VeraQuest

End-to-End Network Segmentation Research

Independent Market Research
Commissioned by

AVAYA

August 2016

Background and Introduction

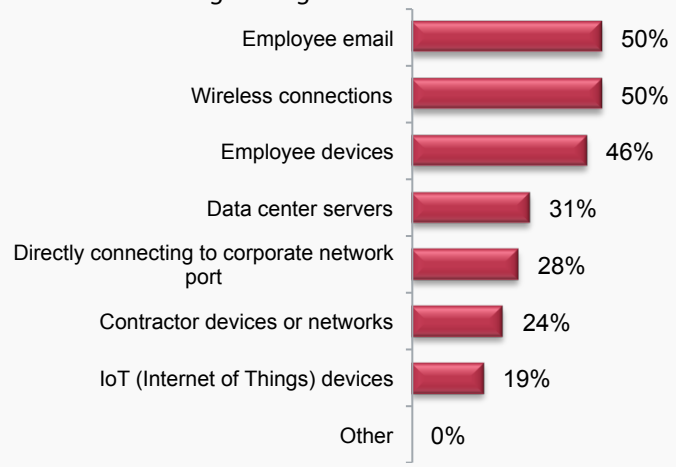
In today's digital world, almost any corporation, large or small, can be brought to its knees in an instant by a network breach. The focus of this research is to: 1) quantify the perceived importance of end-to-end segmentation in protecting medium-to-large corporations, 2) assess how widespread end-to-end segmentation actually is, and 3) identify barriers to the implementation of end-to-end segmentation.

This study was conducted online by VeraQuest, an independent survey research firm, between August 15 and August 18, 2016. The sample consists of 400 IT professionals in medium-to-large organizations who are actively involved in dealing with networking issues for their company, have responsibility for the corporate network, or have security or risk management responsibilities for the corporate network. The margin of error associated with this study is +/- 4.9 percentage points.

Executive Summary

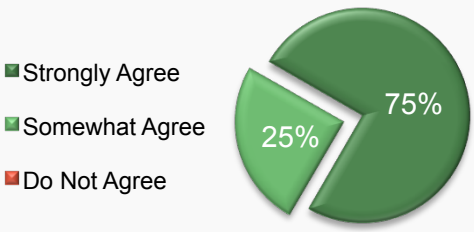
Although virtually all respondents in our survey agree that end-to-end segmentation is an essential security measure (75% of whom strongly agree), only about one-in-four (23%) say their organization actually implements end-to-end segmentation. Since the vast majority of breaches are thought to occur toward the network periphery, the relative absence of end-to-end network segmentation can be somewhat puzzling until we examine the underlying reasons. *Complexity*, reported by 35% of respondents, is a key stumbling block, while 28% say a *lack of resources* is an impediment. Another 22% of respondents are *not aware* that end-to-end segmentation is even possible. Only a fifth of IT professionals (20%) do not perceive a need for end-to-end segmentation within their organizations. Among the minority of IT professionals who *do* implement some form of end-to-end coverage, *VLAN Chaining* is by far the most common technique.

Breaches occurring through…



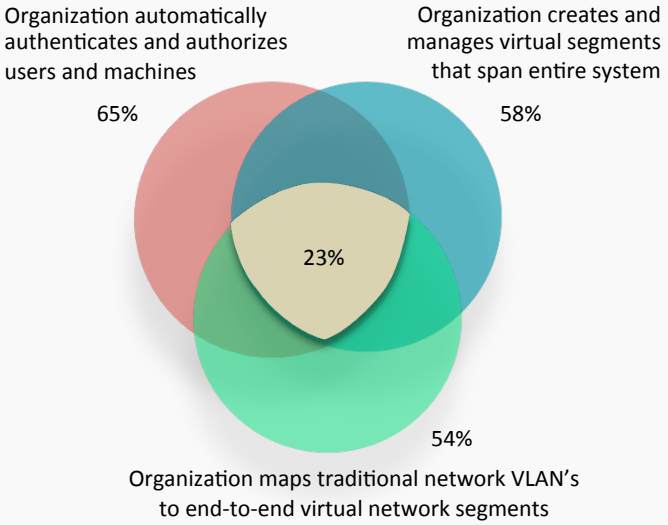
Greatest Entry Point Threats to an Organization's Network

While all the entry points are of some concern to IT professionals, three areas stand out more than the rest. Half (or nearly half) of respondents point to employee email (50%), wireless connections (50%), and employee devices (46%).



Belief that End-to-End Network Segmentation is Essential

Virtually every respondent in our survey agrees that employing end-to-end segmentation is an essential security measure. In fact, three-quarters strongly agree.



End-to-End Network Segmentation Capabilities Currently in Place

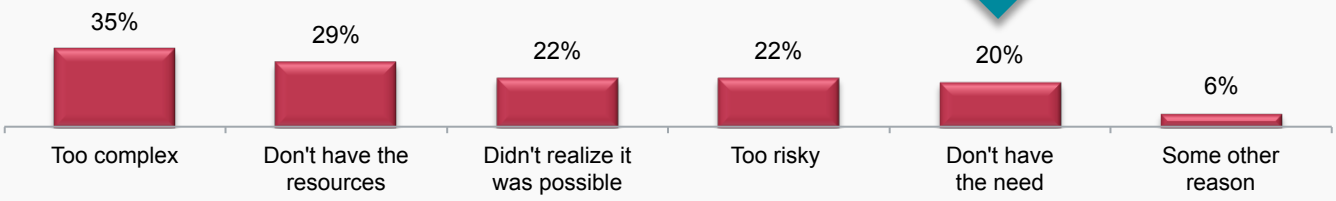
While most IT professionals report implementing at least one of the three components necessary for complete end-to-end segmentation (automatic authentication, managing segments that span the entire system, and end-to-end VLAN mapping), only about a fourth implement all three components.

23% of medium-to-large companies currently employ complete end-to-end segmentation

Reasons for Not Deploying End-to-End Network Segmentation

Over a third of respondents (35%) believe that implementing an end-to-end segmentation strategy is too complex, while 29% say they don't have the resources. A sizeable number (22%) don't realize it is possible, while another 22% say it's too risky.

Only one-in-five IT professionals say they don't have a need for end-to-end segmentation



Primary Technique Used to Implement End-to-End Network Segmentation

Among those IT professionals who report implementing a complete end-to-end segmentation system, the primary technique utilized for implementation is VLAN Chaining (42%). Far fewer (18%) use TRILL, IPsec tunneling (15%), SPB (13%) or MPLS (12%) .

42% of IT professionals that employ end-to-end segmentation use VLAN Chaining