It's Time to Rethink 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 cost
6. Limits data visibility

For years, organizations have been using data loss prevention (DLP) solutions to detect and prevent potential data breaches and data exfiltration incidents.

Legacy DLP tools work by monitoring and blocking data in use, in motion and at rest. They typically stop users from moving data outside designated spaces, and block unauthorized downloads, uploads or other data sharing or removal. For example, one of the most common uses of these tools is identifying the patterns of regulated data such as social security numbers and credit card account numbers to prevent them from leaving an organization.

The problem is that the narrow prevention orientation of legacy DLP solutions no longer meets the needs of today's IP-rich organizations. In today's knowledge economy, companies are shifting towards cloud-based tools that drive collaboration and innovation. The data movements that make cloud-based collaboration tools so effective, however, are the same movements that legacy DLP solutions restrict. That's why it's time for organizations to rethink their concept of DLP and shift their focus from prevention to protection.

Next-generation data loss protection (next-gen DLP) provides security and IT teams a way to more quickly and easily protect their organization's data while maintaining an open and collaborative culture for their employees.

Key traits of next-gen DLP

Next-gen DLP represents a fundamental shift in philosophy from legacy DLP. The prevention focus of traditional DLP forces a productivity trade-off that isn't right for all companies — and isn't successfully stopping data breaches. Rather than blocking the day-to-day work of employees with rigid and ineffective prevention policies, next-gen DLP clears the way for innovation and collaboration. Security and IT teams can monitor, identify and analyze file activity without the negative impacts to end users or burdening administrators with policy management or false positives.

Next-gen DLP arms security and IT teams with the following file-focused capabilities:

- **Collection:** Next-gen DLP automatically collects and stores every version of every file across all endpoints, and indexes all file activity across endpoints and cloud.
- **Monitoring:** Next-gen DLP helps identify file exfiltration, providing visibility into files being moved by users to external hard drives or shared via cloud services.
- **Investigation:** Next-gen DLP helps quickly triage and prioritize data threats by searching file activity across all endpoints and cloud services in seconds, even when endpoints are offline; and

rapidly retrieves actual files — one file, multiple files or all files on a device — to determine the sensitivity of data at risk.

- **Preservation:** Next-gen DLP can retain files for any number of employees, for as long as the files are needed to satisfy data retention requirements related to compliance or litigation.
- **Recovery:** Next-gen DLP enables rapid retrieval of one file, multiple files or all files on a device even when the device is offline, or in the event files are deleted, corrupted or ransomed.

Because next-gen DLP automatically collects and stores every version of every file across all endpoints, there is no need to set policies around certain types of data.

The next-gen advantage

These file-focused capabilities have recast the historical approach to legacy DLP — and created a new paradigm of data protection that has notable advantages over its traditional counterpart.

Works without policies

With a focus on protection rather than prevention, next-gen DLP does not require policies or all of the complexity and effort associated with managing and policing rules.

To enable legacy DLP systems to stop data loss, companies need to create policies, which can be difficult to build, often requiring third-party vendors to create them. Many organizations will require hundreds of policies to protect their data. Creating and deploying these policies can take months or even years. And setting policies is never "done." Because new tools and employees constantly enter an organization, adjusting the rules within policies is an ongoing process.

Furthermore, each policy comes with exceptions that need to be accounted for, so companies end up creating a long and growing list of exemptions. In short, setting up and maintaining policies is a key reason why legacy DLP systems take so long to properly implement.

Because next-gen DLP automatically collects and stores every version of every file across all endpoints, there is no need to set policies around certain types of data. When data loss incidents strike, affected files can simply be restored, whether the incident affected one file, multiple files or multiple devices.

Monitors but doesn't hinder user collaboration

Next-gen DLP is designed to enable employees to work without hindering their productivity and collaboration. Employees are not slowed down by "prevention-first" policies that inevitably misdiagnose file events, deny data use and interfere with their ability to get their work done.

Legacy DLP solutions take a "trust no one" approach, blocking all behaviors that trigger a policy, even when that behavior is benign. For example, policies designed to prevent social security numbers from being exposed assume that all nine-digit numbers are social security numbers. If an organization uses nine-digit numbers for another legitimate use, such as product codes, legacy DLP will block them from being shared, hampering legitimate work.

Next-gen DLP, on the other hand, offers full

file visibility from endpoints to the cloud — so security and IT teams can observe and verify employee data use. For instance, next-gen DLP alerts administrators when unusually large amounts of data are transferred to removable media or cloud services. If files do leave the organization, next-gen DLP allows security and IT teams to see exactly what was taken and to restore the exfiltrated files. With these capabilities, the decision to block users can be based on facts, rather than on the often-inaccurate policy-based guesses associated with legacy DLP.

Next-gen DLP offers full file visibility from endpoints to the cloud — so security and IT teams can observe and verify employee data use.

Focuses on files rather than policies

Shifting DLP from a prevention to a protection orientation requires a solution architecture that is focused less on restrictive rules of behavior and more on total visibility to and collection of the data in an organization. A protection approach has three essential traits:

- Unified file visibility into file activity across endpoints and cloud services to speed security investigations. This differs from legacy DLP, which only provides a view of select data.
- Fast retrieval of file contents and historical file versions, to perform detailed analysis or recovery from data incidents. Legacy DLP solutions don't collect the contents of files, and thus can't make them available for analysis or recovery.
- Long-term file retention to help satisfy legal and compliance requirements as well as to provide a complete data history for as long a time period as an organization requires. Again, legacy solutions don't retain file contents and so they aren't able to provide this history.

Lives in the cloud

As a cloud-native solution, organizations with next-gen DLP are freed from expensive and challenging hardware management, as well as complex and costly modular architectures. Legacy on-premises DLP systems, on the other hand, do not provide the flexibility, scalability and economic advantages provided by cloud-based services.

Because next-gen DLP is cloud-native, it can collect and store every version of every file across all endpoints, and index all file activity across endpoints and other cloud services. By storing collected files and file metadata in a secure cloud, files can be examined and recovered even when the endpoint where the files originated is offline.

Deploys within days, not months

As anyone in the security and IT profession knows, timing is critical. Data security solutions that take too long to implement can leave organizations vulnerable to damaging attacks.

Next-gen DLP solutions can be rapidly implemented, since the extensive time and effort required to create and refine legacy DLP policies is not needed.

Next-gen DLP is also much easier to manage once deployed than legacy DLP. By focusing on total visibility to files and file movement in an organization rather than restrictive policies, productivity is

maintained for both administrators and end users. This is especially important for organizations that lack the internal staff or skills to manage and maintain security tools.

It's time for a DLP reboot

Safeguarding data does not mean you have to lock down data access and block employee productivity and collaboration with restrictive policies that govern use. While legacy data loss prevention solutions have historically taken this narrow approach, it simply no longer works. Despite the best prevention tactics, the reality is that data loss incidents happen — and once they do, the focus turns to remediation and recovery.

Instead of blocking data motion, next-gen DLP provides full visibility to where every file lives and moves and gives security teams the tools they need to collect, monitor, investigate, preserve and recover valuable company data in the event of a loss. These capabilities also integrate with other security technologies such as security information and event management (SIEM), device management, and identity management to speed up threat detection, investigation, compliance and incident response.

Companies today are looking for better ways to protect their high-value data — while freeing knowledge workers to create the ideas that drive the business. By choosing next-gen DLP, organizations will be able to keep their vital data protected without hindering productivity and innovation.

Growing insider threats

The primary purpose of DLP tools is to prevent data loss incidents that originate inside an organization. Insider threats can present in many ways: malicious outsiders posing as insiders; malicious and negligent insiders; stolen credentials; unsanctioned applications; user errors; lost or stolen devices; weak passwords; unpatched systems; shadow IT; technology product and service integrations; and vendors, partners, contractors and consultants.

A report by International Data Group (IDC) based on a survey of 9,500 business and technology executives worldwide showed that three of the top five most common high-value information incidents involve actors inside the organization.[1] Another study by the Ponemon Institute, conducted in conjunction with the Thales Group, showed that four of the top five most common sensitive data threats are everyday pervasive data risks such as employee mistakes or system and process failures.[2]

[1] IDG (CSO); PwC; CIO
2018 The Global State of Information Security Survey
Published by IDG
Release date: December 2017

[2] Ponemon Institute; Thales Group; Website (vormetric.com)
2018 Global Encryption Trends Study
April 2018

FOR MORE INFORMATION: CODE42.COM/CONTACT

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