Set up decryption on an MS Exchange server

Published: 2024-04-02

SSL decryption is a powerful tool for increasing visibility into your network. The MS Exchange vulnerability, CVE-2021-26855, presents a compelling reason to set up decryption on Exchange servers. This vulnerability enables attackers to conduct server-side request forgery (SSRF) attacks by sending tailored HTTP requests over unauthenticated connections. These requests are usually encrypted over HTTPS, so the only way to know if a request contains those tailored instructions is to decrypt the HTTPS payloads.

By installing a session key forwarder on your Exchange server, you can ensure that ExtraHop can decrypt Exchange traffic safely. Because CVE-2021-26855 was exploited over HTTPS, we recommend that you specifically decrypt HTTP traffic by following the instructions in the following section: Add a global port to protocol mapping.

Learn more about SSL/TLS decryption.