WHY SHOULD I ENCRYPT MY DATA?

When news about e-mail marketer Epsilon's data breach hit the streets, people were both surprised and concerned. How many other businesses out there have been using third party sites to handle their customer information? The reality is that…It's a lot. Given the global size of networks out there today, companies are forced to utilize third party carriers. In doing so, these third party service vendors introduce additional vulnerabilities.

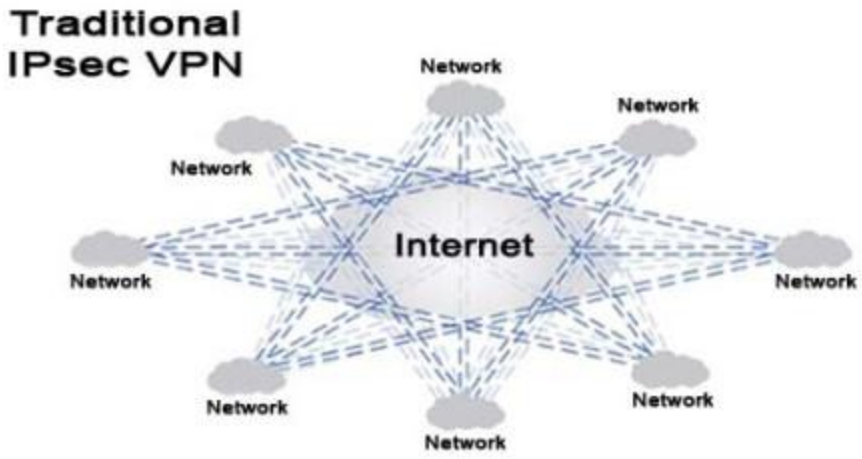
Even if third party vendors aren't used, more and more organizations are using the Internet to send data to branch offices. Authentication is critical, but many companies don't encrypt their data because it's traveling on a "safe" MPLS network. Although MPLS networks provide more reliable connections than the Internet and aren't as public, you can't put all your eggs in the MPLS basket.

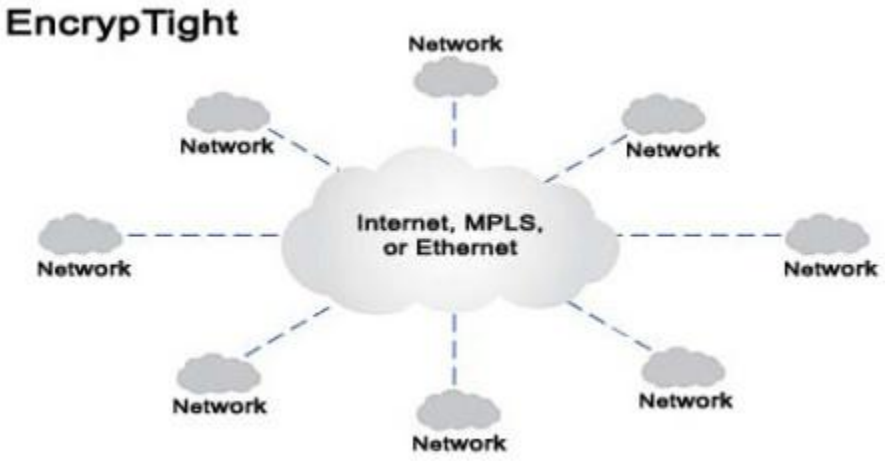
When vendors say MPLS is secure, what they mean is that the traffic is kept separate from other traffic. Separate data is not the same as data security, and separate traffic is even easier for hackers to attack. The vendor might have processes in place to prevent unauthorized data snooping, and tell you that their employees probably aren't going to snoop either. In fact, your data probably won't be stolen on an MPLS network, but you have no way of being sure and no way to tell if your data has been breached.

The only way to ensure data security over an MPLS network is by encrypting data as it travels across the WAN. This is accomplished through a traditional IPsec VPN. Although this approach is fairly simple to set up between only two points, when remote sites multiply, the number of tunnels increases exponentially. A tunnel is needed between each pair of sites, leading to administrative hassles every time a remote site is

added. With growth comes the addition of personnel, router and re-structuring costs. Not to mention, a lag in network performance.

Enterprises can stop bleeding money and still deploy network-wide data protection without compromising performance. EncrypTight™ is an encryption solution that overcomes the limitations associated with IPsec VPN tunnels. It brings you air-tight encryption across a WAN—even the Internet—without the hassle of setting up a VPN tunnel for each connection. Plus, EncrypTight doesn't add latency to bog down network operations—it's totally transparent. The "stealth" Layer 4 encryption capability leaves packet headers intact, making encrypted data far more compatible with network operations.





Because there are no tunnels to set up, it’s easy to deploy EncrypTight across large WANs. For instance, an organization with many sites around the world could add a new site to its WAN without having to establish a VPN tunnel to every other site.

Additionally, EncrypTight Management Software enables network administrators to centrally manage security across the entire WAN using a simple drag-and-drop interface. A company's headquarters in the United States can have all the control over encryption polices and key generation and distribution, but still protect sensitive data being transported to branch offices in Europe and Asia.

Source: https://bboxblog.wordpress.com/2011/05/16/why-should-i-encrypt-my-data/