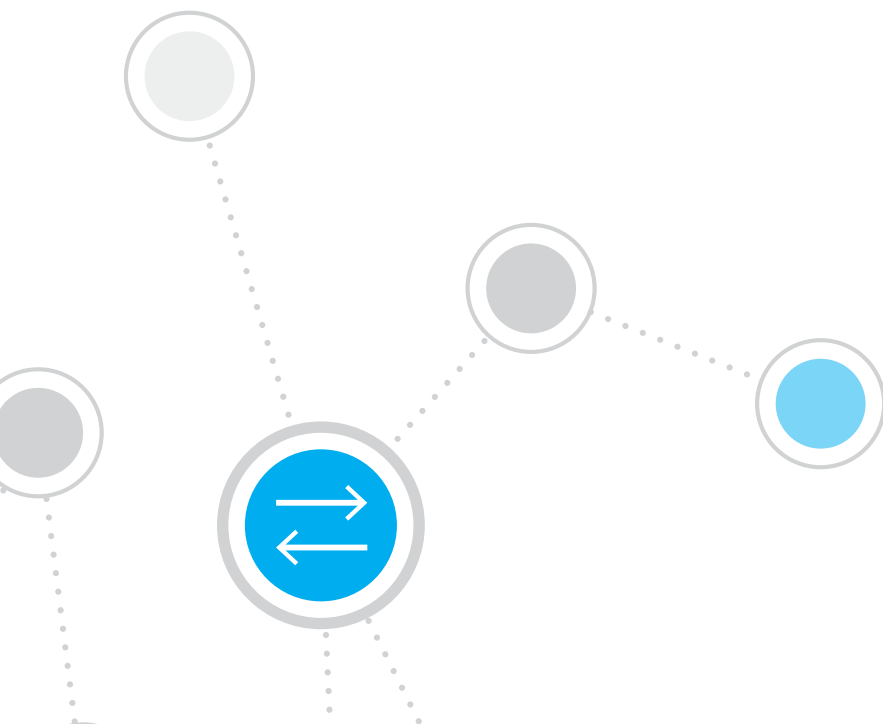# ForeScout Agentless Visibility and Control

ForeScout Technologies has pioneered an agentless approach to network security that effectively helps address the challenges of endpoint visibility and control in large, dynamic and diverse environments. The ForeScout platform discovers servers, desktops, laptops, tablets, smartphones, Internet of Things (IoT) devices, operational technology (OT) systems, peripherals, network infrastructure components and rogue devices the instant they connect to the network—even if they don't have security agents installed. It gathers detailed information about device types, users, applications, operating systems and more. It then allows, denies or restricts access to internal network resources, issues notifications and initiates remediation based on established policies and discovered security state.

The ForeScout platform's distinctive features and advantages have been widely discussed elsewhere. This paper describes the technical innovations that make them possible. We will describe how the ForeScout platform:

- Detects and assesses network-connected infrastructure and devices without installed security agents

- Collects, correlates and analyzes device information to assess and continuously monitor security posture

- Auto-classifies new devices using cloud-based intelligence

- Provides passive-only monitoring to inventory OT devices safely

- Uses discovered insights to autonomously control endpoints and protect the network

- Supports rapid, efficient deployment in heterogeneous environments

The ForeScout Platform: An Introduction

The ForeScout platform comprises three core components:

ForeScout CounterACT® — An agentless security appliance (physical or virtual) that dynamically identifies and evaluates network endpoints and applications the instant they connect to the network. CounterACT quickly determines the user, owner and operating system, as well as device configuration, software, services, patch state and the presence of security agents, then it provides device remediation, control and continuous monitoring.

CounterACT Enterprise Manager — A centralized management and control solution for multiple ForeScout CounterACT appliances in large network environments. It maintains the policies and network configuration and deploys them to the CounterACT appliances. This simplifies implementation, as the Enterprise Manager provides a single, centralized configuration and management portal for all CounterACT appliances.

ForeScout Modules — ForeScout Base and Extended Modules expand the see and control capabilities of ForeScout CounterACT to other security and IT management solutions. Your organization can share contextual device data with third-party systems, automate policy enforcement across disparate solutions, bridge previously siloed IT processes, accelerate system-wide response and more rapidly mitigate risks. Modules support more than 70 third-party solutions*, allowing the combined system to accelerate response, achieve operational efficiencies and provide superior security by making formerly disjointed security products work as one.

The ForeScout platform offers a range of capabilities that span three categories:

See

- Discover devices the instant they connect to the network without requiring agents
- Classify and profile devices, users, applications and operating systems
- Assess device hygiene and continuously monitor security posture

✋ Control

- Notify end users, administrators or IT systems about security issues
- Support your efforts in conforming with policies, industry mandates and best practices such as network segmentation
- Restrict, block or quarantine non-compliant or compromised devices

⇄ Orchestrate

- Share contextual insights with IT, security and management systems
- Automate common workflows, IT tasks and security processes across systems
- Accelerate system-wide response to quickly mitigate risks and data breaches

How does ForeScout realize these capabilities? What technical innovations make them possible? Let's take a look.

How ForeScout discovers and classifies network endpoints without an installed security agent

There's a reason other network security solutions require a software agent on connected devices: an onboard agent makes it easy to communicate with the device and monitor its state and activity. The downside of this dependence is equally obvious: the security solution can't see or inspect devices that are not already under management or that lack an operational, up-to-date agent. To see what other security solutions can't, ForeScout uses multiple, agentless discovery methods.

Devices	User	Operating System	Applications
◉ DHCP ◉ SNMP ◉ SecureConnector ◉ Remote Inspection ◉ 802.1X ◉ Nmap ◉ NetBIOS ◉ NetFlow	◉ SecureConnector ◉ Remote Inspection ◉ 802.1X ◉ NetBIOS ◉ AD and Other Directory Servers	◉ DHCP ◉ SPAN ◉ Nmap	◉ SPAN ◉ SecureConnector ◉ Remote Inspection
Security Agents	**Network**	**Peripherals**	**Virtual Servers/Desktops**
◉ SecureConnector ◉ Remote Inspection	◉ DHCP ◉ CLI ◉ Traps ◉ SNMP ◉ SPAN ◉ NetFlow	◉ SecureConnector ◉ Remote Inspection	◉ VMware® vSphere API Calls ◉ SecureConnector ◉ Remote Inspection

Figure 1: ForeScout device discovery and interrogation techniques

CounterACT employs a combination of active and passive methods to discover and classify devices on an organization's network. Utilizing active discovery methods it polls switches, VPN concentrators and wireless controllers for a list of connected devices. Using NBT scans and Nmap, or via WMI for deeper inspection of corporate-managed devices, it inspects workstations running Windows, Mac or Linux (requires SSH) without the use of agents. Its passive inspection methods include receiving SNMP traps from switches and wireless controllers, monitoring a network SPAN port to see network traffic and

leveraging information such as TCP window sizes, session information, HTTP traffic, DHCP banners and NetFlow traffic data. If 802.1X is implemented, ForeScout can monitor a RADIUS server whether built-in or external. In addition, ForeScout technology can import external MAC classification data or request LDAP data. And we continue to add new discovery methods, such as the recently added Power over Ethernet (PoE). Figure 1 illustrates the range of ForeScout discovery techniques.

ForeScout's comprehensive approach to passive monitoring is especially useful in industrial IoT and OT environments where active probing and scanning techniques can cause system and business disruption. The ForeScout platform allows you to detect and monitor devices in such environments without actively scanning or interrogating connected devices, and without agents.

ForeScout also offers an optional, dissolvable software agent, SecureConnector,™ which can be downloaded to a client machine as it connects to the network. SecureConnector interrogates the device and collects security posture information, which is forwarded to ForeScout via an SSL connection. It can be dissolved after a single session or permanently installed on devices that are directly managed. It supports session-specific policy enforcement in which control actions may vary depending on factors such as the time of day or the domain to which a device is attached. SecureConnector can detect ARP spoofing, block man-in-the-middle attacks, and harden open ports by diverting traffic to a quarantined VLAN.

How ForeScout correlates and analyzes the device data it collects

Not surprisingly, these varied discovery methods quickly produce and continuously refresh a vast amount of information on device identity, state and behavior. Figure 2 illustrates the depth and diversity of this data.
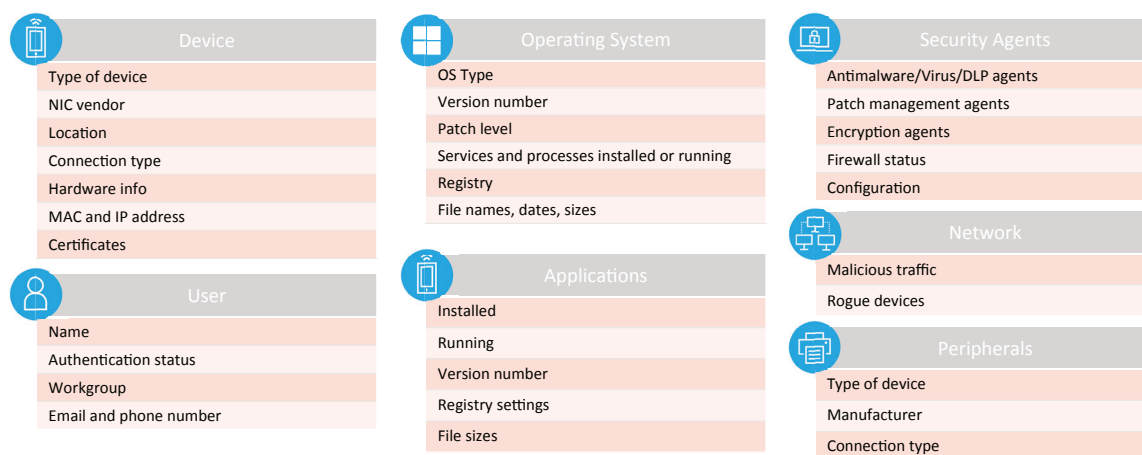
Device		Operating System		Security Agents	
Type of device		OS Type		Antimalware/Virus/DLP agents	
NIC vendor		Version number		Patch management agents	
Location		Patch level		Encryption agents	
Connection type		Services and processes installed or running		Firewall status	
Hardware info		Registry		Configuration	
MAC and IP address		File names, dates, sizes		**Network**	
Certificates				Malicious traffic	
User		**Applications**		Rogue devices	
Name		Installed		**Peripherals**	
Authentication status		Running		Type of device	
Workgroup		Version number		Manufacturer	
Email and phone number		Registry settings		Connection type	
		File sizes			

Figure 2: Endpoint data collected by ForeScout

The ForeScout platform's adaptive abstraction layer ingests billions of packets of raw data across a wide array of heterogeneous network systems. It then consolidates this data into a unified view to create a real-time depiction of the devices on the network by type. ForeScout does not require vendor-specific network equipment, upgrades of existing infrastructure or reconfiguration of switches and switch ports to support 802.1X. As organizations adopt virtual and cloud environments, this technology has the flexibility to integrate with hypervisor technologies and cloud platforms.

The abstraction layer adapts to the IT enterprise environment and continuously enriches its information as organizations make more data available. As an example, organizations can choose to consume NetFlow data, the metadata of actual network traffic. ForeScout can use this information to expedite new device detection, collect device properties such as IP addresses and session protocols, and understand which devices are talking to each other. If organizations choose to allow full network traffic

monitoring through a SPAN port, ForeScout can extract very granular information such as device type, MAC address, HTTP user agent and the applications in use. These insights can be used to identify malicious traffic.

How ForeScout can help you auto-classify new devices

The ForeScout Device Cloud is a constantly expanding repository of device insight that currently covers more than three million devices. This rich source of device data is the crowdsourced creation of a community of over 500 ForeScout customers across more than 10 industries. Together, the ForeScout Device Cloud and the ForeScout platform provide a rich taxonomy to auto-classify devices by their type and function, operating system and version, and manufacturer and model.

Auto-classifying devices is essential for creating security policies for network access, device compliance and network segmentation. You can leverage new and updated auto-classification profiles published by ForeScout on a frequent basis. In addition, the ForeScout platform lets you create custom classification policies to auto-classify devices unique to your environment.

How ForeScout uses device visibility to autonomously control endpoints and protect networks

ForeScout innovations include a policy engine that continuously checks devices against a set of policies that dictate and enforce device behavior on the network. While other vendor technologies rely on periodic checks or operator queries, our policy engine provides continuous, real-time monitoring for more than a million devices. Our policies are triggered in real time by events that occur either on a specific device or in the network. These can be network admission events, such as plugging into a switch port or changing an IP address. They can be authentication events like those received by a RADIUS server or detected in network traffic. Policies can also be invoked by changes in device attributes. Figure 3 illustrates the range of control actions available to the ForeScout platform when a policy is triggered.
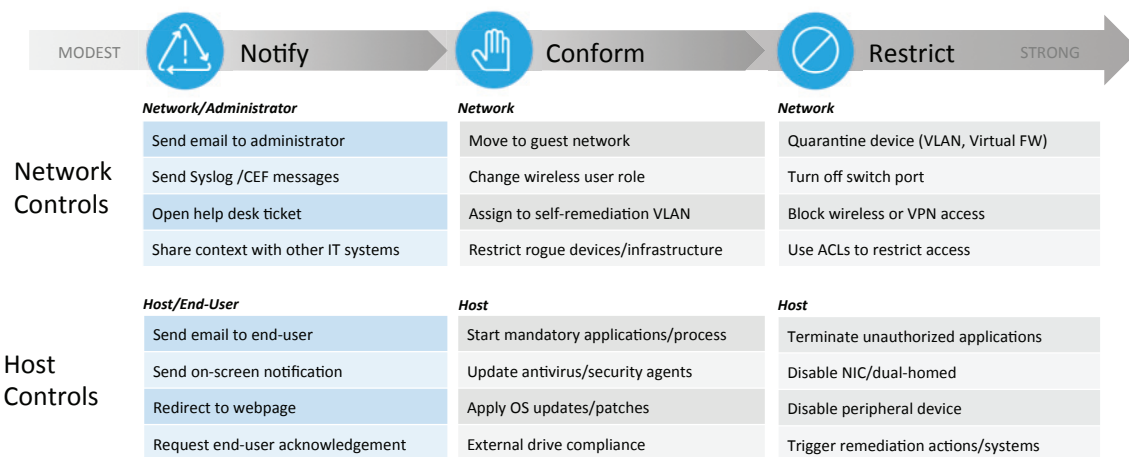
	MODEST — Notify	Conform	Restrict — STRONG
	Network/Administrator	**Network**	**Network**
Network Controls	Send email to administrator	Move to guest network	Quarantine device (VLAN, Virtual FW)
	Send Syslog /CEF messages	Change wireless user role	Turn off switch port
	Open help desk ticket	Assign to self-remediation VLAN	Block wireless or VPN access
	Share context with other IT systems	Restrict rogue devices/infrastructure	Use ACLs to restrict access
	Host/End-User	**Host**	**Host**
Host Controls	Send email to end-user	Start mandatory applications/process	Terminate unauthorized applications
	Send on-screen notification	Update antivirus/security agents	Disable NIC/dual-homed
	Redirect to webpage	Apply OS updates/patches	Disable peripheral device
	Request end-user acknowledgement	External drive compliance	Trigger remediation actions/systems

Figure 3: Available ForeScout control actions

The policy engine leverages both infrastructure- and host-based controls. Controls in the network provide policy-based segmentation, enabling or restricting access according to user identity, role and device state. ForeScout integrates natively with more than 30 switch and wireless vendors* and

provides generic integration with routers that run the Linux operating system. Depending on the vendor, various methods are used individually or in combination, including SNMP, CLI and NETCONF. Working at a network switch, this technology can change a VLAN assignment, add an ACL or disable a switch port. At a wireless controller, it can blacklist a MAC address or change the role of a user. In addition, our technology can restrict remote VPN users.

The ForeScout platform also works with next-generation firewalls to provide dynamic, policy-based segmentation. Next-generation firewalls provide network control based on user, device, application and traffic classification. They leverage user and device context from a variety of sources, including the ForeScout platform, to enforce granular access policies with precise and flexible control over resources. This enables IT organizations to implement dynamic network segmentation and create context-aware security policies within their next-generation firewalls based on endpoint context information from ForeScout.

The ForeScout platform's host-based controls, on the other hand, enforce device hygiene. Working on a host, our technology can start and stop applications, update antivirus security agents, disable peripheral devices and request end-user acknowledgement. The policy engine applies these policies automatically regardless of a device's location. It can follow a device as it moves within the corporate network, into the data center and across the cloud. ForeScout determines the type of infrastructure and, based on policy, applies the appropriate control actions.

How ForeScout segments the network without reconfiguring the infrastructure

ForeScout offers a Virtual Firewall (vFW) mechanism that allows network access control and segmentation with no writing to the network infrastructure. ForeScout vFW technology can block, limit or quarantine hosts on the network by detecting their network traffic and disrupting their communication with a target host or server. It works by detecting a connection request from a source host that is subject to a vFW action, then emulating that source host and sending TCP reset packets to the target, instructing it to terminate and ignore the TCP/IP connection request from the source host.

ForeScout vFW technology can be used to:

- Create network security zones
- Quarantine non-compliant or non-corporate hosts
- Quarantine infected or malicious hosts

One especially compelling use case for vFW segmentation is IoT device security. Many IoT devices are difficult to protect with conventional endpoint security solutions because they are thin clients and have limited hardware performance and memory. Therefore, network segmentation has emerged as the best-practice method.

With its agentless visibility, ForeScout discovers, profiles and categorizes IoT devices as they connect to the network. It can then limit their operation and resource access to appropriate network segments. Through policy-based assignment to VLANs or ACLs, ForeScout restricts IoT device access to limit the network's attack surface.

How the ForeScout platform's solution architecture supports simple, efficient deployment in large or small environments

ForeScout Enterprise Manager uses distributed computing algorithms, so ForeScout CounterACT

physical or virtual appliances can independently manage devices within their control. This enables organizations to expand their deployment by simply adding more CounterACT appliances. Enterprise Manager aggregates the device information from the appliances and consolidates this data into a unified view of the extended enterprise for the administrator. The algorithms allow the administrator to search for security-related information such as users, processes and services—across the CounterACT deployment in real time—and retrieve it in seconds.

CounterACT offers centralized, distributed and hybrid deployment models to accommodate enterprise environments across a wide range of scalability requirements and varied levels of complexity.

Centralized deployment architectures

Figure 4 shows a centralized deployment architecture in which an Enterprise Manager communicates with, manages and deploys policies to multiple CounterACT appliances in a data center or other major site. The Enterprise Manager contains the database of endpoints (active and inactive) from the appliances it manages.

In this type of deployment, CounterACT appliances require IP connectivity to the remote sites in order to manage devices and other endpoints located there. Traffic from the remote locations is sent to the CounterACT appliances via a SPAN interface for monitoring and assessment. If DNS, DHCP, User Directory or other centralized services are utilized, the CounterACT appliances can monitor these services to detect threats or potential rogue activity and initiate remediation.
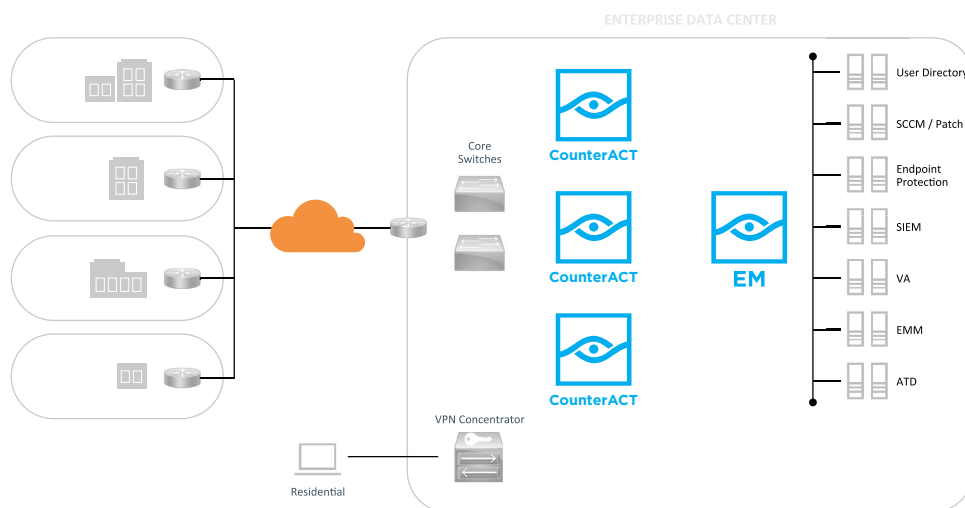

Figure 4: ForeScout centralized deployment

Distributed deployment architectures

Figure 5 shows a decentralized deployment model utilizing a mixture of CounterACT appliances located in both a central facility and various remote sites. An Enterprise Manager manages and provides policies to various CounterACT appliances, physical or virtual, and maintains a database of active and inactive endpoints.

In addition to the features available in a centralized model, distributed deployments enable the use of virtual firewalls, browser redirection and endpoint authentication to a server when a local CounterACT appliance is at that site.

The Enterprise Manager functions as the central notification point, communicating via email or Syslog and bi-directionally for SIEM services via CEF or LEEF messaging to perform endpoint actions and to notify systems of endpoint status.
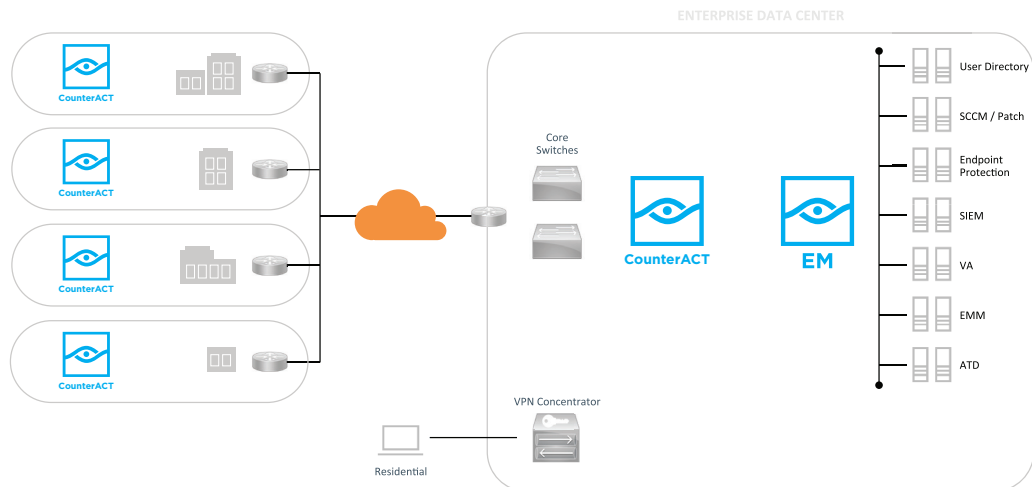
Figure 5: ForeScout distributed deployment

Hybrid deployment architectures

Figure 6 illustrates a hybrid deployment model using a mixture of CounterACT appliances in a central location and in remote sites. Each appliance monitors the network segments it is associated with and configured to manage. The Enterprise Manager maintains a database of the infrastructure and issues policies for the appliances.

As in distributed deployments, hybrid implementations support virtual firewalls, browser redirection and authentication verification of an endpoint to a server when a local CounterACT appliance is deployed at that site.
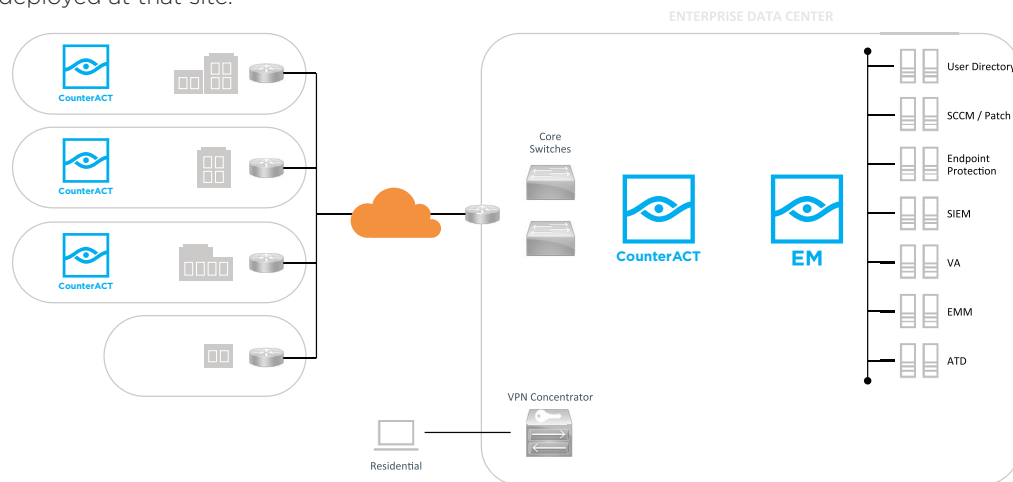

Figure 6: ForeScout hybrid deployment

Securing enterprise networks without endpoint agents

The ForeScout platform allows network security teams to see, assess and control the device as soon as it connects to their networks, without first enrolling it in a management system or installing a software agent. For the first time, the endpoints that so often escape security control—BYOD, IoT and rogue devices—are made visible, profiled to determine ownership and security posture, and automatically brought under policy-based control. This is why agentless visibility and control are so critically important.

How you can evaluate the ForeScout platform for yourself

The best way to gain a better understanding of ForeScout's agentless visibility and control capabilities is to see them firsthand. ForeScout offers many ways to gain greater insight into the ForeScout device visibility and control platform, including:

- **Take a Test Drive:** Experience the before-and-after difference of the ForeScout platform with a hands-on test drive that takes you through five powerful use cases.

- **Request a Demo:** Visit the ForeScout demo page to request a personal demo and access a full complement of on-demand demos and video options.

- **Use the ForeScout Business Value ROI Tool:** Quantify the business value the ForeScout platform can provide to your organization (as calculated by IDC's Business Value Model) in just 10 minutes.

Acronym Glossary

ACL (Access Control List)

ARP (Access Resolution Protocol)

BYOD (Bring Your Own Device)

CEF (Common Event Format)

CLI (Command Line Interface)

DHCP (Dynamic Host Configuration Protocol)

HTTP (Hypertext Transfer Protocol)

IoT (Internet of Things)

IP (Internet Protocol)

LDAP (Lightweight Directory Access Protocol)

LEEF (Log Event Extended Format)

MAC (Media Access Control)

NetBIOS (Network Basic Input/Output System)

Nmap (Network Mapper)

NBT (NetBIOS over TCP/IP)

NETCONF (Network Configuration Protocol)

PoE (Power over Ethernet)

RADIUS (Remote Authentication Dial-in User Service)

SNMP (Simple Network Management Protocol)

SPAN (Switch Port Analyzer)

SSH (Secure Shell)

SSL (Secure Socket Layer)

TCP (Transfer Control Protocol)

VLAN (Virtual Local Area Network)

VPN (Virtual Private Network)

WMI (Windows Management Instrumentation)

Learn more at
www.ForeScout.com

ForeScout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591
Fax +1-408-371-2284

About ForeScout

ForeScout Technologies, Inc. is transforming security through visibility. ForeScout offers Global 2000 enterprises and government organizations the unique ability to see devices, including non-traditional devices, the instant they connect to the network. Equally important, ForeScout lets you control these devices and orchestrate information sharing and operation among disparate security tools to accelerate incident response. Unlike traditional security alternatives, ForeScout achieves this without requiring software agents or previous device knowledge. The company's solutions integrate with leading network, security, mobility and IT management products to overcome security silos, automate workflows and enable significant cost savings. As of March 31, 2018, more than 2,800 customers in over 80 countries improve their network security and compliance posture with ForeScout solutions.

*As of March 31, 2018