



**Media contact:**  
Deb Montner  
*Montner & Associates, Tech PR*  
203-226-9290  
[dmontner@montner.com](mailto:dmontner@montner.com)

## **Survey Indicates Network Access Control Perceived as Most Effective Security Technology to Defend Against Cyberthreats**

*2014 Cyberthreat report finds 77 percent of IT professionals choose NAC for mobile security*

**CAMPBELL, Calif. — Feb. 5, 2014—** The “2014 Cyberthreat Defense Report” found that respondents rated network access control (NAC) highest of all the security technologies in its potential to defend against today’s cyberthreats and that 77 percent of IT professionals are using or plan to use NAC for mobile security. The survey also showed the compelling need for continuous monitoring and mitigation; more than 60 percent of participants had been breached in 2013, with a quarter of all participants citing a lack of employer investment in adequate defenses as a factor.

The research, which is the first of its kind to offer a 360 degree view of organizations’ perceptions of security threats and their security investments, was completed by CyberEdge Group, LLC and sponsored by [ForeScout Technologies, Inc.](#), the leading provider of pervasive network security solutions for Global 2000 enterprises and government organizations, and eight other information security companies. Surveying more than 750 security decision makers and practitioners in organizations with 500-plus employees in North America and Europe, the report is designed to complement Verizon’s annual Data Breach Investigations Report.

### **Key Findings**

The Cyberthreat Defense Report offered unique insights into challenges faced by professionals in IT. Some of the key findings relevant to network security and next-generation NAC include:

- Participants were asked to rate—on a scale of 1 to 5, with 5 being highest—their perception on the effectiveness of various cyberthreat defense solutions. NAC received the highest marks at 3.71
- NAC is the most often used technology (53 percent of respondents) to detect host security misconfigurations
- NAC is most often used technology to detect vulnerabilities and security misconfigurations within transient laptops and mobile devices (51 percent)
- Adoption of BYOD policies is anticipated to move from 31 percent in 2014 to 77 percent in 2016
- Endpoints are cited as the weakest link in most organizations’ IT environment

more

Information security is becoming more challenging due to three disruptive changes that nearly all enterprises are experiencing: IT infrastructure complexity due to an exponential increase in network connections and use of mobile, virtualization and cloud technology; diminished capacity to manage endpoints caused by growing network-enabled and personal device use at the workplace; and difficulty to efficiently mitigate exposures within a growing attack landscape. To address these challenges, many organizations are supplementing their existing security investments with next-generation NAC to dynamically see and control user, device, application and access diversity. Organizations are also progressing their traditional layered defense model to one that leverages infrastructure interoperability in order to better support continuous monitoring and mitigation processes.

In the report, one quarter of organizations noted they are conducting full network scans weekly or daily, indicating a greater understanding of the tremendous value of continuous monitoring. However, 52 percent of responding organizations conduct full network vulnerability scans quarterly or annually. Alarming, one in five organizations admitted to rolling the dice by doing nothing to assess the state of their transient devices between regularly scheduled active scans. This provides a large window of opportunity for a successful cyberattack against the transient system.

“While many researchers focus on the threats and breaches that impact organizations’ protection efforts, until now, no one has polled security decision makers and practitioners to understand their perceptions of security threats, response plans, processes and investments,” said Steve Piper, CEO of CyberEdge Group, LLC. “It is obvious from our research that NAC is an important weapon within many organizations’ arsenals and for good reason. Many of our respondents saw it as a versatile tool that could support protection efforts ranging from BYOD policy enforcement to configuration management.”

“We are delighted to be a sponsor of this insightful Cyberthreat Defense Report from CyberEdge. The report not only conveys the techniques and technologies being applied to address cyberattack risks, but highlights growing awareness among security practitioners of the value that NAC offers,” said Scott Gordon, chief marketing officer at ForeScout. “We believe that NAC, with its ability to dynamically resolve security exposures, enhance control content and automate remediation capabilities, is the cornerstone technology to advance continuous monitoring and mitigation programs.”

Interestingly, the researchers concluded that most respondent organizations are combining multiple technologies together to establish a unified solution to meet an enterprise’s specific needs for defending

their endpoints. This bodes well for ForeScout's CounterACT platform, which helps organizations gain visibility and automated control for devices, users, systems and applications attempting to connect to or on an enterprise network. CounterACT identifies security control gaps, such as rogue devices, non-compliant systems or personal mobile device use, and it offers options to isolate threats and dynamically fix issues with little or no IT intervention. Furthermore, the firm's ControlFabric technology enables network and security products to dynamically share information and allow enterprises to more rapidly respond to a broad range of security issues. This architecture brings disparate solutions together to provide operational context and policy-based remediation.

### **Report Available Now**

The 2014 Cyberthreat Defense Report is available now from ForeScout at [http://www2.forescout.com/cyberedge\\_cyberthreat\\_2014](http://www2.forescout.com/cyberedge_cyberthreat_2014)

### **Relevant Links**

[2014 Cyberthreats Infographic](#)  
[ForeScout Blog](#)  
[ForeScout Twitter](#)  
[ForeScout Facebook](#)

*Tweet This: Next-Gen NAC Perceived as Best Option to Defend Against Today's Cyberthreats, Finds 2014 Cyberthreat Defense Report* <http://bit.ly/1iUZoXJ>

### **About CyberEdge Group**

CyberEdge Group is an award-winning research, marketing, and publishing firm serving the diverse needs of information security vendors and service providers. Headquartered in Annapolis, Maryland with consultants based across North America and Europe, CyberEdge boasts more than two dozen of the security industry's top vendors as clients. The company's annual Cyberthreat Defense Report provides information security decision makers and practitioners with practical, unbiased insight into how enterprises and government agencies in North America and Europe are defending their networks against today's complex cyberthreat landscape. For more information, visit [www.cyber-edge.com](http://www.cyber-edge.com).

### **About ForeScout Technologies, Inc.**

ForeScout delivers pervasive network security by allowing organizations to continuously monitor and mitigate security exposures and cyberattacks. The company's CounterACT platform dynamically identifies and assesses all network users, endpoints and applications to provide complete visibility,

intelligence and policy-based mitigation of security issues. ForeScout's open ControlFabric technology 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, flexible and scalable, they have been chosen by more than 1,500 enterprises and government agencies. Headquartered in Campbell, California, ForeScout offers its solutions through its network of authorized partners worldwide. Learn more at: [www.forescout.com](http://www.forescout.com).

ForeScout Technologies, Inc. is a privately held Delaware corporation. ForeScout, the ForeScout logo and CounterACT™ are trademarks of ForeScout. Other names mentioned may be trademarks of their respective owners.

###