FORESCOUT

Business Challenges

- Protect intellectual property and sensitive data
- Comply with regulatory mandates pertaining to your company or industry
- Establish segmentation policies while maintaining user and IT productivity
- Automate enforcement of network segmentation policies
- Leverage existing network security investments

Technical Challenges

- Establish an active security segmentation framework
- Protect against pivot/lateral/insider and DDoS attacks
- Gain comprehensive visibility and control of devices—with or without security agents
- Ensure scalability of segmented networks over time
- Securely address IT/OT network consolidation
- Continuously monitor and maintain segmentation integrity over time

Network Segmentation

Define and enforce secure network segmentation policies for users, applications and devices

Cybercriminals dream of flat, unsegmented networks. Why? Perimeter defenses have become easy to sidestep through phishing attacks, social engineering and even malicious insiders within your organization. Once inside an unsegmented network, attackers can reach any resource on that network to steal your sensitive data or disrupt business operations. Learn how ForeScout Technologies secures networks from the inside out with policy-based network segmentation.

The Challenge

Perimeter security alone no longer protects your network

Before the digital ink dries on this solution brief, there will likely be another major network breach or Distributed Denial of Service (DDoS) attack that perimeter security alone had no way of stopping. Why? Cyberattackers have become adept at skirting perimeter defenses. Social engineering is a very common way for someone with malicious intent to compromise a legitimate user's system. Once the system is breached, the adversary attempts to move around the network to locate targeted information. Network segmentation limits the lateral movement ability of the compromised endpoint—reducing the attack surface. Consider these facts:

- In September 2016, more than 100,000 IoT devices—primarily security cameras and DVRs—were used to attack Domain Name Service provider Dyn.[1]
- Phishing attacks targeting unsuspecting employees continue to rise. The Anti-Phishing Working Group (APWG) observed that the number of phishing attacks detected in the first quarter of 2018 was up 46 percent over the last quarter of 2017.[2]
- 68 percent of breaches took months or longer to discover in 2017.[3]

Also, note that unscrupulous employees are an ongoing risk. According to a recent survey, 44 percent of respondents said that they would sell their credentials for less than $1,000.[4] Therefore, it should come as no surprise that in Gartner's Predicts 2016: Security for the Internet of Things report, the analysts state that, "Network segmentation and isolation will be a significant focus for future security budgets. Discovery of devices, provisioning new and existing devices, authentication services for those devices and protecting device data to and from them will account for at least 50% of the remaining security spend in organizations."

A Higher Degree of Protection for Universities

Universities must serve the needs of ultra-connected students who use multiple devices throughout the day. One major university uses the ForeScout platform to automatically move student game consoles to a secure VLAN upon connection, and then move the port back to the primary dorm VLAN when a PC or other device is plugged in. ForeScout also blocks rogue switches and routers that students attempt to add to the network.

Segmentation defined

Network segmentation significantly reduces system attack surfaces. Users only "see" the servers and other devices necessary to perform their daily tasks. Segments are created by grouping common user types and limiting network access to those resources that users require to do their jobs. Users in this context can be people or device types. Building control systems or point-of-sale (POS) systems should be put on their own segments to increase security.

Network segmentation can be achieved through a number of physical or logical means, such as properly configured internal network firewalls, switches and routers with strong access control lists (ACLs), or other technologies such as virtual local area networks (VLANs) that restrict access to particular segments of the network. Policies for endpoint types, security and compliance postures and end-user access privileges can be used to determine appropriate network segments to which the endpoint can gain access.

Old-school segmentation required IT staff to manually update network access on multiple network devices. Today, the ForeScout platform uses real-time device context to automate policy-based assignment and enforcement of ACLs and VLANs.

Why agentless visibility is essential for effective segmentation

Ask any IT security architect what they see as the most important requirement for network segmentation and you are likely to get one answer: Visibility. You must be able to see devices, users and applications, classify them and assess their security posture to determine if and to what extent they should be allowed on to the network.

Two major trends have significantly complicated enterprise visibility: workforce mobility and the Internet of Things (IoT). The increase in mobility and employees, contractors and guests bringing their own devices (BYOD) to work—and often using multiple devices in a given day—has placed incredible pressure on IT staff to validate the identities of users and the compliance status of this flood of unmanaged devices trying to access their networks. Employee-, guest- and contractor-owned devices can require different levels of network access, and all typically lack functional security agents.

The second trend, the Internet of Things, comprises a few billion invisible agentless devices that are currently connected to networks, and will soon encompass billions more that will be connecting to networks over the coming decade. The IoT poses risks unlike anything businesses have seen before. The growing list of IoT endpoints includes POS devices; smart printers; projectors; security cameras; heating, ventilating and air conditioning (HVAC) equipment; lighting systems; healthcare equipment; manufacturing sensors; vending machines and more—most of which aren't capable of supporting traditional security agents. To secure these types of devices, you must first see them. That's where agentless visibility comes in.

> Network segmentation and isolation solutions will account for 33% of all IoT security spend through 2020."
>
> — ***Predicts 2016: Security for the Internet of Things*, December 9, 2015, Gartner Inc.**

The ForeScout Solution

ForeScout helps organizations improve security through segmentation in three distinct ways:

See The ForeScout platform's agentless visibility capabilities allow it to see a comprehensive range of devices—managed and unmanaged, corporate and personal, physical and virtual, wired and wireless—even personally owned BYOD endpoints and rogue devices. It sees devices in incredible detail, identifying and evaluating network devices and applications as well as determining the device user, owner, operating system, configuration, software, services, patch state and the presence of security agents. Our platform also detects IoT devices that can't support management agents and automatically classifies a growing number of them. In addition, it continuously monitors devices, ports and connections.

Control Once you are aware of each device on your network, its owner and purpose, the ForeScout platform automates a broad range of network access controls. For example, it provides dynamic segmentation based on real-time device context. This allows you to restrict access to a noncompliant device, limit access to Internet-only, quarantine devices within a secure VLAN or grant access to appropriate corporate VLAN segments. The ForeScout platform simplifies this process for 802.1X, non-802.1X and mixed environments. Its unique Virtual Firewall feature can complement your segmentation strategy, allowing greater flexibility in mixed switching environments.

Orchestrate ForeScout offers extensive interoperability with leading switch manufacturers' products. Unlike solutions that limit you to one switch vendor, ForeScout supports mixed environments—an essential capability for business agility and growth, especially in an era of increasing mergers and acquisitions. In addition, next-generation firewalls (NGFWs) are playing a larger role in restricting inbound and outbound traffic as well as securing network segments' access to the data center. ForeScout offers integration with leading NGFWs, wired/wireless switches, VPN concentrators, cloud-based management systems and a total of more than 70 network, security, mobility and IT management products* via ForeScout Base and Extended Modules.

Segmentation Use Cases

IT staff can easily define polices within the ForeScout platform to control network access based on device types, user profiles, applications or numerous role-based characteristics shared via Active Directory or a Lightweight Directory Access Protocol (LDAP)-based directory service. Our policy engine enables network segmentation to abstract policies away from physical IP addresses. This allows for automated, on-the-fly segmentation control, eliminating the need for IT staff to manually change network access on multiple network devices. ForeScout allows broad flexibility in creating segmentation polices to match your company's organizational and security needs—as well as the performance and scalability to effectively apply growing policy lists.

Here are a few common segmentation policies.

Guest access

Corporate networks support company-owned devices, BYOD and guest devices. Guest access includes visitors, contractors and consultants—where different guest types likely need different network access. Network security requires excluding certain device types from the network. Therefore, network access should be

limited to just the network segments that guests and others need to accomplish their roles or functions. For example, visitors should only have access to the Internet. Consultants, on the other hand, may be assigned to specific network segments that have limited access to broader corporate networked resources.

ForeScout discovers devices when they initially connect to the network and assesses device type (company-owned, BYOD or guest). The platform enforces corporate-created policies for device classes and applies the appropriate VLANs or ACLs to place BYOD, contractor and guest devices on the appropriate network segments, allowing productive access while limiting the overall security risk. Also, through continuous monitoring, the ForeScout platform can dynamically re-assign devices to segments to address changes in device behavior, security posture or network modifications.

Role-based access

The functional roles of employees typically coincide with a required list of network resources. Grouping similar functional roles and their required resources results in network segmentation that fortifies the network against malicious insider behavior or an exploited corporate device.

When the ForeScout platform discovers a corporate-owned device on the network, it can determine the user's role from a directory service and then assign the appropriate VLAN or wireless LAN controller role to that user. In addition, it can verify the device's compliance posture by determining security patch status, whether antivirus software is up to date and running and other customer-defined requirements. Based on your security policies, the solution can alter network access and redirect the user to a secure VLAN until a device is made compliant.

Defining policies for assigning IoT devices to network segments

Security is all about layers of defense at the network and host levels. However, host-level security is not likely for many IoT devices due to their thin-client architecture and limited hardware performance and memory. Therefore, network segmentation is emerging as a best-practice method.

Every IT security professional is painfully aware of the brand damage and legal consequences associated with recent data breaches. During one of the largest in history, an overwhelmed IT staff could not respond quickly to alerts from its security systems. According to reports, the exploit entry point was an online vendor portal using an HVAC contractor's log-in credentials. From this pivot point, the hacker ultimately gained access to the POS system and customer data. Network segmentation of the vendor portal from the POS systems' segment would have made this customer data compromise much less likely. Moreover, segmentation could have minimized damage caused by a recent IoT hack of video surveillance cameras used in a DDoS attack.[5]

Thanks to agentless visibility, the ForeScout platform discovers both traditional and IoT devices on the network. It also profiles and categorizes many of these devices, allowing you to limit their operation and access to network segments containing only those resources that are appropriate for the device or user's role or security posture. In this way, our technology provides policy-based assignment of VLANs or ACLs to limit the attack surface of corporate IoT devices.

This same segmentation functionality is effective for manufacturing sensors, medical devices, security cameras or other IoT devices.

Here's how:

1. IoT device connects to the network.
2. ForeScout discovers the device, determines type of device and ownership.
3. If the IoT device is corporate-owned, ForeScout places it in the appropriate VLAN or applies an ACL to limit network access to necessary resources only. If the device is not corporate-owned, it is denied access.
4. ForeScout monitors the IoT segment for anomalous behavior, leveraging a third-party Security Information and Event Management (SIEM) system through a ForeScout Extended Module for SIEM.
5. Based on policy, if one of the third-party systems reports malicious behavior, the IoT device(s) is moved to a restricted VLAN segment for further analysis.

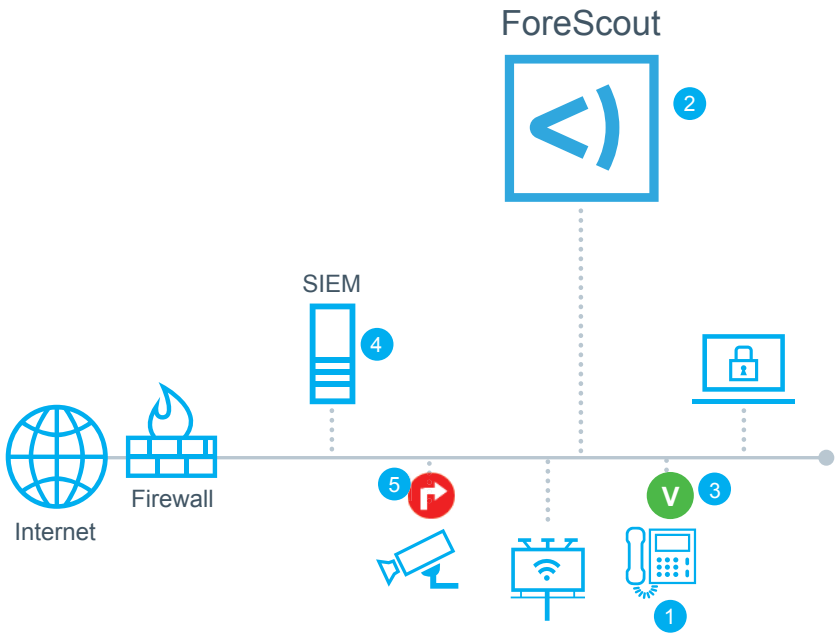

Figure 1: How the ForeScout platform applies policy-based network segmentation to IoT devices.

Learn more at
www.ForeScout.com

FORESCOUT

ForeScout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support 1-708-237-6591

[1] TechTarget, October 2016
[2] APWG Phishing Activity Trends Report, 1st Quarter, 2018
[3] 2018 Data Breach Investigations Report, https://www.verizonenterprise.com/verizon-insights-lab/dbir/
[4] Fortune, http://fortune.com/2016/03/30/passwords-sell-poor-sailpoint/
[5] http://www.thejournal.ie/webcam-iot-hacking-2860398-Jul2016/

*As of June 2018