CODE42

White Paper | **Next-Gen Data Loss Protection**

The Six Failures of Legacy DLP

SIX MAJOR ISSUES WITH LEGACY DLP

1. Complex to deploy
2. Difficult to manage
3. Blocks employee productivity and stifles collaboration
4. Fails to protect sensitive data
5. Requires high acquisition and operational costs
6. Limits data visibility

In today's enterprise, as many as 50 percent of data loss incidents involve insiders in some way.[1] These incidents pose a critical threat to organizations as they often include intellectual property (IP), which according to Deloitte can account for up to 80 percent of an organization's value.[2] It should be no surprise then that organizations are under more pressure than ever before to protect their valuable data from loss, leak, misuse and theft. As a result, deployment of data loss prevention (DLP) products is growing steadily. Despite the reliance on these products and increased usage, businesses are struggling with the poor performance of these solutions.

Legacy DLP products are designed to prevent known data threats and "best-case" information workflows. They can recognize the patterns of regulated data, such as social security numbers, credit card numbers or health records. And when set up properly, their strict rules usually prevent users from moving that structured data outside designated spaces — stopping unauthorized downloads, uploads or other data sharing or removal. However, even when implemented properly, legacy DLP solutions have failed to deliver on the promise to prevent data loss from insider threats in six important ways:

1 Complex to deploy

In order for legacy DLP solutions to avert data loss incidents, prevention policies must be created. Many are simple and logical. For example, basic rules to stop files containing nine-digit numbers from being moved to USB drives are often employed to prevent social security numbers from being exposed. While individual policies may not be difficult to create, most organizations will need dozens, hundreds or even thousands of policies to protect their data. Developing and implementing these policies can take months or even years.

It only gets more complicated once legacy DLP solutions are initially up and running. With each policy comes the exceptions that must be accounted for. Are all nine-digit numbers social security numbers? For instance, what if a retailer also has nine-digit inventory numbers? Businesses quickly realize that the only option for alleviating IT and user productivity burdens is to create a long and continually growing list of exemptions. Adjusting the rules when too much or too little data is blocked is an ongoing process; it can take years — and a lot of dedicated staff time — to find the right balance. One legacy DLP customer has been in the process of optimizing their solution for the past two years. The company has yet to roll it out to all employees, due to the complexity involved in optimizing DLP policies.

The heavy lift to set up and fine-tune policies is a major reason why legacy DLP solutions take so long to properly implement, but other factors contribute as well. Legacy DLP products require on-premises hardware appliances, which come with their own investments in time and money. Between setting up policies and physical hardware, legacy DLP often takes years to roll out and get off the ground.

2 Difficult to manage

Data usage patterns are complex and dynamic, requiring a never-ending effort to adjust and fine-tune DLP policies. Because of this complexity, legacy DLP products tend to generate a lot of false positives — alerts for perfectly normal, safe activity. To make matters worse, many policies are simply variations of others — causing a single false positive to generate dozens of notifications. In case the alerts signal a real threat, they have to be cleared by an administrator, which can create a significant drain on IT and security productivity and lead to “alert fatigue.”

In addition to managing policies, legacy DLP solutions must manage the behavior of people. To maximize the effectiveness of these tools, employees need to behave differently. This requires communications, processes and training sessions to ensure that employees understand how legacy DLP tools will affect their actions and their workflows. This adds even more time and complexity to an already-challenging policy administration process.

> Oversensitive DLP policies inevitably misinterpret employees’ actions or their intent, and users are regularly blocked from completing their work.

3 Blocks employee productivity and stifles collaboration

Legacy DLP solutions take a toll on the productivity of employees who are generating the valuable intellectual property (IP) that fuels business performance. Despite the effort spent refining DLP rules to fit the unique users and specific business use cases, oversensitive DLP policies inevitably misinterpret employees’ actions or their intent, and users are regularly blocked from completing their work.

To streamline legacy DLP deployments, most organizations fall back on policy defaults that apply blanket rules to large groups of users, data formats and data movement types or actions. This one-size-fits-all approach simply doesn’t work for real-world digital productivity workflows. Despite having legitimate reasons, employees inevitably need to use data in ways that break the rules. Even the most responsible employees begin looking for workarounds.

4 Fails to protect sensitive data

Legacy DLP products were primarily designed to recognize the patterns found in structured, regulated data. The challenge, however, is that the vast majority of IP exists as unregulated data. And while unregulated data can be just as valuable to business success as more structured data, DLP policies often leave this less structured data exposed.

Though some organizations have attempted to solve this problem by tagging unstructured IP data with metadata readable by the DLP tool, this approach can’t account for the constant evolution of IP. Ideas and content are continuously being modified and re-imagined — legacy DLP products simply cannot keep up. And when the imperfect prevention-oriented walls associated with legacy DLP fail, the tools offer no avenue to replace the lost data. Without collecting the contents of files or capturing file history, legacy DLP solutions are ill-equipped to identify or recover from unexpected threats.

5 Requires high acquisition expense and operational costs

Legacy DLP solutions are expensive to implement and maintain. They are designed and priced for implementation by large, enterprise-scale organizations. Full deployment is such a significant effort that it is rarely achieved by even the largest companies. Unless the business commits a large team and years of time to optimize and manage the solution, legacy DLP is typically underutilized — limited to monitoring only, for example.

Legacy DLP solutions are generally not effective for mid-sized and smaller companies.

Mid-sized and smaller companies, while having the same data protection needs as larger companies, are not staffed or mandated to effectively use even a fraction of the capabilities of legacy DLP solutions. DLP solutions are generally not effective for these types of organizations.

6 Lacks data visibility

By focusing on restrictions and rules, companies implementing legacy DLP can actually end up reducing visibility to important corporate data. With a focus on known data risks and behaviors, organizations can create a blind spot for unexpected activity.

For instance, take the case of the malicious insider who exfiltrated data before alerting human resources that he would be leaving the company. A legacy DLP policy that tightens restrictions once employees announce their departure does nothing to protect against data loss for the most likely exfiltration window: just before employees reveal that they are leaving.

As another example, consider an organization that uses its legacy DLP solution to monitor only protected health information (PHI) and personally identifiable information (PII). While some of their customers' most critical data is protected, this organization's legacy DLP tool offers little protection for its business-critical IP. The organization may stop malicious insiders from taking customer data, but without visibility into unstructured data, critical files, like strategy documents, sales tools or product information, are still vulnerable.

Rethink DLP

All of these issues with legacy DLP ultimately stem from the same root problem: a narrow focus on prevention. It's time for businesses to rethink legacy DLP and shift their focus from prevention to protection. Based on this new approach to DLP — next-generation data loss *protection* — security teams can more quickly and easily protect their organization's data while maintaining an open and collaborative culture for their employees.

A next-generation DLP solution is built with the following considerations in mind:

- **Built to monitor, not block.** Next-generation DLP enables employees to work without hindering productivity and collaboration. With full file visibility, security teams can block employee data use when needed — but based on facts, rather than often-inaccurate policy-based guesses.

- **No policies.** With a focus on protection instead of prevention, next-generation DLP solutions don't require policies, avoiding the complexity and effort to manage and police those rules.

- **Deploy in days, not months.** Solutions can be rapidly implemented — extensive time and effort required to create and refine DLP policies is not needed.

Rethinking DLP: protection over prevention

- Built to monitor, not block
- No policies
- Deployed in days, not months or years
- Native to the cloud — no hardware required
- Focused on files

- **Native to the cloud — no hardware required.** Next-generation DLP lives in the cloud, providing full visibility to files and activity across endpoints and cloud services.

- **Focused on files.** A protection-oriented next-generation DLP architecture focuses less on restrictive rules of behavior and more on the data itself. It delivers visibility across all files on endpoints and cloud services, seamless retrieval of file contents when needed, as well as long-term retention of files to satisfy legal and compliance requirements.

Legacy DLP has failed to protect businesses from significant and growing insider threats. By taking a new approach — next-generation data loss protection — organizations are finally able to keep their important data protected without hindering the productivity of the employees who are driving the value of the business.

[1] The Human Element of Cyber Risk — McKinsey, September 2018

[2] dupress.deloitte.com/dup-us-en/deloitte-review/issue-19/loss-of-intellectual-property-ip-breach.html

FOR MORE INFORMATION: CODE42.COM/CONTACT

CORPORATE HEADQUARTERS | 100 WASHINGTON AVENUE SOUTH | MINNEAPOLIS, MN 55401 | 612.333.4242 | CODE42.COM