DUO for...

CISCO SECURE

PCI DSS Compliance

Easily meet compliance requirements with Duo

THE CHALLENGE:

Protecting Stolen Credentials and Personal Data

Payment Card Industry Data Security Standard (PCI DSS) applies to all organizations that store, process, and/or transmit cardholder data. It covers technical and operational system components included in or connected to consumer data. If a breach occurs and the organization is not in compliance with PCI DSS, it could face hefty fines plus negative publicity and potential lawsuits.

With version 3.2, PCI DSS expanded the scope of multi-factor authentication (MFA) to apply to users with non-console access into the cardholder data environment (CDE), as well as users with remote access into the corporate network, including third-parties. PCI security standards 7.0-7.3 restrict access to cardholder data by a business need-to-know stance, and PCI standard 8.0-8.8 requires identifying and authenticating access to system components by implementing a multi-factor authentication solution with policies to restrict and protect customer data from breaches.

Duo integrates with the most popular apps, including:

CISCO CITRIX vmware JUNIPER NETWORKS Outlook Office 365

Duo for PCI DSS

THE SOLUTION:

Duo's Trusted Access Platform

Duo's Trusted Access platform is built on Zero Trust and provides three key benefits to help meet PCI DSS requirements:

01

Remote Access

Verify your user's identities with strong multi-factor authentication before granting access to applications that may contain personal identifiable information (PII) and block or limit access from employees and third-parties.

Use granular policies to block access based on IP, countries, anonymous networks, and more to strengthen control and stay in compliance.

Identify company-owned and personal devices accessing your corporate applications, and get visibility into which corporate-managed and unmanaged devices are accessing company applications and data, without using an agent.

02

Protect Personal Data

Comply with PCI standards by verifying user identities, checking the health of all user devices and remediate out-of-date software. Secure access to any application before granting trust. Notify and restrict access of users with risky devices.

Take a zero trust security posture stance of "trust no one, continually verify." Allow only trusted endpoints to access specific applications and continuously monitor for trust and mitigate risk. Provide secure remote access from anywhere, to any application, with any platform.

Demonstrate compliance during audits with automated system reporting of users and devices accessing applications.

03

Secure Access to Any Application

Control which internal applications are accessible by remote users to limit exposure to personal information, and enforce access policies at an application level by geolocation.

Secure virtual private networks (VPNs) and remote access gateways like Juniper, Cisco AnyConnect, Fortinet, Citrix, F5, and more to add another layer of security to applications containing sensitive information.

Easily secure both on-premises and cloud environments – like Microsoft Azure, Amazon Web Services, and Google Cloud Platform – with or without a VPN.

Key PCI Requirements

Establish Zero Trust

- **6.2** Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release
- **7.1** Limit access to system components and cardholder data to only those individuals whose job requires such access.
- **7.2** Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.

DUO for PCI DSS

Implement MFA

- **8.2** Employ at least one of these to authenticate all users: something you know, such as a password or passphrase; something you have, such as a token device or smart card; or something you are, such as a biometric. Use strong authentication methods and render all passwords/passphrases unreadable during transmission and storage using strong cryptography.
- **• 8.3 Secure all individual non-console administrative access and all remote access to the cardholder data environment using multi-factor authentication.** This requires at least two of the three authentication methods described in 8.2 are used for authentication. This requirement applies to administrative personnel with non-console access to the CDE from within the entity's network, and all remote network access originating from outside the entity's network.

How Duo Protects

PCI DSS Payment Card Industry Data Security Standard, Version 3.2 Requirements: 6.2, 7.1, 7.2, 8.2, 8.31, and 8.3.2	• Provides strong MFA capabilities to protect access into the cardholder data environment.	• Restricts access to systems and applications containing cardholder data verified users and healthy devices.	• Validates user identities and establishes trust in devices. • Reduces the risk of accessing the cardholder data environment from outside the network.

Duo Editions

Feature	Benefit	Duo MFA	Duo Access	Duo Beyond
MFA	Establish user trust	✓	✓	✓
SSO	Login once to multiple apps	✓	✓	✓
Passwordless SSO	Secure Access without a password	✓	✓	✓
Adaptive Authentication	Grant access based on policies		✓	✓
Trust Monitor	Detect abnormal login attempts		✓	✓
Device Insight	Gain device visibility		✓	✓
DHA	Ensure device is healthy		✓	✓
Trusted Endpoints	Limit access to trusted devices			✓
DNG	Access internal apps without VPN			✓