PKWARE

PKWARE ENTERPRISE MANAGER

ORGANIZATION-WIDE CONTROL OVER SENSITIVE DATA

The PKWARE Enterprise Manager enables organizations to maintain control over sensitive data across the enterprise. It controls data discovery, data classification, and data protection activity, as well as encryption key management, key synchronization, and key delivery.

With PKWARE, your data security policies don't exist only on paper—they control where sensitive data exists and who can access it. PKWARE lets you create a tailored data protection solution that closes security gaps and eliminates user confusion.

SIMPLER AND SMARTER

Administrators use the Manager's intuitive interface to define data security policies and manage Smartcrypt agents installed on user devices, servers, and other IT assets. Access to protected data can be granted or revoked at any time, and user activity can be monitored and audited in real time.

PKWARE's innovative key management technology lets organizations grant and revoke access to encrypted data at any time, while ensuring that data remains available for auditing, DLP processing, and other essential functions.

The Enterprise Manager integrates with Active Directory to simplify administration and align data security policies with existing business processes and workflows. Administrators can configure policy groups to enable multiple levels of access for different departments or user profiles within the organization.

Organizations can also make retroactive changes to data access (for example, when teams gain or lose personnel) without sacrificing the time and resources needed for re-encryption.

TAKE CONTROL OF YOUR DATA

Uncontrolled encryption can be as problematic as a lack of encryption. PKWARE solutions can be configured to include at least one of the organization's public keys in every encryption operation, eliminating the possibility that the organization could lose access to its own data. Encryption policies also facilitate access to protected files by data loss prevention scanners, improving DLP efficiency and effectiveness.

GAIN INSIGHTS AND SIMPLIFY COMPLIANCE

PKWARE's advanced reporting capabilities give security administrators and auditors full visibility into encryption activity across the entire enterprise. Administrators can monitor which files have been encrypted, who has access to the files, and where the files have been shared. Security reports can be generated using the data security intelligence interface in the management console, picked up by a SIEM agent, or retrieved via API for transformation and load to a customer datamart..

SUMMARY

Administration console used to define and apply data discovery, classification, and protection policies across the entire organization.

Manages PKWARE agents installed on user devices and servers.

Provides centralized key delivery and key exchange, automating the key management process for end users.

Managers can provide retroactive access to protected data, without the need for re-encryption.

Data Security Intelligence tools provide detailed event reporting without the need for a third-party reporting tool.

Available as software-only or a hardened virtual appliance. Also available in a FIPS 140-2 Level 3 hardware appliance.

SMARTKEY TECHNOLOGY

The Enterprise Manager allows organizations to implement PKWARE's 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.

Smartkeys are automatically generated, shared, and synchronized between authenticated devices without changing or interrupting user workflows. Smartkeys also allow users to encrypt data for external parties such as vendors or partners.

DEPLOYTMENT OPTIONS

The Enterprise Manager is available as software, a virtual appliance, or a hardware appliance.

When deployed as software, the PKWARE Enterprise Manager can be integrated with an organization's existing database and application infrastructure. PKWARE Appliances offer streamlined deployment, together with enhanced security capabilities including an optional FIPS 140-2 Level 3 hardware security module and a full-entropy quantum random number generator.

TECHNICAL SPECIFICATIONS

OPERATING PLATFORMS
Windows Server 2008, 2008 R2, 2012, 2012 R2

INTERNET INFORMATION SERVICES
IIS 7.0, IIS 7.5, IIS 8.0

SQL SERVER
SQL Server 2008, 2008 R2, 2012

KEY STORAGE AND RETRIEVAL
OASIS KMIP
PKCS #11

FILE ENCRYPTION CERTIFICATE AND KEY TYPES
X.509 Digital Certificates
OpenPGP

MODEL NAME	200v	300h	300r	350
Virtual/Hardware	Virtual	Hardware		
Operating Sytems	Linux-based VM	Hardened Linux OS		
Simplified administration	✔	✔	✔	✔
Enterprise-wide control	✔	✔	✔	✔
Data security intelligence	✔	✔	✔	✔
HSM Support (Master Key)	✔	✔	✔	✔
Failover	✔	✔	✔	✔
High Availability	✔	✔	✔	✔
Data Residency	✔	✔	✔	✔
FIPS 140-2 level 3 key storage		✔		✔
Full-entropy quantum RNG			✔	✔

PKWARE®

www.PKWARE.com

PKWARE solutions help organizations eliminate security gaps, manage sensitive data, and meet their data compliance goals.

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

+ 1 866 583 1795

EMEA HEADQUARTERS
79 College Road
Suite 221
Harrow HA1 1BD

+ 44 (0) 203 367 2249