FLEXIBILITY VS SECURITY: WHY ORGANISATIONS CAN HAVE IT ALL

Why Organisations Can Have It All

Every organisation is on a mission to achieve agility; if 2020 & 2021 taught us anything, it's that the need to be flexible is essential in order to adapt and thrive in new and uncertain environments. The increased adoption of technology in all forms - from increased connectivity, to the cloud or collaboration tools for remote working - has greatly enabled organisations to achieve this. Powered by the adoption of software-defined wide area networking (SD-WAN) technology, organisations have been able to take advantage of this new-found flexibility, ease of management and ability to scale, but many have realised that the compromise to data security is too big a risk.

The dichotomy is real: ignoring the benefits that SD-WAN technology can bring only leads to dated and costly solutions being used for connectivity; not only impeding the ability to realise the real-world direct cost savings available with SD-WAN, but also limiting the scope for building the future-proof agile environment that's needed as part of any organisation's ongoing digital transformation. On the other hand, for the public sector and other highly regulated industries in particular, securing data has never been a simple task, but adopting an SD-WAN model has only highlighted that traditional security solutions are no longer enough. These solutions simply do not have the flexibility, performance or interconnectivity that SD-WAN connections require, and because of this, data is increasingly being left unprotected and vulnerable to malicious actors. The numerous data breaches that the industry has seen over the last few years are only proof of this.

Something clearly must change and organisations need to be able to deploy the benefits of SD-WAN with the confidence that the necessary controls are in place to ensure guaranteed levels of protection for high assurance data. As Paul German, CEO, Certes Networks, explains, a software-defined approach to data assurance will enable organisations to remain flexible and reap cost savings whilst ensuring their data is kept private and handled in accordance with compliance needs.

> *...a software-defined approach to data assurance will enable organisations to remain flexible and reap cost savings whilst ensuring their data is kept private and handled in accordance with compliance needs.*
>
> **Paul German, CEO, Certes Networks**

Turning Business Intent into Business Value

Business intent is defined by the key goals that an organisation sets out to meet with its data security strategy in order to achieve business value. For example, this could include being proactive to meet new and existing regulatory compliance requirements; being agile to move to hybrid environments; or being protected to keeping data secure and staying ahead of malicious actors.

Business value will be achieved when the organisation's data security posture is visible, scalable, observable, and above all, provable. In practice, a provable security strategy is quantifiable, measurable and outcomes-driven, and will turn data security into a strategic investment that mitigates risk and that delivers a quantifiable contribution to the overall value of the business.

Having the intention to make changes and meet business goals, though, is only one part of the process as there are numerous challenges to overcome in order for business intent to turn into business value.

Achieving Business Value Within SD-WAN

An example of business intent is an organisation moving toward SD-WAN and adopting Zero Trust as an approach to ensure their data is kept secure, whilst staying flexible. However, the challenge that stops business value from being reached in this example is that the separation of duties cannot be achieved when security protocols are tied into the network infrastructure, which is often the case when organisations have not yet adopted a network-agnostic approach to data security. Business value will be achieved by deploying a secure overlay that's agnostic to the underlying network infrastructure, giving security teams total control and visibility of the security posture.

Similarly, an organisation might have the aim of being agile and moving to a hybrid or SD-WAN environment, but the challenge of a disaggregated or antiquated network infrastructure will often mean that this intent cannot be turned into value for the business.

By decoupling security from the network, the organisation can be safe in the knowledge that the data will be protected wherever it travels. Furthermore, by matching security policies to business intent requirements, organisations won't be beaten by continuously evolving regulations, solving two challenges and delivering business value with a future-proof approach to data security as a result.

Overcoming these challenges with a provable security strategy that encompasses auditing and analytics and that automates cryptographic key rotation for each classification of business intent, ensures that even if a hacker is able to infiltrate the network, there will be no lateral movement between applications. And, with real-time monitoring of the data assurance posture, CISOs can react and remediate the attack at speed, greatly limiting any damage that could be caused and enabling business value to be achieved.

Making Flexibility & Security Entirely Possible

Ensuring that data remains secure should be front of mind when making any organisational changes, particularly when it comes to the adoption of new technology. There is simply no point in making the company's processes and operations flexible and agile to suit the new working environment if data is left vulnerable and open to compromise as a result.

But organisations don't have to choose between flexibility and security - both can easily be achieved with a strategy that not only overcomes the data security challenges presented by an SD-WAN environment, but that also provides value by achieving business intent. A software-defined data assurance strategy successfully delivers 'data first' security to ensure that data remains protected and is handled in accordance with compliance needs, whilst providing the ability to react and adapt to both external and internal changes as required.

It's a win-win, so now is the time for organisations to really consider the viability of an SD-WAN environment where data security is decoupled from the network in order to truly realise the benefits.

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