PKWARE®

A BLUEPRINT FOR CUI SECURITY COMPLIANCE

Department of Defense acquisition regulations have required government contractors and sub-contractors to assert compliance with the NIST 800-171 standard for securing "controlled unclassified information" (CUI) that the government shares with the defense industrial base.

The DoD is now rolling out a compliance certification regime using a cyber maturity model framework, CMMC. Vendors to the DoD will be required to have a third-party assessment of the company's cyber controls that attests that the company is able to protect CUI under the CMMC guidelines. Vendors who are not assessed at a certain maturity level will not receive new contract awards from the government.

This paper provides a methodology for protecting CUI that is easy and cost-effective for an organization to implement and will satisfy the CMMC maturity requirements of a company's DoD contracts. This CUI-centric data protection methodology assures that CUI data can only be accessed by employees and sub-contractors that have appropriate clearance, or program authorization from the government.

CONTENTS

WHAT IS CUI-CENTRIC SECURITY?

CUI-centric security is a fundamentally different approach for protecting sensitive data from theft or misuse.

Most security technology focuses on **where** data is—protecting, for example, all the data stored on a specific laptop or server, or all the data that crosses a specific network. The problem with this approach is that as soon as data moves somewhere else, another solution is required, or data is left unprotected.

CUI-centric security, on the other hand, focuses on **what** needs to be protected—the files containing sensitive information—and applying the appropriate form of protection no matter where the data happens to be.

CUI-CENTRIC SECURITY IN ACTION

The defining characteristic of CUI-centric security is that protection is applied to data itself, regardless of the data's location. To be effective, this must happen automatically—sensitive information should be identified and classified as soon as it enters an organization's IT ecosystem, and should be secured with policy-based protection that lasts throughout the data lifecycle.

A typical implementation of CUI-centric security consists of software agents installed on every IT asset where sensitive data might be created or stored—laptops, desktops, servers, mainframes, mobile devices, and elsewhere. These agents are controlled by a centralized management console, where administrators define the appropriate form of protection for each data type and use case.

Each time a file is created or modified, the system scans the file to determine whether it contains sensitive information, classifies the information, and automatically applies the appropriate protection. End users may be given the ability to modify these actions manually, but are otherwise not involved in the process. Protected data remains available to authorized users, but cannot be accessed by unauthorized users, even when files travel outside the company network.

When implemented on an organization-wide scale, data-centric security reduces or eliminates the impact when network and device protections inevitably fail, while at the same time removing data silos and other internal obstacles.

DEFINING CUI

Controlled unclassified information is grouped into approximately 20 "organizational index groupings," including defense, intelligence, financial, and law enforcement information.

Defense-related CUI is defined by the following four categories:

Controlled Technical Information: Technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.

DoD Critical Infrastructure Security Information: Information that, if disclosed, would reveal vulnerabilities in the DoD critical infrastructure and, if exploited, would likely result in the significant disruption, destruction, or damage of or to DoD operations, property, or facilities.

Naval Nuclear Propulsion Information: Information related to the safety of reactors and associated naval nuclear propulsion plants, and control of radiation and radioactivity associated with naval nuclear propulsion activities.

Unclassified Controlled Nuclear Information - Defense: Information relating to Department of Defense special nuclear material (SNM), equipment, and facilities.

KEY PRINCIPLES OF CUI-CENTRIC SECURITY

Each organization requires a unique solution—one tailored to fit the company's threat exposure and business needs. However, all successful implementations of CUI-centric security have certain characteristics in common: they're tightly controlled from a **centralized management** system, they provide coverage across the entire organization with **no security gaps**, they rely on **automation** rather than manual intervention, and they're **adaptable** enough to grow and change along with the organization.

Every CUI-centric security solution must be designed with these key principles in mind, or the finished product will fall short of its goals.

CENTRALIZED CONTROL

Centralized management is essential to ensure that data is protected according to the organization's security policies, and that data remains available for appropriate use.

Most organizations, even those that have not adopted the data-centric model, already have some data-level protection in place. Typically, this takes the form of user-applied file encryption—when employees encrypt files with passwords before sharing them with colleagues or external recipients.

Though very common, this approach creates three significant problems:

- Employees might neglect to apply protection when needed, or might choose methods that don't provide adequate protection.
- When they do encrypt their files, employees must then find a way to share the passwords (the encryption keys) with the recipients, which typically requires the use of unencrypted email or another unsecured method.
- User-applied encryption leaves employees, rather than administrators, in control of encryption keys. When keys are not available (for example, when employees fail to share them, forget them, or leave the company without providing them), the organization can permanently lose access to critical data.

An effective encryption strategy eliminates these issues and gives the organization complete control over CUI from the moment that each file is created.

- Access to protected data can be granted or revoked at any time.
- All activity is logged for auditing and reporting.
- Ad hoc encryption, which blinds an organization's DLP system, is eliminated.

GAPLESS PROTECTION

Network-centric and device-centric security strategies inevitably leave gaps between protected systems, because data has to be decrypted or otherwise stripped of protection before it can be transferred between operating systems or platforms. Even experienced security managers can be unaware that sensitive information is being sent or stored without protection. Hackers and malicious insiders, however, are adept at finding and exploiting these gaps.

Organizations can eliminate gaps by implementing a data protection solution that provides both of the following:

- **Persistent protection** that travels with files, even when they are sent outside the company network.
- **Cross-platform operability** that allows the organization to protect files (and make them available for authorized use) on every operating system within its IT architecture.

AUTOMATION

Automated workflows are the key to success in information security. End users do have a part to play in protecting an organization's information, but they should not be expected to shoulder the burden of evaluating and securing the large and constantly growing volumes of data they handle each day.

Automation takes user error out of the equation, and allows employees to do their jobs without interruption and without jeopardizing the security of CUI.

An organization's security technology must apply its data protection policies in real time, across the entire enterprise, without user intervention. This requires technology that continuously monitors file activity, and automatically applies the appropriate classification and protection as soon as sensitive data appears.

ADAPTABILITY

CUI-centric security is not a "one size fits all" proposition. Within a single organization, there can be dozens of security policies, hundreds of data types, and thousands of use cases. Some data might require encryption, while other data may need to be redacted, deleted, quarantined, or left as is.

An effective security strategy will be tailored to meet the organization's unique requirements, while accommodating changes in those requirements over time. Organizations must have confidence that they can add and remove infrastructure, change business processes, and create new partnerships, without having to rebuild their data security solution each time.

POLICIES, RULES & WORKFLOWS

As in any rapidly evolving industry, cybersecurity's vocabulary is always changing. However, the following terms are commonly used to describe the distinctions between an organization's high-level security requirements and the ways those requirements can be implemented in the "real world" of the organization's IT ecosystem.

POLICIES	RULES	WORKFLOWS
Policies are written documents that define an organization's standards and goals for data security. Without automated technology, an organization must rely on employees to remember and follow its data security policies.	Rules are specific software configurations that apply an organization's policies to different use cases. For example, if an organization's written policy states that all files containing a certain project name must be encrypted, it can create rules in its software to specify which devices and locations need to be monitored for files containing the project name, and which encryption methods and keys should be used to protect the files.	Workflows are the internal processes used by software to carry out the actions specified by rules. Workflows describe each step taken by a system in a given use case, including monitoring file activity, scanning for sensitive data, applying classification tags, and applying encryption or other forms of protection.

BEFORE YOU BUILD

In order to design a successful CUI-centric security solution, an organization needs a thorough understanding of its data risks and business needs. The more an organization knows about its data and the threats facing it, the more able it will be to keep data safe from misuse, while allowing files to move freely between authorized users.

A detailed data risk assessment, followed by a review of existing security policies, will allow your organization to get the maximum value for its investment in CUI-centric security.

CONDUCT A DATA RISK ASSESSMENT

Risk assessments are a necessary step in any cybersecurity effort, and are called for in a variety of guidelines and mandates, including the National Institute of Standards and Technology's cybersecurity framework.

Even if your organization has conducted cyber risk assessments in the past, it's best to make a fresh assessment before beginning a data-centric security implementation. This will ensure that you account for any recent changes to IT infrastructure or business processes, and identify any data specific issues that may not have been documented in previous assessments.

Specifically, your data risk assessment should focus on the following elements:

- The types of data being created and acquired by users, applications, and automated processes
- The use cases for each type of data and each user group
- The risks associated with each data type and use case
- Which users and/or roles should have access to data in each use case
- The role and effectiveness of any existing data protection technology
- Any applicable government or industry standards relating to data security, such as CMMC, GDPR, or HIPAA, and the consequences of noncompliance

With this information in hand, you will be prepared to set your organization's data security priorities, and define policies that will guide you as you choose your new technology and build your security solution.

DEFINE YOUR DATA SECURITY POLICIES

Written security policies provide the foundation for a CUI-centric security strategy. In addition to communicating the organization's security standards to administrators and end users, written policies provide assurance to regulators, corporate boards, and customers that the company understands the importance of information security.

Most organizations' written policies focus on protocols for device access and network access, because those are the areas that traditional security technology can address. With a data-centric approach, however, companies gain the ability to enforce specific standards for how each type of data should be managed and protected, regardless of where the data resides.

If your organization's written policies do not already provide guidance on how different forms of data should be treated, the policies should be expanded to answer the following questions:

- What are the organization's data security compliance obligations?
- What are the expectations of the organization's customers, employees, board members, auditors, and government regulators?
- Which types of data are considered sensitive?
- Which user groups or profiles should have access to each type of sensitive data?
- What forms of protection or remediation are required for different data types?
- What are the required time frames for data retention or deletion?

CHOOSING YOUR TECHNOLOGY

Once your organization has documented its data security goals and requirements, the next step is to choose a technology that can help it meet those objectives.

To make the right decision, your organization will need to consider its capacity for implementing new technologies, the basic architecture of a data-centric security solution, and the capabilities it will need in order to enforce your written policies across the enterprise.

PLATFORM VS. POINT SOLUTIONS

Point solutions—products that address only one or a few use cases—are commonly used for network and device security, but are not well suited to the data-centric security model. Using multiple independent products to apply data-level protection can create data silos and security gaps, defeating the purpose of the implementation.

Rather than purchasing multiple products from multiple vendors, organizations are better served by implementing a comprehensive data security platform—a solution that integrates the full set of capabilities they require, and provides options for adding or creating new capabilities in the future.

Not only does the platform approach simplify administration by giving managers a single point of control for all data security activity, it simplifies the process of expanding or enhancing the solution in the future to address changes in its infrastructure or business processes.

ARCHITECTURE

A data-centric security system typically consists of a management console and an array of software agents, along with any supporting infrastructure the organization might require.

- The **management console** is the central component of the solution, where administrators convert the organization's written policies into automated rules and workflows that will be carried out by agents across the enterprise. The management console should also provide reporting and auditing tools that allow the organization to monitor activity and identify emerging threats.
- **Agents (or apps)** installed on laptops, desktops, servers, mobile devices, and other IT assets are responsible for monitoring file activity and taking action on sensitive data. Agents must remain in regular communication with the management console in order to receive policy updates and to deliver data for logging and auditing.
- **Supporting infrastructure** might consist of a hardware appliance to host the management console, as well as any additional elements such as hardware security modules, true random number generators, or KMIP (Key Management Interoperability Protocol) connectors.

KEY CAPABILITIES

In order to address the variety of data types and use cases required by a large organization, a security solution must provide a wide range of capabilities. Each of features and functions listed below is likely to be necessary for a corporation or government agency.

POLICY MANAGEMENT	The primary function of an administration console. An organization's written security policies need to be translated into system settings, automated rules, and other configurations that control how sensitive data is identified and protected. The more complex an organization's use cases, the more important it is that the administration console provides an intuitive way to create and organize those settings.
DATA DISCOVERY	Data discovery involves monitoring file activity and automatically scanning new or modified files to determine if they contain sensitive data. As each organization will have its own definition of "sensitive data," the solution must allow administrators to define criteria that will identify a file as sensitive.
CLASSIFICATION	Classification is the process of tagging files with metadata and visual labels to indicate their contents and appropriate use. In most cases, classification should be automatically applied based on the results of a data discovery scan. Some organizations also give end users the ability to add, remove, or change file classifications.
PERSISTENT ENCRYPTION	Persistent encryption is the strongest form of data protection, rendering data inaccessible to unauthorized users while allowing authorized users to decrypt and read a file's contents. A robust key management feature is essential to ensure that encrypted files are accessible to only the proper users at all times.
DATA REDACTION	Data redaction involves replacing sensitive data with non-sensitive data (for example, replacing credit card numbers with strings of asterisks). These approaches are often used when files contain sensitive information along with other information that needs to be made widely available.
MOVING AND QUARATINING	Moving and quarantining data is often necessary when files containing sensitive information are saved in inappropriate locations. For example, if employees are not permitted to save project information on their laptops, a data-centric security solution can be configured to copy files to a secured server and delete the files from the laptops where they appeared.
FILE DELETION	File deletion may be necessary in cases where a file contains data that should not be saved or stored in a specific location, or should not exist within the organization at all.
AUDITING AND REPORTING	Auditing and reporting are essential for detecting threats and demonstrating compliance with internal and external mandates. A solution's management console should provide detailed reporting on which files contain sensitive data, where the files are located, and who has been granted access to them.
INTEGRATIONS	Integrations with other key elements of the organization's IT infrastructure helps streamline workflows and ensure that all sensitive data is managed appropriately. A data security solution should be able to work with the organization's ERP systems, proprietary applications, productivity tools, and other technology

BUILDING AND IMPLEMENTING

Many organizations take a phased approach when implementing data-centric security, addressing their most critical security risks (and/or their most straightforward use cases) first, before expanding the solution to additional user groups, operating systems, and business units.

Typically, the implementation process consists of defining criteria that will be used to identify sensitive data, creating automated rules and workflows that apply the organization's written policies to different data types, and deploying agents to enforce the organization's policies wherever sensitive data can be created, acquired, modified, or stored.

DEFINING SENSITIVE DATA

Most organizations categorize information as "sensitive" if its ownership or use is restricted by a government or industry mandate, or if it cannot be made public without damage to the organization's reputation and ability to compete.

An organization's general definition of sensitive data should be established in its written policies, but security administrators typically need to create more detailed definitions in order to correctly identify files that require protection. Criteria for identifying data can be defined in a number of ways:

- Patterns are sequences of characters that match specific formats, such as Social Security numbers or credit card numbers. To prevent false positives, discovery scanning technology needs to incorporate the specific algorithms that are used to generate these data types.
- Dictionaries are lists of specific terms (such as "patient" or "confidential") that may be found in files containing sensitive data.
- Regular expressions are logical statements that can be used to identify certain types of data, and are particularly useful for detecting data that one organization might consider sensitive, but is not generally considered sensitive by other companies.

APPLYING RULES

Rules are the mechanisms for applying the organization's written policies to its sensitive data, and define what should happen to files containing sensitive data in different situations.

Data protection rules can take many different forms, depending on the organization's IT infrastructure and approach to granting access to sensitive data. In general, though, most rules follow a general pattern:

- Define the **data type** to which the rule applies (for example, credit card numbers)
- Define the **conditions** under which the rule should be executed (for example, when a file containing a specific term is saved on an employee laptop)
- Define the **action** to be taken when the rule conditions are met (for example, encrypt the file with a specific key, or copy the file to a quarantined location and delete the original)

As with the definition of sensitive data, an organization's list of data protection rules will likely be more detailed than the general standards described in its written policies. A large organization may need to create hundreds of rules to address its full range of data types and use cases.

After an organization's security administrators have defined the data types requiring protection and the rules to be followed when sensitive data is detected, the remaining step is to deploy software agents that will enforce those rules across the enterprise.

A NEW DEFINITION OF SECURITY

Once an effective CUI-centric security solution is in place, it becomes impossible for government sensitive data to exist in violation of the organization's security policies.

Files are automatically scanned upon creation or modification, tagged with visual labels and metadata, and given appropriate protection without the need for action by end users. If a protected file is shared in an unsecured cloud location, mistakenly emailed to an unauthorized user, or stolen by an intruder, the data contained in the file remains safe from exploitation.

CUI-centric security is the only approach that provides this level of security, and the only approach that can deliver meaningful protection against today's constantly evolving cyber threats.

PKWARE's automated data security platform that allows organizations to detect, classify, and protect sensitive data on every enterprise operating system.

With PKWARE, your organization can meet its compliance obligations and keep data safe from internal and external threats, without disrupting the way you do business today.

PKWARE's encryption technology has received a Designation as a Qualified Anti-Terrorist Cyber Security Technology by the Safety Act Commission administered by the Department of Homeland

PKWARE®

www.PKWARE.com | 201 E. Pittsburgh Ave. | Suite 400 | Milwaukee, WI | 866-583-1795