

Editorial Contact:

Peggy Tierney Galvin
Nadel Phelan, Inc.
(831) 440-2405
peggy@nadelphelan.com

Enterprise CISOs Demand More Integration and Automation From Their Existing IT Security Tools

SC Magazine Survey Findings Show Majority Still Not Deploying Continuous Monitoring and a Proliferation of Siloed Security Solutions, Despite Demands from Users

CAMPBELL, Calif., Sept. 29, 2015 – ForeScout Technologies, Inc. today announced that a survey it commissioned from SC Magazine has found that enterprise CISOs are looking for more integration and automation among their existing IT security tools, and that most are only periodically monitoring and mitigating events in their network environments. For more information, visit: <http://www.forescout.com/it-security-managers-speak-out/>.

The survey collected responses from 350 corporate executives and consultants with information security responsibility across multiple industry verticals, including technology, finance, government, healthcare and manufacturing. The findings explored respondents' current use of security tools and goals for future security portfolio capabilities around automation, communication and remediation.

Key details of the survey include:

- **Stand-alone security solutions are proliferating:** Some 52 percent of large enterprises, defined as organizations with more than \$1 billion per year annual revenue, said they operate more than 13 different security tools.
- **Yet aren't talking to one another:** Despite the large number of security tools in use, the survey identified that it is rare for these tools to directly collaborate with each other. 69 percent of the participants in the survey said that aside from their security information and event management (SIEM) systems, they had only a couple of tools that could directly share security-related context or control information.
- **Large enterprises desperately want collaborative security solutions:** 95 percent of large enterprise respondents said it would be “helpful or very helpful” if their IT security and management systems shared information about devices, applications, users and vulnerabilities on the network. In addition, 93 percent of

large enterprise respondents said it would be “helpful or very helpful” if a majority of their risk analysis systems were linked to automated security controls such as firewalls, network access control, or patch management systems.

- **Collaborative security seen as preventative measure:** The vast majority of respondents (78 percent) said that linking security systems to automated security controls will help prevent future compromise.
- **Majority of respondents only perform periodic security health checks:** Nearly 60 percent of respondents perform periodic, rather than continuous, monitoring and mitigation of their network environments to ensure that all software is up-to-date and patched, leaving gaps in visibility that can be exploited by hackers or malware.

Pedro Abreu, chief strategy officer, ForeScout Technologies, said: “The explosion of the number of endpoint devices connecting to the network is creating new entry points for cyber criminals into an organization. Yet, survey results found that nearly 60 percent of respondents only perform monitoring and mitigation on a periodic basis of endpoints, instead of continuously. Customers are looking for integrated solutions that offers the ability to continuously see all devices connected to their network, control access and ensure endpoint compliance while sharing valuable information with other devices to increase overall security posture. Forescout delivers this integrated solution to ensure optimum security and preserving the flow of business.”

About ForeScout Technologies, Inc.

ForeScout enables organizations to continuously monitor and mitigate security exposures and cyberattacks. The company’s CounterACT™ appliance 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 more than 62 countries. Headquartered in Campbell, California, ForeScout offers its solutions through its global network of authorized partners. Learn more at www.forescout.com.

©2015 ForeScout Technologies, Inc. is a privately held Delaware corporation. ForeScout, the ForeScout logo, ControlFabric, ActiveResponse and CounterACT are trademarks or registered trademarks of ForeScout. Other names mentioned may be trademarks of their respective owners.

Relevant Links

- [**ForeScout CounterACT**](#)
- [**ForeScout ControlFabric**](#)
- [**ForeScout Blog**](#)
- [**ForeScout Facebook**](#)

ForeScout Twitter

###