GUIDANCE SOFTWARE is now opentext™ | LIFARS

PROTECTING YOUR SENSITIVE DATA BEYOND THE PERIMETER:

Five ways EnCase Risk Manager Complements Data Loss Prevention

INTRODUCTION

When the first Data Loss Prevention (DLP) solutions were introduced over a decade ago, the interest and expectations were very high. Regulatory requirements such as HIPAA, PCI DSS, and others were likely the most important driving factors. There was growing pressure on organizations to protect their data and the focus was primarily on the perimeter. As a result, it was widely believed that DLP could be deployed similarly to an Intrusion Detection System (IDS), with one exception – the focus would be placed on outgoing traffic. From 2008 to 2012, the complexity of DLP deployment, significant resource requirements, functional shortcomings, and misconceptions about its use all led to a decrease in popularity and deployments. It became evident that a new approach to DLP was necessary.

The current DLP market is transitioning to meet the ever-growing popularity of cloud-based solutions, yet still be able to adapt to newer in-house data storage solutions. This includes the prevalence of newer languages and file types that could store data. Some DLP solutions are now able to monitor data at rest, in use, and in motion, while being able to classify and determine movement in and about the cloud as well. Managed DLP solutions have also appeared in recent years – alleviating the organizations' burden of deployment and management.

Although the DLP and Information Governance market has evolved in recent years, organizations still have needs that are unmet by most DLP solutions – including the ability to access data on endpoints, collect files on supported sources, automatically find and categorize private and sensitive data, leverage and grow historical data intelligence, review file content to validate system categorizations, and many more. Integrating with off-premise cloud-based repositories has proven to be a challenge as well. Most of today's DLP solutions struggle to protect data not available locally, creating major hurdles that will become key differentiators for solutions on the market. If a single solution does not work for all storage types, it adds not just complexity, but increases the costs of a comprehensive DLP deployment as well.

EnCase Risk Manager addresses the gaps found in the current generation of DLP solutions on the market today in a single unified solution. It can be used to complement a variety of Information Governance and DLP solutions within organizations or function as a standalone solution.

EXTENSIVE DATA COVERAGE

As new software is developed and deployed throughout various industries, the number of data types and formats is ever-increasing. Many industries use relatively obscure data formats that can present a challenge to standard DLPs. These data formats are often found in extremely old, new, or esoteric systems. Sometimes if the format is new, it can be a challenge for DLPs to keep up with the development of file formats. A large number of disparate data formats and file types can be difficult to manage and even harder to protect. Finding sensitive data within the organization is challenging on its own, not to mention analyzing where the data is traveling.

The current generation of DLP also struggles with data classification related to the use of outdated methods, such as keywords and regular expression-based classifications. These methods of classification work well in specific situations and well-structured data. However, simple errors and misspellings have the potential to cause incorrect categorizations. As a result, the amount of false positives grows and strains the system – causing slowdowns; additionally, blocking large amounts of data transmissions due to high levels of false positives will negatively impact business operations.

To address the file classification challenges, many DLP solutions need to be used in conjunction with data classification and file analysis tools to identify and classify sensitive and private data. Unlike traditional DLPs, sensitive data and risk management solutions should not be required to

use additional tools to classify data. An effective solution should be able to identify and classify sensitive data and even leverage historical data prior to its deployment – a feature unavailable with traditional DLP solutions which start tagging documents from the time of deployment onwards. Additionally, once data is identified as true positive or false positive, the system should retain that categorization. EnCase Risk Manager is able to classify sensitive information and retain that historical intelligence throughout the entire data lifecycle.

As emerging programs store data in newer ways, a solution that can adapt to the growing variety of data types will be important to ensure that all data is protected and not left vulnerable because of missed file types. These types of inadequacies could render a traditional DLP helpless if it were to be exploited.

NATIVE API INTEGRATION

In the past, most data were stored on-premises due to slow network connections and the lack of affordable virtualizations. With the relatively recent rise of cloud computing and its rapid adoption, many solutions fall short in this respect. DLP solutions have only recently seen the need to develop API integrations – primarily due to the fact that storage of sensitive data on the web was infeasible in large quantities or simply unlikely from a security perspective. As companies now migrate towards web-based cloud solutions, DLPs need to develop this integration, which proves to be challenging when cloud solutions are numerous and ever-changing. Older, more traditional DLPs, have not fully integrated this feature or only implement it among a small set of APIs.

Native API integrations will enable the use of solutions across distributed and disparate data sources, opening doors and enabling more possibilities. Data can be on multiple solutions and managed by the same client if the APIs are integrated. This functionality is key, as it allows for the management of data spread across many platforms. EnCase Risk Manager can leverage the native APIs of data stores without requiring a new DLP solution, keeping costs and management complexities low.

SINGLE AGENT, MULTIPLE SOLUTIONS

Security solutions are becoming more diverse and numerous on the market. Each is specialized, requiring heavy configuration, management, and maintenance. As the number of specialized, individual, and separate tools grows in an environment, so does the complexity. Many security architectures have large numbers of single solutions that are covered by multiple agents and can become an administrative headache, leaving some solutions unused altogether. DLP is often deployed at the agent level or at the network level, alongside other solutions, which can complicate matters. The IT team has the task of ensuring all the parts work together and that the integration is architected correctly. Many organizations find it to be a major challenge to correctly determine a DLP solution's place in the schema of protection and its order of execution, requiring extensive research to ensure that other solutions do not hinder their effectiveness.

The EnCase suite of products and EnCase Risk Manager offer a single unified agent that covers multiple areas of security and information management (eDiscovery, Endpoint Security, Risk Management, Investigations, etc.), which provides a major advantage in terms of management, deployment, maintenance, and oversight ease. Having a single solution also translates to lower overall costs - both for the solution itself and the cost of labor. A lightweight agent that integrates seamlessly with the other security technologies can greatly reduce the complexities of security architecture and therefore lead to faster deployment within an organization.

FAST, USABLE, AND SAFE

Among some of the top business challenges is the fact that security is frequently incompatible with usability. The desire is to have a solution that is both powerful and fast enough to have little to no business impact. A tool that impedes business is not worth the security, but a tool that is insecure can negatively affect the business as well. Many DLP solutions block transmission of data in-line, meaning that any false positives that it picks up can directly affect the business. DLPs need to be configured accurately, which can take time to deploy and still result in slowing down

data transmissions as it struggles to adjust, or it will simply block data entirely as a result of false positive flags. These problems stem from the fact that many DLP solutions rely on keywords without context. The key is to have a solution that allows the business to operate while still managing risks effectively. EnCase Risk Manager delivers both - security and business value.

Protecting the business does not mean just keeping the data safe, but keeping it flowing to the right users as well. As a fast, yet lightweight agent application, EnCase Risk Manager can provide an efficient and comprehensive data security platform to secure data in all formats. EnCase Risk Manager delivers a fast, context-aware solution that can correctly determine sensitivity and catagorize data based on a variety of factors. The contextual intelligence includes information about the user, machines, geolocation, and more. As a result, data is both usable and secure. EnCase Risk Manager takes a proactive approach by targeting sensitive data at the source, at rest, and virtually anywhere data is stored. It can leverage its context-aware capabilities to quickly determine whether data should reside where it is or if it can leave the source as needed.

SINGLE SOLUTION

Having everything under one roof, within a single solution, means there is no need to deploy, manage, and maintain a variety of different tools throughout the environment. This reduction in complexity means that what is deployed can be better maintained and leveraged, optimizing the use of the solution and maximizing the return on investment. There is a danger in complexity, and the more solutions an organization implements, the higher the chances of having a configuration error leading to an open security hole. In addition, DLPs often rely on other solutions to fill their needs. This problem in the data lifecycle usually means that data classification software is used to address data at rest, file analysis tools are used to determine changes and permissions, and a number of other solutions are used to manage data scattered throughout the enterprise.

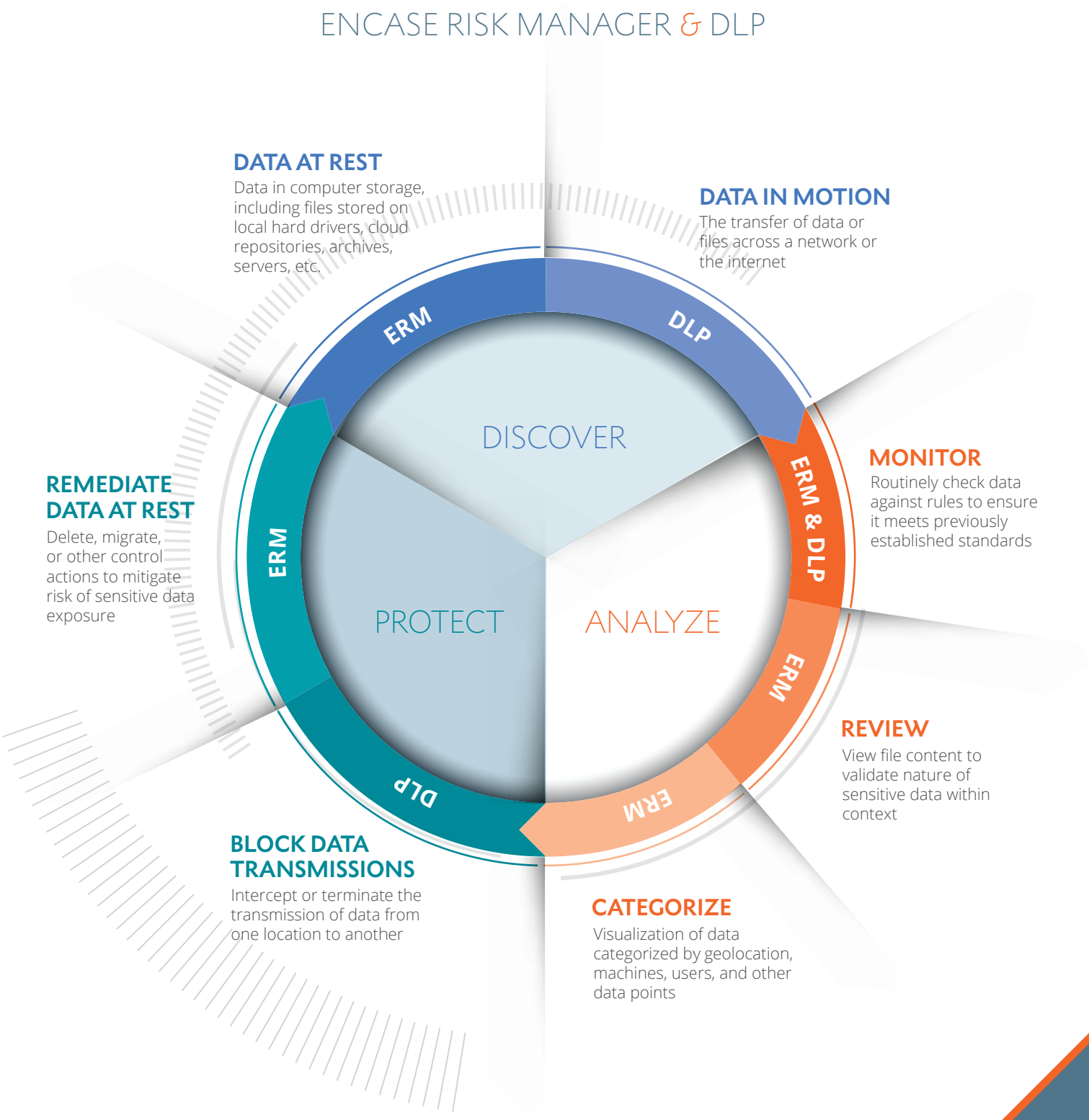
EnCase Risk Manager is vendor-and system-agnostic, which means that it can be deployed alongside other products that are used in the environment and not depend on other applications, such as backup or archiving systems. It is immune to problems that can be caused by the failure to properly integrate products with a competing solution. Vendor agnosticism also allows for platform independence and can help solve problems that arise from a diverse environment.

All major file systems are covered by EnCase Risk Manager, giving it the power to work with all major computing systems that are found in businesses of all sizes - from major corporations to small businesses alike. In addition, EnCase Risk Manager covers data throughout its entire lifecycle without relying on other solutions to fill those gaps.

SUMMARY

Traditional DLPs present a number of serious shortcomings and challenges for companies deploying them, creating a clear gap in the market that EnCase Risk Manager fills – whether as a standalone solution or a complementary technology. Over the years, we have seen the development of traditional DLPs and with advanced attackers on our doorstep, it is clear that more needs to be done to protect company data. EnCase Risk Manager, with its flexibility in data coverage, a single agent, native API integration, and more, provides a more accessible, less costly, and more effective solution to help manage and secure your sensitive data. DLPs tend to be monolithic, single solution-single problem, and can interfere with the business. Their common lack of operational capabilities, independent of additional software such as data classification tools, has made them difficult and expensive to deploy while their complexity and limited scope of functionality leaves a lot to be desired. EnCase Risk Manager is a significantly more versatile, efficient, and effective solution with quick deployment that can complement any DLP solution or be deployed independently.

ENCASE RISK MANAGER & DLP



DATA AT REST

Data in computer storage, including files stored on local hard drivers, cloud repositories, archives, servers, etc.

DATA IN MOTION

The transfer of data or files across a network or the internet

MONITOR

Routinely check data against rules to ensure it meets previously established standards

REVIEW

View file content to validate nature of sensitive data within context

CATEGORIZE

Visualization of data categorized by geolocation, machines, users, and other data points

BLOCK DATA TRANSMISSIONS

Intercept or terminate the transmission of data from one location to another

REMEDIATE DATA AT REST

Delete, migrate, or other control actions to mitigate risk of sensitive data exposure

GUIDANCE SOFTWARE

ABOUT GUIDANCE

Guidance exists to turn chaos and the unknown into order and the known-so that companies and their customers can go about their daily lives as usual without worry or disruption, knowing their most valuable information is safe and secure. The makers of EnCase®, the gold standard in forensic security, Guidance provides a mission-critical foundation of market-leading applications that offer deep 360-degree visibility across all endpoints, devices and networks, allowing proactive identification and remediation of threats. From retail to financial institutions, our field-tested and court-proven solutions are deployed on an estimated 33 million endpoints at more than 70 of the Fortune 100 and hundreds of agencies worldwide, from beginning to endpoint.