TOP 6 DANGERS OF NOT INSPECTING SSL TRAFFIC

By 2016, it's estimated that 67 percent of Internet traffic will be encrypted.[1] Although encryption can be used for good—improving message confidentiality and integrity—it can also be used as a means to conceal hackers' activities. Without SSL inspection in place, your business could fall victim to the kind of encrypted traffic that has malicious intent behind it.

SSL TRAFFIC IS ON THE RISE

29.1% of traffic was encrypted in 2015
67% of traffic will be encrypted in 2016
100%? of traffic will be encrypted in future

2015 2016 Future

INVESTMENTS ARE FALLING SHORT, LEAVING GAPING HOLES IN CORPORATE DEFENSES

$73.3 BILLION
was spent on information security worldwide in 2014[2], yet organizations still suffered over 2,000 data breaches[3]

LESS THAN 20%
of organizations with a firewall, an IPS or a UTM appliance decrypt inbound or outbound SSL traffic[4]

IN 2017 MORE THAN HALF
of the network attacks targeting enterprises will use encrypted traffic to bypass controls[5]

PERFORMANCE CAN DROP 75%+
for firewalls when decrypting SSL traffic

HOW ATTACKERS ARE HIDING IN ENCRYPTED TRAFFIC

3 MALICIOUS FILE IN INSTANT MESSAGING

4 COMMAND AND CONTROL SERVER COMMUNICATION

2 DRIVE-BY DOWNLOAD FROM AN HTTPS SITE

5 STOLEN DATA SENT VIA EMAIL OR TO CLOUD STORAGE SITES

1 MALICIOUS ATTACHMENT SENT OVER SMTPS

6 MALWARE RECEIVING C&C UPDATES FROM SOCIAL MEDIA SITES

WHAT BUSINESSES CAN DO TO EXPOSE THREATS

A **dedicated SSL inspection platform** gives businesses the **power to decrypt and analyze traffic**—to protect key systems and data.

UNCOVER HIDDEN THREATS

MAXIMIZE UPTIME

PREVENT DATA BREACHES

GAIN VISIBILITY WITHOUT DEGRADING NETWORK PERFORMANCE

Find out how A10 Thunder® Application Delivery Controller (ADC) with SSL Insight™ Technology can help your organization defend itself against malicious encrypted traffic.

Call **1-408-325-8616** or visit **a10networks.com/contact-us** today.