

# What are the security considerations for TLS 1.3?

PCI SSC FAQ | Article 1461 | January 2019

---

Transport Layer Security (TLS) is a protocol that provides security over networks and is widely used for internet communications and online transactions. TLS version 1.3 introduces protocol changes that may improve security and performance while removing complexities and streamlining the protocol stack. These changes, however, also introduce new considerations for organizations using TLS for security controls.

Organizations implementing TLS 1.3 will need to ensure their implementation is properly configured. Factors to consider when evaluating a TLS implementation include the services and options enabled, the cryptographic algorithms supported, and the strength of the cryptographic keys used.

Organizations should also be aware that the features of TLS 1.3 could affect the functionality for some types of security solutions, such as those that rely on decryption to inspect the packets before they reach the endpoint. For example, organizations using web application firewalls and intrusion detection/prevention systems may find that these systems no longer function as expected, as they may not be able to analyze the encrypted TLS 1.3 connections. This may require changes in the way organizations satisfy certain PCI DSS requirements.

Additionally, devices that do not yet support TLS 1.3 may react differently when presented with TLS 1.3 encrypted traffic. The result could be that traffic is allowed to pass through without inspection, potentially leaving malicious payloads or activities undetected. Other devices could fallback to an earlier or insecure version of the protocol, resulting in data having a lower level of protection than intended. These issues may result in organizations needing to reconfigure or adapt their systems so that they continue to perform as expected.

As with all new technologies, organizations should evaluate and review the possible implications that TLS 1.3 may have on their environment. Organizations are encouraged to contact their security solution vendors to determine any potential impact and whether alternative configurations or other workarounds are recommended.

PCI SSC continues to monitor the evolution of security protocols and their impact on security solutions for the payment industry, and will keep stakeholders informed as updates become available.

Source: <https://www.pcisecuritystandards.org/faqs/1461/>