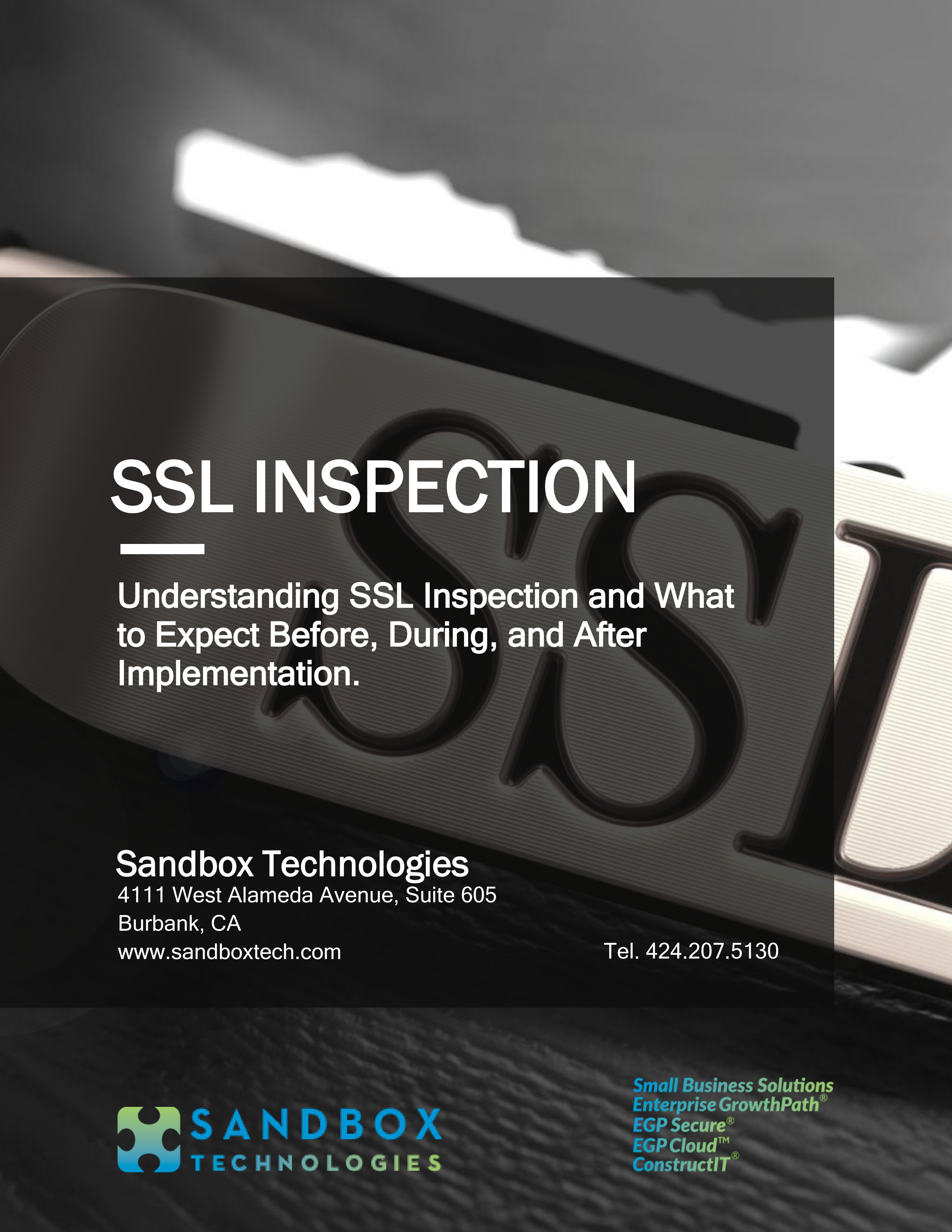

SSL INSPECTION

Understanding SSL Inspection and What to Expect Before, During, and After Implementation.

Sandbox Technologies
4111 West Alameda Avenue, Suite 605
Burbank, CA
www.sandboxtech.com
Tel. 424.207.5130

SSL Inspection

Before understanding SSL Inspection, it is important to first understand Secure Sockets Layer, or “SSL”. SSL is an encryption technology used to secure connections between Web servers and remote computers as users engage in activity on the Internet. SSL encryption is widely used, and strongly recommended as a means of preventing the interception of communication by malicious actors.

Why SSL Inspection?

A caveat to SSL encryption is that, while it is an effective deterrent to online eavesdropping, it renders most corporate firewalls incapable of inspecting encrypted communications for the presence of viruses, malware and other threats.

Because malicious actors are aware of this limitation, an increasing number of attacks seek to circumvent protections by deliberately transmitting malware via encrypted connections.

This problem is what precipitated the needs for SSL inspection. SSL inspection essentially works by intercepting communications as they transit an organization’s firewall and replacing the user’s encryption key with its own key, thus rendering it capable of inspecting encrypted traffic and taking the appropriate protective action(s) when a perceived threat is identified.

Mitigation of Issues and What to Expect

Despite the importance of SSL inspection, IT Administrators are sometimes hesitant to implement it. Although not unreasonable, the most common reservations can be overcome with the proper planning and preparation.

The performance of some firewalls that offer SSL inspection can be noticeably slower when the feature is enabled. To mitigate this drawback, Sandbox Technologies recommends the use of a firewall that employs a dedicated chip for the purpose of performing SSL inspection at a faster rate of speed.

Perhaps the next most common reservation expressed about employing SSL inspection is that high security websites (e.g., Banking, and similar institutions) often utilize advanced methods to detect and prevent the interception of encrypted communications. Consequently, there is a risk that communication with important websites could be initially disrupted. For the most part, this problem can be mitigated by making proactive inquires prior to implementation, identifying relevant sites, and exempting them from inspection.

Encrypted threats are here to stay. While it’s normal for a site or two to be overlooked initially and for occasional problems to occur, with the proper implementation and planning, the positives of adopting SSL inspection vastly outweigh the drawbacks. For this reason, SSL inspection is one of the most highly recommended protections for today’s threat landscape.

For additional information, contact your Sandbox Technologies Engineer, Account Manager or Consulting CIO, or send an email to inquiries@sandboxtech.com.