DataComm

What is SecurMFA powered by DUO?

To enhance the overall security posture, DataComm can incorporate DUO Security as the **two-factor authentication** solution for your existing IT infrastructure. DUO is a cloud-based security software that allows secure access to your network's services and data. Two-factor authentication will allow for a second layer of security for any type of login utilizing an extra authentication device along with a password or passcode. This will prevent anyone, except for the intended users, to access an account, application, or network.

Why Duo?

Reduce Security &Compliance Risk	**Improve End User Productivity & Experience**	**Reduce Total Cost of Ownership**	**Enable Organizational Agility**
Improve enterprise security and risk posture while ensuring regulatory compliance.	Effective, scalable security that is easy to use, easy to deploy and easy to manage.	Efficient and affordable security with lower investment and management overhead.	Deliver modern security solutions that support evolving enterprise needs, at scale.

Duo's Unified Access Security solution ensures only trusted users and trusted devices can access every application.

TRUSTED USERS
✓ Verify your users' identities with two-factor authentication.
✓ Enforce user access policies.
✓ Authentication methods to support every user.

TRUSTED DEVICES
✓ Check the security health of all your users' devices.
✓ Enforce device access policies.

EVERY APPLICATION
✓ Secure access to any application-cloud on premises, or custom.
✓ Enforce application access policies.

Duo Tiers:

Duo MFA
✓ Full-feature two-factor authentication for every organization.

✓ Overview of device security hygiene.

✓ Automate the management of your Duo solution through Admin API's.

✓ Single Sign-On to provide seamless and secure login across on-prem and cloud applications.

✓ Protect your on-premise and cloud applications

Duo Access
✓ Essential access-security suite to address risks from clouds, BYOD, and mobile.

✓ Complete visibility into BYOD

✓ Enforce rules on who can access which applications under what conditions.

✓ Encourage users to update their devices by enforcing access based on device hygiene.

✓ Identify users vulnerable to phishing through phishing campaigns

✓ Detailed and granular device insights

Duo Beyond
✓ The first commercial implementation of Google's BeyondCorp architecture.

✓ Gain complete visibility into BYOD and detect if a device is managed or unmanaged.

✓ Enforce policies to allow only managed devices to access sensitive applications

✓ Improve security by controlling what a remote user or device can access on your network

Duo in Action By Industry:

- ✓ **Education:** Protect access to student and employee logins, portals and data with Duo's trusted access solution.
- ✓ **Federal:** Duo's trusted access solution mitigates risks of data breaches and helps comply with NIST requirements.
- ✓ **Healthcare:** Duo helps healthcare organizations secure patient data by protecting EHR systems and e-prescription software.
- ✓ **Legal:** Secure access to confidential client data with Duo's trusted access solution, providing easy two-factor authentication for law firms.
- ✓ **Retail:** Meet PCI DSS while securing access to your applications and customer cardholder data with Duo's trusted access solution.
- ✓ **Technology:** Protect access to your applications and user data while reducing the risk of a data breach with Duo's trusted access solution.
- ✓ **Financial Services:** Verify users' identities and check device security health to keep financial data and online transactions out of the hands of criminals.

Integration – Duo MFA Supports Your Work Applications

Duo Solutions for Every Security Use Case

Whether you need to secure unmanaged devices or access to the cloud, Duo's trusted access is a solution for every need.

BYOD Security

Mixing personal devices and work data can be a security nightmare, as IT has no visibility into these devices and much less control than ever, weakening the overall security profile of a company.

Regain control and secure your BYOD environment with Duo's Unified Endpoint Visibility and device access policies to block login attempts from risky devices based on location, network type, software version and more.

Cloud Security

Secure data no matter where it is - both on-premises and in the cloud with Duo's trusted access solution.

Our solution integrates seamlessly with enterprise cloud apps for ease of use and administration. As a cloud-based solution, Duo can quickly scale to meet your company demands. Learn About Cloud Services

Endpoint Security

Endpoint security used to require installing an agent on your users' devices. But they prove ineffective for security since new threats emerge faster than agents can be updated.

Duo provides a streamlined solution to get insight into the security health of your users' devices and the ability to enforce device access policies - all without the use of the agent. Learn About Device Access Policies

Mobile Security

Living in a mobile-first world means there's an app for every need - and a ton of confidential data accessible online. Organizations need to ensure both devices and data are secure.

Duo gives you insight into the security health of your mobile devices and the mobile security controls you need to strengthen your security profile, without installing an agent. Learn About Trusted Devices

Meet Compliance Requirements

Every security best practice guide and regulation asks for MFA and device visibility

PCI — Meet MFA requirements outlined in PCI-DSS 3.2 Section 8.3

NIST — Helps meet NIST 800-63 and 800-171 access security requirements

DEA — Meet DEA's EPCS requirements when approving e-prescriptions

GDPR — Aligned with GDPR data protection laws in Europe

FFIEC — Meet FFIEC requirements for financial applications

HIPAA COMPLIANCE — Get visibility into personal devices used to access PHI

Duo's solutions for the workforce can help you satisfy industry compliance regulations that require or recommend strong multi-factor authentication, access security controls and device management.

Security Control Assessments

Frameworks such as <u>NIST</u>, CIS/SANS 20 or ISO 27001 have separated themselves as the best practice frameworks for organizations to assess their practices to protect sensitive data, and provide secure access to critical assets. Duo offers solutions that provide organizations with the ability to adopt the best practices outlined in these frameworks by providing organizations the tools to verify users and establish access policies for systems while permitting access only from known devices and sources.

Data Privacy Guidelines and Regulations

Regardless if your organization is subject to regional data privacy regulations like GDPR, or PIPEDA, or if you need to adhere to state specific legislation such as CCPA, Duo helps you implement strong technical controls to protect access to backend systems that contain sensitive data that falls under the data privacy guidelines and regulations. With Duo, organizations can check the security hygiene of user devices before granting access and block users with risky devices. These controls protects sensitive resources by giving organizations the ability to enforce policies granting access only to verified users from identified sources and provides reports for audit purposes.

Protect Patient Data

Duo for HIPAA Compliant Security

Duo helps healthcare organizations meet HIPAA (Health Information Portability and Accountability Act) omnibus compliance requirements with easy to use authentication and access policies that don't interfere with patient care. Duo's ability to provide controls for the enforcement of security posture on the devices that are accessing sensitive patient health information with system reporting can help provide evidence of device encryption in the event that equipment is lost or stolen.

Duo for EPCS

The DEA (Drug Enforcement Agency) requires practitioners to use strong multi-factor authentication to access electronic prescription applications to sign prescriptions for controlled substances. That MFA solution must meet at least the criteria of FIPS 140–2 Security Level 1. Duo's authentication methods were reviewed by Drummond Group, a DEA accredited security auditor, to meet EPCS requirements.

Protect Financial Data

FFIEC, NYDFS & NAIC Security

Verify users' identities with Duo's multi-factor authentication (MFA) to protect financial data and online transactions from criminals. The FFIEC, NYDFS Cybersecurity Regulation and NAIC mandate the use of MFA to protect access to sensitive data for financial institutions, insurers, banks and many other organizations.

Duo's MFA and trusted access solution can help you comply with regulations and protect access by every user, device and application.

Multi-Factor Authentication

The FFIEC recommends against using one form of customer authentication to protect online transactions and accounts. NYDFS Cybersecurity Regulations require MFA to securely connect to internal networks for financial organizations that operate or conduct transactions in New York.

Duo's MFA offers a more secure and easy-to-use method by sending push notifications to users' smartphones via Duo Mobile. Plus, Duo's other methods support all types of login scenarios, including offline users or those without smartphones.

To meet compliance and pass audits, you need to protect your mix of cloud, older on-premises and custom apps. Duo integrates with more apps regardless of where they reside - protecting hybrid environments, remote access VPNs, single sign-on and more. To support remote employees (insurance agents and financial planners), Duo offers easy self-enrollment and automated enrollment options to ensure successful deployments at scale and reduce help desk tickets.

Device Visibility & Policies

To support insurance agents as contractors using their own personal devices, Duo provides greater device insight without an intrusive agent. Get visibility into all user devices - including corporate or personally-owned laptops, smartphones, desktops and PCs. Detect devices running out-of-date software, and identify endpoints that are jailbroken, rooted, tampered with, unencrypted and more.

Useful for daily, weekly or monthly compliance audits, Duo's reports give you detailed insight into user and device risks that can easily be expo

Adaptive Authentication

Based on a risk assessment, NYDFS requires that financial institutions use effective controls such as risk-based authentication (also known as adaptive authentication) to protect against unauthorized access to their information systems.

Duo's solution lets you set policies to block access attempts based on an individual or group, geolocation, network type and device security. Enforce stricter login controls for unmanaged, personally-owned devices used by third-party service providers. Require encryption or enabled passcodes, and block access by devices without enabled security controls.

Duo for PCI DSS Security

Duo can help you meet PCI DSS standards by protecting credentials with strong two-factor authentication, and limit access to cardholder data with strong access controls. Duo's device insights provide visibility into the devices being used to connect to systems storing sensitive information and enables organizations to establish security policies that prevent unauthorized access.

Duo for Financial Services

Financial Services organizations – insurance providers, banks, brokerage firms and others - often have regulatory controls beyond PCI DSS that include things like FFIEC, NYDFS and NAIC, which require not just the implementation of strong authentication controls, but require access controls to ensure that only verified internal or external users can gain access to systems.

Follow Best Practices

Overarching security frameworks like ISO 27001 and NIST provide recommendations for security best practices, which inform many compliance guidelines that span across multiple industries and verticals.

Foundational Framework	How Duo MFA Helps	How Duo Access Helps	How Duo Beyond Helps
ISO 27001 International Organization for Standardization A.9.1.2, A.9.2.1, A.9.4.1, A.9.4.2, A.9.4.4, A.9.4.5, A.12.4.1, A.12.4.2, A.12.4.3, A.13.1.2, A.14.1.2, A.14.2.4, A.14.2.6, A.14.3.1, A.18.1.3, A.18.1.4	• Syncs w/ existing identity access management (IAM) solutions. • Provides a layer of strong authentication. • Automates user provisioning and de-provisioning of authentication factors. • Reports on event logs recording user activities.	• Enforces adaptive access policies for role-based access. • Controls access to systems and applications with a secure log-on procedure, where required by the access control policy. • Limits access to source code to verified users.	• Provides secure access to internal applications without exposing them to external risk. • Allows only trusted endpoints to access specific applications. • Enables limited access for external third-parties to specific applications and systems.
NIST 80053, NIST 800171 & DFARS National Institute of Standards and Technology 800171, Revision 2 (June '19) SP 800633b guidance NIST 80053 Control: IA2, IA3, IA5, IA6, MA4, SC7, SC11 NIST 800171 Control: 3.1.1, 3.1.1, 3.1.3, 3.1.7, 3.1.11, 3.1.12, 3.1.14, 3.1.15, 3.1.18, 3.1.20, 3.3.1, 3.3.2, 3.3.8, 3.4.1, 3.4.2, 3.5.2, 3.5.3, 3.5.7, 3.7.5	• Uniquely identifies and authenticates users. • Meets NIST digital identity guidelines. • Limits system access to authorized users. • Provides inventory of all endpoints accessing protected applications. • Provides local access protections online/offline for DFARS requirements.	• Limits applications that authorized users are permitted to access. • Grants access only to healthy and compliant devices. • Adds a layer of authentication for privileged accounts.	• Routes remote access via managed access control points. • Controls connection of BYOD. • Identifies and verifies specific devices before establishing a connection. • Restricts access to controlled unclassified information (CUI) in a compliant manner.
FIPS 140-2 Federal Information Processing Standards Control: 1402 lv13	• Leverages FIPS 140-2 validated cryptographic modules to achieve compliance. • Zerotouch implementation for FIPS 140-2 compliant mobile authentication; no configuration required by administrators.		
SOC2 Systems and Organization Controls Report 2017 Trust Services Criteria (TSC) Reference Number: CC6.1, CC6.2, CC6.3, CC6.6, CC6.7, CC7.1	• Provides automatic provisioning and deprovisioning of MFA tokens. • Integrates with a SIEM for fraudulent push authentication reported by users. • Provides visibility of endpoints accessing business applications.	• Implements the concepts of least privilege to establish role-based access policies to applications. • Restricts access from devices that are out of date and provides users with self-remediation options.	• Restricts access to known devices and locations. • Provides secure external access that can be tracked and limited to protect internal resources. • Establishes trust in BYOD in environments with an agentless approach.

Address Areas of Compliance Guidelines

Risk and Compliance teams will often work with Security teams to ensure their security strategy is in line with the compliance requirements to avoid potential financial penalties.

Compliance Guidelines	How Duo MFA Helps	How Duo Access Helps	How Duo Beyond Helps
CJIS Criminal Justice Information Services Version 5.6 Section: 5.5.2.3, 5.5.6.1, 5.5.6.2, 5.6.2.1, 5.6.2.1.3, 5.6.2.2, 5.6.3.2, 5.10.4.1, 5.10.4.4, 5.13.7.1, 5.13.7.2	• Supports multiple methods for an additional factor of authentication. • Provides automated management of authentication methods. • Provides methods for users to report fraudulent access attempts.	• Ensures end users have up-to-date security patches on their devices. • Provides guidance for self-service remediation for systems that are out of date.	• Restricts access to information protected under CJI from unmanaged/unknown devices. • Blocks access from unverified BYOD sources.
EPCS Electronic Prescriptions for Controlled Substances (75 FR 16236, March 31, 2010) [Docket No. DEA218, RIN 1117AA61]	• Protects individual / institutional practitioners from misuse of their credentials by insiders as well as from external threats. • Meets cryptographic requirements and is verified by a DEA accredited auditor.	• Ensures that only authorized practitioners are able to gain access and digitally sign for controlled substance distribution with granular access policies based on role.	• Permits access only to known/ trusted devices accessing systems for e-prescribing. • Enforces security controls and encryption on BYOD devices.
FFIEC Federal Financial Institutions Examination Council Version Sept 2016 Title: II.C.5, II.C.7, II.C.7(a), II.C.7(e), II.C.10(d), II.C.13(e), II.C.15(b), II.C.15(c), II.C.15(d), II.D, III.C	• Provides controls to require multi-factor authentication for access to local workstations. • Provides a detailed view of the security posture of the devices that are connecting to sensitive applications. • Implements a robust authentication method consistent with the criticality and sensitivity of the application.	• Enforces access policies based on group membership for sensitive applications. • Provides guidance for device updates and remediation through self-service. • Blocks access for unauthorized devices connecting to applications.	• Restricts remote access to authorized network areas and applications. • Ensures seamless and secure remote access to sensitive applications. • Ensures BYOD devices connecting to sensitive information are reported and meet the latest security criteria before granting access.

Continued on next page

DataComm

Compliance Guidelines	How Duo MFA Helps	How Duo Access Helps	How Duo Beyond Helps
GBLA Gramm-Leach-Bliley Act FIL222001 Title: V Subtitle A Section 501(3)	• Provides MFA to strengthen secure password policy.	• Ensures devices and browsers accessing sensitive application are patched and updated.	• Verifies that protected screen lock is enabled on mobile devices. • Makes sure device encryption is enabled on mobile devices.
HIPAA Health Insurance Portability and Accountability Act, CFR 45 revised October 1, 2007 Standard: 164.304, 164.308(a)(1), 164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B), 164.308.(a)(4), 164.308(a)(4)(ii)(B), 164.308(a)(5)(ii)(A), 164.308(a)(5)(ii)(C), 164.308(a)(6)(ii), 164.312(d)	• Implements strong authentication requirements that protect electronic protected health information (ePHI) from unauthorized access • Provides visibility into endpoints accessing systems that contain PHI • Provides emergency access options in the event of a lost or stolen authentication method.	• Implements access controls to reduce risks and vulnerabilities. • Enforces access policies to ensure that ePHI is not available or disclosed to unauthorized persons. • Enforces access restrictions based on group membership to applications containing ePHI. • Prompts users for self-remediation on devices that don't meet security controls.	• Restricts remote access to Enables secure BYOD access to ePHI by establishing devices meet minimum security requirements. • Establishes security protections for remote access to protected applications containing sensitive ePHI.
NERC North American Electric Reliability Corporation CIP005 Table R2 Part 2.3, CIP0076 Table R5 5.1, CIP0102 Table R2 2.1	• Enforces multi- factor authentication for user access.	• Offers user security training with phishing assessments for user security and audit reporting. • Blocks access from unknown sources	• Enforces controls for remote access to protected resources. • Restricts access to managed devices.
PCI DSS Payment Card Industry Data Security Standard, Version 3.2 Requirements: 6.2, 7.17.2, 8.3.1 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 to verified users and health devices.	• Validated user identities and establishes trust into devices. • Reduces the risk of accessing the cardholder data environment from outside the network.

Provide Technical Controls for Data Privacy

With additional requirements around data privacy impacting businesses that have an online presence, there is added complexity for organizations as they strive to implement security solutions to protect operations while rolling out new technologies and keeping employees productive.

Data Privacy Controls	How Duo MFA Helps	How Duo Access Helps	How Duo Beyond Helps
PIPEDA Personal Information Protection and Electronic Documents Act Guidelines for Identification and Authentication	• Provides strong authentication options for users accessing protected systems.	• Provides the ability to elevate or relax authentication requirements based on application sensitivity with access controls. • Restricts access from unknown locations or devices.	• Restricts remote access to applications containing sensitive information. • Provides technical controls to deliver external access while protecting internal systems.
GDPR EU General Data Protection Regulation (EU) 2016/679 Article 5 Section 1(f) and 2, Article 24 Section 1, Article 32 Section 1(b) and 2	• Prevents unauthorized access to sensitive information. • Delivers detailed logs of access events.	• Provides granular policy controls to manage and restrict access.	• Provides visibility into which corporate-managed and unmanaged devices are accessing company applications and data.
CCPA California Consumer Protection Act Section 1798.150. (a) (1)	• Verifies users' identities with strong two-factor authentication before granting access to applications that may contain personal information.	• Ensures only trusted and authorized users and healthy devices can access critical business applications and the data they store.	• Ensures that only healthy, trusted devices gain access to sensitive resources and can block unauthorized devices.