NEXTLABS®

White Paper

NextLabs' Solution for the Cybersecurity Maturity Model Certification (CMMC) Program

The DIB encompasses entities that provide goods and services to the Department of Defense (DoD).

INTRODUCTION

The Cybersecurity Maturity Model Certification (CMMC) is a framework developed by the U.S. Department of Defense (DoD) to enhance the cybersecurity posture of organizations in the Defense Industrial Base (DIB). It establishes a structured system of cybersecurity requirements and maturity levels that contractors and suppliers must adhere to in order to qualify for DoD contracts. CMMC certification ranges from basic cybersecurity hygiene to advanced practices, promoting a culture of continuous improvement and enhancing the overall security and resilience of the defense supply chain.

The primary goal of the Cybersecurity Maturity Model Certification (CMMC) program is to bolster the cybersecurity resilience of organizations within the United States Defense Industrial Base (DIB). This is accomplished by protecting Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) that is shared with United States Department of Defense (DoD) contractors and subcontractors through acquisition programs.

- In alignment with the Federal Acquisition Regulation (FAR), FCI is defined as “information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government.” This does not include information provided by the Government to the public or simple trasactional information, such as that necessary to process payments.

- CUI is information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.

CMMC is largely based on NIST Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations." Published in February 2020, this document provides agencies with recommended security requirements for protecting the confidentiality of CUI. Unfortunately, prior to the existence of a certification program, the DoD found that contractors were falsely claiming to fully uphold all the NIST 800-171 standards. This led the DoD to develop a certification process to ensure that contractors were compliant with a basic set of cybersecurity controls, resulting in the CMMC.

In an era marked by escalating cyber threats and potential breaches of sensitive defense-related information, the CMMC acts as a proactive strategy to safeguard national security interests. It seeks to ensure that DIB organizations uphold a consistent, verifiable, and adaptive level of cybersecurity across their supply chains. The model's multi-tiered approach, ranging from basic cybersecurity hygiene to advanced practices, addresses the dynamic nature of cyber risks and encourages a continuous improvement mindset.

Through mandatory certification, the CMMC mitigates vulnerabilities, reduces the likelihood of cyberattacks, and safeguards sensitive data, intellectual property, and critical infrastructure. Furthermore, it fosters a culture of cybersecurity awareness, driving organizations to implement effective risk management, incident response, and cyber resilience strategies.

CMMC 1.0

The first version of the CMMC was published by the DoD on January 31, 2020. This initial version, outlined the framework's structure, requirements, and objectives for enhancing the cybersecurity posture of organizations within the DIB. CMMC 1.0 consisted of a set of cybersecurity requirements organized into five maturity levels, ranging from "Basic Cybersecurity Hygiene" to "Advanced/Progressive." Each level corresponded to specific practices and processes that organizations must implement and demonstrate to achieve certification. The practices covered various aspects of cybersecurity, including access control, incident response, risk management, security training, and more.

CMMC Level 1: Basic Cyber Hygiene

Level 1 of CMMC 1.0 referred to the basic cyber hygiene of an organization needed to protect FCI. The requirements for this level (17 practices) were similar to the ones specified in 48 CFR 52.204-21 for "the basic safeguarding of contractor information systems that process, store or transmit Federal contract information."

CMMC Level 2: Intermediate Cyber Hygiene

Level 2 consisted of a subset of requirements specified in NIST SP 800-171 and other standards. Becoming certified at this level meant that the organization had established and documented the necessary policies and practices to easily mimic them and develop mature capabilities.

CMMC Level 3: Good Cyber Hygiene

Level 3 was geared toward the protection of CUI and included all the security requirements listed in NIST SP 800-171, along with 20 additional practices. An organization had to establish and maintain a plan to demonstrate the set of activities needed to comply with CMMC to gain this level of certification.

CMMC Level 4: Proactive Cyber Hygiene

A Level 4 certification could be given to an organization only after demonstrating the capability to review practices for effectiveness and take corrective action. This level focused on protecting CUI from advanced persistent threats (APTs).

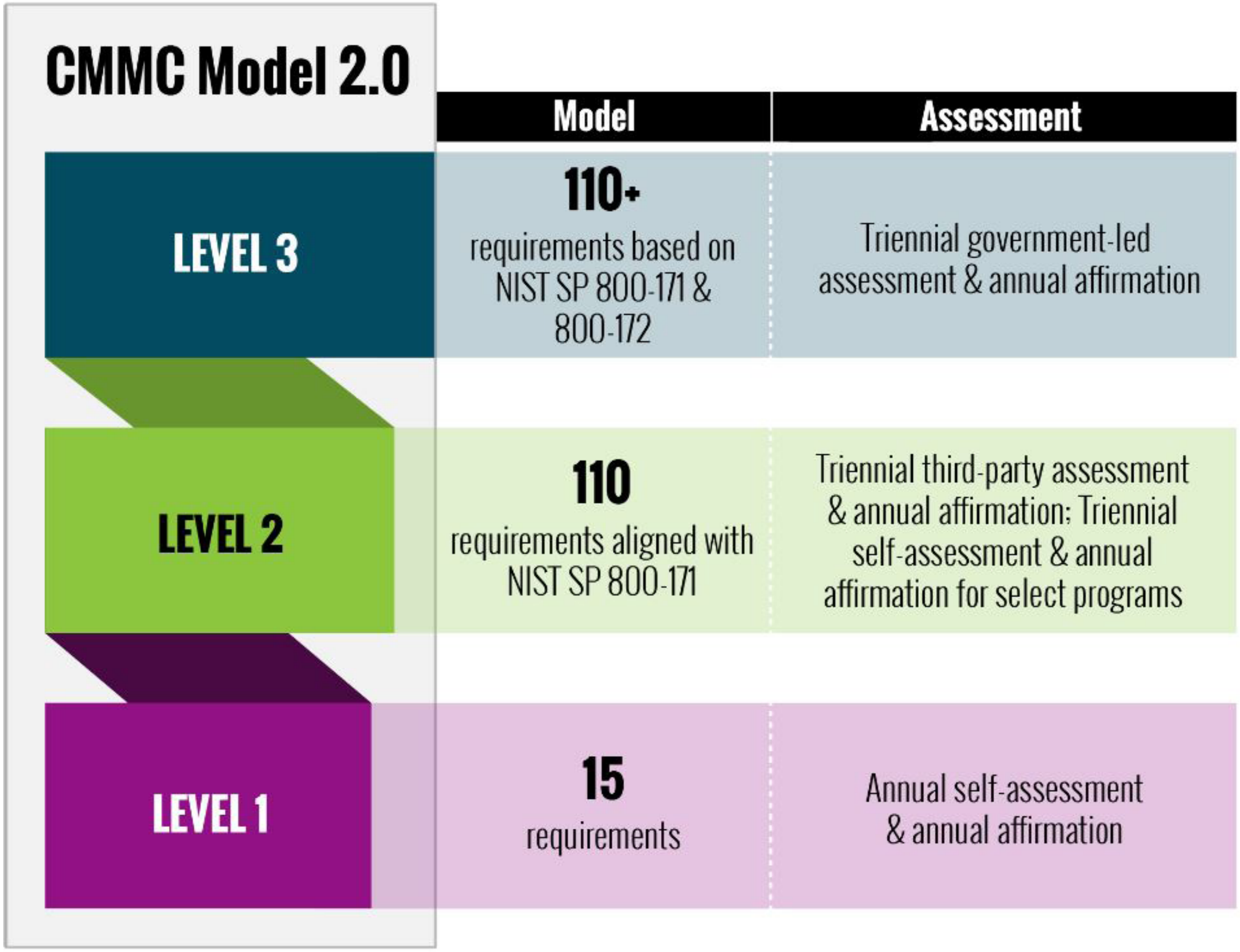
CMMC Level 5: Advanced Cyber Hygiene

At this level, organizations are expected to standardize and optimize processes across the organization with an increased focus on protecting CUI from APTs. To achieve this level of certification, they had to manage a total of 171 practices.

CMMC 2.0

In March 2021, the DoD initiated an internal assessment of CMMC 1.0 implementation. This assessment came following an interim rule the DoD published in September 2020 to the Defense Federal Acquisition Regulation Supplement (DFARS) in the Federal Register, which implemented the DoD's initial vision for the CMMC program (CMMC 1.0) and outlined the basic features of the framework. The interim rule became effective on November 30, 2020, establishing a five-year phase-in period. The assessment also came after CMMC 1.0 received criticism from small and midsize businesses (SMBs) over the complexity of the framework and its associated compliance costs. SMB owners became increasingly concerned that the costs associated with becoming certified would eventually force them out of the DIB.

This assessment of CMMC led cybersecurity and acquisition leaders within the DoD to refine policy and program implementation, eventually resulting in CMMC 2.0 which updates the program structure and requirements. CMMC 2.0 streamlines requirements from five levels to three levels of cybersecurity and aligns the requirements at each level with well-known and widely accepted NIST cybersecurity standards.



CMMC Model 2.0

	Model	Assessment
LEVEL 3	110+ requirements based on NIST SP 800-171 & 800-172	Triennial government-led assessment & annual affirmation
LEVEL 2	110 requirements aligned with NIST SP 800-171	Triennial third-party assessment & annual affirmation; Triennial self-assessment & annual affirmation for select programs
LEVEL 1	15 requirements	Annual self-assessment & annual affirmation

Figure 1: The Three Levels of CMMC Model 2.0

CMMC 2.0 Level 1: Foundational

Level 1 is the minimum requirement for organizations to bid on defense contracts. The new Level 1 applies to organizations that access, process or store FCI only and do not deal with CUI. It includes 17 practices that must be implemented to secure FCI. Documentation of a formal cybersecurity program is not required. Level 1 contractors will be required to self-assess and have an executive sign off on their compliance.

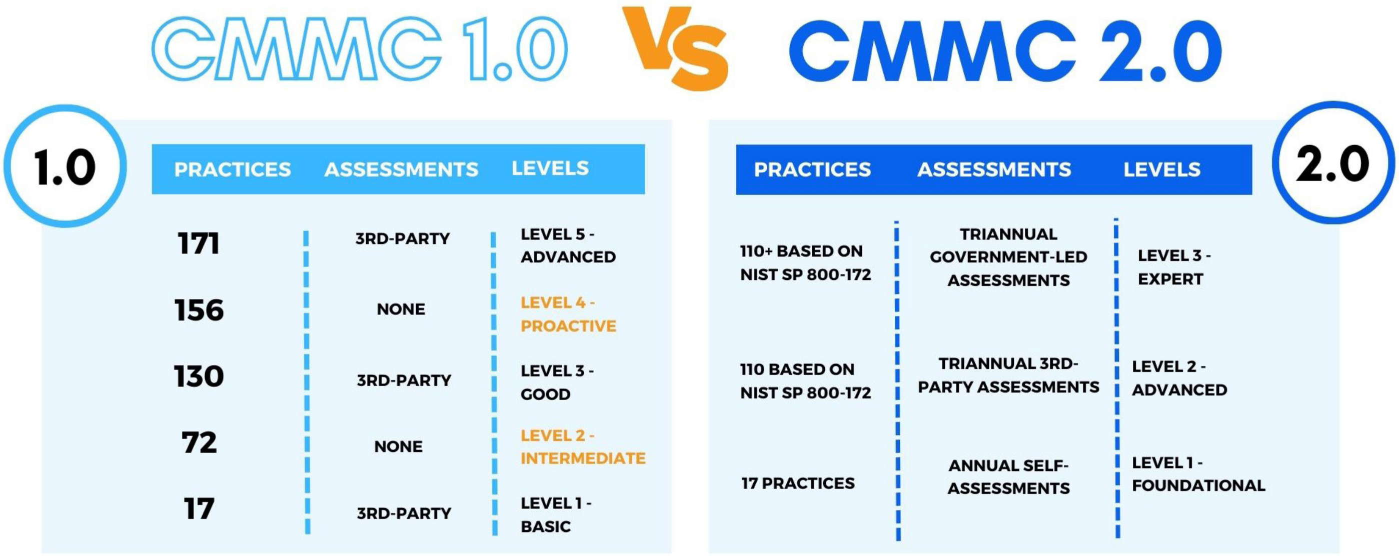
CMMC 2.0 Level 2: Advanced

Level 2 is the minimum level required to protect CUI or covered defense information (CDI), Level 2 includes all 110 cybersecurity controls found in NIST SP 800-171 and also requires a fully documented cybersecurity program and necessitates an independent assessment. As CMMC 2.0 rolls out, until assessment capacity builds, some Level 2 contractors may be allowed to self-assess their compliance.

CMMC 2.0 Level 3: Expert

Even though the DoD is still developing the specific security requirements of Level 3, it has indicated that it will include all 110 NIST SP 800-171 controls plus a subset of the advanced threat controls in NIST SP 800-172.

In each level, the number of controls has also decreased. With CMMC 2.0, the DoD has eliminated all maturity processes, which measure the degree to which an organization has integrated the security practices into their operations. 20 security requirements were also dropped — the new level only needs organizations to implement the 110 security controls mentioned in NIST SP 800-171 to ensure the protection of CUI.



CMMC 1.0 VS CMMC 2.0

1.0

PRACTICES	ASSESSMENTS	LEVELS
171	3RD-PARTY	LEVEL 5 - ADVANCED
156	NONE	LEVEL 4 - PROACTIVE
130	3RD-PARTY	LEVEL 3 - GOOD
72	NONE	LEVEL 2 - INTERMEDIATE
17	3RD-PARTY	LEVEL 1 - BASIC

2.0

PRACTICES	ASSESSMENTS	LEVELS
110+ BASED ON NIST SP 800-172	TRIANNUAL GOVERNMENT-LED ASSESSMENTS	LEVEL 3 - EXPERT
110 BASED ON NIST SP 800-172	TRIANNUAL 3RD-PARTY ASSESSMENTS	LEVEL 2 - ADVANCED
17 PRACTICES	ANNUAL SELF-ASSESSMENTS	LEVEL 1 - FOUNDATIONAL

Figure 2: CMMC 1.0 vs. CMMC 2.0

The key differences to CMMC 2.0 include fewer levels, self-assessments, and flexible timing. Instead of the original five levels of certification, CMMC 2.0 only has three, which are more closely aligned with existing cybersecurity standards.

Level 2, for example, will comply with NIST SP 800-171, the guideline that governs how contractors handle regulated unclassified data. Further, self-assessments are allowed for Level 1 and Level 2 certifications. This will save many, if not all, contractors the time and cost of conducting a third-party evaluation. However, it will also increase the risk for contractors who wrongfully certify their compliance. Contractors can be certified even if they do not satisfy all the standards provided, given they have a clear strategy for when and how they will accomplish the standards.

Why do organizations need CMMC?

Over 300,000 members of the DIB — defense contractors, manufacturers and SMBs — must comply with CMMC. Depending on the data an organization manages or is looking to manage, they must implement the requirements of the certification level needed to either continue their current contract with the DoD or enter a new one.

Further, implementing the CMMC can yield substantial business benefits for enterprises beyond the obvious security advantages. First, CMMC certification can significantly broaden a company's market reach. With many industries recognizing the importance of robust cybersecurity practices, holding a CMMC certification can be a valuable differentiator that attracts clients and partners beyond the defense sector. This can lead to expanded business opportunities, partnerships, and increased revenue streams.

Additionally, CMMC implementation often translates into operational improvements. The framework encourages organizations to establish clear processes, documentation, and incident response plans. This heightened organizational clarity can streamline operations, reduce errors, and minimize downtime during incidents, in turn resulting in a more agile and competitive position in the market. In essence, CMMC serves not only as a security measure but also as a strategic business asset with the potential to drive growth and operational excellence.

NextLabs' Solution for CMMC

NextLabs® patented dynamic authorization technology and industry leading zero trust policy platform helps enterprises identify and protect sensitive CUI and FCI, monitor and control access to the data, and prevent regulatory violations – whether in the cloud or on premises – in order to receive Cybersecurity Maturity Model Certification.

As a member of the NIST National Cybersecurity Excellence Partnership (NCEP) program, NextLabs helps organizations meet the security requirements of the National Institute of Standards and Technology (NIST), in turn aiding in compliance with CMMC as it is largely based on NIST SP 800-171.

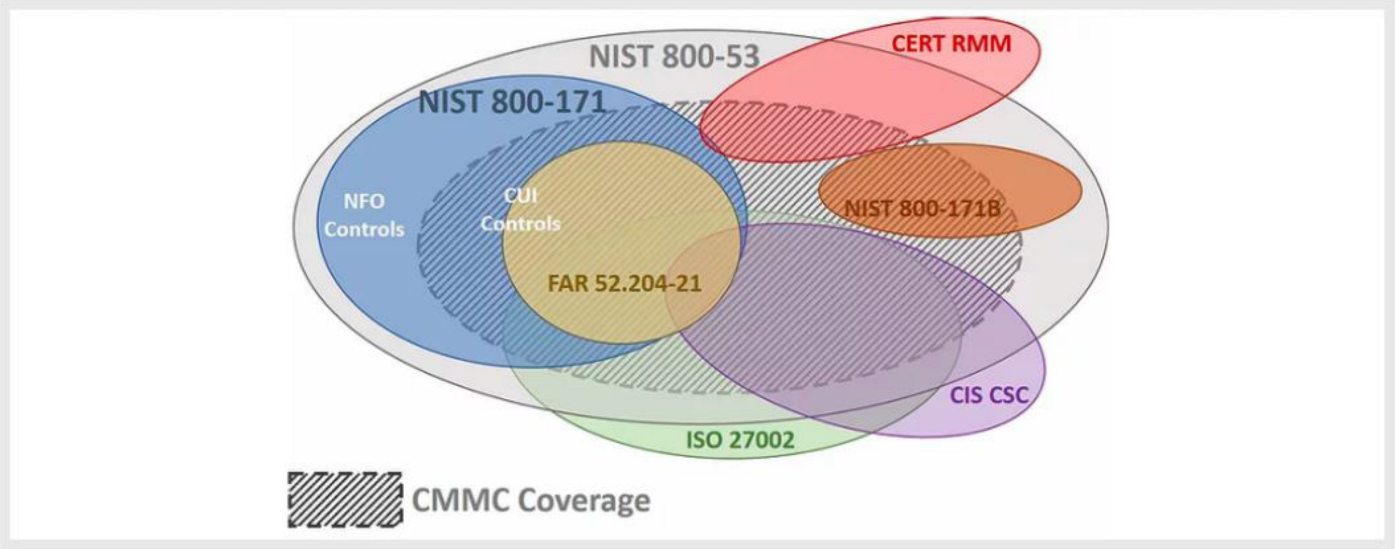


Figure 3: NIST Special Publications overlap with other security requirements

NIST 800-171 vs CMMC

To address CMMC requirements, NextLabs provides a zero trust data-centric security software suite which uses ABAC and dynamic authorization to automate access management, prevent wrongful disclosure, secure data access, and protect data. NextLabs applies an identity-centric approach that utilizes multi-dimensional profiles containing subject and resource attributes to protect and secure access to critical enterprise resources. By ensuring least privilege access continuously in real-time, enterprises can enforce secure access to network resources and segregate data. Equally important, is the capability to secure business-critical application and data with externalized authorization management, secure global data access, and persistent protection of data at rest and on the move.

The DoD has defined 14 domains that organizations need to address as part of full CMMC 2.0 Level 3 compliance. NextLabs products can help organizations in most of these domains as described below.

Access Control	With NextLabs' zero trust policy engine, organizations can create policies that leverage contextual factors, at the time of request, that influence whether users should be granted permission to access sensitive information, like CUI, and apply them consistently across the organization. These factors, or attributes, may include group, project, classification, device, and network, as well as any other relevant variables. The attribute-based policy platform enables organizations to automate controls to prevent regulatory and corporate violations, monitor information access and usage, and streamline the audit process.
Awareness and Training	NextLabs' zero trust policy engine can provide alerts and messages to inform end users when handling CUI and FCI data in real time. When developing their security training and awareness programs, organizations can train their employees to fully utilize NextLabs solutions to improve data security across the entire enterprise.
Audit and Accountability	NextLabs CloudAz policy platform allows organizations to centrally audit and manage fine-grained authorization across all application, database, file servers, portals, and document management systems in the enterprise to reduce administrative and audit costs and satisfy compliance requirements.
Security Assessment	NextLabs centralized monitoring, auditing, and reporting allows administrators to oversee all data access activity, including when data access is denied, across all applications to ensure that only authorized users are accessing sensitive information. With the use of API's and SDK's, NextLabs centralized policy management allows policies to be changed on the fly, even with internally developed software.
Configuration Management	With NextLabs centralized policy management, administrators can configure access policies based on the principle of least privilege, where users and devices are only granted access to the resources they need to perform their duties. Centrally managed policies provide the flexibility to make changes to access rights and data security needs on the fly without complex customization and manual procedures.
Identification and Authentication	NextLabs Zero Trust Data Security Suite is identity centric and identity provider agnostic. With attribute-based access control polices, each attribute of the user trying to access the data is evaluated before granting access. Factors such as location, network, device, time, classification, role type, and more must be correctly satisfied before access to sensitive data is granted, ensuring that only the correct users obtain access.
Incident Response	NextLabs centralized monitoring, auditing, and reporting allows administrators to oversee all data access activity in real-time, including when data access is denied, across all applications to ensure that only authorized users are accessing sensitive information. This activity data can facilitate incident response and allow administrators to proactively mitigate threats before breaches occur.

Maintenance	NextLabs centralized policy management platform makes maintenance and security updates easy as policies can be added, adjusted, and deployed quickly.
Media Protection	N/A
Physical Protection	N/A
Personnel Security	With ABAC technology, NextLabs solutions can filter individuals before granting access to systems containing regulated unclassified information (CUI). When a person is transferred or terminated (their attributes change) they will no longer have access to the same data as these access decisions are made dynamically in real-time.
Risk Assessment	The NextLabs zero-trust policy engine allows organizations to define specific, attribute-based policies tailored to their needs and what type of data they need to protect. Classifying this data and applying a custom security policy to it ensures that only authorized users who satisfy the attributes specified in the policy gain access.
Systems and Communications	The NextLabs policy engine allows administrators to define custom policies that support their specific data security needs. The policies are attribute-based and grant access dynamically in real-time, meaning only authorized users will have access to sensitive data.
Systems and Information Integrity	NextLabs CloudAz allows administrators to factor in the status of the system where a request is originating from or where data is being accessed so that requests are not granted if they are coming from potentially compromised or insecure systems.

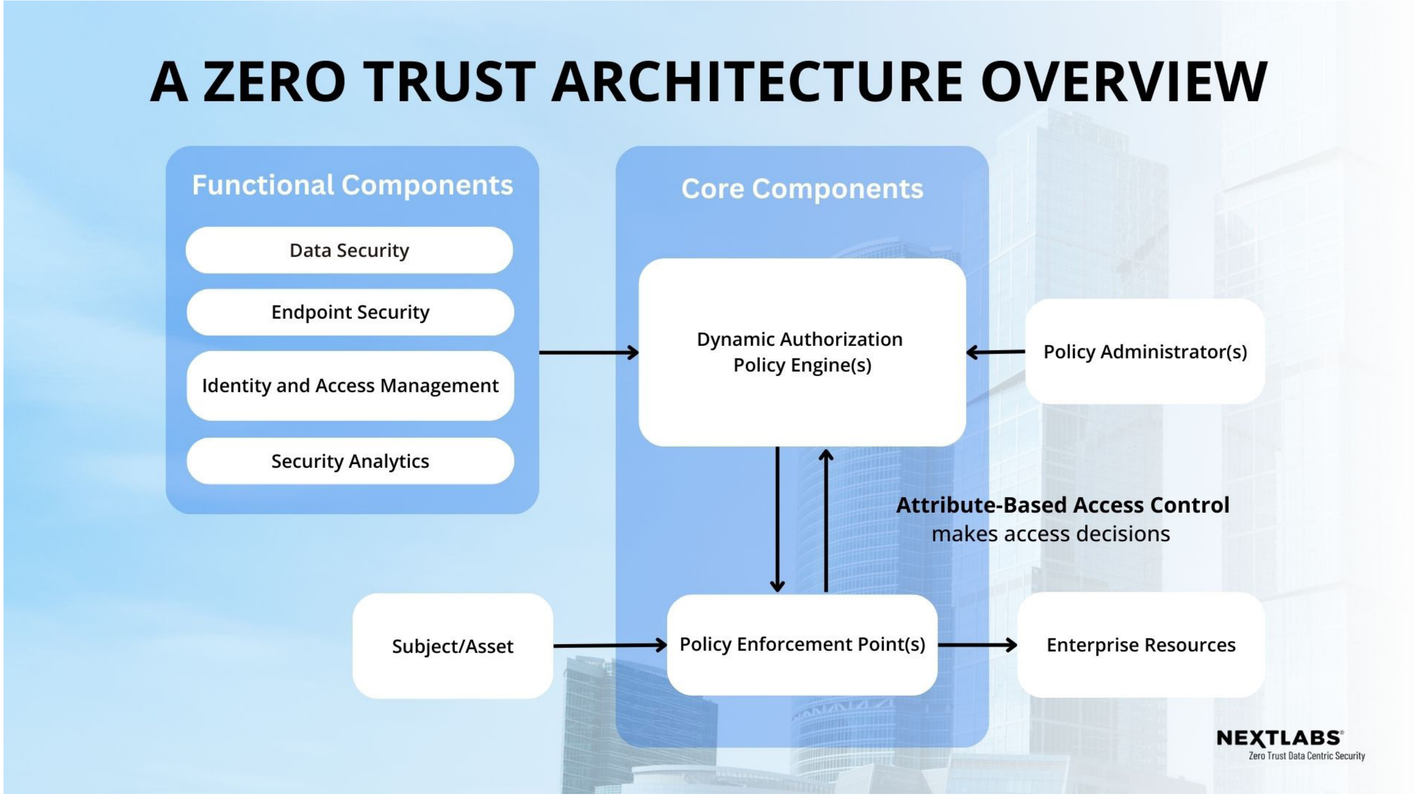

A ZERO TRUST ARCHITECTURE OVERVIEW
Functional Components
Data Security
Endpoint Security
Identity and Access Management
Security Analytics
Core Components
Dynamic Authorization Policy Engine(s)
Policy Administrator(s)
Attribute-Based Access Control makes access decisions
Subject/Asset
Policy Enforcement Point(s)
Enterprise Resources
NEXTLABS
Zero Trust Data Centric Security

Figure 4: How a ZTA works with ABAC

NextLabs' Zero Trust data-centric security suite consists of:

1. **CloudAz**, a unified policy platform that centralizes administration and utilizes the "never trust, always verify" principle, ensuring data is protected at any access point.

2. **Data Access Enforcer (DAE)** helps enterprises protect data access from anywhere, by securing access and protecting critical data stored in databases and data lakes.

3. **SkyDRM** ensures persistent protection of critical files and documents to protect data on the move and at rest.

4. **Application Enforcers** can be used to secure applications, enforce data security controls, and simplify role management to protect data at the source by externalizing authorization with Attribute-based Access Control (ABAC) principles.

With a unified policy engine, enterprises can have a cohesive security ecosystem that is flexible and provides consistent enforcement, monitoring, and auditing to protect critical assets both inside and outside of the enterprise. Access policies are managed externally from the protected application, which means they can be modified without requiring code changes or application downtime. This enhances organizational agility and allows companies to respond quickly to ever-changing business conditions and regulatory environments.

Key Takeaways

Cybersecurity Maturity Model Certification is a crucial initiative for companies in the DIB due to its role in bolstering cybersecurity practices, enhancing eligibility for DoD contracts, improving business reputation, and mitigating cyber risks. It positions companies to navigate the evolving cyber threat landscape while demonstrating their commitment to both national security and sound business practices.

Implementing NextLabs' Zero Trust Data-Centric Security Suite, with its unified policy engine that applies dynamic authorization and zero trust principles, helps enterprises achieve CMMC by identifying and protect sensitive CUI and FCI, monitoring and controlling access to the data, and preventing regulatory violations. To learn more about our Data-Centric Security Suite, please visit our website.

References

NIST 800-171 vs CMMC. (2023, 10 31). Retrieved from Compliance Forge: https://www.complianceforge.com/blog/nist-800171-vs-cmmc/

A Guide to CMMC Compliance. (2023, 10 31). Retrieved from Compliance Manager GRC: https://www.compliancemanagergrc.com/blog/a-guide-to-cmmc-compliance/

About CMMC. (2023, 10 31). Retrieved from US Department of Defense: https://dodcio.defense.gov/CMMC/about/

CMMC Model. (2023, 10 31). Retrieved from U.S. Department of Defense: https://dodcio.defense.gov/CMMC/Model/

Externalized Authorization Management. (2023, 10 31). Retrieved from NextLabs: https://www.nextlabs.com/products/technology/externalized-authorization-management/

FAR. (2023, 10 31). Retrieved from Acquistion.gov: https://www.acquisition.gov/far/subpart-4.19

NIST SP 800-171 Rev. 2. (2023, 10 31). Retrieved from NIST Community Security Resource Center: https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final

ABOUT NEXTLABS

NextLabs®, Inc. provides data-centric security software to protect business critical data and applications. Our patented dynamic authorization technology and industry leading attribute-based policy platform helps enterprises identify and protect sensitive data, monitor and control access to the data, and prevent regulatory violations – whether in the cloud or on premises. The software automates enforcement of security controls and compliance policies to enable secure information sharing across the extended enterprise. NextLabs has some of the largest global enterprises as customers and has strategic relationships with industry leaders such as SAP, Siemens, Microsoft, and IBM. For more information on NextLabs, please visit http://www. nextlabs.com.