Swot analysis of vpns for business: the importance of encryption

Business

In this article we look at the best VPNs for your business. Plenty of high-quality publications, like Forbes, are now beginning to advise the business world about the importance of utilizing cybersecurity products in order to encrypt and lock down their data in order to promote a secure workplace.

What do we mean by business VPNs? The terminology can be rather confusing, not least because there are no standardized uses of the term business VPN.

It can refer to traditional corporate VPN intranets, which allow remote workers to access company resources in a secure way. Alternatively, it can refer to bulk VPN licenses that can be deployed by businesses in order to provide their staff with the benefits of a personal VPN.

Setting up a corporate VPN intranet is expensive and requires constant monitoring by a team of IT professionals. For this reason, it is very much an in-house affair.

This article deals with the second type of business VPN, although some innovative new services are now combining the low costs and cloud-based flexibility of a personal VPN service with traditional corporate intranet VPN connectivity.

Strengths

Sensitive data is encrypted when remote workers connect to the internet over insecure public WiFi. This is because the connection between their devices and VPN server is encrypted. Remember, it’s not just criminal

hackers that you need to watch out for – if anything, unreliable WiFi hosts are an even bigger danger.

A few VPN services offer greater functionality for businesses. This includes the ability to create private VPN servers on-the-fly and assign team members to different servers with different privilege levels.

Depending on the service, it may even be possible to connect these private servers to corporate LAN, cloud, and IoT resources with granular access for each team member.

Weaknesses

Most commercial business VPN packages are simply bulk-license private VPN plans.

Getting team members to actually use the VPN when connecting to insecure networks may be an issue, although some business VPNs allow you enforce automatic VPN activation whenever a team member connects to an unknown or untrusted network.

Opportunities

The main advantage of most business VPN packages is to ensure that remote workers do not compromise sensitive information when using public WiFi networks. A VPN will also prevent their domestic ISP from being able to see company data.

More advanced business services, which allow you to connect private servers to corporate resources, have the potential to provide similar functionality to

traditional corporate VPN intranets, but at a fraction of the initial cost and upkeep such intranets usually require.

Threats

As always, when using a commercial VPN service, a certain amount of trust is required in the VPN provider who might be able to see sensitive data as it passes through its servers.

This issue can be mitigated against to some extent by creating private on-the-fly private VPN servers, but these software-based private servers will not be as secure as bare-metal servers run directly by a VPN provider.

Image “ VPN / DNS” by Richard Patterson is licensed under CC-BY 2. 0