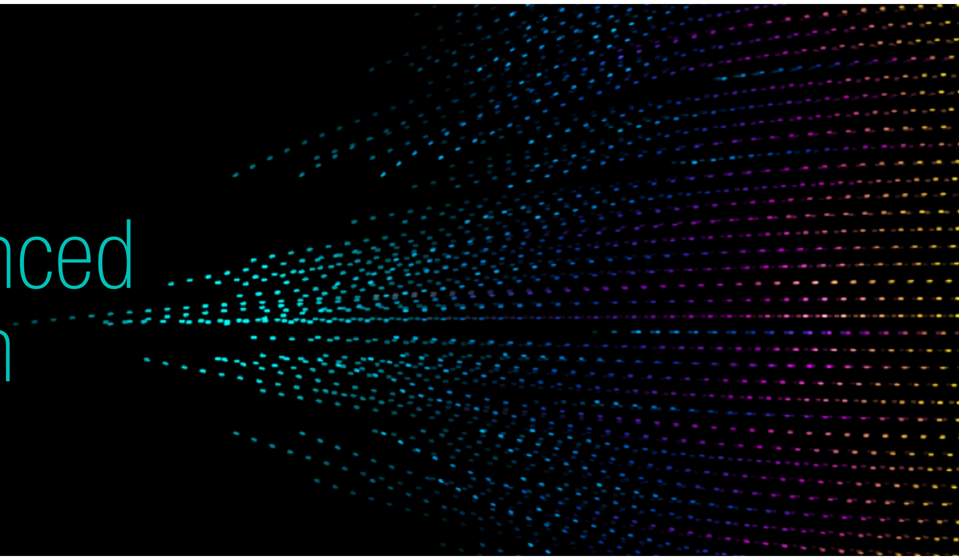
SYNNEX Westcon

Transform Advanced Threat Detection



What is SSL Decryption?

SSL encryption transforms sensitive data into an unintelligible, unreadable "ciphertext." Cybercriminals exploit SSL encryption by camouflaging malware into encrypted data with the intent of executing on the server and infecting the end point or other network systems. Malware makes it back to the end point because SSL decryption features are frequently not turned on to inspect the encrypted data coming back to the end point from the server.

What Are the Challenges?

FIREWALL STRAIN

SSL decryption takes valuable processing power, making the firewall less effective.

INEFFICIENCY AND OVERLOADING

Several different network monitoring appliances do not need to repeat the same decryption task.

INTERNAL THREATS

Encrypted communications that travel internally remain uninspected, a huge risk considering that internal communications may comprise some 80% of encrypted network data.

DATA COMPLIANCE

Without the correct safeguards in place, anyone with network monitoring tools can see personally identifiable information.

SYNNEX
WESTCON

How to Effectively Deploy SSL Decryption?

PROPER CONFIGURATION:

- Configure the firewall to handle traffic and place it in the network.
- Load or generate a Certificate Authority Certificate on the firewall.
- Configure SSL decryption rules.
- Enable SSL decryption notification web page (optional).

Refresh firewalls to be able to handle SSL Decryption feature (typically requires increased throughput).

Lean on SYNNEX for trusted white-glove configuration support.

How can SYNNEX help?

With our strong secure networking portfolio, specialization, and services offerings, SYNNEX serves as your trusted advisor to help ensure you and your customers are protected and well-positioned to defend sensitive data.

Email SecureNetworking@synnex.com to learn more, or click to join our "SYNNEX Westcon" Secure Networking Partner Enablement Portal.

Email Us

Join Our Portal