Written by Frederick Douglas
20 April 2018

British security vendor Sophos has a few "dirty secrets" to reveal on the state of firewalls in enterprise-- IT managers cannot identify 45% of network traffic, and 25% of managers cannot identify 70% of traffic.

Such findings come from "The Dirty Secrets of Network Firewalls," a global survey of 2700 IT decision makers from mid-size businesses in 10 countries, including the France, Germany, UK, US, Canada, Australia, Japan, India and S. Africa. It shows 84% of respondents agree a lack of application visibility is a serious security concern, but firewalls with signature-based detection do not provide adequate visibility into application traffic. This is due to the increasing use of encryption, as well as browser emulation and advanced evasion techniques.

“If you can’t see everything on your network, you can’t ever be confident that your organisation is protected from threats. IT professionals have been "flying blind" for too long and cybercriminals take advantage of this,” Sophos says. “With governments worldwide introducing stiffer penalties for data breach and loss, knowing who and what is on your network is becoming increasingly important. This dirty secret can’t be ignored any longer.”

According to the company, organisations spend 7 working days remediating 16 infected machines per month. Smaller organisations (100-1000) organisations spend around 5 days remediating 13 machines, while larger organisations (1001-5000) spend 10 working days on 20 machines per month. A single network breach can easily compromise multiple computers, and recent exploits such as MimiKatz and EternalBlue serve as reminders network protection is critical to endpoint security, and vice versa.

Such issues lead a lack of network visibility and lost productivity, as stated by 52% of survey respondents. IT can hit productivity if it cannot prioritise bandwidth for critical applications, even

more so in the case of industries using custom software to meet specific business needs. In addition, a lack of visibility creates a blind spot for the potential transfer of illegal or inappropriate content on corporate networks, making companies vulnerable to litigation and compliance issues.

Another survey finding points out a business opportunity-- 79% of IT managers want "better protection" from their current firewall, 99% want firewall technology able to automatically isolate infected computers, and 97% want endpoint and firewall protection from the same vendor allowing direct sharing of security status information.

“Organizations need a firewall that protects their investment in business-critical and custom applications by allowing employees to have prioritized access to the applications they need,” Sophos concludes. “Increasing network visibility requires a radically different approach. By enabling the firewall to receive information directly from the endpoint security, it can now positively identify all applications – even obscure or custom applications.”

Go The Dirty Secrets of Network Firewalls