PKWARE

VISIBILITY AND CONTROL

THE ROLE OF CLASSIFICATION IN ENTERPRISE DATA PROTECTION

Data-centric security—security that protects data itself, rather than focusing on perimeter or device protection—is the best way to manage the risks associated with large amounts of sensitive data and increasingly complex IT environments.

As data volumes continue to increase and cyber threats grow harder to predict, data classification has emerged as an essential element of data-centric security. By improving visibility and control over sensitive information, classification keeps end users engaged in the organization's data protection efforts and makes other security technology more effective.

GIVING STRUCTURE TO UNSTRUCTURED DATA

When implemented in conjunction with data discovery and data protection capabilities, classification enables an enterprise to defend itself against internal and external cyber threats while unlocking the full potential of its data.

In practical terms, classification is the process of organizing and labeling unstructured data—which constitutes 80% of a typical company's data—to ensure that it is protected by appropriate measures while remaining available for its intended use. Data classification involves three key steps:

- **Categorizing files** based on sensitivity, value, file type, or other criteria.
- **Defining policies** that govern how each category of data should be protected and how it should be used.
- **Applying labels** and metadata tags to files belonging to each category

These steps can be implemented in a variety of ways, ranging from completely manual processes to fully automated solutions that scan and classify files with no user involvement.

Classification should be viewed as a component of an organization's overall security strategy, rather than a complete security solution on its own. While file labels do increase user awareness of the organization's policies, they do not protect data from unauthorized use, unless classification is paired with technology that can apply encryption, masking, or other forms of protection.

> **YOU CAN'T BE FOLLOWING BEST PRACTICE IN TODAY'S WORLD WITHOUT DOING DATA CLASSIFICATION.**
>
> RENEE MURPHY, FORRESTER RESEARCH INC.

IMPLEMENTATION OPTIONS

In the past, data classification was managed as a manual process, based on an organization's paper policies. If a policy called for certain type of file to be labeled and handled in a certain way, employees were expected to add the label and observe the handling rules themselves. Given the exponential increases in data volumes and data exchange in recent decades, this paper-based approach is no longer feasible. Classification can only be implemented effectively through the use of software that simplifies the process and integrates with other IT infrastructure.

Software-based classification gives organizations the ability to label user-generated files, email messages, files created by automated processes, and other forms of data across the entire enterprise. Depending on an organization's unique needs, classification can be initiated by end users, handled automatically, or managed through a combination of the two approaches.

AUTOMATED CLASSIFICATION

Automated classification takes place without user involvement, through integration with data discovery technology. In an automated classification workflow, a software agent scans files at the point of creation and each time a file is modified. After evaluating the file's contents, the agent initiates classification according to the organization's policies.

The automated approach allows for the company's classification policy to be consistently applied across all touchpoints, without the need for major communication and education initiatives. The automated workflow also provides a viable solution for situations in which files are created with no user involvement, such as reports generated by ERP systems.

USER-DRIVEN DATA CLASSIFICATION

The user-driven approach to classification makes employees responsible for deciding which file label is appropriate, and attaching it using a software tool at the point of creating, editing, sending or saving. The advantage of involving the user in the process is that their insight into the context, business value and sensitivity of a piece of data enables them to make informed and accurate decisions about which label to apply. However, relying entirely on user decisions raises the possibility that policies will be ignored, or that files will be inadvertently mislabeled.

AUTOMATED CLASSIFICATION PAIRED WITH USER INPUT

For maximum effectiveness, user-driven classification can be enabled as an additional security layer to complement automated classification. In this approach, files are scanned and labeled according to organizational policy without the need for user action. Once files have been classified, users have the ability to modify labels as needed. This approach reduces the incidence of false positives (in which files are tagged as requiring protection when it is not actually needed), and allows users to tag files that might not match the typical definition of sensitive data but still require protection.

Involving users in classification leads to other organizational benefits, including increased security awareness and greater compliance with organizational policies. Security managers can monitor users' classification activity to identify employees who need additional training, and to identify potential insider threats.

BENEFITS OF CLASSIFICATION

Data classification delivers a wide range of benefits, making an organization's sensitive data more secure and easier to manage.

GUIDE SENSITIVE DATA AS IT TRAVELS

In addition to adding human-readable file labels, classification applies metadata tags that can direct the actions of other downstream enterprise security and data management solutions – triggering rules so that, for example, a cloud access security broker (CASB) solution will block employees from uploading the file to a cloud file share service. Meta tags also enhance the effectiveness of security incident and event monitoring (SIEM) tools, allowing earlier detection of unusual and potentially risky user behavior. If a user is consistently downgrading confidential files, for example, or is copying sensitive documents to a storage device, the activity will be logged and can be addressed through training, disciplinary procedures, or strengthening of policy.

DEMONSTRATE REGULATORY COMPLIANCE

Regulatory violations can lead to crippling fines, long-term public relations damage, and even criminal charges. Classifying data makes it easier for a business to meet the data governance requirements of the European General Data Protection Regulation (GDPR), the UK's Data Protection Act, the Sarbanes-Oxley Act, HIPAA, and many others. The embedding of metadata within files allows an enterprise to audit exactly who is accessing sensitive information and keep a detailed trail of any policy violations or unusual behavior. In addition to enabling identification of potential threats, user activity logs can be used to demonstrate that information is being appropriately controlled, protected, and documented.

BUILD A CULTURE OF SECURITY

Human error is to blame for a large percentage of security breaches. Heavy workloads, new technology, and insufficient training can lead employees to violate data security policies unintentionally. The inclusion of end users in the classification process helps to build a culture of security awareness across the organization. It emphasizes the message that everyone has a role to play in protecting and managing the organization's sensitive information.

FACILITATE SAFER COLLABORATION

Data classification provides a means of building security into the corporate culture in a way that encourages, rather than inhibits, productivity and collaboration. A single set of classification policies, applied consistently across the entire organization, removes obstacles that might otherwise prevent employees from sharing important information with colleagues and partners.

PKWARE: INTEGRATED DISCOVERY, CLASSIFICATION AND PROTECTION

PKWARE's automated data security platform integrates classification in an automated workflow with data discovery and protection. It's the simplest, most efficient way for organizations to secure their sensitive information against loss, theft, or misuse.

While other classification products can create a false sense of security by tagging files but leaving them otherwise unprotected, PKWARE applies policy-based protection as soon as sensitive data is discovered and classified. Protected data remains safe from unauthorized use, even when it is shared or copied outside the company network.

COMPLETE ENTERPRISE DATA PROTECTION

PKWARE's data-centric security workflow provides the capabilities organizations need to take control of their sensitive data and meet their information security goals.

- Administrators use the PKWARE Enterprise Manager to define and apply data discovery, classification, and remediation policies. Policies can include detailed rules for different user groups, locations, and forms of sensitive data.
- PKWARE scans new or modified files for sensitive information as defined by the organization. When sensitive data is detected, PKWARE initiates automated classification and applies encryption, masking, or other protective measures based on the organization's policies.
- PKWARE also allows end users to apply manual classification to files that require protection even though they do not fit the organization's definition of sensitive data. After manual classification, PKWARE will automatically apply the appropriate form of protection to the tagged file.
- PKWARE's Data Security Intelligence feature provides insight into activity across the organization, making it easy to demonstrate compliance with internal policies and government mandates.