Enterprise firewalls have been forced to adapt to the new security challenges that come with digital transformation and a growing remote workforce. One critical challenge is the demand for greater data throughput that uses Transport Layer Security (TLS) or Secure Sockets Layer (SSL). Today, enterprise firewalls must do more, which requires expanded functionality and improved performance.

Selecting the right firewall vendor, with the right capabilities, is critical for realizing a secure and productive enterprise now, and into the future. Here are a few distinguishing factors that every infrastructure and cybersecurity leader must look for:

1. **What happens when Fortinet’s FortiGate is put to the test?**

   In the NSS Labs Next-Generation Firewall (NGFW) Group Test, the results speak for themselves.

   **Proven FortiGate**

   - HTTPS SSL/TLS isn’t just nice to have – it’s a standard.
   - According to our survey, more than 90% of Fortinet customer traffic is HTTPS.

2. **Performance levels before SSL is applied are never the same as after SSL. Make sure you are comparing apples with apples by putting firewalls to the test.**

   - Exploits and threats are not constant and continue to grow internationally.
   - Interestingly, vulnerabilities first discovered in 2018 claim the highest exploitation prevalence (65%), indicating organizations are not updating and securing their systems.

3. **As threats and exploits expand, so must the firewall**

   - The FortiGate security effectiveness rating is also the highest in the industry.
   - To learn more about Fortinet FortiGate go to [https://www.fortinet.com/products/next-generation-firewall](https://www.fortinet.com/products/next-generation-firewall)

   The Fortinet Security Fabric secures organizations across the globe with the largest security device footprint in the industry. This unique advantage provides an unparalleled view across the cyber-threat landscape, providing key insights into how to best defend organizations from emerging and evolving threats.