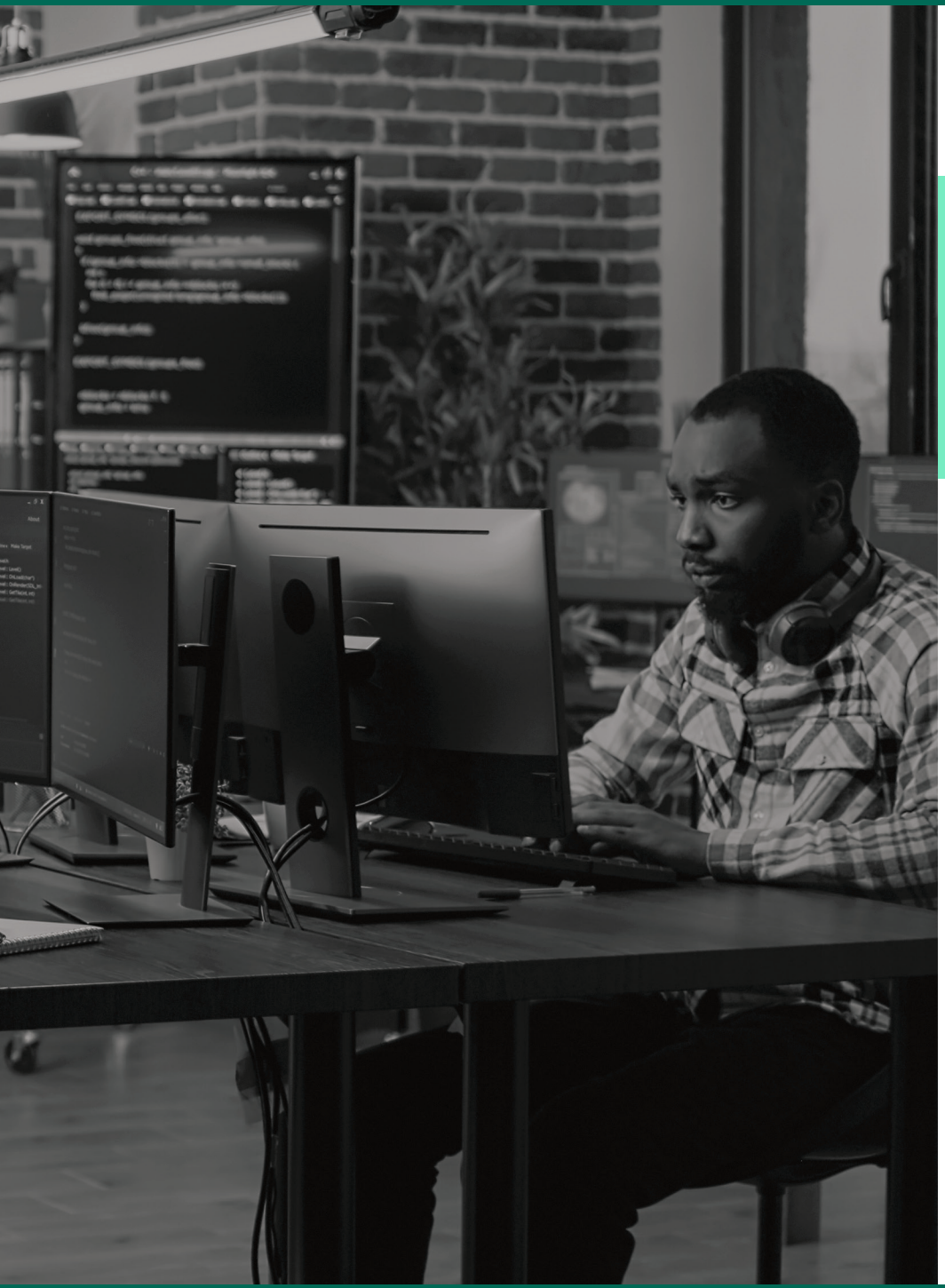
FORTRA™

5 Steps to Effective Data Protection

Every day, businesses create more and more data. Data gets saved, employees move on, data gets saved, but then that data becomes forgotten and gets lost. Valuable information sits on your file servers and document stores, unprotected and unrecoverable because no one knows where to find it. Using a data classification solution helps regain control over your unstructured data. By involving your users in data classification, they become more data-aware, with a greater understanding of your policies and the value of your organization's data.



This eBook takes you through 5 steps to implementing effective data classification within your organization, and details how data classification can enhance previously implemented tools such as data loss prevention (DLP) tools, data discovery tools, data governance tools, and more.

STEP 1

Identify Your Data Diamonds

Using data classification as part of a strategy to secure corporate data assets is akin to locking up your most precious gems - your data diamonds. But data security neither starts nor ends with the act of controlling *access* to information. Nor should a security policy be limited to protecting only the most valuable data; even information deemed less critical can damage the business if it's lost or leaked.

The smart first step is building a strong foundation of knowledge around your data, to understand exactly what exists and the potential risks to its security. Picture your organization as fortress. If you don't know where your data diamonds (and less sparkly assets) are, you'll end up locking every door – or leaving the wrong doors open, exposing them to risk.

This process begins with identifying the types of data that are of greatest importance to the business, so you can pinpoint where you need to focus protection and controls.

IBM estimates that between

0.5 - 2%

of an organization's data is ‘critical’ - in other words, it has a significant financial value to the company.

This can account for up to 70% of brand or market value.

Your most valuable and confidential data (those data diamonds) might include:

- Data assets - such as the information on a CRM database
- Business-critical documents - including strategic plans and agreements
- Documents or information that are subject to regulations
- Intellectual property (IP) - such as product designs and technical specs
- Personally identifiable information (PII) - for instance employees' details

More often than not, a company's most vulnerable point will not be its data diamonds; it's likely that data has already been recognized and heavily protected. It's the everyday sensitive data that people don't think about such as customer lists or contracts, or time-sensitive documents like financial results and press releases that are most likely to be leaked or lost. This data must also be identified and protected.

Quantifying Risk

A helpful way of determining the value of a piece of information – and the risks to be managed – is to think about the impact if it was leaked or lost. Is the organization going to suffer reputational brand damage? Could it incur a fine for breaching regulatory laws (such as GDPR, CCPA, ITAR, and more)? Is there a risk of eroding competitive advantage if information was in the public domain? Could it expose customers, partners, or suppliers? Would employee security or privacy be put at risk? Could it cause a breach of contract?

After you've defined the data that is most at risk, you can start to find out where your sensitive data is located.

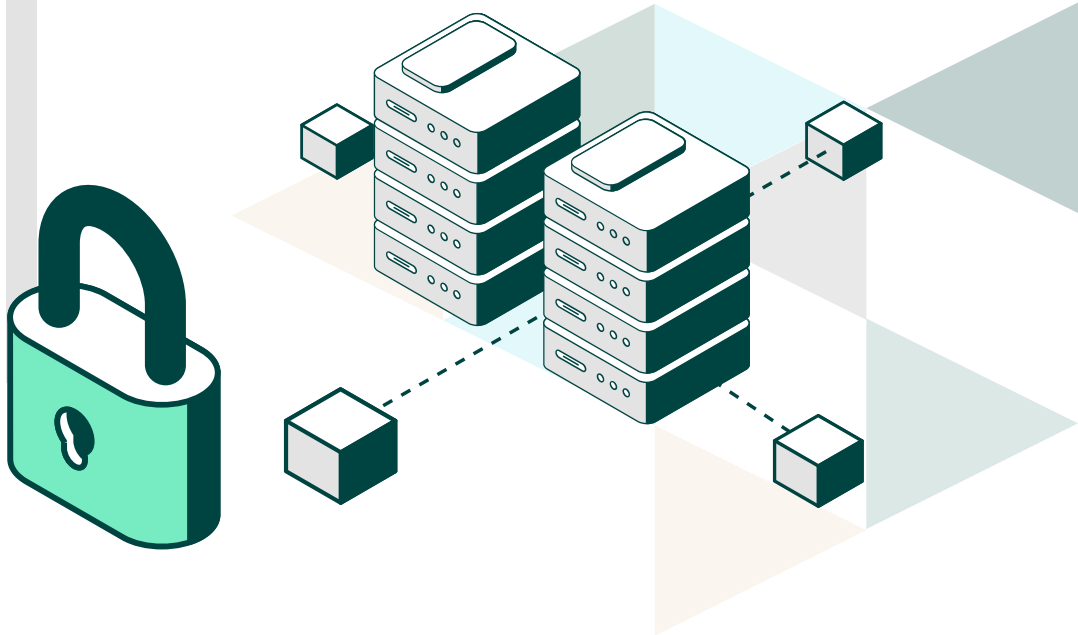
STEP 2

Discover Before You Defend

By classifying data according to its value or sensitivity, organizations can reduce the risk of security breaches by ensuring that appropriate protections are implemented and consistently enforced. Having identified your data diamonds, and other data that needs safeguarding, it's time to carry out data discovery to find out exactly what you've got, where it is and who might have access to it.

Unknown data makes you vulnerable to attack. The best thought-out security policy is ineffective if you're not certain what you hold and, therefore, what controls are necessary. Data governance and adhering to regulatory compliance requirements is impossible when you don't know where key documents reside and who has access to them.

A discovery exercise will give you visibility of your data and how it's being accessed and used. This enables the protection strategy and solutions to be built around the types of data that exist. This is also an opportunity to cut retention costs by disposing of redundant data. Discovery also makes it easier to use data as a resource, deriving insights that will inform strategies and improve operations.



Getting a grip on this is a challenge. Alongside structured data held in on-site databases, companies typically have huge volumes of unstructured data such as emails, PowerPoint decks, Excel files, and PDF documents.

Information is also stored and shared across an expanding variety of systems, devices and platforms, including the cloud, collaboration tools like Microsoft SharePoint, file share sites like Dropbox and OneDrive, and 'shadow IT' (unsanctioned tools and apps not designed for enterprise use).

Data discovery tools and software provide an efficient and accurate way to find assets you can then classify. They examine file stores and databases, scanning for certain types of information, key words, criteria and classification metadata.

This enables you to see what your data is, its location, and who has access. According to Forrester 44% of North American and European technology decision-makers use data discovery tools. Once you've defined the data within your organization, you'll be able to home in on the most valuable and confidential information and make accurate decisions about how it should be handled, and who is allowed to access which files. You'll then be ready to classify it according to its importance or sensitivity, to ensure data is appropriately controlled.

You Will Need To Establish

STEP 3

Classify Your Data

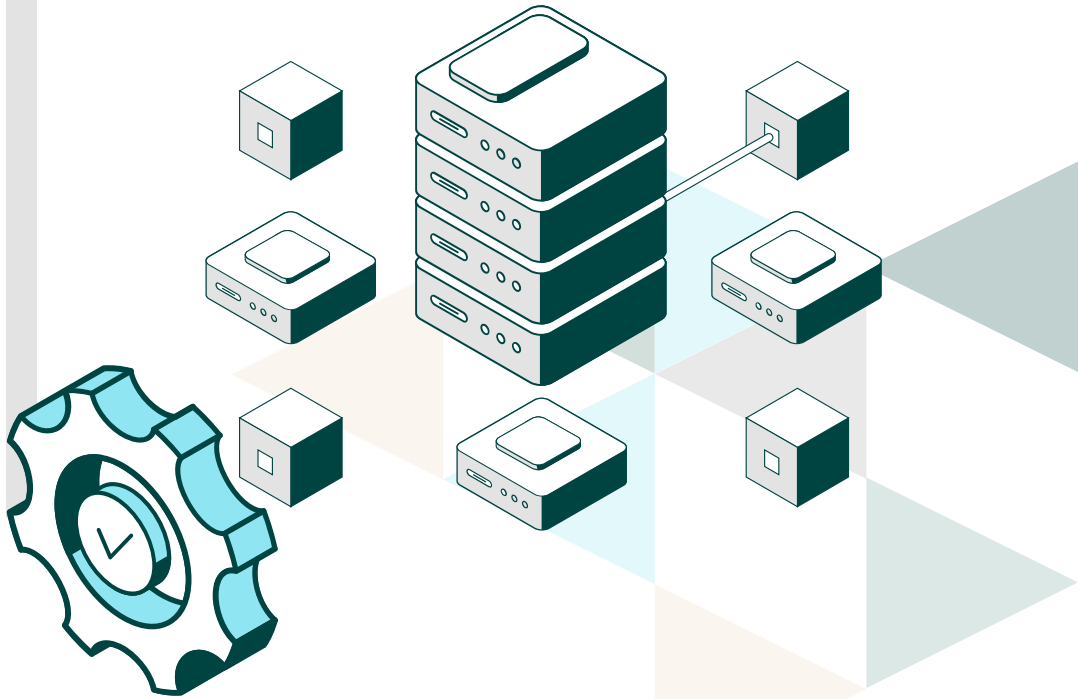
A corporate data security policy that sets out how valuable information should be handled will be ineffective unless it's consistently and accurately enforced. Organizations often have a written policy that's available on their company intranet and shared with new hires. However, in practice are employees sure how to apply it to their daily activities?

Security policies need to be made actionable, and the best way of doing this is by classifying data. This is the first of the two steps that involve actively securing data, with the second being the implementation of downstream data protection solutions such as data loss prevention, and secure collaboration - classification improves the effectiveness of both..

Data classification is the categorization of data according to its level of sensitivity or value, using labels. These are attached as visual markings, and also embedded into the metadata of the file. When classification is applied in association with downstream security solutions, the metadata ensures that the data can only be accessed or used in accordance with the rules that correspond with its label.

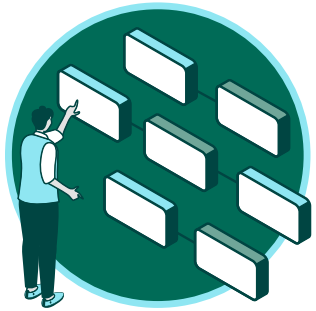
It's possible to completely automate the process, but our clients get the best results when they combine human input with the use of software toolsets to support successful implementation. This is known as user-driven data classification.

With this approach the employee is responsible for deciding which label is appropriate, and attaching it at the point of creating, editing, sending or saving. The user's insight into the context around the data leads to more accurate classification decisions than a computer could ever make.



Defining The Classification Policy

First, be clear on who should have access to each type of data. The work you did in steps 1 and 2 will prepare the ground for this. Next, decide how many categories you'll have. Aim for three or four – the fewer the options the simpler it is for users. Labels that indicate Confidential, Internal only and Public are a good start, with perhaps a fourth category relating to information that's subject to regulatory controls – such as EU GDPR, ITAR controlled, or HIPAA/HITECH restricted.



Selecting Your Classification Tool

The right technology will help your users to consistently apply the classification scheme and will also add the all-important metadata. The most effective tools make classification a seamless part of business-as-usual; integrating the labeling process into the standard applications employees already use. Ensuring breadth of coverage across operating systems and application types is vital to future-proof your investment.

Rolling It Out

Start by classifying your 'live' data – the emails, files and documents that are being created and handled right now. If you've followed steps 1 and 2 you'll know exactly what and where it is. By doing this, you're ensuring that all your data diamonds will be safely locked up from this point forward. When that is established decide how to label the existing and legacy data that is stored and held around the organization. This process usually works well in combination with a discovery agent or tool.

Once you've labeled your data, it's time to turn your attention to the enterprise security solutions and information management technologies that will control and protect it throughout the remainder of its journey.

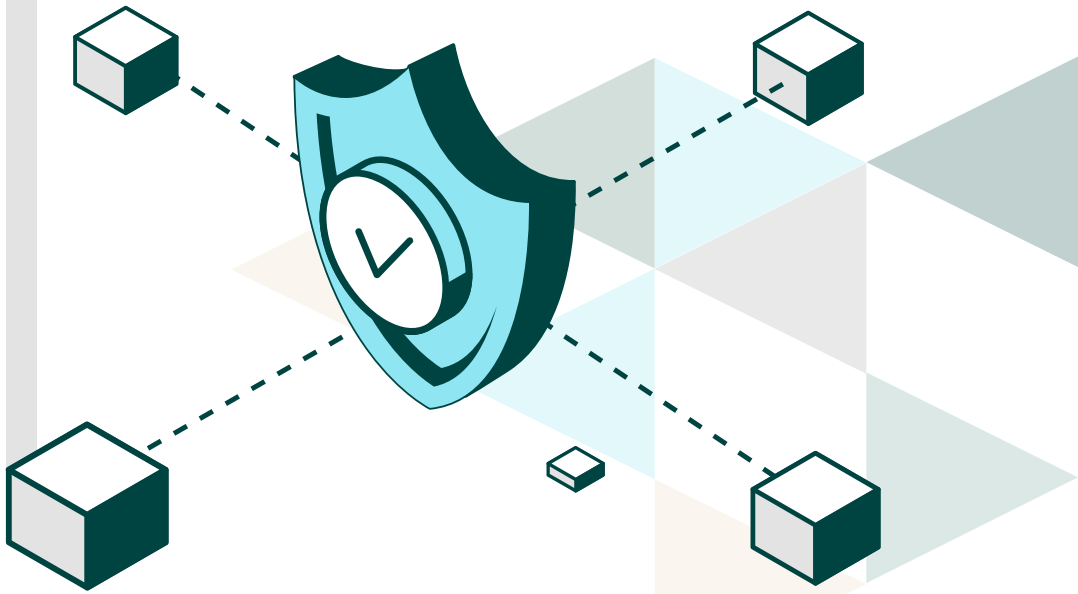
STEP 4

Secure Your Data

Data that has been classified according to its sensitivity instantly has a layer of protection surrounding it. The next task (having identified, discovered, and classified your data) is to put in place the higher-grade controls – in the form of enterprise security and information management solutions – that will safeguard it when it's accessed or used later. By classifying it first, you'll already have added the magic ingredient that makes these solutions more effective: The metadata sitting in the properties of each document, message, or file.

The embedding of metadata supports the consistent enforcement of data protection policies by directing the actions of downstream solutions – triggering automatic rules that correspond to the label the data has been given.

This means the technology makes more accurate decisions, reducing the false positives that slow business down and minimizing the risk of data being exposed because it isn't recognized as sensitive. It also supports governance, compliance, and data management efficiencies.



Solutions that become more effective when combined with data classification include:

Data Loss Prevention (DLP)

These will shield the business against intentional and accidental data loss, such as blocking employees from uploading a file marked 'Confidential' to Dropbox, or stopping a file containing credit card numbers from being emailed to a third party.

Email Gateways

These will automatically encrypt any file marked 'Confidential'.

Discovery Tools

Enabling employees to rapidly locate information and understand instantly how it can be used.

Security Incident And Event Monitoring (SIEM) Tools

These pick up on potentially risky user behavior before a breach occurs – flagging up, for example, if someone keeps copying sensitive documents to a storage device. Concerns can then be addressed through training or strengthening of policy.

Search And Retrieval Tools

Making it easier to keep an audit trail and quickly find documents needed to prove compliance with industry standards, or to meet information requests from regulators.

Access Control Tools

These use classification labels to dictate who can access a file in a shared area.

Data Governance Tools

The label enables these to audit who is accessing sensitive information, and who might be violating policy, keeping a detailed audit trail of any risky behavior or activities. This also supports the demonstration of compliance.

Data Retention

Once you've marked what's valuable, you can more clearly see what isn't important or needed, and therefore what can be archived or deleted. Retention rules can also be set for different classifications – for instance, 'keep this type of file for 10 years' or 'expire after 6 months' – perhaps for files which should not be held for legal reasons.

The impact of data classification paired with other security technologies and toolsets is exponential protection for your most sensitive data, with strong walls around your data diamonds. But data protection doesn't stop there. Like any walls, these must be consistently monitored and maintained to keep them strong and intact.

STEP 5

Measure And Evolve

If you have followed the first four steps in this series (Identify, Discover, Classify and Secure) you'll have successfully secured the organization's valuable and confidential information by using data classification and downstream toolsets to enforce the security policy. There is however more to be done.

Legislation, internal and external threats, and the business itself will constantly evolve, while demands from regulators and the board for better governance will intensify. Ongoing measurement of the effectiveness of your security policy is the only way to check that the controls you've put in place remain fit for purpose.

The monitoring of classification activities is a powerful way of doing this. Monitoring and reporting tools track how data is being accessed, used, and classified, while providing visibility to the business via structured audit data and analytics. This improves the chances that a breach will be quickly detected – helping the business to comply with notification periods required by regulators, as well as to minimize damage. If there is a breach, the detailed audit information will allow you to demonstrate that the appropriate steps to protect data were taken.

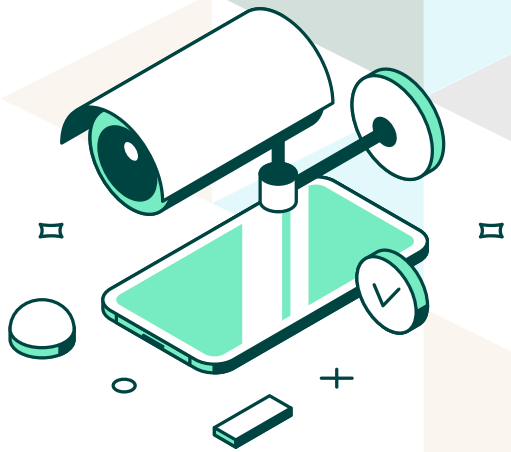
Utilizing reporting capabilities enables you to keep track of what users are doing with data (and identifying potential insider threats) and where data is stored, as well as making sure organizational policies and compliance regulations are being met. As information security becomes more people-focused, the need to 'Trust but Verify' user behavior is critical.

Ongoing monitoring builds an organization-wide picture of how effective the security policy is – a picture which can be shared with the board – along with an understanding of how to improve it.

Using a classification reporting tool in conjunction with a SIEM solution and a behavioral analysis toolset is the gold standard in situational awareness. The combined data makes it possible to forensically analyze an individual's behavior to establish the cause, as well as to highlight broad behavioral patterns and trends. For example, if a large number of people regularly under-classify documents, this may indicate a weakness in the policy or simply show that it's not properly understood.

This insight will equip you to make informed decisions about how to address the issue: through tightening the security policy, providing further training, or carrying out disciplinary procedures.

Integrating monitoring and reporting capabilities into the data security strategy is the only way an organization can fully realize the value of its data classification and other security solutions. Measuring effectiveness will provide the intelligence needed to evolve the strategy in line with threats and business changes. It will also give you the information you need to demonstrate value – proving that the solutions purchased are delivering expected benefits and ROI. This assurance will communicate the value of the security organization and secure the future investment that will keep the data diamonds safely locked up for good.



FORTRA™

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

© Fortra, LLC and its group of companies. All trademarks and registered trademarks are the property of their respective owners. | fta-corp-ebook-0223-r1-as