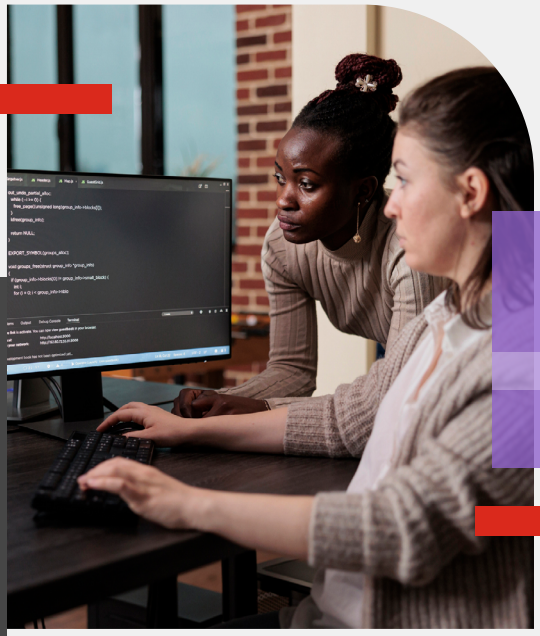
POINT OF VIEW

# Address Legacy Data Loss Prevention Challenges

## Understanding Cloud-Native Endpoint DLP



### Executive Summary

Security teams are increasingly exasperated with legacy data loss prevention (DLP) solutions that can't effectively and efficiently adapt to the complexity of today's network environments. The adoption of the cloud, the proliferation of sanctioned and unsanctioned SaaS applications, and the advent of fully remote and hybrid remote workforces have increased the points of egress for sensitive data to be leaked or exfiltrated by both external actors and insiders. Because of the changes in network conditions, organizations need a new DLP approach better suited to today's network environments.

Negligent employees were responsible for 55% of incidents (contributing as many as 14 incidents per year) across organizations and an average of $7.2M in total costs associated with resolving the incidents.[1]

### The Challenges of Legacy DLP Solutions

Cloud adoption and SaaS applications have changed the computing landscape. The explosion in data growth, the introduction of generative AI (GenAI), and the combination of remote and hybrid workforces using company-provided equipment and personal devices have increased the complexity of today's IT environments. Because of these changes, significantly more egress points exist for a company's high-value data to be accidentally or intentionally leaked.

Unfortunately, traditional DLP tools with static policies are no longer enough for many organizations to protect data across complex IT environments. In many cases, the tools have become less about data protection than checking a compliance box. Traditional DLP approaches and solutions are sub-optimal because:

- Data classification programs and data discovery scans are required before implementation.
- Time to value is long and adversely impacts operational costs and the overall return on investment.
- Visibility and control over data movement are dependent on static policy definitions.
- Solutions are ineffective at protecting intellectual property such as design files and binary file formats.
- Excessive false positives are produced because of the dependency on content inspection to detect data.
- Low-level operating system (OS) techniques intercept data for analysis, causing system instability.

## What Is Next-Gen DLP?

A company's sensitive data is no longer contained in a tightly controlled environment. It's transmitted between cloud services, SaaS apps, and the laptops of remote workers who can be located anywhere in the world. Whether an employee uses a company-issued laptop or personal mobile device, protective measures must be in place to ensure data is not deliberately misused, stolen, or accidentally exposed.

The next generation of endpoint DLP solutions couple data loss prevention with insider risk management. This approach makes perfect sense when you consider that employees cause accidental data loss and deliberate data exfiltration. Next-gen endpoint DLP solutions also excel at automated data identification and tracking. The best solutions can classify data in real time to ensure that all information is correctly classified and protected at the point of access by employees. This feature includes the ability to detect and protect both sensitive data, such as personally identifiable information and personal health information, in addition to intellectual property, such as design files and source code. It can detect this data based on content, sensitivity label, or the origin of the data, such as an application like Salesforce.

A modern DLP solution has multiple benefits that help overcome the obstacles associated with traditional DLP approaches. A next-gen DLP solution:

- Unifies data loss prevention with insider risk management and SaaS data security for a holistic view of data in use and at risk
- Is cloud-native to provide the latest data identification technologies and risk analytics
- Is endpoint-based to provide DLP protection centered around employee or user behavior
- Delivers visibility into business data flows immediately and greatly accelerates time to value
- Identifies and detects sensitive data and intellectual property in real time at the point of use by users
- Protects data when endpoints are online or offline
- Conducts user education at the point of use of sensitive data by employees or other users
- Captures activity context events for use in investigations and forensics activities
- Scales to support organizations with hundreds of thousands of endpoints and users

## Why Cloud-Native Endpoint DLP?

A next-gen endpoint DLP solution continuously monitors data access and use, user behavior, and all egress points. It covers remote and in-office employees and enforces security policies even when offline. Sensitive data remains secure no matter where an employee attempts to access it based on the DLP policy definitions in place. The solution uses machine learning, integrated into the endpoint agent, to identify normal, novel, and anomalous activity. A DLP endpoint works by:

- Continuously tracking and analyzing data as it moves across and from endpoint devices
- Performing both contextual and content-level inspection of data when accessed by users
- Scanning files, emails, and other communications for sensitive information to ensure compliance with security policies
- Enforcing data protection policies to control how data can be accessed, used, and shared
- Preventing unauthorized data transfers to external devices, cloud storage, or email

With a robust endpoint DLP solution, different levels of security can be implemented for specific devices or data assets. For instance, an employee may be able to view sensitive data to perform their job but be restricted from copying it to a removable device. Endpoint DLP enforces policies that control where and how an individual can use data.

Automated DLP enforcement can warn users that an action they are trying to take is against company policy or perform any number of actions based on policy. Next-gen endpoint DLP solutions can also report on attempted usage of sensitive data to enable management to address specific individuals who may require additional training about data security policies.

For most companies, the most critical aspect of an effective endpoint-based DLP solution is that it reduces the probability of an insider accidentally or maliciously exposing high-value data. Because most data breaches are caused by careless and malicious insiders (including threat actors with stolen credentials), simply restricting the unapproved use of data resources can drastically reduce the chance that valuable information is compromised.

## A New Approach to DLP

Traditional DLP approaches are poorly suited to the complexity of today's ever-evolving network environments, so security teams need modern DLP solutions that can protect data in use by employees no matter where they are located or the devices they use.

Security teams should look for solutions where automated enforcement of DLP policies is facilitated by machine learning and use advanced content inspection to identify high-risk data elements. Solutions should also deliver employee education with instructive popups that advise users on why an activity was restricted and how they can avoid future warnings.

"Malicious insiders," or employees with malicious intent toward their organizations, were responsible for an additional 25% (six incidents per year) of incidents. Compare this to credential theft involving threat actors, which contributed to 20% of incidents.[2]

[1] Ponemon Institute, 2023 Cost of Insider Risks, 2023.

[2] Ibid.





November 19, 2024 5:41 PM / MKTG-345-0-0-EN