PKWARE

pkware.com

Making Sense of Sensitive Data

How Data Discovery Facilitates Meaningful Action on Unstructured Data

2021

Contents

Executive Summary

Digital transformations are fundamentally changing the way organizations store and access information. Traditional security solutions like network and device protection, while never a complete answer, are even less effective in a mobile-focused, cloud-based business environment.

Despite the obvious need for data-level security, many organizations are struggling to implement security strategies that address today's challenges. Uncertainty about the extent and nature of sensitive data, together with concerns about software usability and effectiveness, can leave an organization unable to commit to a data-centric approach to information security.

Integration between data discovery and data protection is the missing link. When organizations can simultaneously identify and encrypt sensitive information on file servers and user devices, they gain unprecedented control and visibility over their data, eliminating the obstacles to true enterprise information security.

PKWARE's PK Protect provides sophisticated data discovery capabilities, allowing organizations to identify sensitive data more easily than ever before. Once information has been identified as requiring protection, PK Protect applies classification tags along with strong data-level encryption or other forms of protection, ensuring that the information will remain protected wherever it is used, shared, or stored.

When organizations can simultaneously identify and protect sensitive information, they gain unprecedented **control** and visibility

A New Model for Information Security

As companies around the world reinvent themselves to take advantage of new technology, they are generating, collecting, and processing data at unprecedented levels. Allowing this data to fall into the wrong hands can irreparably harm an organization's reputation, with consequences even more serious than the fines or court judgments that typically follow a security breach.

In order to compete in the new digital environment, organizations must transform their security strategies along with their business models. Many companies still rely on a decades-old approach to security based on protecting networks and devices. While firewalls and passwords may still have a place in cybersecurity architecture, recent events have shown that hackers can gain access to any system if they believe they can find information to exploit. Adding new layers of outmoded security will only postpone the inevitable.

The ongoing shifts toward cloud computing and mobile, decentralized employee teams have further exposed the limitations of network and device protection. Restricting access to internal file servers, for example, does little good when employees are saving their work on external resources, or are sharing vital information with partners and vendors via email or FTP.

It has become clear that the only way to guarantee the long-term security of sensitive information is to protect the data itself. A data-centric security strategy, based around strong encryption of regulated or proprietary information, can help an organization ensure that information remains safe even when files are copied, shared, mishandled, or stolen. Encrypted information is accessible only to individuals who have the key for decryption, rendering it useless to thieves and other unauthorized users.

Employees no longer have to keep data in their company network: Whether it is Dropbox, OneDrive, Intralinks, or other "collaboration productivity tools," organizations are rapidly losing control of where their data lives

Obstacles to Strong Data Protection

Although strong encryption technology has been available for decades, relatively few organizations have put it in use, especially in industries not subject to information security regulations. Resistance to enterprise-wide encryption is typically rooted in a few fundamental challenges that organizations have faced when attempting to develop and implement a data-centric security strategy.

Defining Sensitive Data

Every organization has a different definition of sensitive data. The information that a company or government entity needs to protect is determined by a combination of factors including regulatory obligations, industry mandates, and unique business requirements. In order to accurately define sensitive data, however, an organization must first have a clear picture of the information they are generating, storing, and exchanging.

Companies in heavily regulated industries like financial services, healthcare, and government services have been subject to stringent information-security regulations for years. While government and industry mandates may dictate that certain forms of data (account numbers and Social Security numbers, for example) must be secured, organizations often struggle to define other types of information that require protection, because they have not fully categorized the data on which they rely.

Companies in less-regulated industries, though they may be collecting and using sensitive information on a large scale, often lack a basic framework for defining sensitive data and simply avoid the issue until a security breach or other incident makes it a priority.

Locating and Quantifying Sensitive Data

Even the most technologically advanced corporation can find itself in the dark regarding sensitive information. Unstructured data—information in documents, images, messages, and other file formats—accounts for 80 percent or more of the data stored by most organizations today. Unless an organization has deployed a data discovery solution on its network and endpoint devices, it has no way of quantifying how much sensitive data it has, or where the data might be.

Some organizations attempt to address the issue by encrypting all of the data stored on certain servers or file paths. While this approach ensures the security of the encrypted data, it can leave lingering uncertainty about how much sensitive data the organization truly has, and raises the possibility that critical information may still reside elsewhere in the organization.

What is Sensitive Data?

Because every organization defines sensitive data in a different way, technology solutions must detect and remediate sensitive data based on a wide range of criteria. Whether it is a search for data based on common formats such as credit card account numbers or Social Security numbers, discovery and remediation technologies must be able to support industry or government mandates including those listed below.

Implementing Endpoint Protection

Endpoint devices represent a growing threat to enterprise data security. Employees routinely save sensitive data onto their laptops, tablets, and phones, often without realizing they have done so. Several recent high-profile security breaches have resulted from the loss or theft of employee devices with unprotected sensitive data.

The growing popularity of cloud storage services creates another potentially damaging scenario. When employees sync their company devices to their personal cloud storage accounts, they add gigabytes of new data to their organization's ecosystem. If some of this data originated with former employers or customers, the organization may find itself unknowingly exposed to fines, lawsuits, and even criminal investigations.

Despite the hazards, organizations with tens or hundreds of thousands of employees often choose not to implement a data-centric solution for endpoint security due to limitations in functionality or usability. Discovery-only solutions that simply identify sensitive data are generally viewed as having low ROI, as they lack remediation capabilities and would require a separate solution to protect the data they identify as sensitive. Traditional encryption solutions like public key infrastructure, on the other hand, are notorious for being difficult to implement and disruptive to employee workflows.

For years, the above issues have discouraged enterprise organizations from implementing data-protection solutions. This lack of action, however, opens the door to a host of potentially devastating security problems, including loss of customer trust, loss of intellectual property, and crippling financial penalties.

Benefits of PK Protect Data Discovery

- Software agents can be configured to identify and encrypt sensitive information based on specific criteria, ensuring compliance with internal policies and industry or government mandates.
- PK Protect automated discovery and encryption process removes the burden from employees and eliminates human error from the equation.
- Discovery and encryption can be applied to file servers, NAS, and local device storage, ensuring protection across the entire enterprise.
- Administrators retain full control over encrypted information, including the ability to add or revoke access, even when data has moved outside the organization.
- PK Protect improves DLP effectiveness by identifying sensitive information, while allowing DLP technology to scan encrypted data through the use of policy keys.

The Path Forward: An Integrated Approach to Data Protection

In order to resolve the uncertainty around sensitive data and move forward with an effective data protection strategy, organizations need the ability to identify, protect, and manage sensitive information with a single enterprise-wide solution.

Integration between data discovery, data classification, and data protection eliminates the obstacles that have prevented many organizations from implementing data-centric security until now. An integrated approach gives organizations the ability to gain a complete picture of their sensitive data, and to tailor their security policies to their unique business needs.

Combining discovery with classification and remediation helps build the business case for implementing endpoint data protection, even in the largest enterprises. When sensitive data can be classified and protected as soon as it is identified on a user device, the effort required to find the data is suddenly justified. Intelligent data discovery also gives companies greater reporting and auditing capabilities, allowing them to document their efforts to comply with evolving industry and governmental security mandates.

Eliminate Security Gaps with PK Protect

PKWARE's PK Protect uses an automated workflow to find, classify, and protect sensitive data across the entire enterprise. PK Protect provides capabilities no other product can match, allowing each organization to create a tailored data-protection solution.

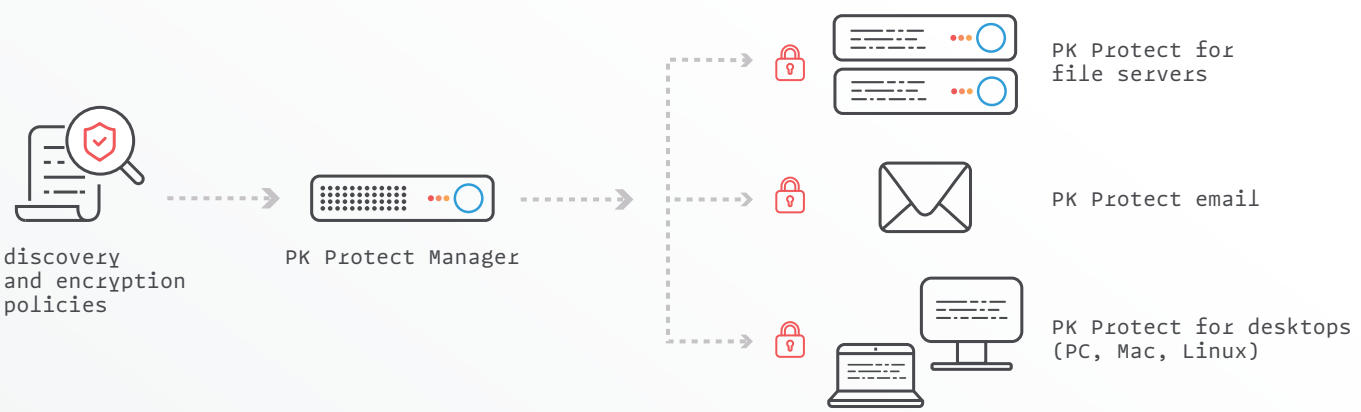
PK Protect's data discovery feature continuously monitors laptops, desktops, and servers for sensitive information. Each time a file is added or modified, PK Protect initiates a scan based on the organization's definition of sensitive data. If the data fits one of the defined patterns, the system can apply classification tags and remediate the data via encryption, masking, or other methods.

The entire process is automated and takes place with no disruption to end user workflows.

Data-Centric Security on Endpoints and Servers

PK Protect's endpoint and server discovery and encryption capabilities allow security managers to apply tailored security policies to individual employees, groups, or the entire organization.

- Administrators select employees or teams to be included in the discovery process
- Administrators create filters consisting of one or more data patterns
- Filters can be grouped together in filter bundles based on compliance mandates (HIPAA, PCI, etc.) or business processes
- Administrators apply filters and filter bundles to employees, groups, or selected file storage locations on servers or NAS ("lockers")
- Administrators select the remediation to be applied when a file meets the definition of sensitive data (encrypt/delete/report), along with the encryption keys to be used in remediation
- Any file activity on an employee's device or in a locker triggers a discovery scan (and remediation if needed)
- When reporting is enabled, every remediation event is captured in full detail
- Administrators can grant or revoke access to encrypted information at any time
- When reporting is enabled, every remediation event is captured in full



Data-Centric Security on Endpoints and Servers

The company that builds data security into the foundation of its business model is the company that will attract and retain consumers in the post-digital environment. PKWARE's PK Protect provides the discovery, encryption, and reporting capabilities that organizations need in order to redefine their approach to security.

Although every company or government agency has unique requirements, the following steps provide a framework that can help any organization implement an effective, long-term data-protection strategy that will enhance its ability to compete in a rapidly changing world.

- Implement intelligent data discovery on network resources and endpoint devices. Some organizations adopt a phased approach to implementation, beginning with the users and servers that are most likely to handle or store sensitive data.
- Use classification tags to indicate the proper use and handling of sensitive files. Classification increases user awareness of the organization's security policies and makes other data protection technology more effective.
- Apply immediate remediation to unprotected sensitive information in order to protect the organization in the event that data is lost or stolen.
- Use PK Protect's Data Security Intelligence tools to gain insight into the types, locations, and quantities of sensitive data that are in use. Unexpected results, such as unnecessary volumes of sensitive data, or data found in inappropriate locations, can indicate areas in which security policies or business processes need to be updated.
- Use PK Protect's key management and access control capabilities to ensure that sensitive data is only accessible to the people who are authorized to use or share it.

About PKWARE

PKWARE offers the only data discovery and protection solution that locates and secures sensitive data to minimize organizational risks and costs, regardless of device or environment. Our ultra-efficient, scalable software is simple to use on a broad range of data types and repositories, enabling precise, automated visibility and control of personal data, even in the fastest-moving, most complex IT environments. With more than 1,200 customers, including many of the world's largest financial institutions, retailers, healthcare organizations, and government agencies, PKWARE continues to innovate as an award-winning global leader in data discovery, security, and compliance. To learn more, visit PKWARE.com.

Enterprise-Wide Policy Management

The PKWARE Enterprise Manager provides a single point of control for data protection activity across the entire organization

Simple Workflow

With PKWARE, data protection is automated for end users and easy for administrators to manage

Easy Implementation

PKWARE supports a variety of deployment options, enabling organizations to implement their data protection solution without time-consuming changes to infrastructure and workflows

Protection Without Gaps

PKWARE works on every enterprise operations system and provides persistent protection that remains with data even if it's copied or shared outside organizations

Integrated Discovery, Classification, and Protection

No other solution has the capability to find, classify, and protect data in a single automated workflow

Multiple Protection and Remediation Options

Organizations can take a policy-based approach to data protection and choose from action including persistent encryption, quarantine, masking, and deletion.

BOOK A DEMO

PKWARE.com

866-583-1795

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