Solution Brief

Prevent data from leaking out of your organization

Data is escaping from most organizations. It sometimes walks out with insiders, but mostly it is stolen by outside actors. It is leaving in multiple forms and channels. Organizations are trying to stop this outflow, for different reasons and with varying degrees of success. Intel Security commissioned the *Intel Security 2016 Data Protection Benchmark Study* to gain a deeper understanding of the people who are behind these thefts, the types of data being stolen, and the ways it is getting outside of organizations.

In the *McAfee Labs Threats Report: September 2016*, we analyzed survey data and detailed our findings. Among other things, we found that:

- The gap between data loss and breach discovery is getting larger.
- Health care providers and manufacturers are sitting ducks.
- The typical data loss prevention approach is increasingly ineffective against new theft targets.
- Most businesses do not watch the second most common method of data loss.
- Data loss prevention is implemented for the right reasons.
- Visibility is vital.

Recommended policies and procedures for effective data loss prevention

It is critical for organizations to create data loss prevention policies and procedures to prevent inadvertent or deliberate transfers of sensitive data to unauthorized parties. A successful data loss prevention initiative begins in the planning stage when business requirements are defined. For example, aligning data classification and data loss policies to the privacy policies and data sharing standards of the organization should be addressed at the planning stage. Establishing sound business requirements helps focus the data loss prevention initiative and protect against scope creep.

intel Security

An important next step in a data loss prevention initiative is to identify sensitive data within the organization. Server and endpoint scanning technologies allow the classification of files based on regular expressions, dictionaries, and unstructured data types. Data loss prevention products often provide built-in classifications for typical categories of sensitive data such as payment card data or personal health information that can accelerate the discovery process. Customized classifications can also be created to identify data types that are unique to the organization.

Complicating this step is both IT-sanctioned and nonsanctioned applications and their supporting data in the cloud. For IT-sanctioned data in the cloud, identifying sensitive data can and should be part of the process when subscribing to the cloud service. When that is the case, it can be relatively straightforward to classify this type of data.

However, functional groups within organizations often circumvent IT to meet their business objectives by subscribing to cloud services on their own. If IT is not aware of these services and the data that supports them, then there is an increased potential for data loss. Consequently, it is important during this step to work with functional groups to identify the locations of data in the cloud and use the preceding process to classify that data.

After completing the sensitive data discovery process, implementing data loss prevention products within the trusted network and on all endpoints can provide visibility and control to important data at rest and data in flight. Policies should be implemented to detect unexpected sensitive data access or movement. Events such as sensitive data being transferred to USB devices or over the network to an outside location could be part of a normal business process or it could be a deliberate or inadvertent action resulting in data loss.

Well-developed security awareness training can reduce the likelihood of data breaches. Justification screens can help coach users on appropriate actions regarding the transfer of sensitive data and allow users to be educated on data protection policies during the course of their normal workdays. For example, a justification screen can notify users that their transfer of sensitive data is against policy and provide alternatives to completing the transfer, such as redacting the sensitive data before attempting the transfer again.

Data owners typically understand how their data is used better than other groups within the organization. Data owners should be assigned and empowered to triage data loss incidents. Separating duties between data owners and the security team reduces the possibility of a single team circumventing data protection policies.

Once approved data movements have been established and policies governing those movements have been incorporated into data loss prevention products, polices to block unapproved transfers of sensitive data can be turned on. With blocking enabled, users are prevented from performing actions that are against policy. Policies can be tuned to provide flexibility depending on the requirements of the business to ensure that users can perform their duties while still being secure.

As the data loss prevention initiative progresses, it is important to validate and tune policies at scheduled intervals. Sometimes, policies are too restrictive or too lax, impacting productivity or posing a security risk.

How Intel Security can help protect against data leakage

McAfee DLP Discover

The first step to properly securing data is to understand where the information resides and exactly what that data is. McAfee DLP Discover protects against data exfiltration by simplifying this first step through these capabilities:

- Identify classifications to detect within the trusted environment using the built-in classifications (for example, HIPAA, PCI, SOX) or creating customized classifications
- Perform an inventory scan and review using the identified classifications to understand where and what types of data reside within the trusted environment. Review for violations of existing policy in the Discover interface.
- Perform a remediation scan to find data stored in unauthorized locations and move it to an authorized location.
- Inventory and remediation scans can be performed on local resources such as network shares or cloud resources such as Box.
- Create new data protection policies based on the findings of the Discover scans.

McAfee DLP Endpoint

McAfee DLP Endpoint monitors and prevents data exfiltration on premises, off premises, and in the cloud. Quickly monitor real-time events, apply centrally managed security policies, and generate detailed forensics and proliferation reports without hindering day-to-day operations.

- After the Discovery phase is complete, create data protection policies to report policy violations. This provides the necessary data to better understand data movement within the organization and enables enforcement of blocking rules. McAfee DLP includes built-in classifications (for example, HIPAA, SOX, PCI, and ITAR) that can be used to identify data within the organization.
- Create coaching screens for users to better understand data protection policies as they perform their day-to-day data transfers. These customizable educational pop-ups are extremely helpful and reduce risky data transfers by employees.
- Review the Incident Manager to identify the properties of data being transferred to unauthorized locations, such as how transfers are performed and who is doing it.
- After data protection policies have been created and tuned to organizational requirements, enable blocking for unauthorized data transfers.
- Enable Manual Classifications, allowing users to classify documents that they have created. As the data owners, they potentially better understand the sensitivity of the documents if the automated classification engine is unable to detect any structured data. This is built into McAfee DLP Endpoint without any additional third-party tools.
- For additional protection, create and implement an Application Access Protection Rule that uses the McAfee Threat Intelligence Exchange to prevent unknown applications from accessing sensitive data. This allows authorized applications to transfer sensitive data but restricts unverified or malicious applications from accessing that data.

McAfee DLP Monitor

McAfee DLP Monitor gathers, tracks, and reports on data in motion across the entire network. Easily uncover unknown threats to data and take actions to protect it.

- Enable relevant built-in policies and rules to detect potential violations within the network.
- Create additional customized policies and rules, such as monitoring sensitive data transfers to the cloud.
- Conduct forensic analysis to correlate current and past risk events, detect risk trends, and identify threats. McAfee DLP Monitor allows security experts to quickly understand the situation and develop rules and policies to address it.
- Create additional capture filters to exclude irrelevant data and tune rules to reduce false positives.
- Configure alerts to send notifications to senders, recipients, data owners, and system administrators when policy violations occur.

McAfee DLP Prevent

McAfee DLP Prevent protects against data loss by ensuring that data leaves the network only when appropriate—whether through email, webmail, instant messenger, wikis, blogs, portals, HTTP/HTTPS, or FTP transfers. Rapidly identifying and mitigating exfiltration attempts often makes the difference between keeping important data safe and becoming the next news headline.

- Integrate McAfee DLP Prevent with web proxies or message transfer agents using built-in policies to prevent unauthorized data transfers through email gateways or web proxies.
- Create McAfee DLP Prevent rules to allow or block sensitive documents based on the match percentage.
- Use built-in DLP templates to protect sensitive data from being transferred to the cloud.
- Review reports of security incidents and adjust policies to reduce false positives and maximize business continuity.
- Configure alerts to send notifications to senders, recipients, data owners, and system administrators when policy violations occur.

Further reading

Intel Security Expert Center Community

- McAfee Data Loss Prevention

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com