Framework Mapping: Cisco Duo + Cybersecurity Maturity Model Certification (CMMC)

Contents

Overview of Cybersecurity Maturity Model Certification (CMMC)

The Cybersecurity Maturity Model Certification (CMMC) is a unified security standard developed by the United States Department of Defense (DoD) to ensure the protection of sensitive information within the Defense Industrial Base (DIB). The DIB encompasses over 300,000 companies in the supply chain that provide research, engineering, manufacturing, and maintenance services to the DoD.

The original CMMC framework was introduced to address the vulnerabilities found in the previous "self-attestation" model, where contractors were responsible for reporting their own compliance without independent verification. CMMC 2.0, the current iteration effective November 2025, streamlines the requirements into three distinct levels, primarily aligning with National Institute of Standards and Technology (NIST) guidelines, including NIST SP 800-171 and SP 800-172. It creates a tiered approach to cybersecurity, requiring contractors to demonstrate a specific level of "maturity" based on the sensitivity of the data they handle. By mandating third-party assessments for higher-level contracts, the CMMC ensures a verified and consistent security posture across the entire defense ecosystem.

Purpose of the CMMC Framework

The primary purpose of the CMMC framework is to safeguard two specific types of unclassified information that are critical to national security:

- **Federal Contract Information (FCI):** Information provided by or generated for the Government under a contract to develop or deliver a product or service.
- **Controlled Unclassified Information (CUI):** Information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and government-wide policies, but is not classified.

Contents

Beyond data protection, the framework serves several strategic objectives:

- **Standardization:** It provides a single, measurable standard for cybersecurity across the DIB, replacing a patchwork of various regulations.
- **Accountability:** By requiring independent validations (C3PAO assessments) for contractors handling CUI, it ensures that security controls are not just documented but effectively implemented.
- **Risk Management:** It allows the DoD to scale security requirements according to the risk associated with a specific program. Not every contractor needs the highest level of security; CMMC allows for a cost-effective, risk-based application of controls.
- **Resilience against Advanced Persistent Threats (APTs):** The framework is designed to protect the intellectual property and technological advantages of the U.S. military from sophisticated cyber espionage and state-sponsored theft.

Key components of the CMMC Framework

The CMMC framework is organized into three certification levels, each representing a progressively advanced set of cybersecurity practices and assessment requirements tailored to the sensitivity of the information handled.

The tiered model (Levels)

CMMC 2.0 is structured into three progressively advanced levels:

- **Level 1 (Foundational):** Focuses on the basic protection of FCI. It consists of 15 practices aligned with FAR 52.204-21. Contractors at this level may perform annual self-assessments.
- **Level 2 (Advanced):** Designed for contractors handling CUI. This level mirrors the 110 security requirements of NIST SP 800-171. Compliance is verified through either self-assessments or triennial third-party assessments, depending on the sensitivity of the program.
- **Level 3 (Expert):** Intended for the highest priority programs and those facing APTs. It incorporates a subset of requirements from **NIST SP 800-172** in addition to Level 2 requirements. These assessments are typically led by the government (DIBCAC).

Contents

Assessment and certification process

Unlike previous models, CMMC introduces a formal ecosystem of assessors:

- **C3PAOs (Certified Third-Party Assessment Organizations):** Independent entities authorized to conduct Level 2 assessments.
- **Assessor Training:** A rigorous certification path for individuals (Certified Professionals and Assessors) to ensure consistency in how controls are evaluated.
- **SPRS (Supplier Performance Risk System):** The centralized database where assessment scores and certificates are recorded for DoD contracting officers to verify.

Implementation and POAMs

A critical component of CMMC 2.0 is the allowance for Plans of Action and Milestones (POAMs). Under certain conditions, contractors can receive a conditional certification if they have a plan to remediate specific, non-critical deficiencies within a defined timeframe (usually 180 days). This provides flexibility for contractors to achieve compliance without immediate disqualification from the bidding process, provided the core security requirements are met.

Understanding Cisco Duo

Cisco Duo is a critical component of Cisco's zero trust security architecture, designed to protect enterprise users by establishing trust for every access request regardless of location. It provides strong authentication methods, including passwordless options such as biometrics and security keys, to verify user identities securely and seamlessly. Duo also offers device trust capabilities, enabling organizations to assess and enforce the security posture of devices before granting access to corporate applications. This approach helps minimize risk by continuously verifying both user and device trust, leveraging adaptive, context-based access controls that monitor user behavior and device health to dynamically adjust policies in real time.

Contents

Beyond authentication, Cisco Duo integrates with other Cisco security solutions like Cisco Identity Services Engine (ISE), Cisco XDR, and Cisco Secure Access to create a comprehensive zero trust environment. It provides unified visibility into user activities and device compliance, enabling organizations to detect anomalies and respond to threats proactively. Duo supports a wide range of applications and devices, offering Single Sign-On (SSO), Multi-Factor Authentication (MFA), and device trust features that simplify secure access while reducing administrative overhead. This seamless integration and adaptive security posture make Cisco Duo a foundational element for organizations aiming to implement zero trust with minimal friction and maximum protection across hybrid and cloud environments.

Benefits of Cisco Duo

Cisco Duo offers several advantages for organizations seeking to strengthen their cybersecurity posture:

- **Enhanced Security and Compliance:** Duo provides phishing resistant Multi-Factor Authentication (MFA) that helps organizations meet compliance requirements across various industries, including FedRAMP, Cybersecurity Maturity Model Certification (CMMC), and Zero Trust Models for both Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Defense (DoD). It protects against phishing attacks by requiring a second factor beyond just a password, significantly reducing the risk of unauthorized access even if credentials are compromised.
- **Advanced Proximity Verification:** In addition to traditional MFA, Duo leverages advanced technical capabilities such as proximity verification to further enhance security. With Duo, user devices need to be in close physical proximity to the computer attempting authentication. This requirement helps prevent remote attackers from successfully completing authentication requests, as only devices that are near the login device can approve access. This mitigates the risk of users being tricked into approving fraudulent authentication requests, adding an extra layer of protection against social engineering and push notification attacks.
- **User Convenience and Productivity:** Duo can remember trusted devices; this reduces the frequency of authentication prompts and improves user experience without sacrificing security. Features like Duo Passport enable seamless access to multiple applications after a single authentication, boosting workforce productivity.

Contents

- **Scalability and Flexibility:** Duo easily adapts to organizations of all sizes and diverse user bases. It supports automated user provisioning and deprovisioning, simplifying identity lifecycle management. Duo's cloud-based architecture allows for fast deployment and lowers total cost of ownership compared to traditional MFA solutions.
- **Comprehensive Device Trust:** Duo's Device Trust capability verifies the security posture of devices before granting access, assessing factors such as operating system version, encryption status, and presence of security software. This helps prevent risky or non-compliant devices from accessing sensitive resources and balancing security with user productivity.
- **Visibility and Control:** Duo offers critical IT visibility into user identities, device health, and access patterns through centralized dashboards and integrations with Cisco Identity Intelligence. This enables organizations to detect suspicious activities, enforce conditional access policies based on context (such as user role, location, and device security), and respond proactively to threats.
- **Reduced IT Burden:** Duo's self-service portal empowers users to manage their authentication devices, reducing help desk tickets. Guided remediation helps users bring devices into compliance without IT intervention, further lowering operational costs.
- **Integration and Ecosystem:** Duo integrates seamlessly with existing identity and security infrastructures, supporting Single Sign-On (SSO), passwordless authentication, and a broad ecosystem of over 250 partners. This maximizes the value of existing investments while enhancing security posture.

Overall, Cisco Duo delivers a robust, user-friendly, and scalable solution that strengthens security, improves compliance, and enhances productivity across hybrid and cloud environments.

Contents

Cisco Duo deployment options

Cisco Duo offers several deployment options to integrate MFA and zero trust security across various Cisco products and environments, including a FedRAMP Authorized federal edition tailored for public sector organizations with stringent security requirements.

- **Cisco ASA or Firepower VPN Integration:** Duo can be deployed with Cisco ASA or Firepower VPN appliances to add two-factor authentication to AnyConnect or Cisco Secure Client logins. This setup uses the Duo Authentication Proxy to mediate authentication requests between the VPN and Duo's cloud service. It supports policies based on network location and fail mode configurations if Duo's service is unreachable. This deployment requires Cisco ASA firmware 8.3 or later or Cisco FTD version 6.3.0 or later managed by FMC 6.3.0 or later. There are two main methods:
  - **RADIUS Authentication:** Cisco ASA or FTD sends authentication requests to the Duo Authentication Proxy, which performs primary authentication (e.g., Active Directory) and secondary authentication via Duo.
  - **Single Sign-On (SSO) with SAML:** For Cisco Firepower Threat Defense (FTD), Duo Single Sign-On can be used with a cloud-hosted identity provider, providing an interactive MFA prompt and device insights during VPN login.
- **Cisco Identity Services Engine (ISE) Integration:** Duo can integrate with Cisco ISE using RADIUS to add MFA for AnyConnect or Cisco Secure Client users. The Duo Authentication Proxy handles authentication requests between ISE and Duo's cloud service. This requires Cisco ISE version 2.4 or later.
- **Device Trust and Endpoint Security:** Duo's Device Trust capabilities verify the security posture of devices before granting access, including checks for operating system version, encryption, and security software presence. Duo Desktop can enforce endpoint health policies and provide self-remediation prompts to users for compliance.
- **Cloud-Based and Flexible Deployment:** Duo's cloud-native architecture allows for rapid deployment and scalability across organizations of all sizes. It supports integration with existing identity providers, Single Sign-On (SSO), passwordless authentication, and adaptive access policies.

Contents

- **Cisco Duo Federal Editions:** Cisco offers two FedRAMP authorized, FIPS-compliant editions—Duo Federal Essentials and Duo Federal Advantage—designed to meet the strict security requirements of federal agencies and public sector organizations. These federal editions provide strong cloud-based authentication and device visibility aligned with FedRAMP, FIPS 140-2/3, and NIST SP 800-63-3 standards.

Key differences from commercial editions include exclusion of telephony and SMS factors, enhanced role-based and location-based access policies, biometric authentication enforcement, and compliance with federal security controls. Eligibility for these editions includes federal agencies, federal contractors, state and local governments, public sector organizations, state universities, and federally funded research centers. Transitioning from commercial to federal editions requires full redeployment and reenrollment of users due to FedRAMP security controls.

Duo Federal editions also support native VPN integration with Cisco ASA and provide unified endpoint visibility to enforce device hygiene policies, enabling or denying access based on device compliance. These capabilities align with FedRAMP/NIST 800-53 security controls and FIPS 140-2/3 compliance requirements for federal organizations.

These deployment options enable organizations to implement strong, context-aware authentication and device security controls across VPNs, network access, and applications, aligning with Cisco's zero trust security framework and federal compliance mandates.

For detailed deployment instructions and federal edition specifics, Cisco provides comprehensive guides and resources including the Duo Federal Guide and eligibility considerations:

- Guide to Duo's Federal Editions | Duo Security
- Duo Federal Editions: Eligibility and Considerations
- Solutions - Trusted Internet Connections (TIC) 3.0 Architecture Guide - Cisco

Contents

Technical features

Cisco Duo offers a comprehensive set of technical features designed to enhance security through phishing-resistant authentication, device trust, and seamless user experience; all aligned with zero trust principles. Key technical features include:

- **Multi-Factor Authentication (MFA):** Duo supports a variety of strong authentication methods including push notifications via the Duo Mobile app, hardware tokens, Universal 2nd Factor (U2F) security keys, and biometric passwordless authentication. Users can authenticate even without network connectivity using offline methods or hardware tokens. Duo Mobile can be provisioned easily through QR codes during enrollment.
- **Passwordless Authentication:** Duo Directory enables organizations to eliminate passwords entirely by supporting passwordless authentication through biometrics, FIDO2 WebAuthn security keys, and integration with external cloud directories or on-premises Active Directory. Duo Desktop bridges gaps for embedded browsers that lack WebAuthn support.
- **Device Trust:** Duo provides deep visibility into device health and security posture before granting access. Features include endpoint health checks (e.g., OS version, encryption, security software), trusted endpoints tracking, and enforcement of compliance policies. Duo Desktop offers self-remediation prompts to users to update or secure their devices. Integration with Cisco Secure Endpoint allows automated blocking of compromised devices.
- **Adaptive Access Policies:** Administrators can create granular policies based on user groups, device health, network location, geo-IP, and risk factors. Duo supports IP allowlisting, trusted devices with configurable time limits, and step-up authentication requirements for higher-risk scenarios — with agentless management.
- **Single Sign-On (SSO) and Identity Federation:** Duo offers cloud-hosted SSO supporting SAML 2.0, OIDC, and OAuth 2.0 standards, enabling seamless access to multiple applications with one login. It can act as an Identity Provider (IdP) or integrate with existing IdPs, supporting multiple authentication sources and routing rules. Duo Passport extends SSO capabilities across browsers, operating systems, and thick clients.

Contents

- **User and Device Visibility:** Duo Device Insight inventories endpoints, providing data on OS, platform, browser versions, encryption status, and device risk indicators like jailbroken or rooted status. This visibility helps administrators identify risky devices and enforce policies accordingly.
- **Integration with Cisco Security Ecosystem:** Duo integrates with Cisco Secure Endpoint, Secure Firewall, Identity Services Engine (ISE), Cisco XDR, and Meraki to provide unified security posture, threat detection, and enforcement of zero trust policies across network and endpoint layers.
- **Administrative Controls and Support:** Duo provides an admin panel for user and policy management, supports custom attributes for identity management, and offers various support tiers including standard, enhanced, and signature support. Hardware tokens are available for one-time passcode authentication, and telephony credits can be purchased for phone-based authentication.

These technical features collectively enable organizations to implement strong, adaptive, and user-friendly security controls that verify both user identity and device trust before granting access to applications and networks, supporting a robust zero trust security framework.

Mapping Cisco Duo

Key

Green = Meets

Yellow = Supports

Table 1. Mapping Cisco Duo

CMMC Family/Domain	Description	Duo CMMC Capability Mapping Level 1	Duo CMMC Capability Mapping Level 2	Duo CMMC Capability Mapping Level 3
Access Control (AC)	The principles of access control are applied to both physical and logical assets. Physical assets include buildings, fences, gates, and doors. Logical access principles are applied to IT assets like servers, laptops, PCs, network communication devices, logic controllers, operating systems, applications, and databases. Core principle of access control are least privilege and zero trust, allowing access only to assets based upon appropriate, authorized, and regular assessment, using Role-Based Access Control (RBAC) Principles.	**Level 1** AC.L1-3.1.1 AC.L1-3.1.2 AC.L1-3.1.10 AC.L1-3.1.20 AC.L1-3.1.22	**Level 2** AC.L2-3.1.1 AC.L2-3.1.2 AC.L2-3.1.3 AC.L2-3.1.4 AC.L2-3.1.5 AC.L2-3.1.6 AC.L2-3.1.7 AC.L2-3.1.8 AC.L2-3.1.9 AC.L2-3.1.10 AC.L2-3.1.11 AC.L2-3.1.12 AC.L2-3.1.13 AC.L2-3.1.14 AC.L2-3.1.15 AC.L2-3.1.16 AC.L2-3.1.17 AC.L2-3.1.18 AC.L2-3.1.19 AC.L2-3.1.20 AC.L2-3.1.21 AC.L2-3.1.22	**Level 3** AC.L3-3.1.2e AC.L3-3.1.3e

CMMC Family/Domain	Description	Duo CMMC Capability Mapping Level 1	Duo CMMC Capability Mapping Level 2	Duo CMMC Capability Mapping Level 3
Awareness and Training (AT)	Cyber is a mission, not a technology risk, and everyone has a part to play in protecting assets and securing the mission of the enterprise.	**N/A**	**Level 2** AT.L3-3.2.1 AT.L3-3.2.2 AT.L3-3.2.3	**N/A**
Audit and Accountablity (AU)	Audit logging is an important requirement for system governance. It provides the evidence of transaction activity, of what users do, on what system, and when. It logs system transactions including systems access, files transfers, and communication records and retains these over time. Logging is important during digital forensic investigations, including those during and following a cyberattack.	**N/A**	**Level 2** AU.L2-3.3.1 AU.L2-3.3.2 AU.L2-3.3.3 AU.L2-3.3.4 AU.L2-3.3.5 AU.L2-3.3.6 AU.L2-3.3.7 AU.L2-3.3.8 AU.L2-3.3.9	**N/A**
Configuration Management (CM)	It is important to standardize the configuration of technology across the organization. This reduces operating costs, simplifies maintenance, and imporves security.	**N/A**	**Level 2** CM.L2-3.4.1 CM.L2-3.4.2 CM.L2-3.4.3 CM.L2-3.4.4 CM.L2-3.4.5 CM.L2-3.4.6 CM.L2-3.4.7 CM.L2-3.4.8 CM.L2-3.4.9	**Level 3** CM.L3-3.4.1e CM.L3-3.4.2e CM.L3-3.4.3e

CMMC Family/Domain	Description	Duo CMMC Capability Mapping Level 1	Duo CMMC Capability Mapping Level 2	Duo CMMC Capability Mapping Level 3
Identification and Authentication (IA)	Identification is the ability to identify uniquely a user of a system or an application. Authentication is then the ability to prove and verify that the user or application is genuinely who that user or what that application claims to be.	**Level 1** IA.L1-3.5.1 IA.L1-3.5.2	**Level 2** IA.L2-3.5.1 IA.L2-3.5.2 IA.L2-3.5.3 IA.L2-3.5.4 IA.L2-3.5.5 IA.L2-3.5.6 IA.L2-3.5.7 IA.L2-3.5.8 IA.L2-3.5.9 IA.L2-3.5.10 IA.L2-3.5.11	**Level 3** IA.L3-3.5.1e IA.L3-3.5.3e
Incident Response (IR)	An Incident Response (IR) plan establishes a clear set of actions to detect, respond to, and recover from an attack. The IR plan can be used to address issues such as cybercrime, data loss, and service outages that threaten operations. The IR plan should be tested frequently to confirm that it is effective and to successfully address the range of possible threats an organization faces.	**N/A**	**Level 2** IR.L2-3.6.1 IR.L2-3.6.2 IR.L2-3.6.3	**Level 3** IR.L3-3.6.1e IR.L3-3.6.2e
Maintenance (MA)	Regular systems maintenance ensures the smooth running of operations and reduces the risk of breakdown. Maintenance procedures that address system speed and performance can help identify inappropriate processes running on devices, and unpatched software and programs that make devices unstable and more likely to fail, causing disruption to operations. System maintenance identifies vulnerabilities with operating systems, hardware and software which if left unresolved can result in systems being compromised by hackers through reconized vulnerabilities.	**N/A**	**Level 2** MA.L2-3.7.2 MA.L2-3.7.3 MA.L2-3.7.4 MA.L2-3.7.5 MA.L2-3.8.2 MA.L2-3.8.5 MA.L2-3.8.6 MA.L2-3.8.8 MA.L2-3.8.9	**N/A**

CMMC Family/Domain	Description	Duo CMMC Capability Mapping Level 1	Duo CMMC Capability Mapping Level 2	Duo CMMC Capability Mapping Level 3
Personnel Security (PS)	People are an organization's most important assets and pose one of the largest risks to the security of data and information. Sixty percent of data breaches occur frominsider threats. Employee screening is an essential activity; it can be used to clarify a person's skills and experience, to confirm the presence of a criminal record, to evaluate reputation, and to confirm legal compliance. It is important therefore that organizations ensure that their staff have been screened appropriately, if hey are to encounter sensitive data such as FCI or CUI.	**N/A**	**N/A**	**Level 3** PS.L3-3.9.2e
Physical Protection (PE)	Physical and logical protection are inextricably linked. Without physical protection it is it not possible to protect assets including computers, laptops, and servers that hold the company's IP. If an unauthorized person can damage, destroy, or steal assets, all the firewalls, intrusion detector systems, cryptography, and other security measures will not stop them from getting access to the organization's IP. Therefore it is critical that physical security measures are applied to prevent unauthorized users from gaining access to areas within an organization they are not authorized to access.	**N/A**	**N/A**	**N/A**

CMMC Family/Domain	Description	Duo CMMC Capability Mapping Level 1	Duo CMMC Capability Mapping Level 2	Duo CMMC Capability Mapping Level 3
Risk Assessment (RA)	Cyberattacks can impact any part of an organization from the board room to the shop floor and extend through the organization's supply chain. Attacks can be targeted or general and can range in impact from minor disruption with no data theft to ransomware attacks that can bankrupt an organization and lead to the theft of its most critical IP. With such a range of possible threats and outcomes, it is important that an organization identifies and manages those risks that it believes are the most significant.	**N/A**	**Level 2** RA.L2-3.11.2 RA.L2-3.11.3	**Level 3** RA.L3-3.11.1e RA.L3-3.11.2e RA.L3-3.11.3e RA.L3-3.11.5e RA.L3-3.11.6e
Security Asessment (SA)	Security assessment is an evaluation of the security posture of the organization based upon its ability to manage its cyber risk profile. The SA identifies an organization's inherent risks, assessing the effectiveness of its controls environment and evaluating its residual risk profile. It is an exercise that continually evolves and improves based upon the changing business environment. An SA can be managed through the creation, adoption, and management of a Systems Security Plan (SSP).	**N/A**	**Level 2** SA.L2-3.12.1 SA.L2-3.12.3 SA.L2-3.12.4	**Level 3** SA.L3-3.12.1e

CMMC Family/Domain	Description	Duo CMMC Capability Mapping Level 1	Duo CMMC Capability Mapping Level 2	Duo CMMC Capability Mapping Level 3
System and Communications Protection (SC)	Organizations use a wide variety of technology devices to conduct their business operations. These devices are connected to form an ecosystem for the creation, transmission, consumption, and servicing of data, which is unique to an organization's business operations. All these devices, networks, communications, and data need to be secured. An organization must have a clear view of its perimeter, including technology, processes, people, and data. Mature security solutions require having appropriate designs in place to leverage all the security solutions available to provide an adequate level of security. These solutions must include network security, access management, data loss prevention, code security, encryption, and sandboxing among other practices.	**Level 1** SC.L1-3.13.1	**Level 2** SC.L2-3.13.1 SC.L2-3.13.2 SC.L2-3.13.3 SC.L2-3.13.4 SC.L2-3.13.5 SC.L2-3.13.6 SC.L2-3.13.7 SC.L2-3.13.8 SC.L2-3.13.11 SC.L2-3.13.13 SC.L2-3.13.14 SC.L2-3.13.15 SC.L2-3.13.16	**N/A**
System and Information Integrity (SI)	Information integrity is a critical requirement to maintain the confidentiality, integrity, and availability of FCI and CUI, which is the primary goal of information security and cyber risk management. System information integrity requires the adoption of a broad range of security practices including the remediation of known software flaws (security by design, vulnerability scanning, and patch management); the identification and management of malicious software (Anti-Virus); Spam protection (the identification and removal of known sources of Spam at all entry points); systems monitoring (the identification and alert of changes in systems security); the oversight of security alerts, advisories, and directives (the assessment of security threats); and information output handling and retention (information is handled in line with Federal Laws).	**Level 1** SI.L1-3.14.2 SI.L1-3.14.4 SI.L1-3.14.5	**Level 2** SI.L2-3.14.1 SI.L2-3.14.2 SI.L2-3.14.3 SI.L2-3.14.4 SI.L2-3.14.5 SI.L2-3.14.6 SI.L2-3.14.7	**Level 3** SI.L3-3.14.1e SI.L3-3.14.3e SI.L3-3.14.6e

Contents

Conclusion

The Cybersecurity Maturity Model Certification (CMMC) 2.0 framework represents a critical shift toward a more accountable and standardized cybersecurity posture within the Defense Industrial Base (DIB). By transitioning from a model of self-attestation to a verified maturity-based system, CMMC ensures that contractors handling Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) maintain a rigorous defense against sophisticated cyber threats. This tiered approach provides a clear, risk-based roadmap for organizations to secure the global defense supply chain and protect vital national security interests.

Cisco Duo delivers critical capabilities for addressing the stringent identity and access requirements mandated by the CMMC. Through its industry-leading Multi-Factor Authentication (MFA), comprehensive device health assessments, and granular adaptive access policies, Duo enables a Zero Trust architecture that verifies every user and every device before granting access to sensitive defense data. Its ability to provide deep visibility into the security posture of both managed and unmanaged devices makes it a versatile tool for organizations striving to reach the “Advanced” (Level 2) or “Expert” (Level 3) levels of CMMC compliance.

By mapping Cisco Duo to the CMMC framework—specifically the Access Control (AC) and Identification and Authentication (IA) domains—organizations can streamline their path to certification. Duo’s capabilities directly address the NIST SP 800-171 requirements that form the backbone of CMMC Level 2, allowing contractors to demonstrate technical compliance while helping to reduce the complexity of the third-party assessment process. Ultimately, integrating Cisco Duo into a CMMC-aligned strategy not only facilitates regulatory compliance but also helps build a resilient security foundation capable of protecting the nation’s most sensitive intellectual property and technological advantages.

Contents

Resources

If you'd like to go deeper on identity security, phishing resistance, or how organizations are using Cisco Duo in real-world environments, the following resources are a good place to start:

- MFA Buyer's Evaluation Guide

  A practical guide to help you understand what to look for in a modern MFA solution and how different approaches compare.

- Guide to Building End-to-End Phishing Resistance

  A closer look at how phishing-resistant authentication and device trust can significantly reduce credential-based attacks.

- Understanding the Business Impact of Cisco Duo

  A look at the business value organizations are seeing with Cisco Duo, based on a Forrester Total Economic Impact™ study showing a 198% ROI and $4.4M NPV.

- Why Customers Choose Cisco Duo for User Authentication

  Insights from customer reviews and feedback highlighted in Gartner Peer Insights™.

- Blog: Hello NIST, Meet Duo - Why Mapping Cisco Duo to NIST CSF 2.0 and NIST 800-53 Matters for the US Public Sector.
- Cisco Duo + CISA Zero Trust Maturity Model White Paper.
- Cisco Duo + NIST CSF 2.0 Solution Guide.

C07-6048931-00 04/26