

# ForeScout CounterACT™

## Continuous Monitoring and Mitigation

**Real-time Visibility**  
**Network Access Control**  
**Endpoint Compliance**  
**Mobile Security**  
**Rapid Threat Response**



## Benefits

### Security

- Gain real-time network and endpoint intelligence
- Continuously monitor and mitigate endpoint configuration and security gaps
- Block rogue devices, malicious activity, unsanctioned software and advanced threats
- Increase security oversight by collapsing information silos and enhancing control context

### Control Automation

- Accelerate endpoint compliance and incident response
- Facilitate onboarding of corporate and personal mobile devices
- Grant appropriate network access based on user, device and security posture
- Coordinate policy-based response across disparate security tools

### Cost savings

- Lower costs associated with endpoint remediation tasks
- Reduce IT overhead associated with provisioning guest access and enabling BYOD
- Reduce mean time to resolve security and operational issues
- Optimize existing network and security investments through advanced interoperability
- Expedite audit, compliance and inventory reporting

## Rethink IT Security

### ***Do you have adequate visibility to the assets and risks on your network?***

The expression “you can’t secure what you can’t see” is all the more relevant in today’s complex IT environment. Most organizations are unaware of a significant percentage of the endpoints on their networks because of the proliferation of mobile, personal, transient and virtual devices. These devices are either not under management, have broken agents, or aren’t detected between periodic scans. As a result, you’re blind to the vulnerabilities and security gaps on these devices. How do you gain real-time insight into the endpoints, users, applications and risks on your network?

### ***Can you enforce network access based on user, device and security posture?***

You’re faced with unprecedented diversity of users, devices and applications on your network — guests, contractors, partners and employees using their personal or corporate laptops, tablets and smartphones. Each requires access to a different set of network resources to remain productive. How do you efficiently provide appropriate network access to only authorized users, approved devices, sanctioned applications and compliant systems?

### ***You’ve secured your corporate endpoints, right? But are there gaps?***

You’ve made substantial investments in endpoint security and configuration management systems — antimalware, data loss prevention, encryption, patch management, etc. But do you have coverage on your managed endpoints? Unfortunately, these systems are typically unaware of blind spots caused by missing, disabled or broken agents. In spite of best efforts, you probably have a gap in protection, leaving your organization vulnerable to infection, breaches and compliance risks. How can you continuously validate and maintain endpoint security defenses?

### ***Do you have an effective mobile and BYOD security strategy?***

Enterprise mobility and IT consumerization are the “new norm” for business, but they also introduce more security and privacy issues. You must protect your network from unsanctioned, rogue and compromised mobile devices in order to prevent malware propagation, data leakage and compliance violations. You need network-based defenses to fortify device, data and application-based defenses provided by your MDM system. How do you mobilize your workforce and enable BYOD while maintaining security?

### ***Can you respond quickly to advanced threats and security breaches?***

Over the years, you’ve invested in a variety of security systems to thwart rising cyber threats. Many of these systems don’t communicate with one another, only issue alerts, and can’t take action to mitigate or contain the threat. As a result, you’re overwhelmed with too many alerts. How do you coordinate security controls and automate response to rapidly contain threats and breaches?

### ***There is good news.***

ForeScout CounterACT™ enables you to efficiently address network access, endpoint compliance, mobile security and threat mitigation challenges within today’s complex enterprise networks.

### ***The intelligence you need. The automation you want.***

# Solutions for Real-time Intelligence, Control and Automated Response

## Real-time Visibility

ForeScout CounterACT provides real-time visibility of users, devices, systems and applications on your enterprise network. Devices are dynamically discovered, profiled and assessed — wired and wireless, managed and unmanaged, virtual and embedded, laptops and mobile. CounterACT uses a multi-faceted approach for device discovery and classification that does not require the use of software agents or prior knowledge of a device.

Who are you?	Who owns your device?	What type of device?	Where/how are you connecting?	What is the device hygiene?
<ul style="list-style-type: none"><li>Employee</li><li>Partner</li><li>Contractor</li><li>Guest</li></ul>	<ul style="list-style-type: none"><li>Corporate</li><li>BYOD</li><li>Rogue</li></ul>	<ul style="list-style-type: none"><li>Windows, Mac</li><li>iOS, Android</li><li>VM</li><li>Non-user devices</li></ul>	<ul style="list-style-type: none"><li>Switch</li><li>Controller</li><li>VPN</li><li>Port, SSID</li><li>IP, MAC</li><li>VLAN</li></ul>	<ul style="list-style-type: none"><li>Configuration</li><li>Software</li><li>Services</li><li>Patches</li><li>Security Agents</li></ul>

Figure 1: ForeScout CounterACT provides real-time asset intelligence and security posture details.

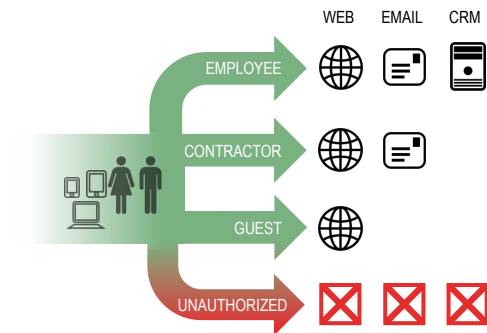


Figure 2: ForeScout CounterACT can be configured to allow appropriate network access control based on user, device, and security context.

## Network Access Control

ForeScout CounterACT lets you grant network access with a fine degree of precision based on user, device and security posture, while restricting unauthorized devices and users. Access policies can be tailored based on user, role, device type, authentication, operating system, device ownership, security posture, location, time of day, etc. CounterACT offers extensive guest registration and onboarding options so you can customize the admission process to suit your organizational needs and alleviate IT administrative overhead.

## Endpoint Compliance

ForeScout CounterACT ensures that endpoints on your network are compliant with your security policies. CounterACT works with both managed and unmanaged devices, and helps monitor your compliance levels, supports regulatory audit requirements and provides on-demand asset intelligence. When CounterACT discovers a security issue or policy violation, such as a missing or inactive security agent, it can automatically fix the problem, or invoke your existing patch management, remediation or helpdesk systems.



Figure 3: ForeScout CounterACT monitors endpoint compliance levels and helps remediate security gaps

## Secure Mobility and BYOD

ForeScout CounterACT enables the secure use of corporate and personal smartphones, tablets and other mobile devices on your network. CounterACT integrates with popular MDM systems and helps automate enrollment processes to reduce helpdesk overhead and enhance end-user productivity. Integration with MDM systems also allows you to reduce mobile security risks by conducting real-time MDM posture assessment of mobile devices at network access time and while on the network.

## Rapid Threat Response

ForeScout CounterACT integrates with leading vulnerability assessment and advanced threat detection systems to reduce your attack surface and expedite response to cyber threats. CounterACT can scan your network for indicators of compromise, determine the extent of infection, and initiate policy-based actions to quarantine or remediate compromised endpoints. This allows organizations to limit internal malware propagation and reduce security breaches.



# The ForeScout Approach

ForeScout CounterACT is a continuous monitoring and mitigation platform that provides real-time visibility and coordinated controls within your complex IT environment. Based on next-generation network access control (NAC) technologies, CounterACT delivers:

- Real-time intelligence about the devices, systems, applications and users on your network
- A wide range of granular controls to help you enforce endpoint security policy
- Information sharing and automation among your existing IT security and management systems to help you rapidly fix security issues and contain breaches

“CounterACT allows us to see and apply policy to everything on our network. The interoperability and control capabilities are phenomenal — it changes the game in terms of being proactive and responsive.”

**Chief Information Security Officer,  
SIRVA Worldwide**

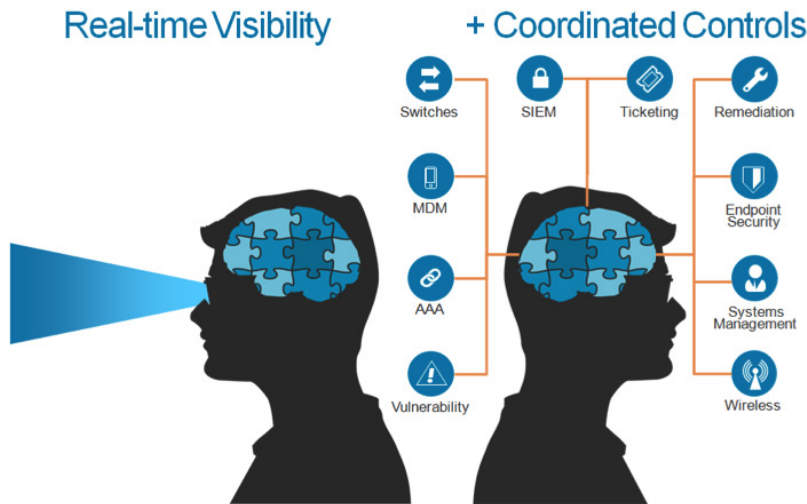


Figure 4: CounterACT with ControlFabric technology delivers real-time visibility and control over your network.

ForeScout CounterACT integrates with your network, security and IT infrastructure through our ControlFabric™ architecture. ForeScout ControlFabric is a set of open integration technologies that enable CounterACT and other IT solutions to exchange information and efficiently mitigate a wide variety of network, security and operational issues. As a result, you can reduce the window of opportunity for cyber threats to penetrate your network, and gain higher return on investment from your existing security products.

“CounterACT is ideally featured to help us manage the unmanaged... we were able to control access to our production LAN... distinguishing laptops from desktops and apply different security policies to each—without needlessly disrupting users or forcing agent-based authentication onto every endpoint.”

**Network Architect and VP of  
Engineering, Bremer Bank**

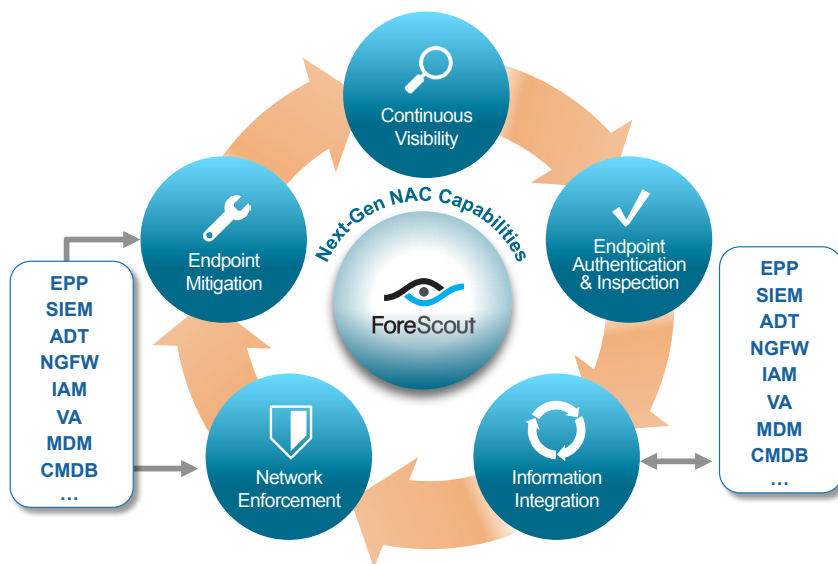


Figure 5: ForeScout CounterACT platform interoperates with popular IT and security management systems to further enhance continuous monitoring, intelligence and mitigation capabilities.

“ForeScout CounterACT, as a network security platform in particular, has excellent visibility, some pretty granular control and more flexible implementation capabilities for both wired and wireless network.”

**CISO,  
Pioneer Investments**

CounterACT currently integrates with more than 60 different network, security, mobility and IT management products. Additionally, ForeScout's open ControlFabric interface allows vendors, system integrators and customers to easily implement custom integrations based on common, standards-based protocols.

ForeScout CounterACT, along with ControlFabric, provides you continuous monitoring and mitigation capabilities, a means to enforce network and endpoint controls, and a mechanism to invoke policy-based automated response to optimize security and compliance management.

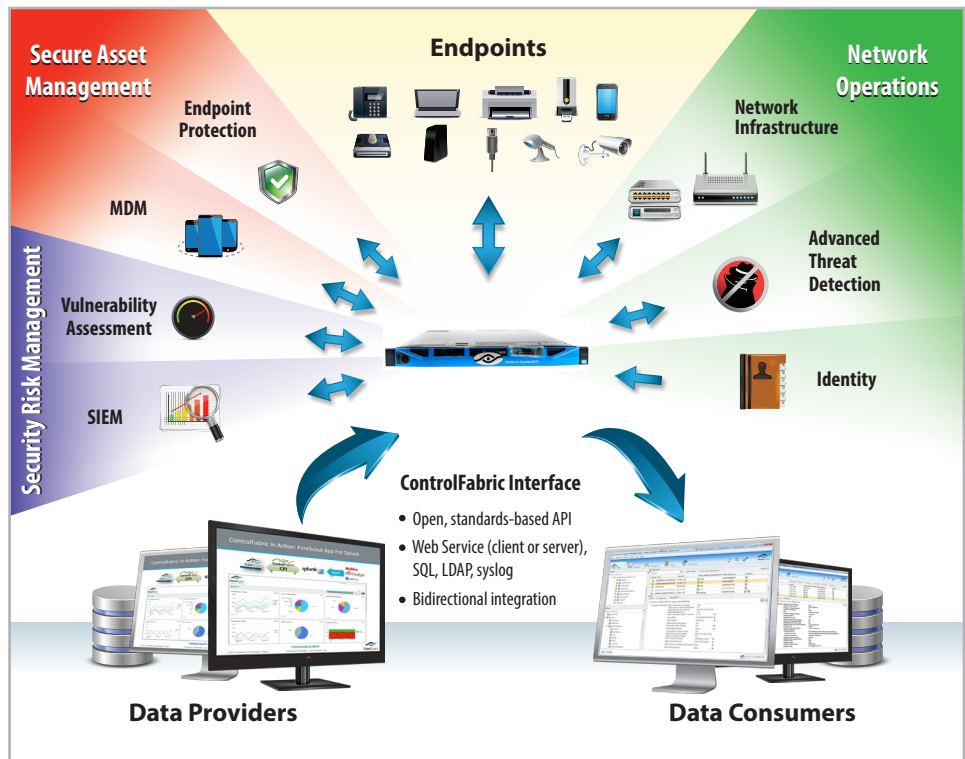


Figure 6: The ControlFabric Interface

## The ForeScout Difference

- **Fast and easy deployment.** CounterACT is an all-in-one physical or virtual appliance that is deployed out-of-band and typically doesn't require network reconfiguration or infrastructure upgrades. Built-in wizards and customizable policy templates support a broad range of security and compliance mandates, and help you configure security policies quickly and accurately.
- **Vendor and infrastructure agnostic.** CounterACT works with a wide variety of popular switches, routers, firewalls, endpoints, patch management systems, anti-malware systems, directories, ticketing systems and more. It works in heterogeneous, multi-vendor and legacy environments without locking you into proprietary architectures that have limited third party device support.
- **Agentless operation.** CounterACT can identify, classify, authenticate and control network access of both managed and unmanaged (BYOD) endpoints without any help from agents or any kind of preconfigured endpoint software. Deep endpoint inspection can also be done without an agent as long as CounterACT has administrative credentials on the endpoint. In situations where CounterACT does not have administrative credentials (e.g. BYOD), deep inspection can be performed with the help of our optional SecureConnector agent.
- **Non-disruptive.** Unlike some security products that immediately disrupt users with heavy-handed controls, CounterACT can be deployed in a phased approach which minimizes disruption and accelerates results. You can start by gaining visibility into your assets and identifying problem spots, then gradually invoke policy-based controls, starting with the highest priority issues, and progressively dialing-up automated enforcement, remediation and mitigation actions.
- **Scalability.** CounterACT has been proven to manage over 500,000 endpoints across multiple sites. Centralized management capability allows you to see and control hundreds of thousands of connected devices, easily configure and maintain policies, and have operational oversight to identify and respond to issues within a global enterprise.
- **Open Interoperability.** CounterACT offers extensive third-party vendor interoperability through our open standards-based ControlFabric integration architecture.

# Take the ForeScout Challenge

What are you waiting for? Give us a call. Tell us which of the solutions described in this brochure would be most helpful to you. We'll arrange for an on-site evaluation and demonstrate how ForeScout CounterACT can work for you.

## About ForeScout

ForeScout enables organizations to continuously monitor and mitigate security exposures and cyber attacks. The company's CounterACT platform dynamically identifies and evaluates network users, endpoints and applications to provide visibility, intelligence and policy-based mitigation of security problems. ForeScout's open ControlFabric architecture allows a broad range of IT security products and management systems to share information and automate remediation actions. Because ForeScout's solutions are easy to deploy, unobtrusive, extensible and scalable, as of January 1, 2015, they have been chosen by more than 1,800 of the world's most secure enterprises and government agencies in over 62 countries. Headquartered in Campbell, California, ForeScout offers its solutions through its global network of authorized partners. **Learn more at [www.forescout.com](http://www.forescout.com).**



## Worldwide Offices

### Headquarters:

900 East Hamilton Ave.  
Campbell, CA 95008

### EMEA:

London +44-1256-843633

### APAC:

Hong Kong +852-2411-4388

### Toll free (US):

(866) 377-8771

### Israel:

Tel Aviv +972-3-6449987

### International:

+1 (408) 213-3191

[www.forescout.com](http://www.forescout.com)