Telstra
Purple

Frequently asked questions

Ask the experts: Helping you stay connected webinar

19 May 2020

Q1

What's the major difference between a traditional VPN and a Zero Trust network access solution?

Answer:

- There’s a few, but the major differences are that a traditional VPN solution connects networks to networks, and Zero Trust Network access solution connects users to applications.
- Another key difference is that authentication and authorization are discrete functions that are performed before a session to an enterprise resource is established. The conceptual advantage has been demonstrated to be particularly effective in mitigating many common network-based attacks such as port scanning, denial of service and SQL injection attacks.

Q2

Zero Trust adoption was mentioned as being a key reason as to why some enterprises adapted well during COVID-19. What specifically, was it about Zero Trust that helped?

Answer:

- One of the key paradigms around Zero Trust is the notion that location should not dictate trust. For example, just because a user connects via a corporate LAN environment, should not dictate that the user should be trusted. Therefore, enterprises that have prepared their workforce with strong authentication and authorization mechanism’s that are agnostic to their location have found the move to remote working relatively seamless.

Q3

Some customers have struggled with security in the past, how do they start on the Zero Trust journey from a relatively low base?

Answer:

- Knowing your environment is a key starting place. Telstra has long advocated clients adopt the 5 knows of cybersecurity which includes: Know the value of your data, know who has access to your data, know where your data is, know who is protecting your data and finally know how well your data is protected. These questions help develop an understanding of your attack surface and can help you prioritise where to start.
- Also, it does not hurt to have a good definition of what Zero Trust is as many vendors have their own definition. The National Institute of Standards and Technology (NIS) has begun helping in this area, by releasing the second draft standard 800-207 which is bringing together the community to help define and standardise the core tenets and architectural components of Zero Trust. This second draft is freely available from the US National Institute of Standards and Technology website for review and comment.

Q4

How is the Telstra workforce currently adapting to the new normal?

Answer:

- Telstra is continuously running surveys to understand what has worked well and what hasn't, to ensure we are continually adapting to the new normal. It is also asking questions such as: Are we going to change our practices? Are we going to work from home more often or are we going to head back into the office?
- Anecdotal discussions highlight concerns- mainly around the practicalities of social distancing in public transport. I expect government measures and communications will be key in helping reduce this risk.
- Discussion around things that will most likely change include hot desking, and the amount of people subscribed to a floor. Ultimately, I believe this will result in a larger shift of people working from home permanently on at least a part-time basis

Q5

Can you give us a view on the technology demands during COVID-19?

Answer:

- Surprisingly, SD-WAN is still on the radar and projects in-flight are being accelerated, yet while the focus traditionally has been on carriage arbitrage (primarily), customers are now considering the supplementary benefits SD-WAN can provide such as: cloud exchange, redundancy, visibility and security.
  - Remote access incorporation into the SD-WAN portfolio by vendors have created a new relevancy for the technology and I foresee a both technologies working in parallel and integrating at some point more tightly Some vendors are already on this journey.
- Cyber-Security - from the endpoint to your data store and application (which could be SaaS) as well as the analytics that provide the deep insights into productivity and performance
- Existing technology has been augmented and evolved to support a post COVID-19 world ie: 5G, edge compute, concepts of the Infrastructure with less branch/user.
- Remote access has accelerated and will continue to be a viable, normalised option for workers - be it cloud-delivered or traditional on premises.
- Scalability focus/on demand - pay for what you need
- Increased demand for managed outcomes - and it's not a conversation about vendors. Customers want to focus on the business, not the technology (or complexity that underpins it).

Q6

What are the trends are you seeing across your customer base?

Answer:

- We have seen that customers have been resilient, looking for opportunities to innovate as well are acting quickly and decisively. At Telstra, we support a variety of industries across a range of technology verticals.
    - Healthcare – ramp-up of IOT, asset tracking and telehealth technology
    - Logistics & utilities – 5G/4G, supply chain tracking, edge compute & digital transformation
    - Manufacturing & Mining – Enterprise Wifi morphing into Industrial Wifi, connectivity, data throughput and security services
    - Retail – infrastructure type delivery has somewhat flatlined due to the unknown future position of income and growth, yet there has been an increase in consulting services to decrease operational technology costs and digital transformation - from traditional bricks and mortar to online. Existing projects in train around SD-WAN and Cloud Connectivity have continued.
    - Financial/FSI – digital transformation, cloud delivered services (ie remote access), load uplifts.

Q7

We are hopefully on the road out of COVID-19, what are the areas to consider in the future?

Answer:

- Rightsizing to ensure your infrastructure and services scale
    - It could be public cloud assets and software, private technology assets, network and security services
- A well-known component of Business Continuity plans is remote access, nevertheless; customers should broadly look at their Disaster Recovery, Backup Services, Data Replication and Storage Infrastructure as a Service (IaaS)
- Look for points of failure be it in the network, security or infrastructure
    - We have seen this unprecedent time an unfortunate increase in opportunistic cyber crime
    - Network Assessments, Security Assessments and Various Consulting Services, Efficacy of Cloud - Multi-Cloud - supports competition
    - broader range of applications availability to an enterprise - best in breed
    - Harmonised Public and private cloud - It’s not always about the public cloud - it could be a private or a combination of public and private clouds - counterweight
- Cyber-Security Technologies that Focuses on the user and what that user is doing and communicating with and provide the right security controls (Zero Trust & Identity)
- Visibility of the network, security analytics and overall cost
- Focus on Simplification - standard architecture and configuration, vendor stack - supports automation, cost out and overall lower operational costs
- It’s all about the network - how do users connect and where, its resiliency, security, redundancy and optimal paths.

Q8

There has been a lot of conversation around Secure Access Service Edge (SASE) of late. What is it and why is it relevant and what does it mean to the security landscape?

Answer:

- Defined by Gartner in August 2019, SASE describes that move network security away from the centre of an enterprise network into the cloud
  - Traditional enterprises place the DC at the core of their services
- At a high level, consumption of cloud-based SaaS that would be typically needing private infrastructure that is on premises
- Central controller, mostly software activated
- Cloud delivered, incorporating deep analytics, SD-WAN, remote access, security.
- Subscription-based, software defined which aims to remove the expense of hardware roll outs
- Combination of multiple technologies: Reduces complexity of the network security side by moving these to one vendor:
  - Secure Web Gateway (SWG),
  - Cloud Access Security Broker (CASB),
  - DNS,
  - Zero Trust Network Access (ZTNA),
  - Identity Management
  - Remote browser isolation capabilities.
- A lot of this we have been doing for a long time. But it is relatively immature, and Vendors are still reconfiguring their portfolio but will get there in time.

Q9

A few points were covered here: Endpoint management, access to internal resources, capacity planning - is there a holistic platform Telstra are using to assist customers that cover all these points?

Answer:

- Microsoft would be closest to a holistic platform, as we use Intune for endpoint management, Microsoft 2FA for remote access authentication and Azure for capacity planning (cloud)

Q10

How can Telstra Purple assist customers with providing a brilliant experience for their customers? (Analytics, AI, Next Generation workplaces)?

Answer:

- Telstra Purple takes a consulting led approach to understand the business outcome that our clients need. This starts with a discovery stage where we gather context regarding your environment and business to ensure the solution is customised to meet your unique needs.
- We have capabilities in a range of areas that include solutions around: Data and Analytics, AI, Cloud, security and Next Generation workplaces.