JUNIPER NETWORKS | Engineering Simplicity

White Paper

GOVERNMENT AGENCIES WIN WITH MULTIVENDOR NETWORKS

Six facts that shatter common misconceptions and myths about perceived advantages of single vendor networks.

TABLE OF CONTENTS

Introduction

The benefits of multivendor networks are well known and many. To start, multivendor networks allow network operators to select from a broader set of offerings, realize lower costs, and deploy best-in-class solutions.

Yet many government agencies at the federal, state, and local levels—themselves operators of large-scale networks—prefer single vendor solutions (networks built on solutions from one manufacturer). They imagine that maintaining a single vendor network, most likely of solutions from a legacy manufacturer, offers cost, performance, and interoperability advantages.

Those perceived advantages, in reality, are misconceptions. This paper identifies and dispels six common misconceptions about maintaining or building a single vendor network, and it explains how multivendor networks provide agencies with advantages over single vendor networks in terms of security, cost, and performance.

Misconceptions and Facts About Single Vendor Networks vs. Multivendor Networks

Misconception 1: Single vendor networks are more secure than multivendor networks.

Fact: Networks with solutions from multiple manufacturers are more secure than networks with solutions from a single manufacturer. Single vendor networks are less secure because they can be subject to a single point of failure. If a network consists of solutions from one manufacturer and that manufacturer's products have a core vulnerability, an exploitation could lead to the shutdown of the entire network. When the network has solutions from multiple manufacturers, however, a vulnerability affecting one manufacturer does not necessarily harm other network segments.

> *"With a multi-vendor network, compromised network devices are compartmentalized and are far less challenging to remediate."*
>
> Andrew Froehlich. "Networking: Best-of-Breed Vs. Single Vendor." Network Computing (March 1, 2016).

There are two reliable options for deploying a multivendor network. One is to have a primary network with solutions from Vendor A and a backup network with solutions from Vendor B. If one vendor's solutions have a fatal flaw, then the other network will not be affected. Another choice is to have half of a local network consist of devices from Vendor A and the other half consist of devices from Vendor B. Again, a flaw impacting one vendor will not affect the other.

Misconception 2: Single vendor networks have a lower total cost of ownership than multivendor networks.

Fact: Agencies that favor multivendor networks can achieve a lower total cost of ownership than agencies that prefer single vendor networks. Single vendor networks put agencies at risk of vendor lock-in and limited options for negotiating lower pricing. Being able to choose from multiple manufacturers (enabled by solutions that deploy open standard protocols, which all manufacturers can do) translates into greater innovation and lower costs for the agency. When competitors can support the same open standards, the major networking manufacturers will compete with each other to offer customers the most innovative and secure solutions at the lowest cost. Solutions based on proprietary standards are not subject to the same competitive pressures, which can increase costs.

> *"Enterprises that do not create and actively maintain a competitive environment can overpay by as much as 50% for the same equipment from the same vendor. Savings can be even greater when comparing to other vendors with a functionally equivalent solution."*
>
> Danilo Ciscato, Vivek Bhalla. "Divide Your Network and Conquer the Best Price and Functionality." Gartner (October 20, 2017).

This reasoning is why procurement guidance at the federal level states a clear preference for the deployment of open, standard-based technologies. The Department of Defense has longstanding guidance (DoD Instruction 8310.01) mandating the use of open, voluntary, consensus standards for IT systems.

Misconception 3: Multivendor networks can have interoperability issues, especially if the existing network deploys proprietary protocols from a single manufacturer.

Fact: Simply stated, solutions in multivendor networks can be interoperable. Solutions from all major network hardware and software developers can be configured to interoperate when they all deploy the same industry-led, open standard protocols. Supporting open standards means that solutions from different manufacturers can integrate seamlessly in a single network.

At the same time, it is important to note that some vendors might claim to deploy an open standard solution, but actually use a proprietary protocol that competing vendors cannot support. For this reason, agencies should ensure that the protocols their networks use are industry-led open standards and not merely disclosed to standards bodies as requests for comment with informational status (a process that does not actually confer status as an open standard).

> *"In order to get established in existing networks and to offer customers migration opportunities, it is essential that your network components are completely compatible with those of other manufacturers."*
>
> EANTC

If an existing network deploys a particular manufacturer's proprietary protocol, the agency can direct the manufacturer to reconfigure the devices toward the appropriate open standard protocol. Manufacturers and third-party organizations will conduct interoperability tests, setting up networks in labs with products from different manufacturers to make sure they work. These testing opportunities enable an agency to introduce competitor manufacturers into its network.

Misconception 4: Multivendor networks increase operational complexity.

Fact: Deploying multivendor networks does not increase an agency's operational complexity. As explained previously, the solutions of all major equipment manufacturers can be configured to use open standard protocols and integrate seamlessly.

Having a common management platform is critical for operational stability. Network administrators can use a common management platform to push out security updates for multiple vendors' products, typically via an API. Each vendor can have its own management solution, but a common management platform reduces the complexity of operating and securing the network.

> *"Major infrastructure manufacturers [included] APIs that allowed administrators access to data—and more importantly—the ability to automate processes across a multivendor environment."*
>
> Andrew Froehlich. "Multivendor Infrastructures Are Easier Than Ever to Manage." Information Week (April 23, 2020).

Misconception 5: Multivendor networks lead to higher training costs.

Fact: The number of vendors in a network does not affect how much an agency will spend on employee training. Some agencies mistakenly assume that engineers already trained on a particular manufacturer's technology do not need to be retrained on future solutions from that manufacturer that the agency purchases. In reality, engineers often need to be trained on updated versions of existing solutions because interfaces and configurations can change. The vendor often includes those training costs in its overall pricing.

In fact, the federal government continues to purchase training for its engineers even when refreshing networks with single-sourced incumbent solutions. In May 2020, for example, the US Navy justified the purchase of incumbent networking solutions on the basis that introducing a new vendor would require additional training. At the same time, the bill of materials for the acquisition included training credits for the incumbent's technology.

In April 2020, the Social Security Administration (SSA) sought to refresh its existing network with incumbent solutions. The SSA justified its single-source approach by saying the introduction of a new vendor would require the engineering staff to undergo training on that vendor's products. At the same time, the SSA was still purchasing training and mentoring for the incumbent's solutions.

Under a brand- and technology-neutral procurement, competitors can propose their most appropriate solutions with training. A competitor's solution with training costs can have a lower total cost of ownership than an incumbent's solution. In short, the perception of increased training costs is not a legitimate reason to preclude a multivendor environment.

Misconception 6: An enterprise license agreement or enterprise agreement (EA) with one manufacturer means acquisition costs from that manufacturer will be lower.

Fact: Buying goods from a manufacturer that has an EA with the government can be more expensive than purchasing goods and services from a competitor that does not have such an agreement. Acquisition officials and engineers sometimes believe that an EA with one network manufacturer means the products and services from that manufacturer are free or at a lower cost compared to products and services from an alternative provider that does not have an EA. This confusion arises because the agency component buying hardware (and needing services) might not be the component that is paying for services under the EA; the agency component buying hardware thus incorrectly assumes the service is free. The EA simply means the price of service or maintenance has been pre-calculated; it still must be paid.

> *"The public interest would be furthered by amending the price evaluation methodology to include [related costs], as this will ensure that the evaluated prices accurately reflect the true costs to the taxpayers of a new . . . contract."*
>
> Arch Chems, Inc. v. United States, 64 Fed. Cl. 380, 402 (2005).

A government agency purchasing hardware should determine the cost of any services that will be attributable to an EA and consider that apportioned cost when conducting the hardware price evaluation. Here is an example:

- Assume that Agency X has an EA for Vendor A's goods but not for Vendor B's goods.
- When an Agency X component conducts an acquisition for goods and services, Vendor A might submit a bid for goods only and not services because the EA would cover services, while Vendor B will submit a bid for goods and services.
- When evaluating the bids, the component must calculate the overall cost for both bids, e.g., goods from Vendor A and proportional Vendor A service cost under the EA, and goods and services from Vendor B.

In fact, at the federal level, the US Court of Federal Claims has made clear that agencies must consider all relevant costs when conducting an acquisition. The underlying principle is that the existence of an EA with one equipment manufacturer does not mean that an agency should purchase products from only that manufacturer.

Conclusion

Even though agencies may perceive obstacles around cost and complexity to deploying multivendor networks, those perceptions might very well be based more on myth than truth. When government agencies support multivendor networks, they often realize better security, lower costs, and improved resiliency. Multivendor networks become a winning combination, enabling best-in-class government networking solutions.

About Juniper Networks

Juniper Networks brings simplicity to networking with products, solutions, and services that connect the world. Through engineering innovation, we remove the constraints and complexities of networking in the cloud era to solve the toughest challenges our customers and partners face daily. At Juniper Networks, we believe that the network is a resource for sharing knowledge and human advancement that changes the world. We are committed to imagining groundbreaking ways to deliver automated, scalable, and secure networks to move at the speed of business.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700

JUNIPER NETWORKS | Engineering Simplicity