

TLS Adoption Research

What We Found After Studying 275B Flows of Real-World East-West and North-South Traffic

What encryption technologies are organizations seeing in their networks, both in north-south and east-west traffic? This document highlights the finding of our research into that question, and the answer is important.

The wide adoption of SSL/TLS underscores the criticality of inspecting encrypted traffic. East-west traffic visibility is needed for multiple reasons: Detection of laterally moving threats (threat actors are adopting the use of encryption in their attacks); compliance with governance standards that mandate data protection; accurate performance measurements; and finally, faster troubleshooting. All of these require inspection of encrypted traffic.

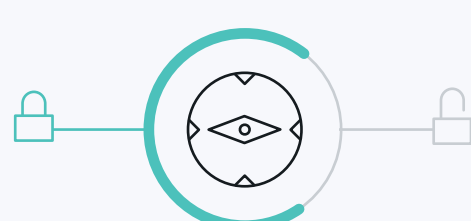


Production Traffic Data



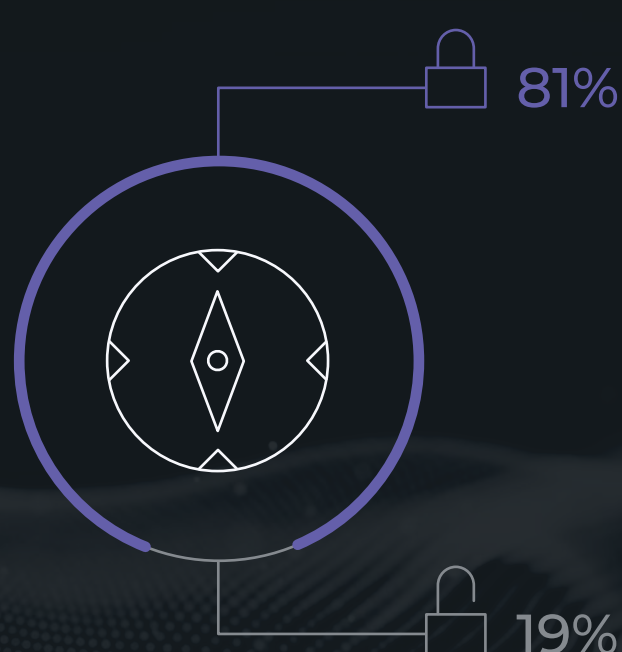
106,061,628,564

North-South Flows



168,681,684,427

East-West Flows

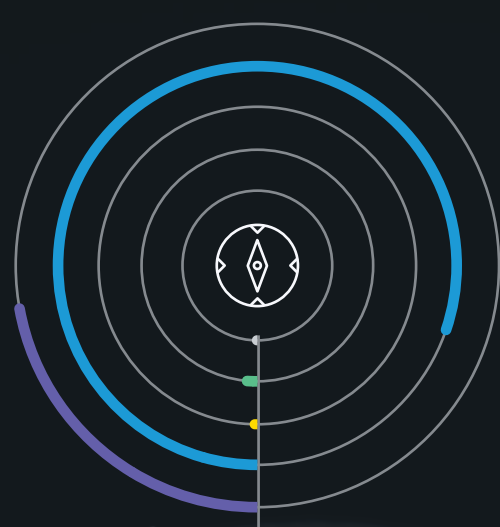
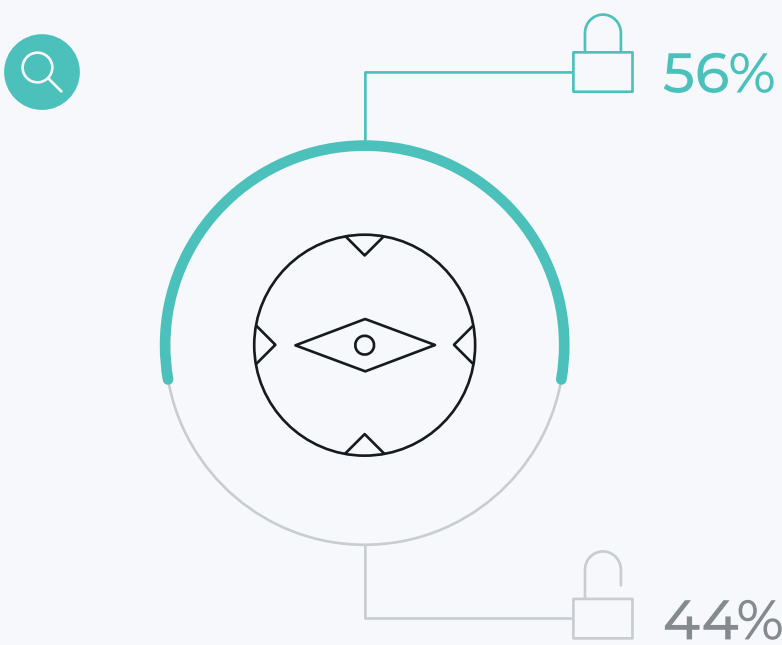


81% of North-South Traffic Is Encrypted

Overwhelming amount of encrypted traffic underscores the importance of decrypting and inspecting this blind spot.

44% of East-West Traffic Is Not Encrypted

Encrypting all feasible east-west traffic is an opportunity for organizations to improve security posture.



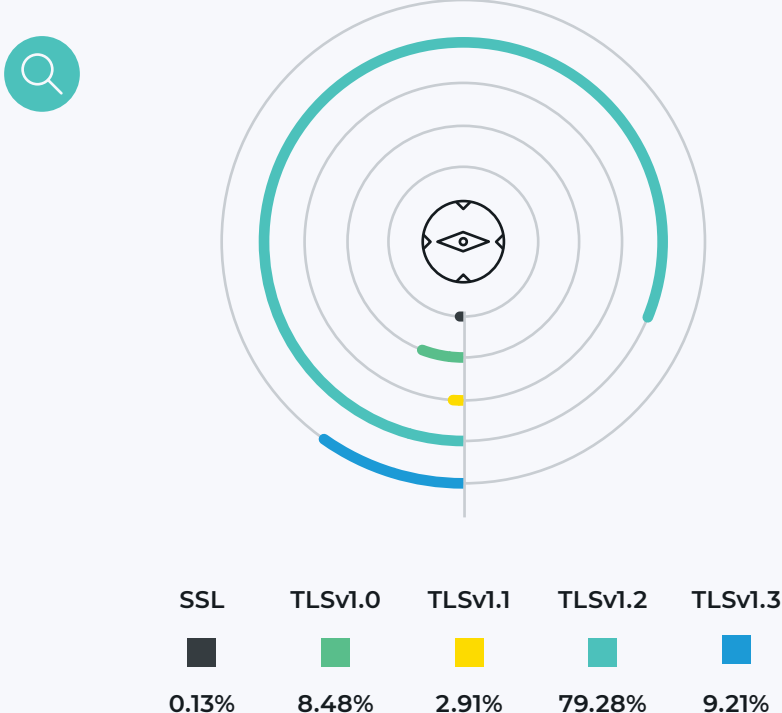
TLS 1.3 Is Off to a Strong Start in North-South Traffic

TLS 1.3 may require some reworking of tool deployment architecture, but allowing this traffic through uninspected poses an increasingly greater risk.



TLS 1.2 Dominates East-West Traffic

Use of outdated protocols poses an unacceptable risk and must be addressed.



SSL Lives – Securing Likes It’s 1999



SSL Encrypted Traffic
0.04%

Total Flows Across Data Set
42,424,651



SSL Encrypted Traffic
0.13%

Total Flows Across Data Set
219,286,189

Read the [report](#) for more findings and actionable TLS inspection recommendations.

Gigamon®