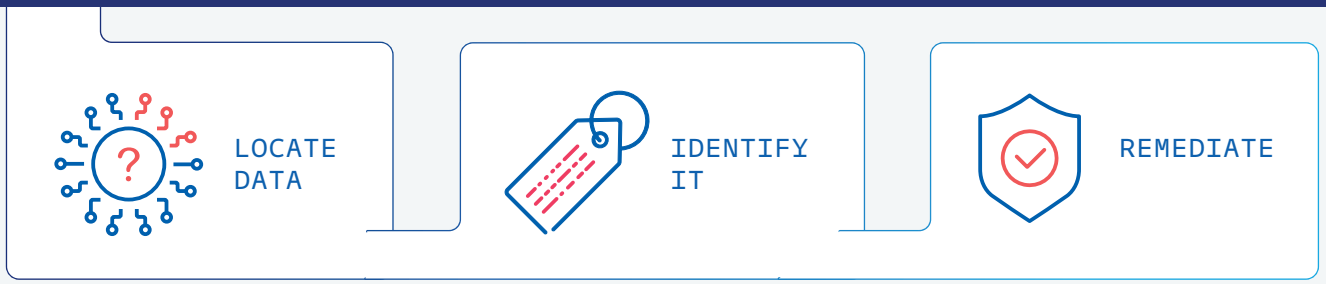
PKWARE

PK Protect

PK Protect

Solution Overview: NIST and CMMC Compliance

The National Institute of Standards and Technology (NIST) was founded in 1901 as a non-regulatory federal agency within the US Department of Commerce and partners with various other departments. In contrast, the Cybersecurity Maturity Model Certification (CMMC) is led within the Department of Defense and focuses on safeguarding supply chain sensitive data. Version 1.0 became available in January 2020.



The NIST 800-171 and the CMMC with PK Protect

Organizations that do business with the federal government often are acquiring, processing, storing, and sharing sensitive data. In some cases, the information is not considered government classified, and yet requires protection against misuse, inappropriate access, loss, or theft.

The NIST Special Publication 800-171 provides standards for ensuring the security and confidentiality of Controlled Unclassified Information (CUI) both when shared outside of federal systems or agencies or when an authorizing law, policy, or regulation does not specifically safeguard the CUI categories. The CCM measures the ability of vendors and their supply chains to protect CUI and Federal Contract Information (FCI).

PK Protect offers a complete and platform-wide approach to meet NIST and CMMC requirements.

Achieving Automated, Data-Centric Security

PK Protect simplifies compliance with NIST 800-171 and CMMC requirements as well as other government and industry mandates and regulations.

PK Protect enables companies and organizations to maintain control over sensitive data even in the most complex use cases. Our platform provides an array of integrated capabilities designed for maximum flexibility, broad platform support, and ease of use.

- Administrators use PK Protect Endpoint Manager to define policies for data discovery, indexing, identity creation, classification, and protection.
- PK Protect endpoint agents monitor file activities on laptops, desktops, and servers. PK Discover scans data repositories in all cloud and on-premises environments. New and modified data in files are scanned at the element level to ensure the organizational sensitive data protection policies are being met.
- Sensitive data can be indexed, classified, encrypted, masked, redacted, moved, or deleted based on company policies.
- PK Protect addresses further requirements for encryption key management and logging.
- Additional PK Protect capabilities extend policy enforcement to mainframe and midrange systems, mobile devices, and proprietary applications.

Industry contributions of the NIST include:

- Online Security through Strong Encryption
- Cybersecurity Framework
- Cybersecurity in Industrial

Control Systems

- Advanced Manuacturing
- Robotics
- Technology Transfer
- Forensic Science and Scientific

Data Systems

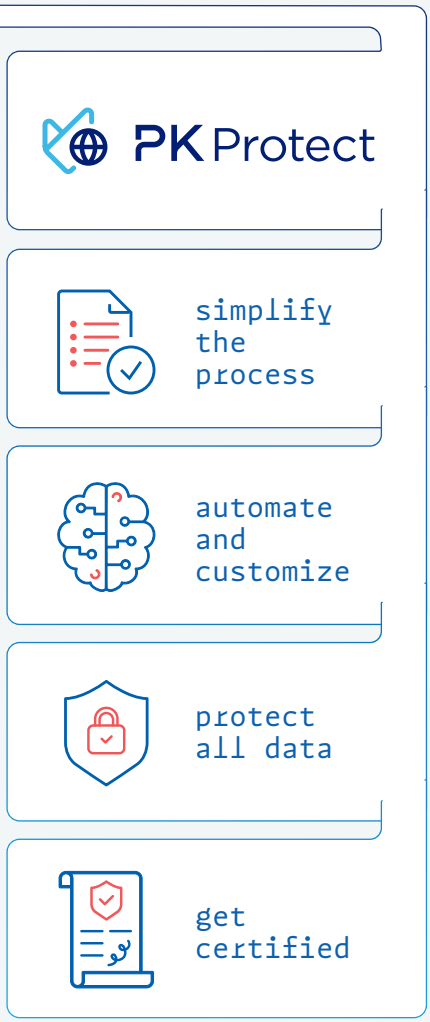
- Environmental Safety
- Water Management
- Infrastructure Resilience
- Health Services
- Reliable Vaccine Storage

The work of the NIST contributes to 80% of global trade's measurement-related standards. US companies depend on the NIST to ensure access to markets. Controlling and securing access to personal data related to all those markets are central to NIST effectiveness.

PK Protect: Automate enterprise-wide location and monitoring of sensitive data, identity creation, data classification, and policy-based data protection techniques ensuring complete privacy for individuals and protection of organizational personal data vulnerabilities.

The PK Protect Approach to Compliance

- Data security mandates like the NIST 800-171 are multi-faceted and complex. They require coordinated efforts of multiple departments and often of vendors, partners, and advisors.
- PK Protect simplifies compliance, providing a wide range of capabilities within a single data protection and security platform.
- Our automated, machine learning-infused technology enables organizations to protect sensitive data on every operating system and in every data store and to create tailored workflows meeting their unique privacy and security compliance needs.
- Companies use PK Protect in meeting a variety of NIST 800-171 standards and in achieving the desired level of CMMC maturity.
- PK Protect is designed to fit easily into your organization's IT and security ecosystem, simplifying deployment and implementation, and helping meet other requirements in functional areas like user authentication, network security, and employee role-based access controls and training.



The NIST Cybersecurity Framework and the CMMC have a lot in common. They both intend to protect controlled unclassified information. The CMMC draws upon the NIST for some of its standards, combining several and mapping them to security controls published by the NIST.

The differences include that the CMMC goes further in protecting sensitive data. Also, compliance with the NIST is either a YES or a NO, whereas with the CMMC there is a range of maturity a company can be granted. To achieve the higher maturity levels, a company will need to implement the NIST controls.

Meeting NIST 800-171 Standards with PK Protect

NIST 800-171 Requirements 3.1 Access Control	Encryption and Key Management
3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, access to devices—including other systems	**PK Protect automatically detects and encrypts sensitive data and their files, as defined by company policy**
3.1.2 Limit system access to the types of transactions and functions that authorized users are permitted to execute.	▪ Files can be encrypted using different keys—with access granted to different users or groups—based on file contents, file type, file location, or other criteria
3.1.3 Control the flow of CUI in accordance with approved authorizations	▪ Every piece of sensitive data across all data stores can be encrypted at the element level
3.1.4 Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	▪ Through integration with MS Outlook, PK Protect detects and encrypts sensitive data in outgoing email messages and attachments
3.1.5 Employ the principal of least privilege, including for specific security functions and privileged accounts	▪ Access to encryption keys is managed at the organizational level, ensuring visibility and control over CUI and FCI at all times
3.1.19 Encrypt CUI on mobile devices and mobile computing platforms	▪ PK Protect can encrypt and decrypt sensitive data on all the popular platforms and every enterprise operating system, including data stores on-premises and in the cloud, servers, endpoints, and mobile devices.

Policy Management and Administration

The PKWARE Endpoint Manager provides a role-based administration console to manage data security activity across the organization.

Administrative functions can be configured to preserve separation of duties. For example, security administrators can create encryption keys based on AD groups, which are managed separately by AD administrators.

3.1 Audit and Accountability	Reporting
3.3.1 Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity	**PK Protect Data Security Intelligence reporting capabilities allow security teams and audit personnel to monitor data discovery, classification, and protection activity across the organization**
3.3.2 Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions	▪ Activity logs indicate what data and which files are protected, where they are stored, and which users have authorized access to them
3.3.5 Correlate audit records review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity	▪ Administrators can filter reporting data by time and event type, and search for specific terms within event logs
3.3.6 Provide audit record reduction and report generation to support on-demand analysis and reporting	▪ Output can be viewed directly, picked up via SIEM agent or retrieved via API
3.3.8 Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	▪ Activity logs are protected and cannot be altered
3.4 Configuration Management	**Administration**
3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational settings	**The PK Protect Endpoint Manager provides granular capabilities for configuring security policies and administrative settings. Policy changes can be configured to require review and approval by a second administrator prior to implementation.**
3.4.3 Track review, approve, or disapprove and log changes to organizational system	

3.8 Media Protection	Encryption and Key Management
3.8.1 Protect by physically controlling and securely storing system media containing paper and digital CUI	**PK Protect applies persistent AES-256 encryption to files containing CUI, FCI, and other sensitive data. Once encrypted, files remain inaccessible to unauthorized users at rest and in transit. Encryption can be used to protect data on endpoints, servers, removable storage devices, and backup media, as well as in production and non-production databases and repositories on premises and in the cloud.**
3.8.2 Limit access to CUI on system media	**Data Classification**
3.8.4 Mark media with necessary CUI markings and distribution limitations	**PK Classification applies visual labels and metadata tags to files containing sensitive data. Visual markers alert users to a file's proper handling, and metadata tags can be used to facilitate action by DLP or other security technology.**
3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards	
3.8.9 Protect the confidentiality of back up CUI at storage locations	

3.9 Personnel Management	Policy Management
3.9.2 Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers	**Access to encryption keys—and encrypted CUI or FCI—can be automatically revoked when a user's Active Directory credentials are suspended or removed. Administrators can also revoke access manually as needed.**
3.13 System and Communications Protection	**Application Programming Interfaces**
3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems	**PK Protect Software Development Kit and command line interfaces provide the means for data protection capabilities to be built into applications and repeatable processes.**
3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards	**Encryption and Key Management**
3.13.10 Establish and manage cryptographic keys for cryptography employed in organizational systems	**A standout feature of PK Protect is strong, FIPS-validated encryption to protect CUI and FCI at rest and in transit.**
3.13.16 Protect the confidentiality of CUI at rest	**PK Protect leverages existing encryption key stores and also provides its own key management system. Additionally, the PK Protect appliance can create and store crypto keys in a FIPS-140-2 level 3 HSM.**

"PKWARE provides industry standard algorithms for data masking and encryption. Data is not ported across the networks, as the masking and encryption happens at the source server. Hence, it zeroes down the data-loss related issues. And the application UI is user-friendly, the development effort is almost seamless, and it's very easy to do the configurations and task creations."

Kanganalapatti Janarthanan Jayanthi
IT Manager, Great Eastern Assurance

Ready To See It Live? Contact Us!

pkware.com/demo

866-583-1795

201 E. Pittsburgh Ave.
Suite 400
Milwaukee, WI 53204

Follow Us

/company/PKWARE

facebook.com/PKWARE

@PKWARE