ALLIANCE Media Group

Alliances

Digital Alliances

continue collaboration

CISO Alliances – UK&I
29th July 2021

In Partnership with :

cisco Cisco Umbrella

Alliance - ‘A union formed for mutual benefit’

DigitalAlliances

continue collaboration

ALLIANCE Media Group

Food For Thought/Topics Discussed

Session Leaders: **Xavi Garcia Faura – Cloud Security Leader, Cisco**
Luke Hebditch – Technical Solutions Specialist, Cisco

Session Title: **Will SASE transform IT security for businesses?**

Session Synopsis:

Organisations have had to deal with more changes in the last year than ever before. As companies turn to the cloud in order to reduce complexity and deliver greater flexibility, they must also adapt to meet these changes head on

The past few months have seen IT transformation on an unprecedented scale as organisations across the globe change how they do business. With the adoption of cloud-delivered services, SD-WAN has proved that it can deliver improved application performance, reduced costs, and simplified branch operations. But, despite all these benefits, security remains one of the biggest concerns.
How do you secure users accessing the internet or cloud apps, either remotely or at multiple branch offices? What is Secure Access Service Edge (SASE) and how can it deliver multiple security functions from the cloud? How does the quality of threat intelligence you have access to help avoid security blind spots and stop false alerts?

Join us as we discuss the latest developments in security networking, understand the key challenges and learn how to setup your business for success today and in the future.

Key takeaways:

What is SASE, why are we seeing a rapid rise in companies shifting to SASE?
How will the business challenges we have seen in the last year adapt the roadmap and vision for an organisation this year?
What does the cloud centric threat landscape look like and the trends we expect to see over the coming months
How are companies adapting to more employees and customers working from home – what added responsibility does this have on the CISO and security teams?
What are the considerations to ensure improved Security Visibility and Automation and what options are available?
What are the trends we are seeing with the implementation of SASE?
Best practice for companies to protect their workers and customers?

DigitalAlliances
continue collaboration

Food For Thought/Topics Discussed

cisco

Cisco: CISO Alliances

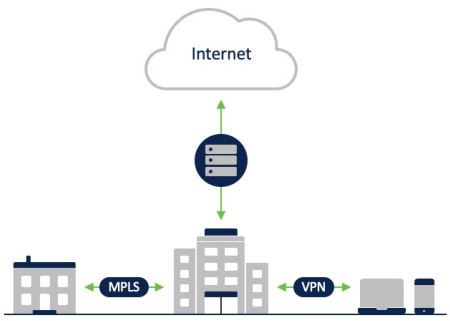
SASE

Xavi Garcia Faura, Sales Leader, Cloud Security
Luke Hebditch, Technical Solutions Specialist, Cloud Security

Thursday 29th July 2021

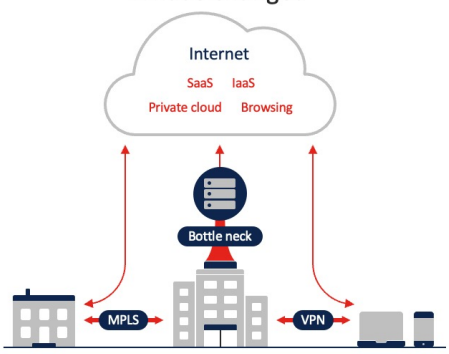
Network transformation

Before



Apps: Hosted in datacenter
Users: Connected to corporate network to work
Network: Centralized
Security: On-premises security stack

What's changed



Apps: More hosted in the cloud
Users: More work done off-network
Network: De-centralized
Security: Gaps in protection

Digital Alliances

continue collaboration

Food For Thought/Topics Discussed

Networking and Security teams struggle to…

…connect users to applications and data

- Poor user experience when accessing cloud apps
- Complexity in connecting to multiple cloud providers
- Lack of end-to-end granular visibility of application performance

…protect against evolving threat vectors

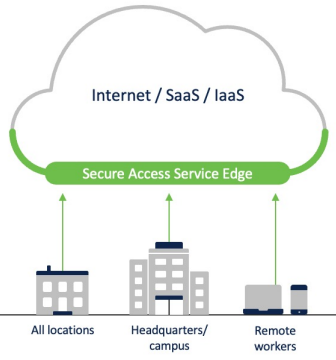
- Gaps in security protection
- Inconsistent policies enforced across disparate locations
- Difficult to verify identity of users and devices

This requires a new approach to networking and security…

Today's cloud-centric world

Drives the need for a secure access service edge (SASE) architecture

- Combine networking and security functions in the cloud
- Connect users to the apps and data needed — in any environment, from anywhere
- Control access and enforce the right security protection consistently

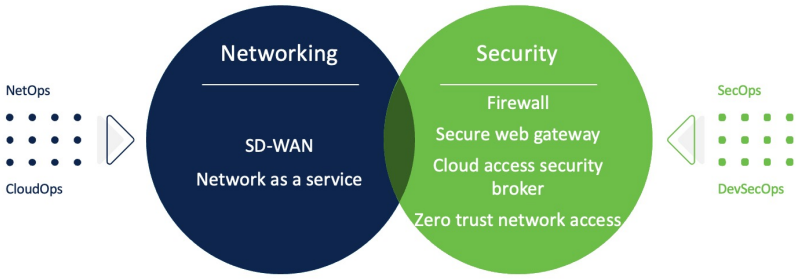


Digital Alliances

continue collaboration

Food For Thought/Topics Discussed

SASE: Convergence of networking and security in the cloud



How is your networking and security adapting to the hybrid way of working?

- The recognition that security boundaries have had to change. Taking more of a look at security around data. Easy to say that the office is secure, another matter when it comes to working at home, coffee shops etc.
- Educating people around the risks that occur from working in different environments.
- A few organisations were already working on public networks, so the pandemic didn't have the affect that others felt.
- However, offices are secure through certain solutions, but when employees go home or work from home, this protection isn't there.
- The pandemic has heightened the need to manage all remotely from the cloud from a secure location.
- Infosec spend is still an issue, so little compared to what is needed. Always put off and compared to what else can be purchased.

Food For Thought/Topics Discussed

- New employees, using their own devices, no access to see what they are accessing, downloading etc. This is this an issue with hybrid way of working.
- Adding more and more solutions into the landscape is not the answer, trying to make the landscape simpler is the way forward.
- Everyone will be looking to their favorite brands to say, we are looking for an end-to-end stack.
- Very difficult trying to use the different suppliers of solutions from Gartner's magic quadrants and trying to make them all work together.
- Another issue is what happens to the date once it has left the server that we manage. Can secure connectivity, but how do we secure the date on devices that we don't manage.
- Very difficult to put in place SASE at present as they all over end points, which is very difficult when there are devices that we don't manage.

What are the networking and security implications of your public cloud adoption strategy?

- Some organizations haven't migrated to cloud and are still on prem.
- Public cloud, some have an issue with it but others are all for it.
- Depending where you operate, certain organisations can't be used. I.e. China.
- One issue with the cloud is, what happens with outages, which have happened this year.
- Moving to the cloud has been a saving grace when it comes to multi level protection scheme.
- The legacy architecture is an issue with SASE, Is sold as the silver built that is easy to achieve, which it isn't.
- The cost again, is another issue when it comes to public cloud.
- Having the board on-board is another issue, when more manpower is needed etc.
- The value outcomes is another issue that cost has a big affect on.

Food For Thought/Topics Discussed

- Moving everything over to a public cloud, is not the be all and end all. It's complicated.
- This view that once it is put into public, its not instantly secure.
- Not every organization will need to push the button on digital transformation, its not a one size fits all.
- Educating the board that question why you need extra budget when you put things into the cloud, helping them understand that it doesn't mean instant security.
- Some organizations are moving rapidly to public cloud, this has been challenging as some organizations are getting rid of buildings during the pandemic.
- Resource is the issue when it comes to unpicking the legacy architecture, doubling up on licenses.

Are you moving to a direct internet access model vs MPLS?

- Some organizations have been for a while, moving to direct internet access model.
- Some organizations are looking at doing this, they are in the process of shutting down their date center sites.
- People, again is another issue, getting the correct people into the organization.

Digital Alliances

continue collaboration

Food For Thought/Topics Discussed

How do you see Zero Trust affecting your approach to security?

- Discussions going on within organizations around what Zero trust really means, some people arguing that they have multi factoring authorization means they are zero trust already.
- Within these discussions, people have completely different views around the meaning of zero trust.
- Understanding what zero trust is, is a good point to start. The word has been created by vendors to sell a fancy solution.
- There is no description around what zero trust is.
- Zero trust has been portrayed as a concept.
- Zero trust, not something that will be put across the whole architecture, will be put across the architecture of critical data assets.
- People are talking to vendors to understand zero trust and see that if can be put across only part of the architecture.
- Giving users the access to applications without the VPN.
- Office 365, in the past could only be accessed through the corporate network, needed to be on premises. Now with two auth factoring, this is being used only via corporate devices.
- The more research around this, the legacy is an issue again and building the concept of zero trust, its going to be a marathon and costly.
- Some organizations, it would not be feasible to go back to access only via corporate devices.
- There is a theme that by going down the route of having a full stack from one vendor will cost most and not feasible for organizations.

Food For Thought/Topics Discussed

Digital Alliances

continue collaboration