Inside Track
Research Note

FREEFORM DYNAMICS

in association with

JUNIPER NETWORKS

Key factors in the network security buying decision

How – and why – network security professionals select solutions and suppliers

Freeform Dynamics, 2020

Introduction

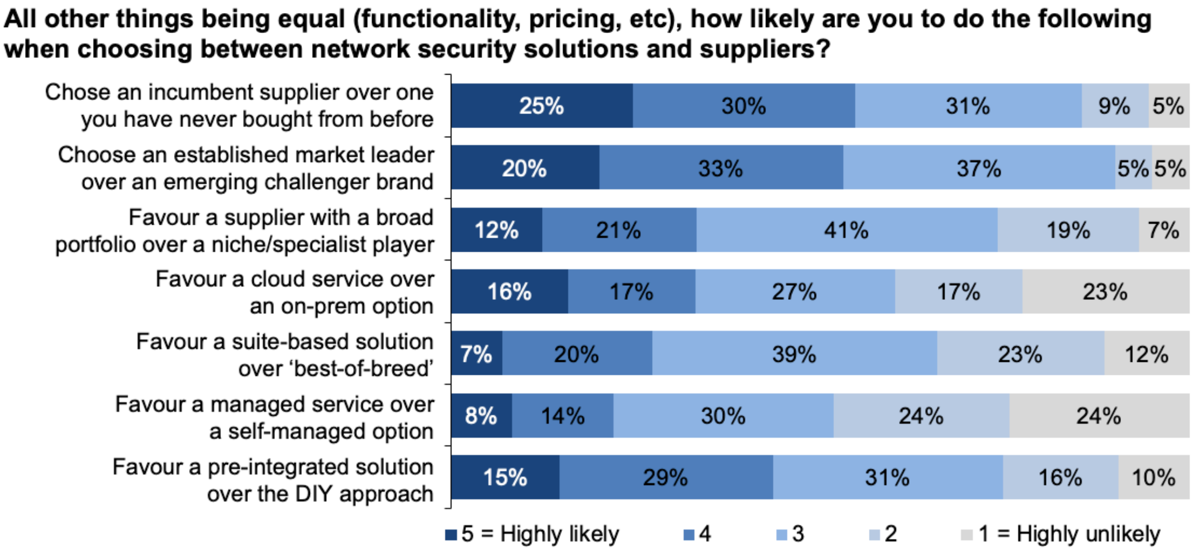
The first half of 2020 saw organizations go through years-worth of digital transformation in just a couple of months, as much of the world pivoted to remote and home working. For professionals in networking, this has helped to make security decision-making even more complex and challenging than it was before. At the same time, when it comes to enabling and ensuring future business success, making the right network security decisions has become more important than ever.

So when we recently surveyed some 223 respondents working in a range of business and technology roles, all of them involved in networking and/or security, we made sure to ask about how they choose solutions and suppliers. What makes a vendor attractive or unattractive? When would they consider a network security solution from a new supplier? And where should those new suppliers focus their efforts in order to convince prospective buyers?

The answers summarized below will make interesting reading for technology partners such as system integrators, resellers and VARs, and indeed for anyone else seeking to understand what motivates those who influence and authorize purchases. For more details on the other results from the survey, and to learn how we identified the minority of network security Top Performers, please read the full Research Report, **Network Security in the Spotlight**.

How buyers choose network security solutions

It was no surprise that more than half of our respondents said that, all other things being equal, they would favor an incumbent supplier or an established brand for their network security solutions – the two could well be the same company, of course. More interesting, perhaps, was that while they were certainly not against suppliers with broad portfolios, suites, or pre-integrated solutions, on average they were less important factors than incumbency or market leadership (Figure 1).



All other things being equal (functionality, pricing, etc), how likely are you to do the following when choosing between network security solutions and suppliers?

Figure 1

The only real difference here between how the Top Performers and the Mainstream[1] see things was that in every case the Top Performers took slightly more of a neutral or ‘unlikely’ stance. This suggests that they may be more open to new and challenger brands, best-of-breed solutions, and to DIY and self-managed approaches than Mainstream organizations.

Of course, in the real world “all other things” rarely are equal, so we turned the question around and asked how much the various potential ‘inequalities’ would encourage our respondents to select a challenger or specialist brand (Figure 2).

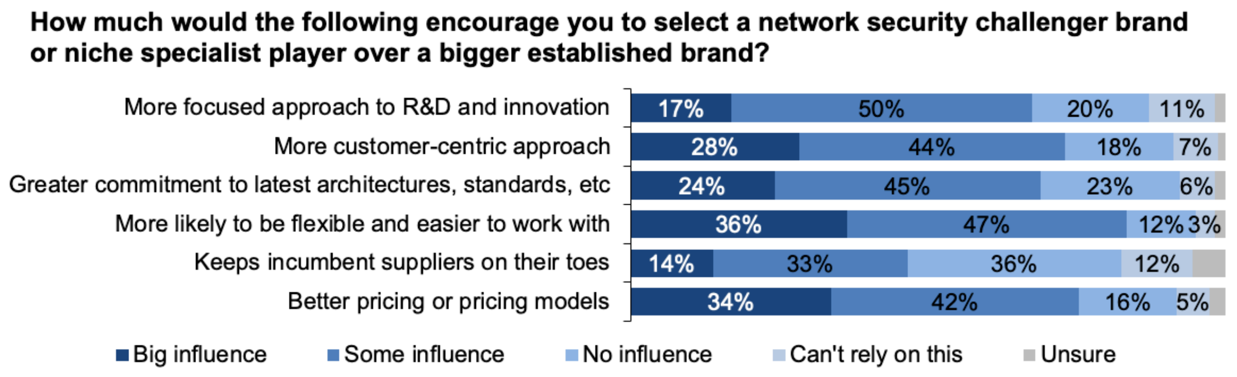


Figure 2

Their answers suggest that challenger and niche suppliers need to ensure that they can clearly demonstrate an advantage in areas such as pricing, customer-centricity, flexibility and innovation, and so on.

Again, the Top Performers and the Mainstream differed little in their perceptions here, with the exception that the Top Performers were more guarded or cautious. More specifically, while both groups were equally likely to be influenced, the Top Performers were more likely to claim it would only be ‘some’ influence and not a big influence.

More vendors or fewer?

Most organizations have to deal with multiple vendors, either for networking, for network security, or for both. Although this introduces some of the complexity discussed earlier, it is often argued that it is an advantage because it allows you to choose the best solution for each task or requirement and then mix-and-match them to create the most effective overall infrastructure. This is often called the best-of-breed approach.

However, only a third of our respondents said that having multiple vendors for both was their preferred situation. Rather more (44%) said instead that their ideal was a more consistent supplier landscape, with a single vendor for either networking or security or both (Figure 3).

[1] As defined by asking our respondents to rate their organization’s current performance on several key areas around network security and creating a Performance Scorecard from the results. See our report **Network Security in the Spotlight** for more details.

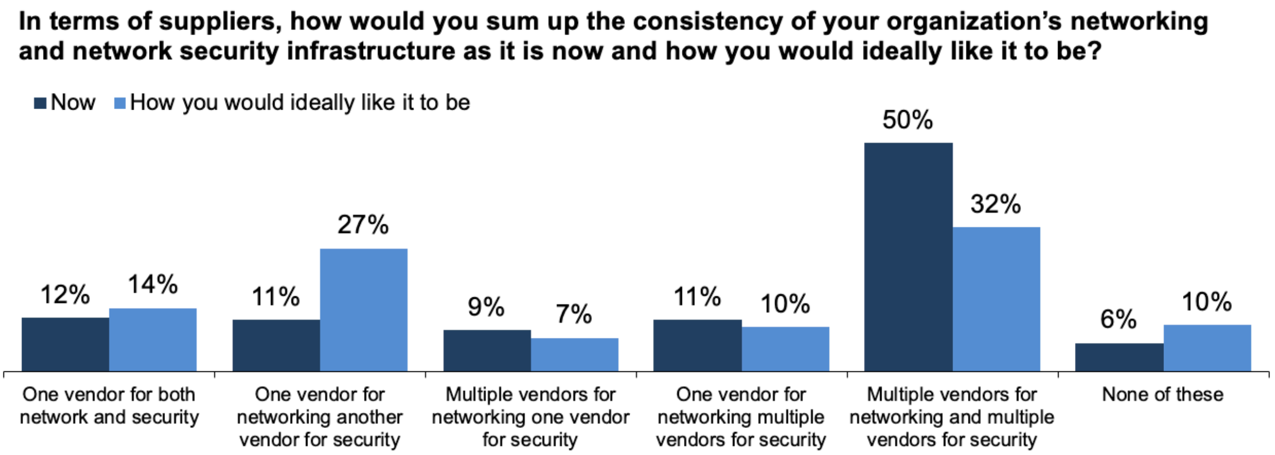


Figure 3

The argument here is that having a single supplier for the networking infrastructure or for network security should make it easier to get different systems working together, not least because it means that if something fails, the supplier can't easily pass the blame onto someone else.

Interestingly, only 14% overall said they would like to have the same single supplier for both networking and network security, although this rose slightly to 18% when we counted just the Top Performers (Figure 4).

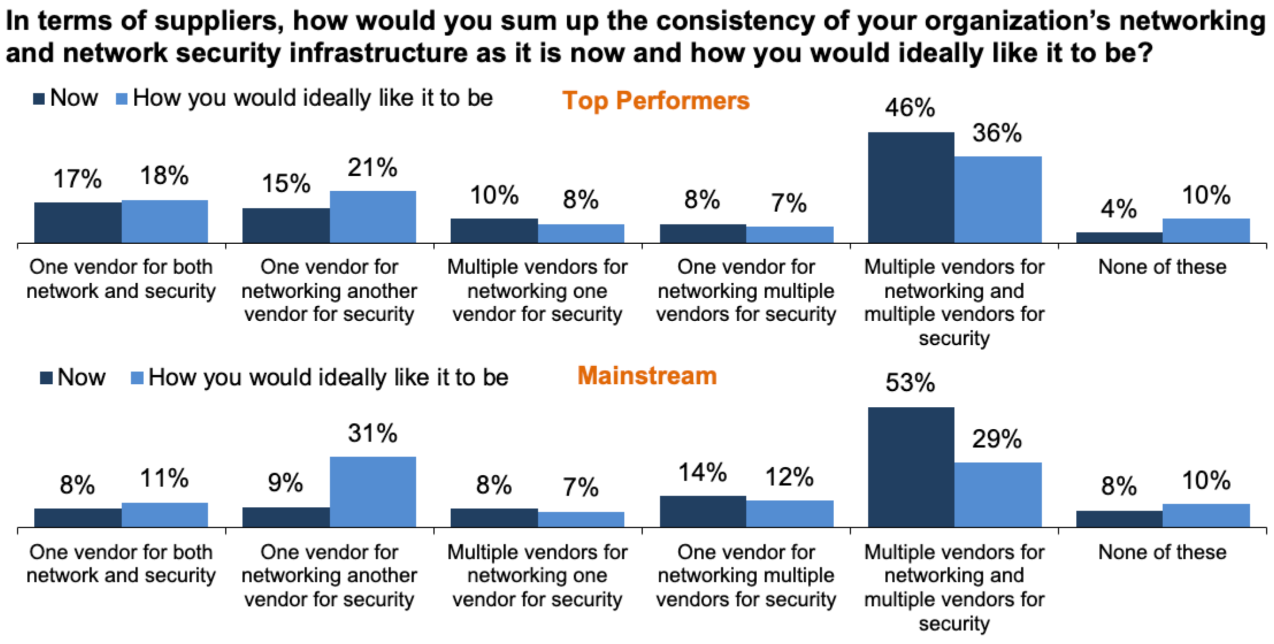


Figure 4

In contrast, twice as many of the Top Performers (36%) said they preferred to have multiple vendors for networking and multiple vendors for network security. Meanwhile, 53% of the Mainstream said they currently had multiple vendors for both, but only 29% said that this was their preference for the future. Either way, there is clearly scope for technology partners to help clients update both the network and security infrastructures they have in place and their supplier strategies.

A question of trust

When we aggregated the preferences shown in Figure 3, we found that single-vendor strategies were a little more popular overall, and that in general there was a slight preference for simpler supplier relationships. However, when we compared these responses with how respondents assessed their organization's performance on network security – this is, whether they were a Top Performer or in the Mainstream group – we found no clear correlation between the infrastructure consistency and their network security performance.

Rather, the choice of whether to go best-of-breed or single-supplier is often based much more on past experience, the availability of skills, familiarity, and – crucially – on issues of trust. To explore these decisions more deeply, we asked our respondents what they saw as the advantages and disadvantages of each approach.

Their answers revealed what almost seemed to be philosophical differences between the two strategies, as well as the distrust that many network security practitioners have in some or all of their suppliers. Among their comments were:

"A lot of vendors are poor, the question is whether you want 'one throat to choke' or to 'spread the pain' with several."

"Most large corporates are happy with a single vendor for routing and switching, but need to have multiple security vendors, which undermines the benefits of consolidation."

"No supplier is best-of-breed in everything – we have two main security solutions now, but we wouldn't go above three."

The single-supplier supporters

Among the advantages frequently cited for this approach by our respondents were faster implementation, more coherent management, and an accountable single source of support. Some added that it can reduce costs, both because of volume purchasing and because there is a lower learning curve and a single support contract.

Several respondents confirmed that they have found it easier to integrate multiple products from a single supplier, whereas integrating systems from multiple vendors is often a challenge. One reason for the latter is that best-of-breed integration is typically either a relatively shallow or lowest-common-denominator variety, based on older standards, or it may use alternative mechanisms that require considerable manual integration work. (A caveat is that this can also be true of single suppliers, if their range includes products derived from the recent acquisition of another vendor.)

The best-of-breed believers

No one vendor is the best at everything – in their comments, several respondents used the expression 'Jack of all trades, master of none.' As well as allowing you to choose cutting-edge technology, having multiple suppliers can give you an overlap, so if one product misses something, another may well catch it.

In contrast, there were several warnings of what can happen if your single supplier has a blind spot or a core vulnerability that's shared across its systems. A single supplier is a single point of failure or of compromise, as some of them noted. It also tends to mean a larger supplier, which may be more cumbersome to deal with, less innovative and less flexible.

While buying from multiple suppliers means dealing with multiple account managers and bills, and getting fewer volume discounts, some suggested that it can encourage competition both on price and service. Vendors can be played off against each other, for example. It also avoids the vendor lock-in that numerous respondents warned can be used to push up prices, hook you into expensive support contracts, or lever you into purchasing products that don’t properly fit your needs.

Closing thoughts: What must newer vendors do better?

Lastly, having already asked what might favor the selection of a network security specialist or challenger brand, we wanted to know what factors might discourage that choice (Figure 5).

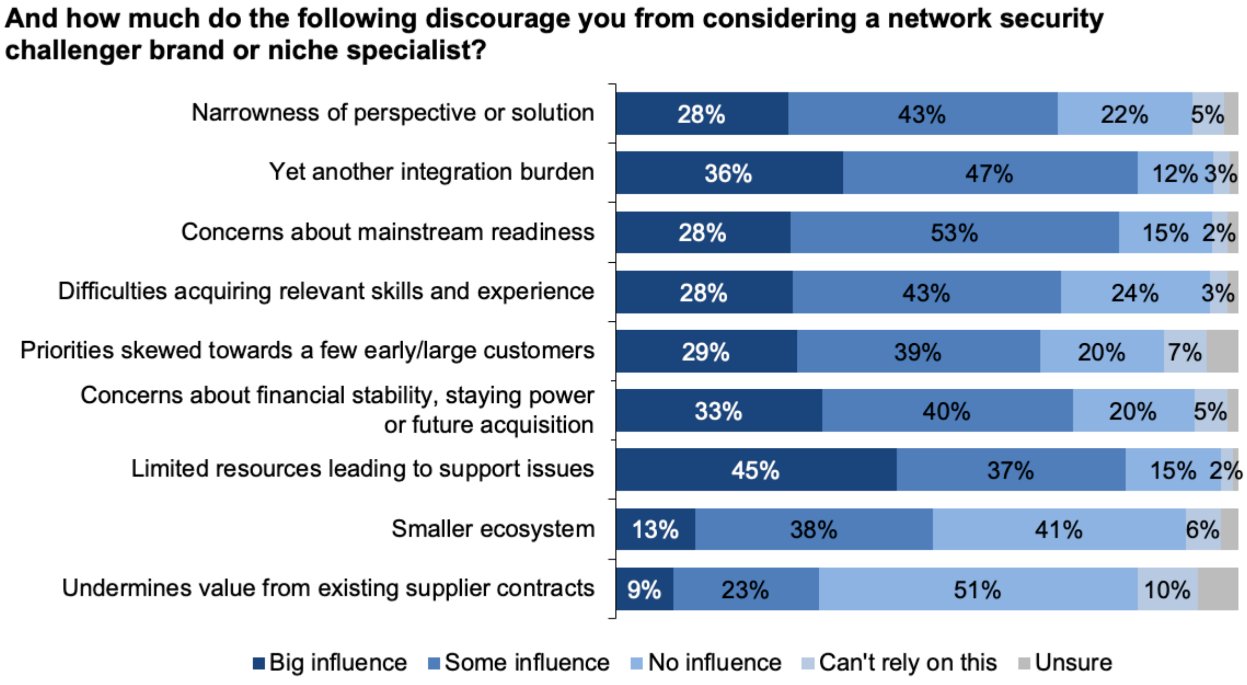


Figure 5

It is clear from these answers and the earlier best-of-breed discussion that such suppliers must work hard to persuade the mainstream. We already saw that they need to show clearly that they can offer advantages in areas such as pricing, technological innovation and customer focus.

Here we see that in addition it is critical for them to address those concerns around integration, support and mainstream readiness, and to reassure prospective customers of their broad vision and financial staying power.

About Freeform Dynamics

Freeform Dynamics is an IT industry analyst firm. Through our research and insights, we help busy IT and business professionals get up to speed on the latest technology developments and make better-informed investment decisions.

For more information, and access to our library of free research, please visit www.freeformdynamics.com or follow us on Twitter @FreeformCentral.

About Juniper Networks

Juniper Networks challenges the inherent complexity that comes with networking in the multicloud era. We do this with products, solutions and services that transform the way people connect, work and live. We simplify the process of transitioning to a secure and automated multicloud environment to enable secure, AI-driven networks that connect the world.

For more information, please visit www.juniper.net

Terms of Use