

Securing Direct-To-Internet Branch Offices: Cloud-Based Security Offers Flexibility And Control

Introduction

As employees use the Internet for more and more business functions, the traditional hub-and-spoke wide area network (WAN) model is no longer critical to making businesses run. Furthermore, IT decision-makers realize that significant cuts can be made in massive telecom budgets by simply allowing their branch offices and remote employees to go direct-to-Internet. Centralized solutions are costly, complex, and carry with them performance challenges. But the alternative — decentralized solutions — offers less control and is difficult to manage via a common policy. IT decision-makers are looking for network security solutions that enable the flexibility, cost, and performance advantages of direct-to-Internet while maintaining or even extending the level of protection of the existing WAN.

In December 2014, OpenDNS commissioned Forrester Consulting to evaluate the specific challenges and adoption trends related to network security for branch and remote offices based on Forrester's own market data and a custom study of the same audience. To do so, Forrester leveraged data from Forrester surveys and supplemented that data with a custom survey of 52 IT leaders at enterprises in North America.

Branch Offices Are Looking For Independence From HQ Infrastructure

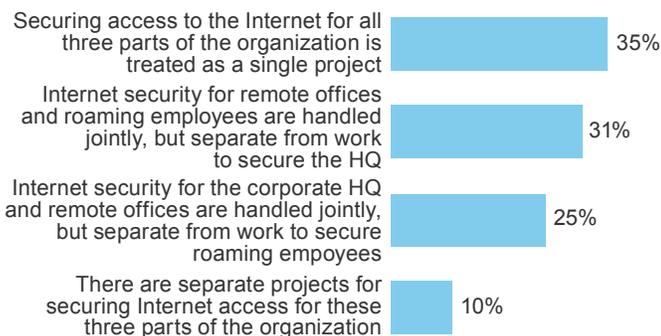
The traditional hub-and-spoke network infrastructure is dying.¹ IT professionals are feeling pressure to scrap their more rigid centralized architectures in favor of point solutions and as-a-service offerings in order to overcome the inflated costs of a centralized infrastructure and meet business demands for high performance, agility, and worker empowerment. Accordingly, network security is moving out to the branch offices to protect their direct-to-Internet traffic.

Our study found that only 35% of companies are securing access to the Internet for their main corporate headquarters (HQ), branch offices, and roaming employees all as a single project (see Figure 1). The rest are dividing security for these groups into separate initiatives.

Similarly, only 31% of branch offices are now accessing the Internet via the data center using a WAN connection. Another 42% go exclusively direct-to-Internet, and 27% have some combination of direct-to-Internet and WAN connections (see Figure 2).

FIGURE 1
Most Companies Handle Security Separately For Remote Parts Of The Organization

“Which of the following best describes how your company handles initiatives to secure Internet access for your main corporate headquarters, branch offices, and roaming employees?”



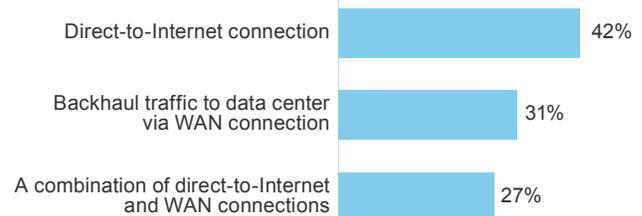
Base: 52 North American IT security decision-makers at firms with 500-plus employees

Note: Percentages may not total 100 because of rounding.

Source: A commissioned study conducted by Forrester Consulting on behalf of OpenDNS, January 2015

FIGURE 2
Organizations Are Moving Away From The WAN

“What percentage of your organization’s branch offices access the Internet via the following means?”



Base: 52 North American IT security decision-makers at firms with 500-plus employees

Source: A commissioned study conducted by Forrester Consulting on behalf of OpenDNS, January 2015

Companies Are Looking For The Right Solution

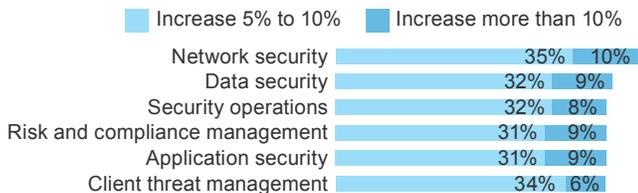
With 2014 in the books as another record-breaking year of data breaches and an ever-increasing array of mobile and personal devices being used in the workplace, businesses are investing heavily to ensure that their sensitive data remains protected.² Forrester’s Business Technographics® Global Security Survey, 2014, shows that network security will further solidify its historic position as the top tech spending area for security in 2015, with 45% of North American firms reporting at least a 5% increase over 2014 (see Figure 3). While branch offices benefit from the agility and performance of local solutions, security pros are now faced with ensuring that these solutions can be effectively managed and don’t leave the business vulnerable.

However, cost and performance concerns dissuade IT leaders from simply beefing up (or reverting to) their controlled hub-and-spoke models for their branch offices.

Our study found that the top challenge that organizations face when relying on a security model that requires network traffic to return to a centralized location is operational costs of maintaining the spoke-to-hub traffic links (48%).

FIGURE 3
Network Security Is A Top Investment

“How do you expect your firm’s security spending in the following technology areas will change from 2014 to 2015?”

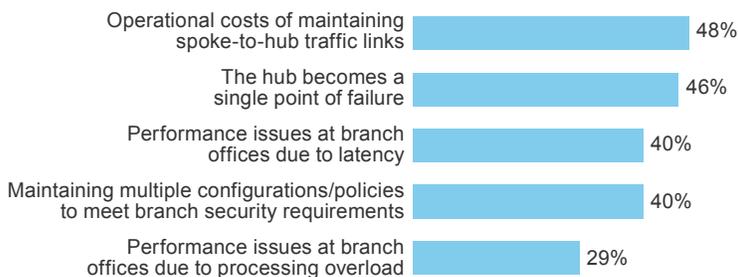


Base: 646 North American IT security decision-makers at firms with 500-plus employees

Source: Business Technographics Global Security Survey, 2014, Forrester Research, Inc.

FIGURE 4
Security Models That Rely On Centralized Inspection Have Huge Shortcomings

“What are the challenges you face when relying on a security model that requires network traffic to return to a centralized location in order to be secured?”



Base: 52 North American IT security decision-makers at firms with 500-plus employees

Note: only top five answers shown

Source: A commissioned study conducted by Forrester Consulting on behalf of OpenDNS, January 2015

Other top challenges include risks associated with the hub becoming a single point of failure (46%), complaints from end users about latency (40%), and complex configurations to accommodate individual security needs at branch offices (40%) (see Figure 4).

As-A-Service Offerings Are Viable Options For Decentralized Networks

Cloud-based network security offerings are now right in the security sweet spot, allowing for the flexibility of decentralization while also providing centralized visibility and control. Forrester’s Business Technographics Global Security Survey, 2014, shows that businesses have adopted (or plan to implement) a number of as-a-service security offerings, with priorities including web filtering (72%), threat intelligence (68%), and comprehensive network filtering (66%).

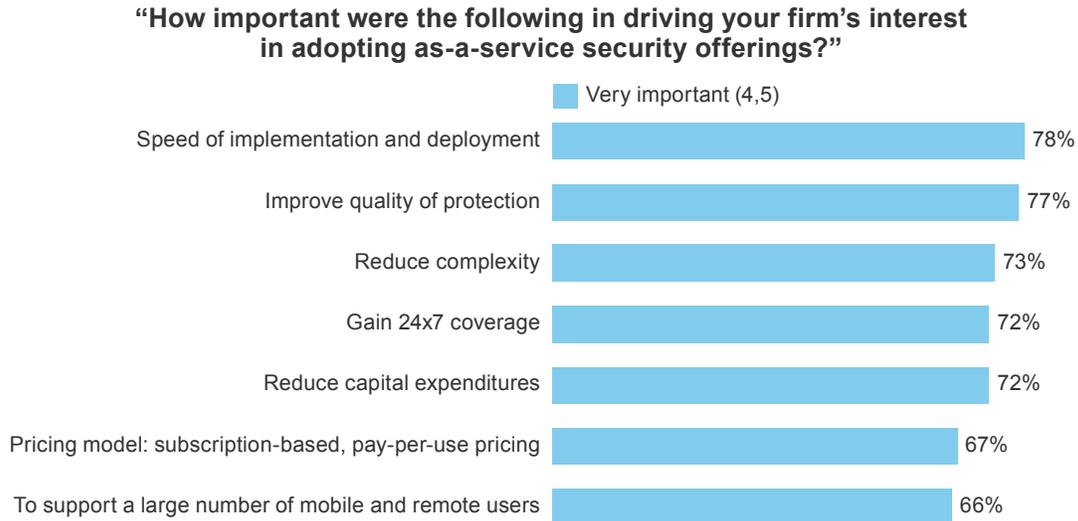
Forrester’s data also shows that there are a number of reasons that IT leaders responsible for branch offices are interested in as-a-service security offerings.

Decision-makers told us that cloud security offers faster implementation and deployment (78%).

Cloud security also provides improved quality of protection (77%), reduced complexity (73%), 24x7 coverage (72%), and reduced capital expenditures (72%), among other benefits (see Figure 5).

Cloud management and services have seen a fair amount of traction, but there is still quite a lot of room for adoption growth. Our study found that 62% of firms are using security appliances without any centralized cloud management in at least some of their office locations; 58% are using some security appliances with centralized cloud management; and only 33% are using security services fully delivered in the cloud (see Figure 6).

FIGURE 5
A Number Of Benefits Drive Cloud Adoption



Base: 116 North American IT security decision-makers at organizations with multiple branches

Source: Business Technographics Global Security Survey, 2014, Forrester Research, Inc.

FIGURE 6
Security Pros Adopt Cloud Management As Well As Full-Scale Cloud Security



Base: 52 North American IT security decision-makers at firms with 500-plus employees

Note: multiple responses accepted

Source: A commissioned study conducted by Forrester Consulting on behalf of OpenDNS, January 2015

Conclusion

Companies must learn to move quickly as they strive to compete in a global and ever-changing marketplace. Deploying branch offices to bring workers closer to their customers or integrate a remote workforce into the enterprise gives companies the power and flexibility to execute their strategic plans quickly and efficiently. Our study of IT leaders tasked with responding to this business challenge found that:

- › **Many businesses are implementing direct-to-Internet connections.** The majority of our respondents are tossing out legacy hub-and-stoke architectures in favor of decentralized models in at least some of their branch offices.
- › **As businesses go direct-to-Internet, they realize the need to bulk up security for branch offices.** Because corporate or HQ locations tend to be the focus of much of an organization's investment in leading protective security technology, remote offices that go direct-to-Internet have become a favorite target for hackers. Security pros who must protect branch offices against increasingly sophisticated and relentless threats are looking for simple yet powerful technologies to free them from hardware appliances, provide unified visibility, and take advantage of collective threat intelligence.
- › **In addition to appliances, many decision-makers are considering as-a-service offerings.** Organizations at the leading edge have found that cloud-based security solutions are now ready for prime time and are a perfect fit for the branch office challenge.

Methodology

This Technology Adoption Profile was commissioned by OpenDNS. To create this profile, Forrester leveraged its Business Technographics Security Survey, 2014. Forrester Consulting supplemented this data with custom survey questions asked of North American IT decision-makers responsible for network security in firms with 500-plus employees. The auxiliary custom survey began in December 2014 and was completed in January 2015. For more information on Forrester's data panel and Tech Industry Consulting services, visit www.forrester.com.

Endnotes

¹ Source: "Three Forcing Functions That Will Extend Your Data Center's Network Services Beyond Its Walls," Forrester Research, Inc., June 9, 2014.

² Source: "Understand The State Of Network Security: 2014 To 2015," Forrester Research, Inc., December 22, 2014.

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

© 2015, Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, RoleView, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. For additional information, go to www.forrester.com. [1-S9JSOV].