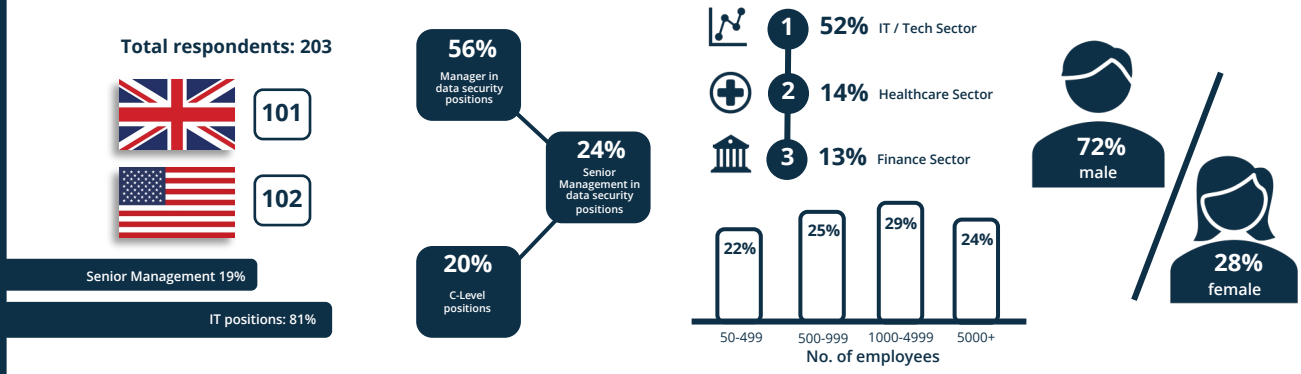
ASSURANCE VS SECURITY

Understanding SD-WAN Risks in High Assurance Industries

Executive Summary

The adoption of Software Defined Wide Area Networks (SD-WAN) has exploded in recent years as companies embrace the lower costs and flexibility to accelerate digital transformation. Yet SD-WAN deployments do not offer the assurances demanded by organisations operating within regulated industries. Standard SD-WAN deployments do not ensure the integrity of sensitive data as it travels across the network environment – leaving organisations with the choice of either leaving data unprotected and vulnerable to malicious actors or remaining with hugely expensive legacy WAN deployments. Neither approach is sustainable.

To understand how SD-WAN security is being approached by regulated organisations, Certes Networks commissioned Sapio Research to undertake a survey of Senior Decision Makers, Managers & above who are responsible for or involved in the management of their organisation's data protection in the UK and USA.



The results are disturbing. The true business impact of data loss is not understood and businesses are expecting service providers to bear the financial brunt of a breach – a situation accepted by the providers. Critically, despite ever tightening regulatory focus on data assurance, the market is still focused on network security, adding to the risk of breach.

This report assesses the SD-WAN deployment levels, as well as perceived strengths and weaknesses of its implementation; discusses the confidence placed in a simply regulatory-compliant approach, as well as the perceived risks; measures where perceived responsibility lies in the event of a data breach; identifies the security functions organisations with SD-WAN are currently able to enact, and as a result the gaps that still exist; and highlights how best to improve confidence and achieve high assurance data.

Escalating the Risk of Cyber Threat

The speed with which SD-WAN adoption has become ubiquitous underlines the acceleration in digital transformation across the world: 91% of companies confirm they have either started or finished SD-WAN implementation. Over half of respondents cite bandwidth efficiency as the key driver for SD-WAN implementation, followed by significant application performance improvement (47%), long term savings (45%) and WAN simplification (44%).

However, a quarter (25%) consider not sacrificing security and data privacy as a driver for implementation, which suggests a widespread lack of understanding, awareness and risk assessment surrounding current security postures. SD-WAN is not a data assurance technology – and for organisations operating in high assurance industries, standard deployments cannot meet regulatory requirements for data integrity.

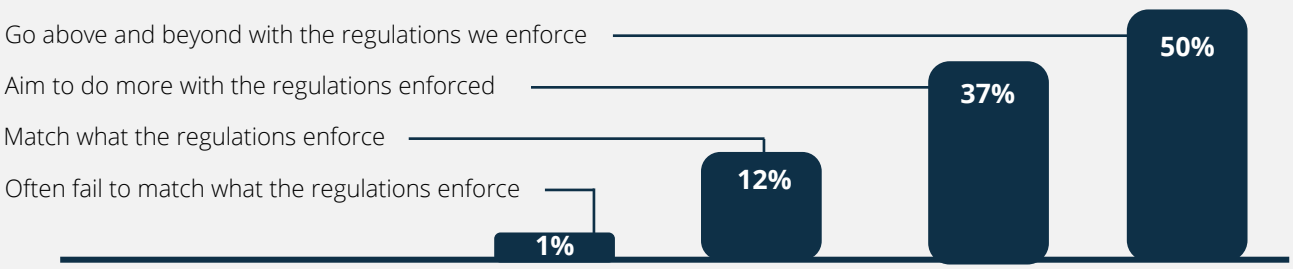
This is becoming a vital consideration in an era of rapidly escalating security breaches - including the growing threat of cyber war. The risk to power grids, water treatment plants, banks and communications networks has placed both private companies and public sector bodies on red alert. The resources behind state sponsored attacks radically raise the stakes, putting pressure on businesses to safeguard operations and regulators to intensify compliance requirements.

Confused Approach

It is interesting to note that there is a widespread awareness that regulation alone is not enough. Despite 96% being confident that regulatory requirements do provide sufficient support and guidance to protect against breaches, 87% also aim to do more or go beyond regulatory requirements. However, only half (50%) achieve this goal.

Meanwhile, almost three quarters (72%) believe there are risks involved in adopting an approach that focuses primarily on compliance first . 48% believe the main risk is that security regulations lag behind hackers' abilities, with 45% saying a threat assessment based on historical and industry data is not done and 42% believing it is a guideline on how to breach.

These responses highlight the confusion within the market. On the one hand, there is a fear that regulation doesn't go far enough. On the other, organisations are either wilfully or unintentionally overlooking the assurance limitations of SD-WAN in order to maximise the operational and cost benefits.



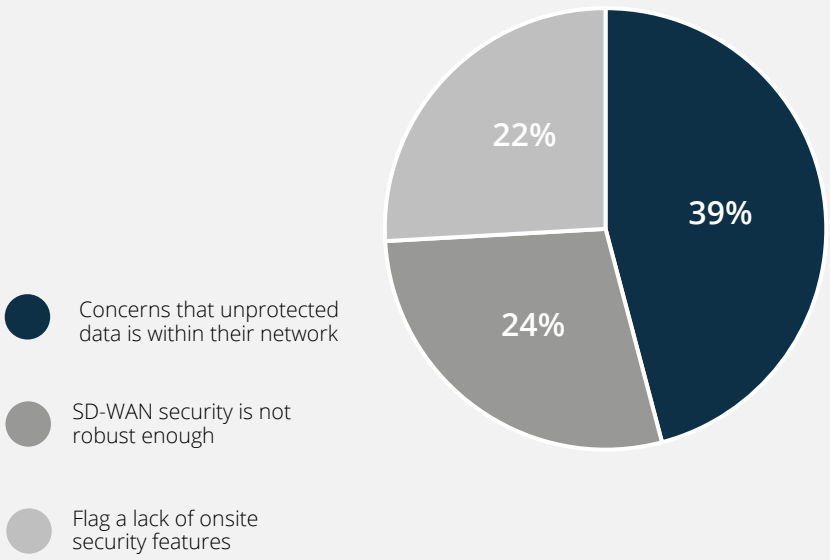
Moreover, far too many companies are failing to take into account the long-term business significance of a data breach. 40% say the financial impact in the long term is not considered, and only 33% consider the long-term business impact of data loss.

Reputational damage associated with a data breach, for example, is no longer limited to headlines and the need to ride out a few months' negative customer perception. For those organisations involved in high assurance markets – including companies supplying to regulated industries – a data breach will often lead to immediate contract cancellation and blocking from future engagement. Public bodies, utilities, banks and travel organisations will no longer accept the operational risk associated with suppliers that cannot safeguard data.

SD-WAN Risks Ignored and Misunderstood

This research confirms that a sizeable proportion of companies are aware of the data assurance limitations associated with SD-WAN. Almost two fifths (39%) highlight concerns that unprotected data is lying within a protected network. Almost a quarter (24%) say that SD-WAN security is not enough and that a data breach in one area could affect the entire organisation, while 22% flag the lack of onsite security features.

Certainly, the way SD-WANs have been deployed highlights the inadequacy of current security postures. Only two thirds (64%) are currently able to maintain network visibility and functionality with their security tools, and just 38% can segment their data cryptographically. Confidence would improve if these functions were in place: 81% of organisations would feel more confident if they were able to provide out-of-policy data visibility, and 71% more confidence if able to cryptographically segment data.



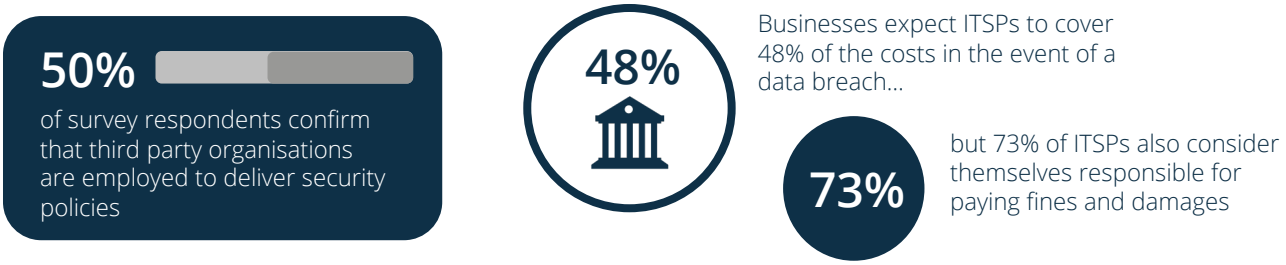
Open Network

There is good reason for the need for more confidence in the security posture. While a SD-WAN overlay looks private, 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, any businesses that partner with or supply to regulated industries – especially utilities and government – are becoming key targets for hackers looking for another route into organisations that have already deployed a high assurance data security model. Adding the sheer flexibility in cloud deployments, the use of local break-out to push day-to-day data created in SaaS tools such as Office365 or Salesforce directly onto the Internet rather than directed to the corporate data centre further adds to the risk. What happens if the local break-out policy accidentally includes sensitive data?

Abdicated Responsibility for Data Assurance

Despite the acknowledged risks, too many organisations are simply handing over responsibility to an IT Service Provider (ITSP) or Managed Services Provider (MSP) – and expecting the provider to pick up the financial cost should a data breach occur. Almost 50% of survey respondents confirm that third party organisations are employed to deliver security policies. Businesses expect ITSPs to cover 48% of the costs in the event of a data breach – but 73% of ITSPs also consider themselves responsible for paying fines and damages, and believe they should pay 51% of the costs.



Simply relying on a contractual agreement for financial remuneration totally misses the fundamental operational risk associated with inadequately assured SD-WANs. But this approach also highlights the confusion between network security and data assurance that dominates the industry, especially within high assurance markets. Companies need to take ownership of their data. Yes, an MSP or ITSP running the SD-WAN will put in place standards to secure the network infrastructure – but who is protecting the data and how?

Open Safe

To put it into context, just because an individual has employed a security company to alarm and monitor a house doesn't mean that company will be given carte blanche access to that house, or keys to the front door and safe. But that is the dominant model for data assurance today within far too many organisations. Monitoring is essential, retaining the integrity and capability of protecting valuable assets – whether personal possessions or corporate data – can only be achieved by limiting access to the keys.

The current approach makes no logical sense for companies – and no financial sense for ITSPs. Any data breach will incur not only immediate financial costs but long-term business consequences that could be terminal – for both parties. Regulated businesses will not just block a supplier that has been breached, but more than likely its MSP or ITSP as well.

Yet even those organisations that appear to have understood the difference between data assurance and network security and have crafted assurance policies, are failing to recognise the risk of not taking ownership of their data. Handing over responsibility to a third party to monitor and deliver that assurance posture is effectively abdicating control – and that is a risk.

> *"By focusing only on security, businesses are misled: they believe a secure network is an assured network. Just because you have a secured message does not mean you have assured data. Network Security is not Data Assurance,"*
>
> **Paul German, CEO, Certes Networks**

Regulatory Disconnect and Zero Trust Confusion

This continued focus on network security rather than assuring vital data is at odds with the goal of regulators. Security regulation is totally focused on data assurance, on safeguarding essential information assets. The solutions traditionally deployed to comply with regulation, however, are about network security, a misguided focus that has left data unassured.

From firewalls to gateways, the goal has been to secure the network, not protect the data. And while many companies might immediately point to the rapid adoption of a Zero Trust approach – the assumption that the network has already been compromised – the reality of the way security postures are deployed fundamentally undermines the regulatory goal of safeguarding data.

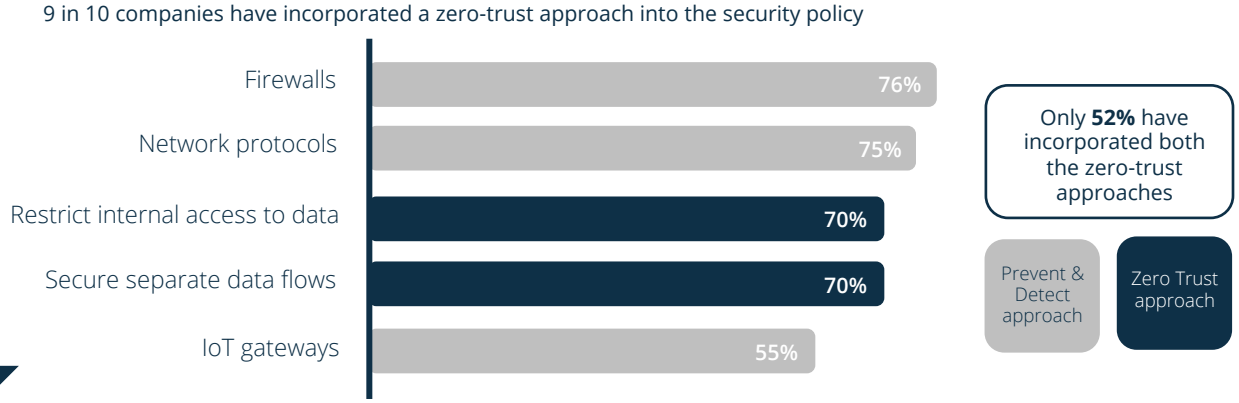
Almost nine in ten (89%) of companies have adopted some aspects of a Zero Trust approach – 70% restrict internal access to data and applications and 70% securely separate data flows between applications. 52% have incorporated both approaches. In practice, however, these organisations are still failing to achieve data assurance which is fundamental within high assurance environments .

The network security model is about locking valuable assets in a box. The Zero Trust concept assumes there is no trust in any infrastructure, indeed that the locked box has already been compromised. The result is that the sensitive assets in that box are not protected (assured) – which means the assurance posture is broken from day one.

> *"You can't have a Zero Trust approach yet trust network security to assure your data – because you are working on the premise that your network has already been compromised."*
>
> **Paul German, CEO, Certes Networks**

Taking Control to Achieve Data Assurance

High Assurance SD-WAN introduces an overlay technology that specifically targets the segmentation and 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 protection team uses fine-grained policies to define the way data is handled across the network with ownership linked to specific encryption keys. The underlying network has no visibility of either the data or its classification nor is it impacted in terms of performance of operational visibility.



Critically, it provides an organisation with control over the assurance of its data. With High Assurance SD-WAN, organisations no longer have to entrust the ITSP with responsibility for data assurance. Whether the network is public or private, trusted or untrusted, is irrelevant: the organisation's data protection team simply needs to define the policy and maintain ownership of the cryptographic keys, resulting in the confidence that data is always protected 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.

9 in 10 companies have incorporated a zero trust approach into their security policy

72% believe there are risks involved in adopting an approach that focuses primarily on compliance first

The main drivers for implementing SD-WAN is bandwidth efficiency and significant application performance

IT Service Providers feel that they should pay 51% of the costs in the event a customer asks them to take responsibility for a data breach

87% aim to do more or go beyond what the regulations enforce when defining their security policies

1 in 3 see the main pain point of implementing SD-WAN to be the need for skilled staff

With this approach, high assurance businesses can take ownership of their data, and remove their reliance on ITSPs and MSPs. The service provider will enable the digital transformation and flexibility through excellent SD-WAN services, while the business retains control over its data.

> *"Service providers should not be responsible for a customer's data,"*
>
> **insists Paul German, CEO, Certes Networks**

In Conclusion: Overdue Mindset Shift

As this research confirms, despite the awareness of regulatory shortfall, there is still a massive disconnect between the current focus of security postures and the reality of the risk exposure. Companies have been handing over responsibility for implementing and delivering their security posture for years; they have continuously pushed the blame across to another organisation. That is no longer acceptable – for organisations in high assurance markets, or supplying high assurance operations, there is no longer any tolerance for data breach.

Service Provider Response

There is also a role for service providers in driving change. Service providers need to mitigate their risk by giving customers the ability to assure their own data. By providing an assurance service where the customers own and control the keys and policies protecting their data, MSPs and ITSPs can drive this change in dialogue. As trusted advisers, these organisations are best placed to explain the data ownership model to organisations and reinforce the vital imperative of businesses retaining ownership, control and assurance of their data.

> *"The move to SD-WAN can be done in a way that provides a level of assurance but today the SD-WAN technology is just focused on connectivity and network security, not assurance of the customers' data. That attitude needs to change urgently,"*
>
> **concludes Paul German, CEO, Certes Networks**

It is only once the responsibility for data assurance is understood by all parties, that the correct steps will be taken to maximise the power of SD-WAN to accelerate business change while mitigating the risk down to the lowest acceptable level.

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