colt | VERSA NETWORKS

Secure SD WAN – how to unify connectivity and security successfully

Secure SD WAN - how to unify connectivity and security successfully

Recently, we hosted a webinar with guest speakers from Versa on the topic of secure SD WAN. In the webinar, the panellists discussed how businesses can successfully unify connectivity and security.

For ease, we have pulled together some of the key takeaways on this hot topic for you. However, before we dive into the webinar learnings, here are just some of the core reasons why businesses need to be looking at an integrated approach to both security and network today:

- In monetary terms, IBM stated the average data breach cost in 2022 was **$4.35 million**
- **60%** saw an increase in the price of their products and services due to the breach
- But it's not just that – it's the **loss of productivity, cost of response or recovery, impact to reputation, fines and judgements**

Jayesh Patel
Director Sales Engineering
Colt Technology Services

Khalid Mahmood
Senior Product Specialist
Colt Technology Services

Rob Bolton
Vice President
Versa Networks

Jon Taylor
Director and Principal of Security
Versa Networks

What do companies need to be thinking about when they're starting their network security transformation journey?

Khalid:

"It's important that businesses have a clear understanding of the 'why' and what they hope to achieve. They need to consider how any transformation contributes to their wider business strategy and how they plan to set themselves up for success. Success criteria should be identified as well as how often they review their progress.

Based on personal experiences, I advise businesses to define their objectives from the outset. This may sound obvious, but it is so critical. On many occasions, we've seen issues arise down the line due to a lack of a clear strategy, well defined objectives and proper planning. My advice would be to go back to the fundamentals. Consider your users, data and applications. Where are they located? How will they change over time? What security is required to protect them? It's also worth giving some thought to your organisational set up. What are your key security and network pain points? What problems do you wish to solve and how are you going to prioritise them?

Companies should work with key stakeholders right across the business to assess the impact of any changes they are planning and to capture those crucial business requirements as well as the potential risks that need to be mitigated. Your operating model also needs to be considered. Ask yourself, 'Do we have in-house expertise to manage and help make a solution work or do we need a partner to help?' If a partner is required, they should look for one with the right blend of experience and credibility.

This is a long-term relationship you're embarking on, so really choose wisely."

Rob:

"Any solution should have customer experience at the centre of it. Ease and usability are so important. At Versa and Colt, customer experience is front and centre of just about everything we do relative to our solutions.

I would also add that a company's ability to manage post implementation is so important. They need to make sure the objectives defined at the beginning of the process are being met and approved by the wider business. Achieving this requires the involvement of people. It's down to processes and the technological element of managing it."

Jay:

"We have encountered both extremes of the customer experience. Some customers come to us with a plan to deploy SD WAN, only to discover a few months down the line that their security department has concerns about the SASE solution they have implemented. This could have been avoided if they had approached us together. That's why Khalid's point about choosing the right partner is crucial. They can support you and deliver way more than what your requirements are."

Why is it so vital to consider security and connectivity at the same time?

Jon:

"Everyone seems to be shifting towards zero trust frameworks, which require continuous authentication, authorisation, and validation for all users of a network and the need to provide least privileged trust to end users and devices. Companies are moving towards more security being built into the ecosystem right from the ground up, with a single point of management for network and security. If you picture a venn diagram, one side is the network, the other side is security, and the union is SASE. SASE brings together security and networking teams, providing infrastructure security in a way never seen before."

Rob:

"What customers are really enjoying about this unified platform is the built-in flexibility. It allows them to phase in the solution to suit their business needs. Many companies still carry scars from past projects; they have experienced failure from trying to integrate a too complex solution with too much risk and no flexibility. What I would add is that businesses shouldn't go 'at it' alone. You have a wealth of resources to assist you, regardless of where you are on your journey."

Khalid:

"You know a SASE solution incorporates security and connectivity and you know it has a range of benefits from operational through to procurement and in-life management of your network, but even in scenarios where you want to integrate into an existing security architecture, it's essential that both connectivity and security are considered simultaneously.

The impact of every change needs to be understood and considered. How will this integrate into that and how will it exist in their ecosystem? Security is paramount – whether it's during transition or post implementation, so it must not be compromised. If you're thinking about a change in network architecture in isolation, you will need to think about what that does in terms of your overall security posture. Will it introduce new vulnerabilities? It's also essential to avoid any unnecessary expenditure by looking at too short-term solutions that will need reworking and replacing down the line. Avoid that short-sighted, short-term approach.

The way we work today is radically different. We demand access to applications from anywhere on any device at any time and, ultimately, this drives a requirement for universal access which has significant security implications with a radically different, more complex security perimeter. And that's the reason why now more than ever we can no longer think about security in isolation."

Jay:

"Once upon a time you had a network. It was MPLS. Your attack zones would be your data centre firewalls or your head office firewall locations. Now the internet is everywhere and it's occurring from all devices to your internet. Your attack surface has now grown two to five times the size and every network point becomes an attack point from a security perspective."

What does considering security and connectivity in the converged approach mean in practice?

Khalid:

“In practice, this means taking a holistic approach from the initial strategy through to planning, procurement, deployment, testing and in-life operations. It’s crucial to avoid short-term solutions and quick fixes. Instead, take a strategic approach that considers every aspect of the transformation. It’s also important to carefully plan and execute the transitional migration phases, which are often a source of concern for customers.

Consider how you will mitigate the risks through proper planning and testing of your technical architectural configuration and business processes. These are so crucial and can often, from our experience, be the weakest link in any transformation.

Consider the operational impact of a much more integrated network and security solution in terms of your people, resources, skills and business processes. Convergence brings the promise of greater efficiency, but it can only be realised with proper planning and proper execution. Your whole business needs to adapt to really capitalise on the true potential of the technology.”

Jon:

“We’re seeing more communication between security and networking teams who are working together more often. The days of networking teams creating something very elaborate and then handing it off to the security team to secure the network has passed. The security team would come and drop in their overlay and then it would cause customer satisfaction issues. Management would then often compromise on security so there was access. Security was often a last thought. The problem now is that cyber security has become more sophisticated, so it can’t be compromised any longer. Security must now be baked in. During the architecture process, the security team needs to be there thinking about how to secure each and every link from a physical and logical standpoint and what mechanisms need to be put in place. Taking this approach helps to create an improved customer experience.”

What are the major pitfalls you've seen and how can businesses avoid them?

Rob:

"One I see often is the approach of integrating multiple point products for specific SASE functionality. This is stitching products together and then expecting all the benefits of unified SASE, which just isn't the case. It just doesn't work that way.

Secondly, customers run into issues when they fail to customise the SSE capabilities to meet their specific needs. One of the major benefits of SASE is to help ensure customers are getting the capabilities they need, but being built in at the pace of the broader transformation. Customers are not taking advantage of the customisation available within a SASE framework."

Jon:

"Another factor that is often overlooked is ongoing management. Implementing a solution is not just about stitching together products, but also considering how the solution will be managed and adopted.

Businesses need to know how it's going to all come together as a cohesive solution. It's essential to consider integration points, authentication platforms, and training for users to ensure ease of adoption and use. Having a knowledgeable partner who can also provide training alongside support is so important. They can walk arm in arm with you through the process. Having that day one support is essential."

Khalid:

"Companies should plan for today, consider requirements for tomorrow and try to avoid short-term fixes because these can be costly. These short-term solutions rarely scale. Businesses need to avoid that piecemeal approach to security and focus on a fully-integrated solution that's going to be scalable. One that's going to deliver the cost benefits and offer a comprehensive set of both networking and security capabilities. Even if you don't need all of these capabilities on day one, ensure that your strategy, your choice of partner, and the solution that you opt for has the flexibility that will scale in the future.

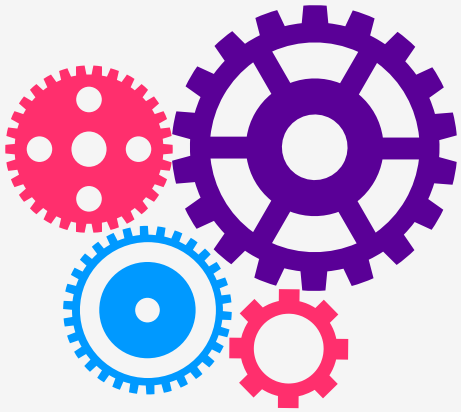
From our experience, many network transformations fail due to poor planning. This is usually because of a lack of the right resources, not engaging with the right stakeholders or failing to test properly. Businesses need to ensure that everything from the business plan down to the technology and final solution offers them the flexibility to adapt and change. It's important that you continually evaluate throughout your journey, reassess initial objectives and adapt or course correct if necessary."

What are your final words of wisdom?

Khalid:

"Firstly, remember your objectives. How does this transformation fit in and help you deliver against your business strategy? Remember, your network is fundamental to your business. Ensure that your analysis and planning is comprehensive from the outset. It's crucial to start with this mindset from day one and not blindly follow any initial assumptions and objectives if they no longer hold true. Consider the organisational impact, especially regarding existing business processes. Companies should think about cultural aspects like the way they work, and how that may need to change.

It's important to think about the technical and security expertise required to execute a transformation plan. Do you need to outsource to upscale your staff members or reorganise your teams? Whilst you will inevitably evaluate the upfront cost and investment required for this transformation, you need to consider the overall total cost of ownership and value. When comparing the different options available, always take a holistic view and consider how you'll measure and demonstrate the return on investment to shareholders and the wider business. When selecting a partner, choose one with the right blend of experience, credibility, and commitment to really help you succeed. At Colt, we really understand the value of selecting the right partner, and the trust that our customers are placing when they embark upon a transformation journey with us. Ultimately, it's in our mutual interest to make it a success."



Jon:

"I'd say understand the benefits right when you start to look at something like unified SASE, not just SD WAN or SSE deployment. When looking at unified SASE and where the market is leading with it, really understand the benefits you're getting as you're planning and looking at your objectives. Take those benefits and apply them to your business objectives. When you're looking at partners, have them highlight all the benefits you will receive. You could learn something new or it could even be an upsell to executive leadership. Another thing to look at is prioritisation. Think about the capabilities you need to build the plan and then deliver it. What are you going to do first? What are you going to do second? Lean on your partner to help you prioritise and develop. Not just a plan for the roll out, but the testing side too. You can then deliver that plan right across the board. Tick each and every box off as you go to ensure you are making this a seamless deployment or transformation."

Rob:

"Through the testing and proof of value phase – ask the right questions and test the right capabilities. Not just on the technology that you are testing but the integrations with other ecosystem components. Make sure whatever solution you choose is the right one."

Looking to embark on your own SD WAN or SASE journey?

If you are about to begin your own SD WAN or SASE journey or are looking to transform your existing networking security infrastructure, please do reach out to us. Our team would be happy to run an innovation workshop for you that will help you map out your own individual journey. Simply get in touch.

In our workshops, we can expand on the advice given in this webinar and showcase some of the technology solutions available to help you decide what's right for your business. And, if you'd like to watch the webinar in full, it can also be viewed.

For more information, get in touch with us at **www.colt.net/contact-us**