SSL/TLS SECURITY

A recent independent survey conducted among IT professionals revealed that over 80% of organisations have been victims of cybercrime over the course of one year, and over 40% of malware used encryption to evade detection.

Transport Layer Security (TLS) and Secure Sockets Layer (SSL), both usually referred to as SSL, are a popular technology for public-key encryption used to secure communications between the client and the server. Although TLS is a newer version of the technology, security experts and internet users have become so accustomed to its predecessor that its name, SSL, is still used as a general term defining both versions of the protocol. In this article, we'll stick to that too.

SSL is hugely popular. You use SSL every time you enter an online bank to check your credit card balance, make a payment via PayPal or send an email to your business partner. If you see a padlock sign in the status bar of your browser, you can be sure that you're using SSL.

However, even being the most widely used encryption protocol, SSL has its vulnerabilities, which can pose major risks to valuable corporate data. To detect any malware that has penetrated your organisation before it's too late, you need to analyse all the traffic that comes in and out of your company's servers. In our brief guide, we'll discuss how to see into the encrypted traffic and protect your business from cybercrime.

How to Deal with SSL Threats

Unfortunately for many enterprises that use SSL, the latest malware knows how to hide in the encrypted SSL/ TLS traffic without being noticed by security tools or having any visible impact on the network's performance. As a result, making this traffic visible is the first and the most important step. The most efficient solution to the problem is provided by SSL inspection platforms that decrypt traffic and forward it to security tools for analysis. These tools may include:

+44 20 7183 5820

info@magora.co.uk
sales@magora.co.uk

- **Malware detection tools:** intrusion detection and prevention systems (IDS/ IPS), next generation firewalls (NGFW) and other common security tools use decrypted traffic to scan the system for malware and threats.
- **Data loss prevention software:** you may not realise it, but malware or users of the network themselves may export confidential information on your business through SSL connections. Command and control (C&C) networks take advantage of the SSL “blind spots” to control Trojans that are used to steal banking information and other confidential data. It’s impossible to detect them without access to decrypted traffic.
- **Cloud service monitoring tools:** various web-based apps and the cutting-edge Internet of things (IoT) technologies all run in the cloud, protected by SSL. To monitor their performance and scan them for malware, you also need to see inside sessions that all look the same because of encryption.
- **App performance monitoring systems:** most business apps use SSL for user authentication, which means that once again you need to analyse the decrypted traffic if you want to detect any unusual behaviour and ensure timely reporting on suspicious activity within your apps.

As you can see, many cyber attacks are cloaked in SSL. With new, more advanced malware appearing every day, it’s high time you invested in data security. The great news is we’re here to help. Experts at Magora can craft a bespoke SSL inspection platform based on the specific security needs of your organisation and advise you on the best data protection strategies.

+44 20 7183 5820

info@magora.co.uk
sales@magora.co.uk