WHITE PAPER

McAfee
Together is power.

# 5 Tips to Help Protect Your Data

## From passive monitoring to proactive protection

# 5 Tips to Help Protect Your Data

## From passive monitoring to proactive protection

Last year we published a **report on data exfiltration**, which found, among other things, that about 20% of data losses were attributed to accidental actions by internals, another 20% to intentional actions by internals, and the remaining 60% by external attackers.[1]

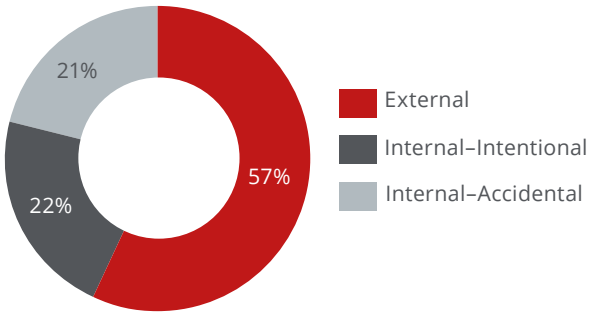


**Figure 1.** Actors involved in data breaches.

Stolen data was most commonly personal information about customers and employees, often in the form of office documents, not databases. With the number of breaches continuing to grow year after year, cyberattacks seem to be an ongoing fact of modern life. Risk is everywhere, and the key is managing it. So the next step is to act on this information, specifically to move from passive monitoring to more protective blocking of sensitive and confidential data. The trick is to do this with the smallest number of false positives and minimal impact to legitimate business processes. Towards that, we have identified five tips, based on real-world deployments and experience, that will enhance your data loss prevention (DLP) implementation.

### Modern Data Protection Challenges

The spread of digital tools and devices creates a data environment that is challenging to protect. The internal data sprawl, spread across a growing range of devices, apps, and file types, is susceptible to both accidental data loss and intentional data theft. Privacy laws vary by country and industry, with increasing requirements to demonstrate proof of compliance. Existing business processes and security training cannot keep up, requiring a different approach.

A modern DLP process needs to be rapidly incremental, focusing on derived value, successful preventative actions, and increasing the risk threshold. Data protection is a job for the whole organization if you want to successfully prevent data loss.

This requires:

1. A corporate champion who is not in IT
2. A governance team
3. An appropriate starting point
4. A bias towards blocking
5. Rules that are context aware

## 1. Identify a Corporate Champion in the Business, not in IT

Data loss prevention is a continual journey, one that requires the efforts of the whole organization to be successful. This cannot be treated as a purely technical issue, with data protection run solely by IT. IT may be responsible for the specs, implementation, and operation, but they cannot be held accountable for the actions and behavior of the whole organization. The majority of breaches have at least one human vulnerability or exploitation involved, whether it is a phishing email, credential theft, or malware infection. It is important to treat this as a business problem, and so requires a corporate champion that is part of the business.

Most departments and business units do not operate at a continuously high level of security awareness. Security training, process changes, and news about other data breaches may briefly heighten awareness, but that can quickly fade. A champion from the business can communicate the business imperatives of protecting the data, lead other department and business unit managers to be champions within their own areas, and better identify conflicts between DLP best practices and essential business processes.

## 2. Build a Governance Team with Distinct Roles

The data protection champion, while highly visible, is one part of a broader data governance team, which is a DLP best practice. It takes a diverse group, representing multiple aspects of the company, to make this work effectively. Security by decree is prone to resistance and too many exceptions.

Effective governance teams include four distinct roles. One role is those responsible for defining and implementing the security solutions and practices, such as the CIO, CISO, and privacy or risk officers, depending on your organization's structure. This group is there to provide their expertise on available technology, best practices from other organizations, threat updates, and continual feedback on what is and is not working. Next are the individuals who are ultimately accountable for the success or failure of the security operations, including the CEO or business unit leaders, but also the owners and creators of the data. Including the data owners and creators is essential to designing secure processes that do not hinder the business, and that have few, if any, exceptions.

Consultants on legal, regulatory, and other external factors are another important part of the governance team, so that processes and technologies work in concert with legal and privacy considerations. This part could include legal counsel, privacy advocates, as well as human resources professionals. The last part of the team is representatives of those who will be working daily with the security processes, so that they are part of the discussion and can inform both the governance

team and their peers of the issues. Risk and operations are best explained by those who live it, and their inclusion helps to ensure that business relationships are not compromised by security practices. Data governance is an ongoing activity that cannot do everything all at once. Start by designing a plan that provides overarching guidance, implementing it, expanding it, and continuing to adapt to the evolving nature of security, privacy, and data.

## 3. Start with Policy, Awareness, Compliance, and Remediation

The purpose of the data governance team is planning and implementing DLP processes. However, it should be immediately recognized that this is a continual journey, not a destination. Data is constantly moving, new types and classifications appearing, and policies and regulations evolving. It is important not to get stuck on any one area, whether it is policy, compliance, or discovery. Many organizations start their process with discovering and classifying their data, but this itself can be an endless task. It is far more important to start by discovering what is leaking out (or being stolen), and at the core of this are your policies. Policies can be developed quickly and refined over time, if they focus on the principle instead of the particulars. For example, a policy could be that all data in transit needs to be encrypted, not the details of the technology and processes that make that happen.

Armed with a set of policies, communication and awareness is next. DLP means blocking activity, as any incident that is not blocked is a breach, and communicating it in this fashion will make dealing with false positives much easier. A false positive can be annoying, frustrating, and slow down business processes, but does no long-term harm. A false negative is a breach. The focus should be on quick wins towards better compliance and faster remediation, not a global understanding of all your data while leaks continue.

## 4. Get to Action, Not Just Monitoring

If you assume that you are already leaking data, the goal is to get to action as soon as possible, addressing the big risks first. Simply monitoring your data losses adds no value to the organization. The easiest progression is from data at rest, to data in motion, to data in use, but that should be modified by your knowledge of what is happening in the organization.

Initial deployments should target false positives between 5% and 10%, which are then quickly analyzed to improve blocking efficiency. If your false positives are too high, and they can approach 30% in typical drop-in deployments, the end result is work-arounds and a return to monitoring only. Instead, build gradually, targeting the biggest risks and leakages. There is a direct but inverse relationship between false negatives and false positives; increasing the sensitivity decreases false negatives but potentially increases false positives.

Increasing the sensitivity of the risk threshold as the rules are refined to be optimally effective improves your loss prevention successes while keeping the false positives within a manageable range.

## 5. Build Rules That Are Both Content and Context Aware

The hard work in all of this is defining and refining the rules that implement the policies and ultimately block potential data loss. The challenge here is to reduce the number of false positives while increasing the risk threshold, which is accomplished by adding context, sensitivity, and specificity to your rules.

For example, an obvious rule is to block documents that include social security numbers (or their equivalent), which in the United States are a 9-digit number of the form 123-45-6789. This seems straightforward using the pattern matching capabilities of regular expressions. However, a 9-digit number could also be a mobile phone number in Singapore, Twitter handle, US Zip+4 code, or a PDF document number. To reduce the false positives, you need more context of the usage in the document, the severity of the potential loss, and the likely sensitivity of the data. You can count to see how many numbers of a similar type are found within the document, and set an initial severity threshold. You can look at how close they are to other personally identifying information, such as a date of birth or credit card number. You can search for textual identifiers close to the risky data, such as "SSN," "First Name," and "Last Name." Compounding these factors together can substantially reduce the number of false positives, in many examples by 50% to 70%.

To aid you in this activity, the governance team needs to clearly communicate that they are implementing the DLP plan, and that people who run into blocked data should call the help desk. Analyzing these notices, which could be a viable process or a true positive, will give you additional factors for the rules and improve efficiency. It is important that there is more than one person involved in creating rules, investigating incidents, and dealing with those responsible, so that there is a separation between police, judge, and jury. Block the worst first and continue iterating until you reach the desired risk threshold.

## Key Takeaways

The costs of data breaches have increased significantly over the past couple of years. These five tips will help your organization implement a comprehensive data protection program and better manage the risks of data loss and theft. The benefits of this type of program extend beyond preventing data leakage, and include facilitating earlier detection and mitigation, reducing the time and cost of breach investigations, enhancing compliance and reporting, and increasing the comfort level of senior management with the organization's risk threshold. Whether you are trying to stop data breaches, demonstrate regulatory compliance, or gain visibility and control of your data across different devices and clouds, an integrated and collaborative approach is necessary.

## McAfee Data Protection Portfolio

McAfee has a range of products and services available to support your data governance activities, including a portfolio of security tools, professional services, and experience assisting with behavioral change and business processes related to controlling data flow.

From endpoint encryption to DLP technology, and from centralized common policy management to automated reporting, McAfee works closely with an extensive community of technology and business partners to deliver the customization and flexibility your organization needs. Whatever stage you are at in your data protection process, McAfee data protection solution and professional services can help you define metrics, offer guidance on best practices, and ease your deployment.

For more information on our data protection products, visit **www.mcafee.com/dataprotection**

For more information on designing and evaluating a data protection program, visit **www.foundstone.com**.

1. **http://www.mcafee.com/us/resources/misc/infographic-data-leaking-your-watch.pdf**

## About McAfee

McAfee is one of the world's leading independent cybersecurity companies. Inspired by the power of working together, McAfee creates business and consumer solutions that make the world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

**www.mcafee.com**.

McAfee™
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com