DUO for...

Duo Security is now part of Cisco.

PCI DSS 3.2 Compliance

Easily Meet New Requirements with Duo

THE CHALLENGE:
Stolen Credentials

In April 2016, PCI DSS version 3.2 was released with new requirements for organizations that collect, store and process cardholder data. New requirements in 3.2 will be enforced starting February 1, 2018, and Duo can help admins easily meet several of them.

With version 3.2, PCI DSS expanded the scope of multi-factor authentication 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. These new requirements were developed to prevent attackers from using stolen credentials to access cardholder data.

Duo integrates with the most popular apps, including:

CISCO CITRIX vmware JUNIPER NETWORKS Outlook Office 365

Duo for PCI DSS 3.2

THE SOLUTION:

Duo's Trusted Access

Duo's Trusted Access solution provides three key benefits to help meet PCI DSS requirements:

01

Multi-Factor Authentication

Requirement 8.3.1:
Use multi-factor authentication for all non-console access into the CDE.
Duo provides out-of-the-box integration with Secure Shell Service (SSH), Remote Desktop (RDP) and any application that support RADIUS or LDAP-based authentication, and offers APIs and SDKs to easily add MFA into proprietary applications that store cardholder data.

Requirement 8.3.2:
Use multi-factor authentication for remote access into the network.
Attackers can compromise user or administrator credentials and access network resources by escalating privileges. However, Duo's Trusted Access platform provides out-of-the-box integration with all leading virtual private network (VPN) solutions and can be deployed within minutes.

02

Limit Privileges

Requirement 7.1-7.2:
Limit access to cardholder data to only those individuals who need it.
To minimize unauthorized access to the CDE, Duo allows organizations to create application policies for specific user and user groups to deny or allow access, based on permissions and need.

03

Protect Against Known Vulnerabilities

Requirement 6.2:
Ensure system and system components are protected from known vulnerabilities.
The standard recommends patching systems and software for protection.

Duo gives IT admins visibility into any outdated devices used to access the CDE, producing detailed reports and collecting device data without the need for an agent.

Admins can also set policies to prevent devices with old versions of operating systems, browsers and plugins from accessing the CDE until they're updated to the latest version.

"Duo security has helped us obtain our present PCI status of Compliant. Our vast network of attorneys is now able to safely and securely do business within our network without compromising data while in transmission."

Greg Church
IT Vice President, Merchants & Medical Credit Corporation