Solution Showcase

# Survey: NAC Business Case Must Be Adjusted to Support IT Shifts

**Date:** April 2017 **Author:** Jon Oltsik, Senior Principal Analyst

**Abstract:** Business initiatives are driving massive changes in IT as CIOs embrace cloud computing, mobile applications, and the Internet of Things (IoT) to help their organizations move toward digital transformation. However, new dynamic IT environments are a mismatch for cumbersome network security controls that weren't designed for automation, orchestration, massive mobility, or scale-up/scale-down cloud computing models. What's needed? Many enterprise organizations are exploring new approaches to access control. The ESG research presented in this document explores the symbiotic relationship between emerging business initiatives, IT trends, and the growing need and fit for SDPs.

## Overview

Large organizations are adopting several IT trends that will have a profound impact on their network security strategies and tactics (see Figure 1).[1] For example:

- Forty-two percent are pursuing business and IT initiatives related to data analytics. All types of data analytics mean moving large volumes of sensitive data over networks, driving the need for security controls that protect data confidentiality and integrity. Companies will also have to bolster authentication and access controls to enforce policies of least privileged access to valuable data assets.

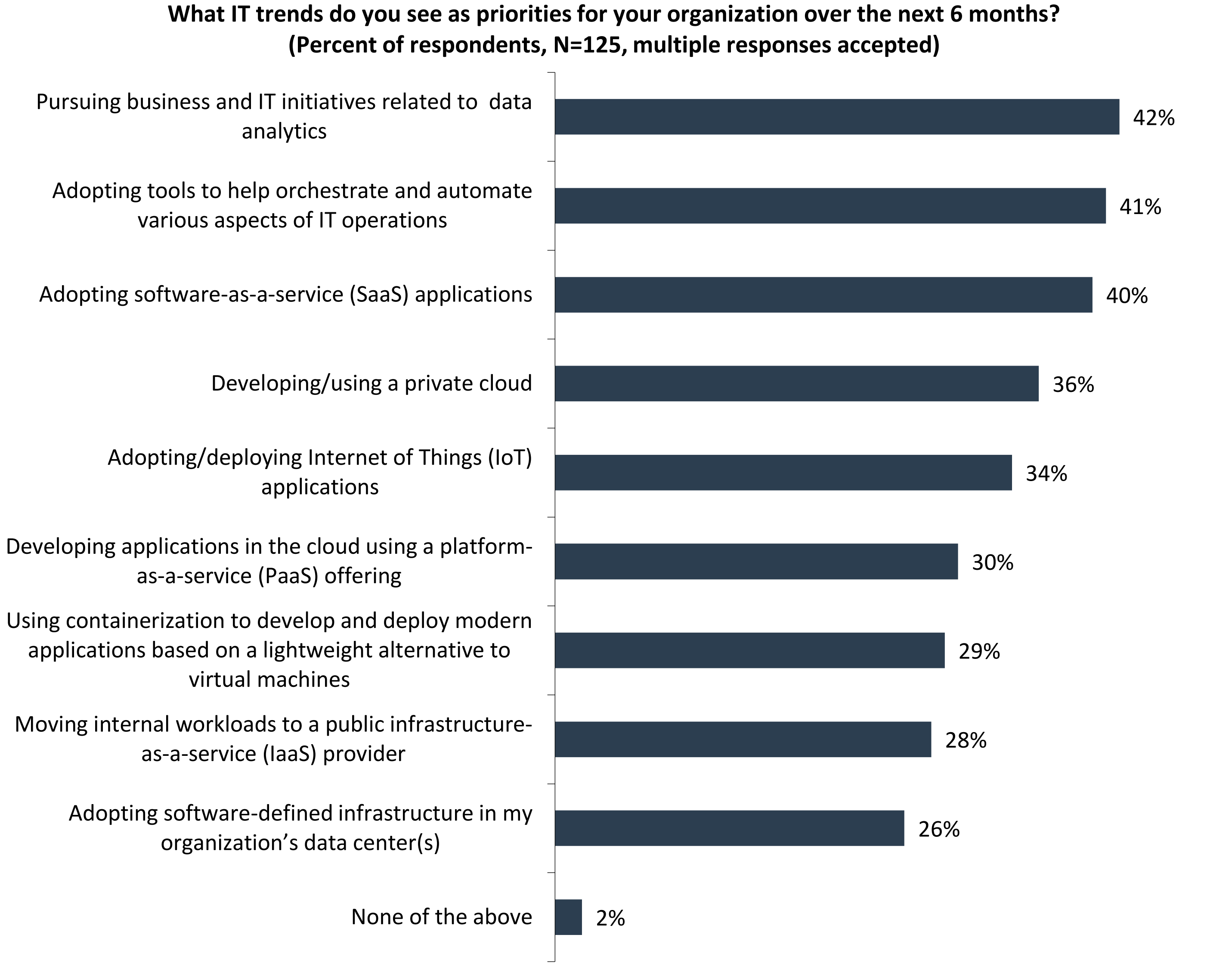
- Forty-one percent are adopting tools to help orchestrate and automate various aspects of IT operations. To accommodate this change, network security tools must be software-based and interoperable with other software controls through APIs.

- Forty percent are adopting SaaS applications. This means they will need the right network access controls to enforce fine-grained access policies to SaaS applications and continuously monitor who does what on these applications.

It is also worth noting that 34% of organizations are adopting/deploying IoT applications. These firms will need to have the right network access polices for these devices, segment IoT communications from other production network traffic, and keep track of device communications at all times. With a forecast of 20 billion IoT devices by 2020, it could be difficult to secure IoT traffic itself, let alone in addition to the increasing day-to-day network traffic.

[1] All data in this paper is based on research ESG performed on behalf of Vidder.

**Figure 1. IT Trend Priorities**



*Source: Enterprise Strategy Group, 2017*

## IT Trends Call for New Security Solutions

The IT trends described previously will demand the right security policies and controls to protect critical business assets. Given this, what are the most important security objectives? The cybersecurity professionals surveyed for this project point to (see Figure 2):

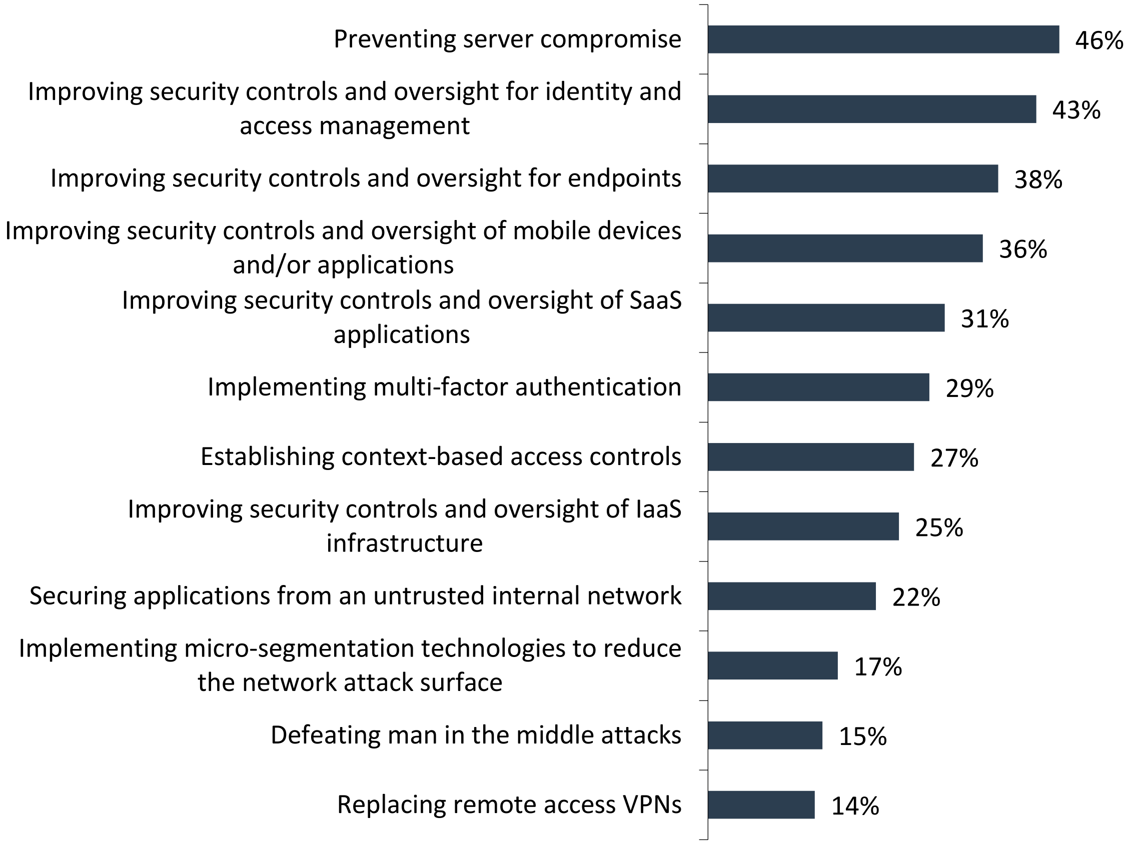
- **Preventing server compromise.** Nearly half (46%) say that this is among their top security objectives. From a network security perspective, this means limiting who gets access to mission-critical servers, segmenting and encrypting sensitive server traffic, and monitoring network traffic as it ingresses and egresses network segments housing valuable servers.

- **Improving IAM security controls and oversight.** Forty-three percent of respondents call for improvement of security controls and oversight related to identity and access management (IAM). Aside from monitoring network access and usage, this also includes attribute-based network access controls, multifactor authentication (MFA), and the creation of end-to-end tunnels from end-user devices to IT services in data centers and public clouds.

- **Improving security controls for endpoints and mobile devices.** Thirty-eight percent of respondents seek to improve security controls and oversight for endpoints while 36% have the same objectives for mobile devices. These objectives relate to things like device security, configuration management, and data integrity on the devices themselves.

**Figure 2. Most Important Security Objectives**

**Which of the following are amongst the most important security objectives at your organization? (Percent of respondents, N=125, five responses accepted)**



*Source: Enterprise Strategy Group, 2017*

## Toward Software-defined Perimeters

The ESG data calls out numerous network security changes needed to align with burgeoning business/IT trends. Furthermore, these changes cascade throughout the network and must align with the automation and orchestration initiatives pervading IT.

CISOs who try to modify their existing network security controls will soon find themselves overwhelmed by bottlenecks. Why? Many hardware-based network access controls are simply too brittle and inflexible. Additionally, network security controls can take days or weeks to test, configure, and provision—a total mismatch with new applications based upon agile development, DevOps, and public cloud computing infrastructure.

So, what's needed? Many large organizations are now considering new trusted access control solutions, leveraging advanced, software-based trust enforcement technologies, including software-defined perimeters. Just what is an SDP? It is a new security model first introduced by the Defense Information Systems Agency (DISA) under the global information grid (GIG) black core initiative of 2007. According to Wikipedia:

> *Connectivity in a Software Defined Perimeter is based on a need-to-know model, in which device posture and identity are verified before access to application infrastructure is granted. Application infrastructure is effectively "black" (a DoD term meaning the infrastructure cannot be detected), without visible DNS information or IP addresses. The inventors of these systems claim that a Software Defined Perimeter mitigates the most common network-based attacks, including: server scanning, denial of service, SQL injection, operating system and application vulnerability exploits, man-in-the-middle, cross-site scripting (XSS), cross-site request forgery (CSRF), pass-the-hash, pass-the-ticket, and other attacks by unauthorized users.*[2]

What type of functionality should be part of an SDP? When ESG asked survey respondents about the type of security control that would be *most* helpful to their organization, several different responses garnered significant traction (see Figure 3), particularly:

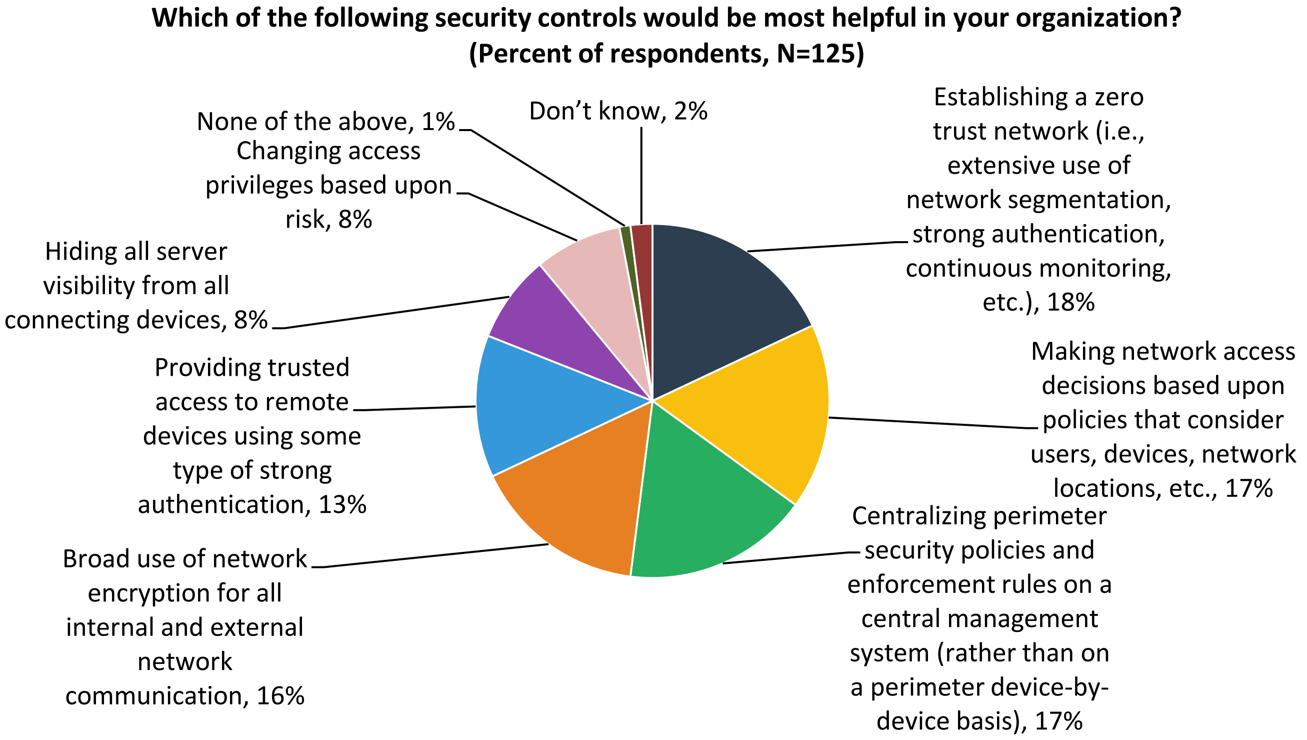
- **Establishment of a zero-trust network.** In a zero-trust network, all devices are deemed as untrusted and restricted from accessing the network without providing the right credentials and profile. In other words, all network nodes are constantly inspected and granted or denied network access based upon their identities, configurations, and other risk factors like software vulnerabilities or ongoing malicious threats targeting particular devices or organizations. SDPs can enforce zero trust, making them a good fit for changing business and IT needs.

- **Granular network access decisions.** As part of a zero-trust network, network access can be based upon a myriad of factors including user attributes, device type, network location, time of day, etc. SDPs can support attribute-based access controls to help minimize the network attack surface while enabling legitimate traffic to flow.

- **Centralized management of distributed controls.** CISOs understand that it is impossible to support and secure the business if network policy enforcement must be configured on a tool-by-tool and device-by-device basis. Alternatively, efficient and effective network security depends upon central command-and-control for things like policy management, configuration management, etc. Central management must also be supported with distributed controls that can interpret, enforce, and monitor policies. Since SDPs are built around software and APIs, they can facilitate this type of architecture.

[2] Source: Wikipedia, *Software Defined Perimeter*.

**Figure 3. Most Helpful Security Controls**



*Source: Enterprise Strategy Group, 2017*

## The Bigger Truth

IT is in a state of rapid change, driven by business initiatives like digital transformation and IT trends like cloud computing, mobility, and IoT. These changes also come with new network security requirements to scale and manage thousands of devices that need access to networks or cloud-based workloads.

Unfortunately, traditional network access controls simply weren’t designed for this type of dynamic environment. Therefore, CISOs who try to force-fit their legacy network security controls will fall further behind while creating massive operational overhead, security complexity, and increased risk.

The ESG research points to the need for a more flexible, scalable, and comprehensive network security model. This is what software-defined perimeters were designed for. Accordingly, CISOs should get acquainted with SDPs, experiment with technologies, and establish projects for proof-of-concept and production SDPs in the near future.

**Enterprise Strategy Group** is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.