PKWARE

PK Protect

PK Protect

Endpoint Data Protection: Intelligent Data Discovery and Encryption for User Devices

Each time a user device is authorized to access a company's network, the exploitable attack surface increases. With the number of endpoint devices in use growing every day, organizations need to find the balance between productivity and protection on all the devices their employees use.

The right endpoint security solution can help organizations detect suspicious instances of data being moved around inside and outside of an organization. PK Protect provides revolutionary data protection that automatically discovers and protects critical information, even when it moves outside of the organization.

LOCATE DATA

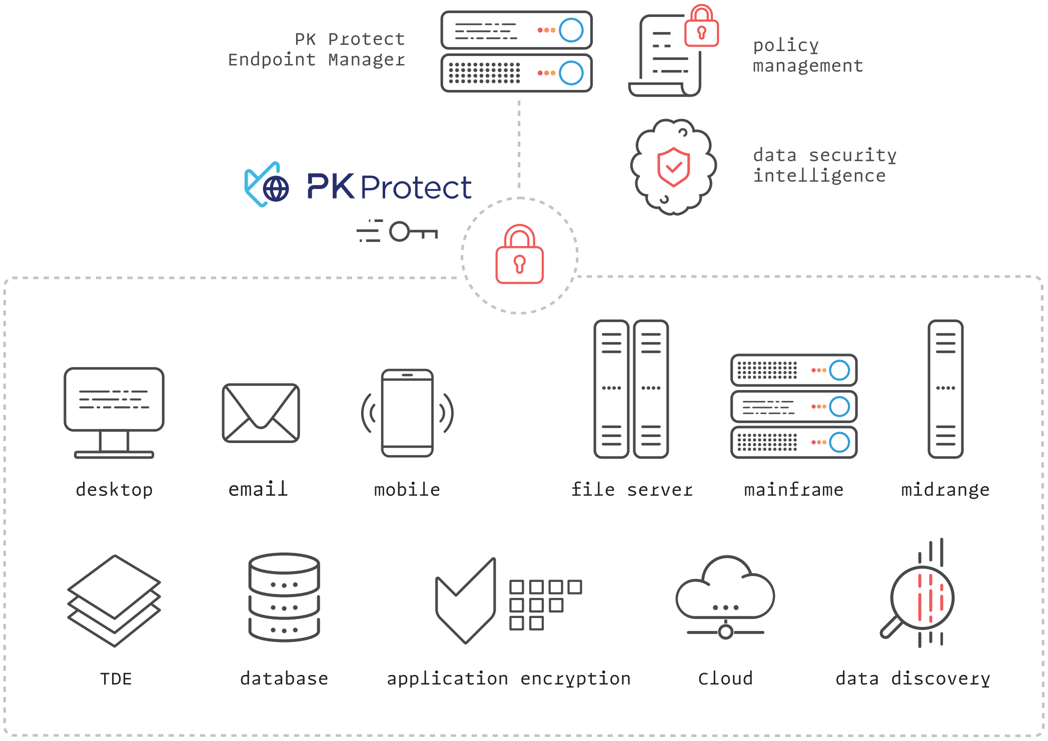
IDENTIFY IT

REMEDIATE

PK Protect Endpoint Manager and Agents

The PK Endpoint Manager (PEM) is the central hub of the implementation, providing integration with identity providers such as Microsoft Active Directory. The PEM's policy management controls encryption across the enterprise, including existing data leakage prevention processes and technology. PK Protect's Data Security Intelligence tools provide enterprise IT, security, and audit personnel with visibility into which files were encrypted, the users who accessed them, the devices they were on, and where the events took place.

Installed on user devices, servers, or other IT assets that store or process sensitive information, PK Protect agents can scan file locations for sensitive data and apply persistent encryption with embedded key management, minimizing user disruption. All key creation, synchronization, and exchange operations take place in the background, making it easy to securely store and exchange data with partners and customers.



Smartkey Technology

At the core of PK Protect is the revolutionary Smartkey technology. With Smartkeys, businesses gain across-the-board control over who can decrypt files and read data.

A Smartkey is a unique key generated for a specific file, folder, or other protected asset. Smartkeys allow administrators to add or revoke user access at any time—even if the files have been shared, copied, renamed, transferred, or emailed—ensuring full lifecycle protection.

Explore PK Protect Use Cases

Data Discovery

PK Protect integrates intelligent data discovery with strong data-level encryption, allowing organizations to identify sensitive information and protect it against loss, theft, or misuse. The solution scans desktops, laptops, and servers for sensitive information based on mandates, search terms, and/or regular expressions. If any file or email message contains sensitive information, PK Protect encrypts the data using the organization's policy-specific encryption keys. Both encryption and decryption can be configured to take place without the need for end user intervention, eliminating disruptions to existing workflows.

Secure Data Exchange

The PK Protect data security solution can be used to add encryption to existing transfer workflows and processes. PK Protect delivers complete cross-platform encryption from mainframe to mobile, securing data through transfer mechanisms including email, FTP, private line, file sync and share solutions, even removable media. File-level encryption means protection travels with the information, preventing unauthorized access no matter where the files are copies or shared, even after the file leaves the organization.

Encryption at Rest

Multiple regulations mandate encrypting data at rest. PK Protect's Transparent Server Agent provides a strong foundation for regulatory compliance and data protection. For enhanced security, PK Protect can apply persistent file level encryption, which protects data at rest, in transit, and in use. Persistent encryption can be applied to data in multiple ways, including: automatic folder encryption, Microsoft Office, Microsoft Outlook, individual file/folder encryption, and stream support.

Automated File Redaction

PKWARE's redaction solutions permanently remove sensitive information as soon as it appears in files or images. The PKWARE endpoint agent can automatically match many sensitive types such as credit card numbers, then redact data within images, text files, and emails to render sensitive information unusable in the event that it is incidentally shared or breached. When an organization needs to preserve original data, a copy of the file can be created in a quarantined location prior to redaction. The unredacted version can be handed off to PK Encryption in order to remain compliant with applicable regulations and mandates.

Data Loss Prevention

When integrated with existing data loss prevention (DLP), PK Protect provides policy key access to DLP personnel and technology, enabling decryption and scanning of end-to-end encrypted content when it has been encrypted elsewhere in the organization. After scanning, DLP can pass the encrypted content along, allowing the security to remain intact, or block the transmission after scanning the encrypted content. PK Protect also allows DLP to apply protection to transmissions it would otherwise need to block.

Audit and Chain of Custody

Evolving regulations and customer demands require that organizations maintain complete control over their data in order to demonstrate regulatory compliance and respond to security events. PK Protect's Endpoint Manager provides an immutable audit log of every encryption, decryption (including failed decryptions), and key exchange operation throughout the enterprise. Digital signing and authentication can further enhance an organization's chain of custody and provide the basis for non-repudiation.

Mobile and BYOD

As more organizations include "bring your own device" policies for their employees' mobile devices, a new threat to data security emerges: Organizations often have no control over employee devices, yet allow employees to use their phones to access necessary sensitive information. PK Protect's mobile app supports native email workflows, integrating with popular file share providers to protect sensitive files on mobile devices. If a device is lost or stolen, organizations can immediately revoke access to encryption keys for that device, rendering any stored sensitive files useless and minimizing the possibility of a data breach.

Enterprise-Wide Protection

PK Protect endpoint protection is available for Windows, macOS, and Linux operating systems, enabling organizations to protect sensitive data regardless of their IT architecture.

Files encrypted by the PK Protect agent are fully interoperable with PK Protect's solutions for file servers, mainframe, midrange, and databases, ensuring that authorized users can always access encrypted files.

Technical Specifications

Operating Platforms

- Microsoft Windows
- Linux: RHEL (.rpm) and SLES (.deb)
- Apple Mac OS and iOS
- Google Android

Algorithms

- Encryption: EES256 (block level encryption in AES-CBC mode)
- Signing: RSA 2048 SHA 512 PSS (metadata)

Key Storage and Retrieval

- OASIS KMIP
- PKCS#11

File Encryption Certificate and Key Types

- Smartkeys
- X.509 Digital Certificates
- OpenPGP

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