June 15, 2011

ForeScout Technologies Is A Leader Among Network Access Control Vendors

Excerpted From The Forrester Wave™: Network Access Control, Q2 2011

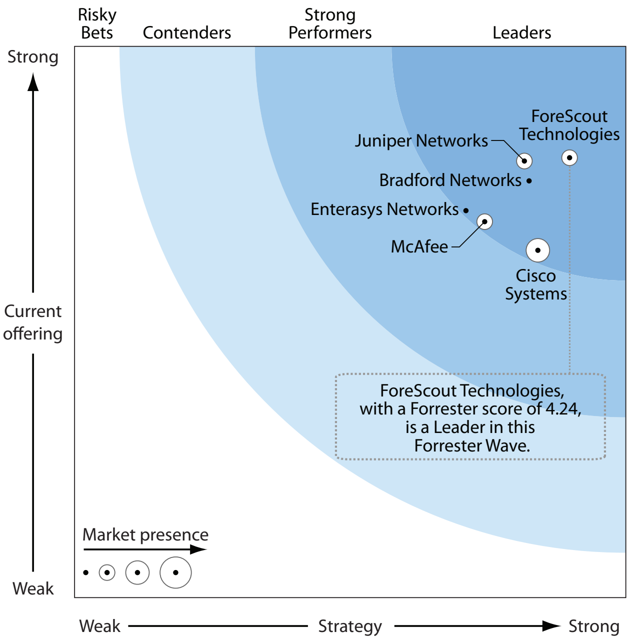
by John Kindervag

with Stephanie Balaouras, Robert Whiteley, and Lindsey Kempton

FORESCOUT TECHNOLOGIES IS A LEADER AMONG NETWORK ACCESS CONTROL VENDORS

ForeScout's NAC solution is entirely integrated into a single appliance that is highly network and security infrastructure interoperable. ForeScout offers five different sized NAC appliances to meet different capacity needs. For scalability, the solution includes an enterprise manager appliance that provides unified management and control of multiple NAC appliances. ForeScout's NAC operates in clientless mode for both corporate-managed and nonmanaged devices to provide real-time visibility, device/user classification, and policy definition. ForeScout also offers an optional lightweight persistent or nonpersistent endpoint client. The product offers extensive pre- and post-admission security posture checking and behavior monitoring with broad enforcement options. ForeScout's solution is available as a physical or virtual appliance. ForeScout's road map includes heavy focus on mobile device control, IT consumerization, and data center virtualization.

Forrester Wave™: Network Access Control, Q2 2011



The Forrester Wave™
Smart data for smart decisions

Go online to download the Forrester Wave tool for more detailed product evaluations, feature comparisons, and customizable rankings.

Source: Forrester Research, Inc.

See below for more information on ForeScout Technologies' current offering, strategy, and market presence.

Headquarters
Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA, 02140 USA
Tel: +1 617.613.6000 • Fax: +1 617.613.5000 • www.forrester.com

ForeScout Technologies Evaluation Overview

CURRENT OFFERING

Overall architecture	ForeScout NAC consists of a single appliance. The appliance comes in five different sizes depending on the scale of the deployment. There is an enterprise manager that is used for unified management and control. ForeScout's proposition is to offer a clientless solution; however, there is a lightweight client available if customers need it. ForeScout NAC is deployed out-of-band. The appliance attaches itself to the network infrastructure such as router and/or switches. It uses traditional mechanisms like SNMP traps, syslogs, etc., to monitor the activity. ForeScout NAC includes a built-in IPS product. The integration is typically useful for customers, as it can provide comprehensive post-admission assessments. ForeScout's NAC solution also integrates with remote access, patch management, security, management, and help desk systems.
Access control architecture	ForeScout NAC has a full range of access control options such as pre-admission, post-admission, quarantine mechanism, and remediation. As ForeScout is out-of-band, it integrates with network infrastructure via SNMP, 802.1X, VPN, virtual firewall, ACLs, etc. Virtual firewall is used when switches don't support SNMP protocol. The pre-admission and post-admission processes can be handled without an agent, but if a customer needs an agent, persistent and dissolvable agents are provided. ForeScout NAC supports a number of OSes such as Windows, Mac OS, and Linux. Among mobile OSes, it supports, Windows Mobile, iOS, Symbian, Android, etc. The post-admission is particularly useful when used in conjunction with IPS. It has the ability to perform an assisted (manual) or automated remediation.
Enforcement architecture	The following enforcement options are supported: 802.1X, MAC-based, VPN, ACL, virtual firewall, Wi-Fi, and MAC blacklisting. Depending on the method, enforcement occurs at the edge (ACL, VLAN assignment, port block), Layer 3 (ACL), or at enforcement points within the network (virtual firewall). Virtual firewall can be split between multiple appliances for scalability. The multiple enforcement and control options that are available allow customers to deploy ForeScout's product using a phased approach, which reduces disruption and improved the success rate of NAC implementations. The phases are: 1) evaluate; 2) educate and remediate; and 3) enforce. Also, since ForeScout can work with or without 802.1X, the ForeScout solution offers customers a way to migrate over time to a complete 802.1X solution if that is the desired objective.
IF-MAP	This is planned as part of its 2011 road map.

ForeScout Technologies Evaluation Overview

Device fingerprinting	ForeScout CounterACT will profile all endpoints, regardless of the OS. The endpoint profiling is done using various methods like passive and active NMAP fingerprinting, banners, RPC, SMB, MS SAMB, and others. They provide information about applications, registry, file system, printers, external devices, serial ports, and more. There's a dissolvable client to complement profiling for hosts that are not reachable and/or manageable such as hosts protected by firewall and guest hosts that are not part of the corporate domain. Based on the information gathered, a profile is built for each host connected to the network, and automatic classification and compliance policies are applied to desired hosts. The classification policy creates groups for each OS and separate devices per their network function. Profile information that NAC gathers can be used for inventory tracking and monitoring a wide range of IT entities like devices, users, applications, services, process, OS, and ports.
Policy architecture	ForeScout has a rich client-side and back-end integration. The policy creation is wizard-driven from CounterACT appliance console. It also integrates with third-party tools like MS NAP, McAfee EPO, eEye Retina, BigFix, ArcSight, and Lumension for policy enforcement and patch management. ForeScout NAC also supports back-end directories such as AD, Sun, Oracle, Lotus Notes, and in addition, any LDAP, RADIUS, and TACACS-based directories.
Scalability	ForeScout's NAC architecture can handle at least 500,000 nodes today. It is not a problem to deploy the product in a mixed environment, e.g., mix of wired, wireless, 802.1X, and non-802.1X. Many of its customers do this. No new licenses or appliances are needed. ForeScout offers a high-availability option (two appliances tied logically together).
Manageability	CounterACT NAC console is feature-rich and intuitive. There are configuration setup wizards and templates. The interface is intuitive and has ease-of-use features built-in. Console shows the inventory of the endpoints detected. They are classified and tracked within a proper category. There is an executive dashboard as well that provides an overview of the network. ForeScout NAC assigns compliance states and vulnerability associated with certain application or user device. There are canned reports for corporate and regulatory compliance. These reports can be customized and exported to many formats.
Managed and unmanaged systems	ForeScout NAC can handle managed as well as unmanaged user devices. Guest access is part of the overall NAC solution. There are various levels of guest access depending upon the role and type of connection. The CounterACT console integrates with help desk system and can send messages about the events. ForeScout NAC can detect rogue devices such as access points by performing an active or a passive scan. It can identify what type of device it is by looking at the header. Mobile devices such as iPhone, iPad, and others are identified and can be controlled per policy (block or allow onto the network).

ForeScout Technologies Evaluation Overview

Compliance	ForeScout provides templates and/or guidelines to enforce PCI, as well as other standards like HIPAA, SOX, GLBA, etc.
Virtualized systems	ForeScout NAC is available in either physical or virtual form factor. Today, it can scan the virtual machines. It identifies VMs in a similar manner to a physical device.
Scenarios	ForeScout performs adequately across the board among all the scenarios. In particular, it is strong in scenarios 4, 6, and 7.
STRATEGY	
Product strategy and vision	ForeScout has a defined road map ahead that includes investment in the data center virtualization and IT consumerization issues. ForeScout is working toward providing finer controls on the mobile devices. ForeScout will continue to partner with third-party vendors where necessary.
Product support	ForeScout offers two support models: 8x5 and 24x7. Support is delivered from a US center and an EMEA support center. A customer can open a ticket either by sending an email or by calling a 1-800 number. Calls are routed to either support center depending on the time of day. Support includes advanced replacement of faulty hardware and software updates/new releases. Presales support is primarily done by sales engineers although complex designs and/or configurations are assisted by the post-sales organization. The post-sales support organization supports the presales organization for any questions or product issues. Post-sales support is done by professional services for product rollout and by customer support for ongoing support. Reference architectures, design services, implementation services, and training are available in addition to maintenance and support. Support is sold as a yearly contract; it is also available as three- and five-year contracts.
Corporate strategy	ForeScout's go-to-market strategy is to focus on organizations with more than 1,000 nodes. The strongest industries for ForeScout have been military, government, and financial services. It will continue to focus on these as well as education, energy, manufacturing, and others.
Financial resources to support strategy	ForeScout did not disclose this information. But Forrester estimates that it's profitable and has dedicated adequate resources toward NAC.
Cost	ForeScout has competitive price options in the NAC market.

ForeScout Technologies Evaluation Overview

MARKET PRESENCE

Installed base	ForeScout has a healthy client base with more than 800 clients worldwide. It has also acquired a good number of new clients, and more than 50% of these customers are on the maintenance agreements.
Revenue growth	ForeScout experienced 52% annual growth over the past year.
Employees	ForeScout has adequate workforce to support sales, R&D, and customer support.
Channel partners	ForeScout OEMs its product to one vendor, and it has a decent reseller ecosystem.

EXECUTIVE SUMMARY FROM THE FORRESTER WAVE™: NETWORK ACCESS CONTROL, Q2 2011

In Forrester's 72-criteria evaluation of network access control (NAC) vendors, we found few notable points of differentiation between vendor offerings. Thus we have a tight clustering of vendors — all with mature products. ForeScout Technologies, Juniper Networks, Bradford Networks, Cisco Systems, McAfee, and Enterasys all came out as Leaders. Longer-term, Forrester expects the market for standalone NAC solutions to disappear in favor of functionality embedded into diverse security products, such as antimalware, firewalls, host AV, intrusion prevention, and domain controllers. In the short term, if your security requirements necessitate the deployment of a standalone solution, you should consider the vendor's entire product portfolio and ease of deployment as top considerations. Ultimately, your NAC purchase must be done in conjunction with endpoint security or as an extension to existing network infrastructure.

Forrester Research, Inc. (Nasdaq: FORR) is an independent research company that provides pragmatic and forward-thinking advice to global leaders in business and technology. Forrester works with professionals in 19 key roles at major companies providing proprietary research, customer insight, consulting, events, and peer-to-peer executive programs. For more than 28 years, Forrester has been making IT, marketing, and technology industry leaders successful every day. For more information, visit www.forrester.com.