HIGH ASSURANCE DELIVERS SD-WAN FOR All

High Assurance SD-WAN Deliver for All

The prohibitive cost of WAN technology has become a major concern for businesses and governments and driven the explosion in adoption of Software-Defined Wide Area Networks (SD-WAN) in recent years. Yet a gap is beginning to emerge between those businesses able to explore the flexibility and low cost offered by SD-WAN and those, typically regulated, organisations that have serious concerns about data security.

Without access to the agility, flexibility and support for cloud-based transformation provided by SD-WAN, these organisations will struggle to keep pace with the innovations enjoyed by 80% of the market. Yet if SD-WAN cannot support the specific security demands of regulated, data sensitive environments, what are the options?

Paul German, CEO, Certes Networks, explains how Certes' High Assurance SD-WAN framework uses crypto-segmentation to enable organisations in all industries to exploit the benefits of SD-WAN, while ensuring data integrity and confidentiality.

Missed Opportunity

The upsides of SD-WAN are significant, especially given the growth of IoT and need for unlimited connections from multiple locations. The software-defined networking approach offers agility and flexibility. It is cost effective – massively so when compared to the MPLS connectivity alternative. For the vast majority of organisations, the ability to create a virtual network over the Internet delivers the same user experience at a lower cost point while also supporting innovation and enabling the rapid evolution of cloud transformation strategies. It's a win: win.

For a significant minority, however, the benefits of SD-WAN are tempered by security concerns. Regulation is affecting an increasing number of industries as well as public organisations – and it is estimated that for around 20% of the market additional protection is required to achieve regulatory compliant SD-WAN adoption.

Regulated organisations are compelled to ensure the integrity of sensitive data as it travels across a network environment and that demands a number of key security principles that basic SD-WAN deployments do not offer. Not only are government bodies, financial institutions and healthcare operators compelled to invest heavily in additional security resources, but they are also missing out on the significant operational benefits SD-WAN can offer.

Overcoming the Stand-Off

The frustration of network teams keen to explore and exploit the value of SD-WAN is tangible but standard SD-WAN deployments do not meet the more stringent security demands associated with handling sensitive data. Data Protection Officers (DPOs) and Chief Security Officers (CSOs) will continue to resist the business' drive to exploit the cost and agility benefits of the internet for fear of compromising sensitive or confidential data.

And for good reason. While a SD-WAN overlay looks private, ultimately there is still a public internet connection plugged in to a business that holds both sensitive and non-sensitive data. There is a very real risk that a regulated business could inadvertently end up with sensitive data on the public internet, through configuration errors or software bugs, and incur a significant regulatory breach in the process.

Furthermore, the sheer flexibility in cloud deployment enabled by SD-WAN adds to the risk – especially for organisations with multiple branch locations. Using break out, the data created in SaaS tools such as Office365, Salesforce, and so on, is pushed directly onto the internet rather than directed to the corporate data centre. However, while this fire and forget model is hugely efficient, is it also risky: what happens if the break out policy accidentally includes sensitive data?

High Data Assurance

Enter Certes' High Assurance SD-WAN framework, which introduces another overlay technology that specifically targets the protection of sensitive data within regulated organisations by using crypto-segmentation to ensure the integrity and confidentiality of sensitive data. The overlay approach supports the regulatory demand for separation of duties: the network team can configure the SD-WAN, while the data security team uses fine grained policies to define the way different data categories are handled across the network with ownership linked to specific encryption keys. The underlying network has no visibility of either the data or its classification.

It is no wonder there is a stand-off between network teams pushing the benefits of SD-WAN and security teams insisting the risks are too high. If organisations are to maximise the financial and operational benefits offered by SD-WAN while still meeting their regulatory security requirements a more robust approach to data assurance is required.

> *Without access to the agility, flexibility and support for cloud-based transformation provided by SD-WAN, organisations will struggle to keep pace with the innovations enjoyed by 80% of the market.*
>
> **Paul German, CEO, Certes Networks**

This also reinforces the essential Zero Trust approach to the underlying network infrastructure – with High Assurance SD-WAN organisations no longer have to entrust the network carrier with responsibility for data security. Whether the network is public or private, trusted or untrusted, is irrelevant: the data security team simply needs to define the policy and, with ownership of the cryptography keys, can be confident that data is protected at all times wherever it goes.

In addition, visibility of key security metrics provides real-time insight into the cyber assurance posture, while integration between key cyber security functions uses this visibility to enable the organisation to efficiently react and remediate out-of-compliance events.

Conclusion

Regulation is increasing globally, and growing numbers of organisations are now facing up to demands to add new layers of protection for sensitive data. Without high data assurance, these organisations will not be able to maximise the value and flexibility of SD-WAN; indeed for those who have already made the move to SD-WAN, additional compliance demands could create huge concerns within security teams.

The availability of a simple to define and deploy high data assurance solution for SD-WAN totally changes the situation for those within regulated industries, de-risking the adoption of a low cost, flexible technology that can transform cloud-based and digital transformation strategies.

Contact Certes Networks

300 Corporate Center Drive, Suite 140
Pittsburgh, PA 15108

CERTES NETWORKS

Tel: 1 (888) 833-1142
sales@certesnetworks.com

www.certesnetworks.com