Surging traffic, rising concerns

Concern regarding the influx of SSL/TLS encrypted traffic is rising, according to an IDC survey of IT professionals.

What’s driving encrypted traffic?

35%

TOP ENCRYPTED TRAFFIC DRIVERS

- Increased SSL/TLS use on social, webmail, and web sites
- Growth of regulated data
- Web applications
- SaaS backup and recovery solutions

What’s hiding in your encrypted traffic?

25%

ATTACKERS USE ENCRYPTED TRAFFIC TO:

- Escape notice from intrusion prevention systems, security gateways, and other network-based anti-malware solutions.
- Hide data exfiltration or the removal of stolen data such as account credentials, credit card data, and intellectual property.
- Shield botnet command-and-control communication so attackers can move laterally within an organization.
- Utilize stolen keys and digital certificates to trick servers and security solutions that trust these credentials.

The paradox of encrypted traffic

0%

Some security devices can’t keep up with encrypted traffic, while others are unable to encrypt it.

Protect your business

1. Reduce encrypted communications’ regular weight with a single step.
2. Ensure network devices can keep up with encrypted traffic.
3. Prevent attacking by encrypting traffic at the source.
4. Secure applications with SSL/TLS integration.
5. Leverage your security investments for value.
6. Greater visibility and control.
7. Reduce total cost of ownership.
8. Consider additional SSL/TLS management tools for more comprehensive protection.
9. Consider a complete SSL solution on any secure web traffic.

To learn more about advanced threat detection strategies, download the IDC white paper, “The Blind State of Rising SSL/TLS traffic: Are Your Cyber Threats Visible?,” sponsored by F5 Networks.