- **H** Import external MAC classification data or request LDAP data
- **I** VMware® vSphere®, AWS® EC2®, ACI and Azure integration
- **J** Analyze PoE data
- **K** Run port, service banner and OS fingerprint scan
- **L** Use credentials to run a scan on the endpoint
- **M** Use optional agent
The Forescout difference: Device Visibility

Discover up to 60% more devices than previously known¹

Forescout Device Cloud
- Provides accurate, real-world device classifications

Granular Device Classification
- Compliance posture, apps, patch status and more

Passive Scanning
- Extends visibility to OT systems and critical infrastructure

Continuous Monitoring
- Point-in-time scanning is too infrequent

Agentless
- No agents required

¹ Forescout end-user customer feedback
Asset Management

Accurately manage and secure connected things.

Manual asset discovery produces inaccurate, out-of-date asset details that undermine your IT and security management initiatives. To effectively manage and secure your business, you must automate the inventory process and maintain accurate asset details across IT and OT networks.

The Forescout difference:

- Maintain an accurate CMDB with real-time updates to improve operational consistency and reduce manual errors
- Inventory and track agentless devices, including IoT devices, VMs and OT/critical infrastructure
- Share contextual data with ITSM tools

"With the Forescout solution, we expect to save millions from exponentially faster audits that produce fewer findings and require less remediation effort."

— Phil Bates, Chief Information Security Officer, State of Utah

Before Forescout

- Limited IoT, OT and unmanaged device visibility = inaccurate inventory
- Periodic scanning misses transient devices = incomplete inventory
- Active scanning discovery solutions = critical infrastructure disruption
- Limited support (build-your-own API integrations = complex configurations, manual CMDB true-ups)
- Complex deployments and vendor dependencies = high TCO (due to agent-based solutions with ongoing maintenance and operational issues)

After Forescout

- Agentless visibility and classification (comprehensive, accurate inventory)
- Continuous asset monitoring = up-to-date inventory (detects changes and transient devices)
- Passive visibility for inventory of OT and critical infrastructure devices
- Plug-and-play automation (eyeExtend modules orchestrate real-time data sharing, alerts and responses with ITSM and security tools)
- Flexible architecture (supports multivendor networks across campus, data center, cloud and hybrid deployments)
How it works: Asset Management

Forescout eyeSight discovers, classifies and assesses all IP-connected device types as they connect to the network.

Forescout eyeExtend powered by eyeSight then updates or creates a new ServiceNow® CMDB Configuration Item (CI) with additional context such as the switch port to which the device is connected, VLAN information, network segment information, location, compliance status, and so on.

The Forescout platform can also verify if the device has the latest patches; if not, it can inform the ITSM platform and trigger remediation actions.

The Forescout platform monitors and updates information in the asset inventory from the time a device enters the network until it leaves the network.

*Note

Forescout also provides eyeExtend Connect for custom integration with other ITSM platforms like BMC and Cherwell.
The Forescout difference: Asset Management

Deliver data and information needed to govern IT assets

- Rich Classification
  - Who, what, where, when, OS version & more
  - Real-world classification

- Automated Process
  - Single view of all IP-connected devices
  - Send data to CMDB (orchestration)

- Real Time
  - Instant inventory assessment
  - Continuous

- Ease of Deployment
  - Agentless
  - Quick to deploy

- Vendor Neutral
  - No network upgrades
  - Campus, data center/cloud and OT (passive)

* IP-based connected devices
Device Compliance

Evaluate and advance compliance with confidence

Vulnerable platforms, unpatched devices, default passwords and broken security software create serious compliance gaps that continue to widen as more devices are added, become virtual and extend into the cloud. Forescout continuously assesses devices, monitors them and enforces compliance policies to reduce risk.

The Forescout difference:

- Maintain continuous compliance instead of waiting for periodic scans
- Top endpoint compliance vendor*
- Enforce compliance policies across all devices: managed, unmanaged, IoT and OT

*IP Central Station customer reviews and ratings, August 2019

“During our assessment, the IT team was able to leverage the Forescout platform to verify that our endpoints were running the latest patches, most recent versions of antivirus software, and so on. The ease of endpoint compliance contributed significantly to preventing intrusion during this exercise. Forescout saw it all.”

— Ryan Morris,
Chief Technology Officer,
California Office of Statewide Health Planning and Development

How it Works

Forescout Difference

Let Us Show You
How it works: Device Compliance

**DEVICES / USERS**
- Corporate Laptops
- IoT
- Mobile
- BYOD / Guest

**ASSESS POSTURE**
- **Security Agent Compliance**
  - agent health checks:
    - AV, EDR, firewall, ITSM, patching
- **Weak IoT Credentials**
  - default? common?
- **Mobile Compliance**
  - Jailbroken? blacklisted app?
- **Vulnerabilities**
  - high, medium, critical?
- **Anti-Virus**
- **Anti-Malware**
- **External HW**
- **Encryption**
- **Applications**
- **More…**

**AUTO REMEDIATE**
- Install security agent
- Update AV
- Patch device
- Trigger SCCM
- Start AV application
- Update applications
- Terminate blacklisted app
- Stop processes
- Update configuration
- Set registry values
- Provide user web instructions
- More ……

**UNIFIED POLICY ENGINE**

Solution Brief
Interactive Demo
Learn More
The Forescout difference: Device Compliance

Achieve and maintain continuous compliance

Continuous Risk & Posture Assessment
- Assess who, what, where, when, OS versions & more
- Validate agent-based security tools

Automated Process
- Single view (extended enterprise)
- Send data to EDR/VA/CMT (orchestration)
- Apply mitigating controls (segmentation)

Manage Weak/Default Passwords
- Agentless IoT devices
- Continuous

Ease of Deployment
- Agentless
- Quick to deploy

Vendor Neutral
- No network upgrades
- Campus, data center/cloud and OT
Network Access Control (NAC)

Control access simply and easily
Traditional authentication and access control of perimeter-based networks no longer work. Forescout unifies policy-based access control across heterogeneous campus, data center, cloud and OT environments—with or without 802.1X authentication.

The Forescout difference:
• **Identify**: discover, classify and inventory all connected devices
• **Comply**: Assess security posture and compliance
• **Connect**: Enforce access policies across heterogeneous networks

“*We were aware of most of what was on our network, but the Forescout platform told us so much more about each device, plus it gave us the automated, granular control capability that we were missing.*”

- Dale Marroquin,
  Information Security Officer,
  Credit Human Credit Union

<table>
<thead>
<tr>
<th>BEFORE Forescout</th>
<th>AFTER Forescout</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent-dependent systems</td>
<td>Agentless visibility of all IP-connected devices and continuous posture assessment</td>
</tr>
<tr>
<td>802.1X design complexity = deployment delays and expense</td>
<td>Fast to deploy &amp; easy to use (802.1X is optional)</td>
</tr>
<tr>
<td>Lack of heterogeneous network infrastructure support</td>
<td>Interoperate to avoid upgrades and accommodate mergers &amp; acquisitions</td>
</tr>
<tr>
<td>Limited automation for network access, control and remediation</td>
<td>Automated guest onboarding, isolation of noncompliant/infected devices without network changes</td>
</tr>
<tr>
<td>Limited integration with third-party tools = disjointed, siloed security management</td>
<td>Out-of-the-box integration with leading IT and security tools via Forescout eyeExtend modules</td>
</tr>
</tbody>
</table>
**How it works:** Network Access Control

1. **Device attempts to connect to the corporate network.**

2. **Forescout classifies the device as a corporate-managed device.**

3. **Forescout queries Active Directory for additional user info and data to ensure access to the appropriate resources (department, geography).**

4. **Forescout does a posture assessment of end-points and remediates, if necessary.**

5. **Forescout scans other devices on the network for the new IOCs and initiates isolation and mitigation actions on infected devices.**
The Forescout difference: Modern NAC

Identify all devices, assess security posture and continuously enforce compliance

Network Access Control

Control Network Access
• Automated access control based on user, device type & security posture

Enforce Device Compliance
• Enforce compliance with security policies and regulations
• Restrict, block or quarantine noncompliant devices

Continuously Monitor
• Monitor and enforce policies upon connect

Automate Incident Response
• Contain threats to minimize propagation & disruption
• Initiate remediation workflows

Heterogeneous
• 802.1X or not
• Fast, pain-free deployment
• Avoid costly network upgrades

Forrester Zero Trust Platform
Network Segmentation

Confidently design, build and deploy network segmentation at scale
Flat networks allow lateral movement of threats and attacks. Want to confidently deploy segmentation without disrupting the business? Need enterprise-wide segmentation without multivendor complexity? Forescout lets you bridge the skills gap with resources and tools to segment your network with confidence. Let us show you.

The Forescout difference:
- Dynamically group devices by business context
- Visualize and map device flows to device groups
- Simulate segmentation policies prior to enforcement
- Orchestrate segmentation across multivendor enforcement points

"Today, we know what’s on our network—including IoT devices. The Forescout platform classifies the device and slips it onto the appropriate VLAN segment."
— Ken Compres, Sr. Network Security Engineer/CSO, Hillsborough Community College

Inability to see IoT, guest, transient & OT devices results in gaps in security & segmentation
Inability to visualize traffic across environments results in ineffective segmentation policies
Reactive and siloed segmentation policies with no ability to test the impact before enforcement
High TCO and low efficiency from managing fragmented segmentation policies across silos
No way to translate policies and consistently orchestrate controls across network domains

Unparalleled insight of campus/data center/cloud reduces risks & enables effective segmentation
Visualize traffic by mapping flows to logical taxonomy of devices, apps, users & services
Proactively simulate and learn a given segment’s impact before deploying policies
Monitor/validate segmentation policies & respond to violations across domains
Orchestrate consistent controls across network domains and multivendor environments

How It Works  Forescout Difference  Let Us Show You
How it works: Network Segmentation

1. The Forescout platform discovers endpoints connecting to the network.
2. Forescout classifies the devices as a corporate-managed device.
   - Forescout helps you to visualize group communication patterns
   - Simulate segmentation policies to tighten communications and adhere with company requirements
   - eyeSegment reacts to any policy violations (alert or enforce)
3. Forescout places finance user with a corporate computer in finance VLAN segment.
4. Forescout segments corporate video camera to only communicate with video server using a restrictive ACL.
The Forescout difference: Network Segmentation
Assess and segment devices on the fly using real-time device context

- **Real-Time Device Context**
  - Classify ALL managed & unmanaged devices
  - Who, what, where, OS version, etc.
  - Continuous compliance posture
  - Understand device groups in business terms

- **Context-Aware Traffic Flows**
  - How devices interact
  - Standard communication flows

- **Simulate Segmentation Policies**
  - Design, test & validate policies before enforcing

- **Monitor and Respond**
  - Continuously monitor and assess segmentation policies
  - Receive proactive alerts

- **Orchestrate Controls**
  - Enforce segmentation across campus, data center, cloud and OT
  - Orchestrate controls across multivendor environments
Incident Response

**Respond and remediate quickly**

The instant your network security is breached, the clock starts ticking. The Forescout platform automates threat detection, prioritization and containment while orchestrating actions with leading SOAR vendors to accelerate incident response and mitigate risk.

**The Forescout difference:**

- Detect cyber and operational threats to IT and OT networks
- Reduce device and network breaches
- Automate threat detection, threat hunting and containment to accelerate incident response
- Gain out-of-the-box workflow interoperability with 20+ security solutions through Forescout eyeExtend modules

“Forescout is like having an automatic threat hunter that hunts for threats around the clock across our global network. Tasks that took hours now take just minutes.”

— Nick Duda, Principal Security Engineer, HubSpot

---

**BEFORE**

- Inability to correctly prioritize alerts and assess threat criticality in ICS
- Lengthy mean-time-to-response
- Potentially never containing the incident due to new devices connecting
- Lack of visibility and threat intelligence
- Standalone, siloed security solutions work in isolation

**AFTER**

- ICS vulnerability database and multifactor risk scoring
- Execute predefined remediation of noncompliant devices at time of connect
- 100% device visibility and posture assessment upon connection
- Hunt for vulnerabilities, IOCs & other attributes
- Out-of-the-box workflow interoperability with leading security orchestration vendors

---

How it Works  >  Forescout Difference  >  Let Us Show You
How it works: Incident Response

1. Forescout eyeExtend powered by eyeSight sends up-to-date endpoint context, classification and compliance information to the 3rd party security systems.

2. Forescout shares device context to SIEM for correlation and incident prioritization. SIEM system sends a trigger to Forescout eyeExtend to initiate policy-based action on the identified endpoints.

3. Based on threat information from an ATD system, Forescout isolates the infected endpoint, hunts for IOC across unmanaged devices and initiates appropriate remediation actions based on policy.

4. Forescout verifies that EPP/EDR agents are installed and operational on all managed devices. Based on information from EPP/EDR Forescout hunts for IOAs across all devices, isolates infected devices and initiates remediation per policy.

5. Forescout continuously analyzes devices for compliance against established policies. It creates security or IT incident from with an ITSM platform and can initiate a network-based restriction to isolate the non-compliant device(s) and trigger remediation of the device(s).
The Forescout difference: Incident Response

Reduce Mean Time To Resolution (MTTR) by 47% (device breaches) and 37% (network breaches)\(^1\)

- **Real Time**
  - On-connect posture assessment, VA scanning and predefined remediation

- **OT & ICS Vulnerabilities**
  - ICS vulnerability database and multifactor risk scoring
  - Via containment, orchestration and faster MTTR

- **Unified Security Policy**
  - Across the extended enterprise

- **Security Policy Templates**
  - Ransomware and malware templates readily available

---

1. IDC, The Business Value of Pervasive Device and Network Visibility and Control with Forescout
Success Stories

**MANUFACTURING**
Discovered and categorized 97 percent of endpoints out of the box within first seven hours

**MEDICAL**
Automatically discovered 4,500 previously unknown devices (15%), including IoT and medical systems

**FINANCIAL**
Fully operational in less than two weeks

**ENERGY**
Detected 400 vulnerable hosts and addressed WannaCry-attached vulnerabilities within 48 hours
Global manufacturer secures IT and OT network and achieves dramatic ROI with Forescout.

**ENVIRONMENT:**

12,000 Endpoints
6,200 EMPLOYEES
20 Production facilities
55 Sales Offices

**RESULTS:**

- Rapid time to value: 97 percent of endpoints discovered and categorized out of the box within the first seven hours
- Discovery of 60 percent more devices than expected
- Savings of 20 hours per week by automating security tasks
- Additional time savings from automating manual processes to find and isolate high-risk devices
- Easier protection of OT and continually moving devices thanks to dynamic network segmentation

“The amount of information we get back from the Forescout platform is incredible. While many other tools will find the IP address of endpoints, it is by far the best tool I have ever used to properly find, identify and control systems. It has been beyond valuable to us.”

Joseph Cardamone, Sr. Information Security Analyst and NA Privacy Officer, Haworth
Counts on Forescout to secure networks, establish accurate device inventory and automate regulatory compliance

**ENVIRONMENT:**

- **30,000** MEDICAL CENTER ENDPOINTS
- **25+** OFFICES/CLINICS

**RESULTS:**

- Automatically discovered **4,500** previously unknown devices (15%), including IoT and medical systems
- Achieved orchestration between Forescout and Palo Alto Networks firewalls
- Streamlined asset inventory and reporting, device management and regulatory compliance
- Gained **$574,000+** annual increase in staff efficiency
- Realized **$174,000+** annual increase in business productivity

“Forescout is a force multiplier. The visibility and automation ability that it gives the security departments, it’s invaluable.”

CISO, Florida Medical Center
Counts on Forescout for device visibility, policy-based segmentation, threat response and compliance enforcement

**ENVIRONMENT:**

- **100 BRANCHES**
- **12,000 CONNECTED DEVICES**

**RESULTS:**

- Fully operational in less than two weeks
- Improved device management and regulatory compliance
- Real-time visibility and policy-based control
- Gained $415,737 in average annual benefits
- Optimized network segmentation
- Realized $215,458 in IT staff efficiencies
- Streamlined asset inventory

"The Forescout platform discovers devices and captures detailed information. It builds inventory over time of what you are seeing. You can switch VLANs on the fly. I mean, it’s a powerful tool. It does what you tell it to do."

Deputy CISO, Financial Services Firm
"We spent weeks trying to come up with the technical architecture that would give our users secure access to the corporate network without comingling with the vendor’s networks. Forescout resolved all of this without adding complex design or costly capital gear. Within a week, it was deployed and off we went."

Manager of IT, North American Energy Company

Counts on Forescout for device visibility, classification and control

**ENVIRONMENT:**

- 20,000 ENDPOINTS
- 3,500 EMPLOYEES
- 25+ SITES

**RESULTS:**

- Automated discovery, identification and classification of endpoints, including IoT devices
- Reduced network planning and deployment in field locations by several weeks
- Obtained automated asset inventory and reporting for patch management and overall device management
- Detected **400** vulnerable hosts and addressed WannaCry-attached vulnerabilities within **48** hours
Experience the Difference

Take a Virtual Test Drive

This 90-minute online test drive will spin up virtual sessions of the Forescout platform and take you through real-world cybersecurity scenarios.

Please note: this is a technical, hands-on session where an online Forescout Expert will coach you through best-practice policy creation and deployment.

Everything you learn can be quickly applied to your environment using the Forescout platform.
Thank you

Learn more at
www.Forescout.com

© 2020 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. The Forescout logos and trademarks can be found at https://www.forescout.com/company/legal/intellectual-property-patents-trademarks/. Other names mentioned may be trademarks of their respective owners. Version 0920