WHITE PAPER

proofpoint™

THE DLP DILEMMA

Why Most Data Loss Prevention Deployments Aren't Working—
and How the Proofpoint Information Protection Suite Can Help

www.proofpoint.com

INTRODUCTION

For most information security professionals, the central link in the security chain is also the weakest: your people. Even well-meaning users click links that they shouldn't. They email information that's supposed to stay private. And they store private data in places where it doesn't belong.

Many IT leaders attempt to implement a "least-privilege" security model to protect users from themselves and limit damage from unintended insider threats. The idea: give users access the network resources—and only the resources—they need to do their job. The least-privilege model is designed to guard against attackers that zero in on users with entitled employees, steal their credentials, and walk off with your data.

But the principles of least privilege quickly break down when they clash with real-world productivity needs—for end users and IT teams alike.

The entitled user trap

Constant network provisioning to limit and segment user access is a chore in itself. Add to that the complexity of knowing when to revoke or downgrade access, a process that is rarely automated. When users have to wait for access to information they need, work slows down—and IT teams quickly earn the reputation of not being "responsive."

Large organizations are home to growing numbers of entitled users, workers with a high level of network privileges. Such privileges are often inconsistent across employee rank and function, making these users difficult to track under normal business conditions. In a merger or acquisition, the task can be nearly impossible.

When control leads to chaos

At the other extreme, organizations that try to control network access too tightly may frustrate users and push them to bypass security controls—defeating the whole purpose. Employees will always find a way to get the data they need to do their jobs. They may share credentials or store sensitive data on cloud services that don't comply with your organization's security policies.

Providing ad-hoc access to sensitive data sources creates its own problems. Users may squirrel away data for later use. So even when user access is closely monitored, telling the difference between malicious exfiltration and bad digital habits can be tough.

Either way, both situations result in an increased attack surface.

Given the structured and unstructured data these users create—and all the locations and devices where it could be located—today's information protection challenges might seem overwhelming.

They don't have to be. This paper explains why with conventional approaches to information protection fall short—and how you can protect your data without slowing down your users.

ATTACKERS EYEING MIDDLE MANAGEMENT

The potential damage from compromised privileged credentials has long been a source of anxiety for security professionals. In the past, their concern centered around the executive suite and the cleverly designed phishing emails that target them.

But today's attackers are broadening their reach. We have seen a dramatic shift to attacks on middle managers. With elevated access, overstretched agendas, and 100 to 200 new emails in their inboxes awaiting a response every day, middle managers can be the perfect target—and there's a lot more of them on the network.

Attackers recognize that a faster pace of work and a heavy email load makes sidetracking them easier. Many don't pay close attention to what they click, what files they open, or where they use their credentials to log in.

THE CHALLENGES OF TRADITIONAL DLP

Many organizations tackle the risks of privileged user access with a data loss prevention (DLP) program. They purchase a wide-ranging DLP suite, hoping for a silver bullet for their information protection challenges. They rarely find one.

DLP requires hefty preplanning

Often, implementation is rushed. Most DLP deployments require meticulous planning. Security teams must consider all the different sources of sensitive data, both structured and unstructured. Then they must decide how to classify all the data sources that need to be protected and securely transmitted.

Consider all the data organizations must properly classify to get value from their DLP deployment:

- Intellectual property
- HR records
- Financial data
- Customer information
- Partner secrets
- Supplier records

Deployment is complicated

Taking on too many vectors too quickly—or worse, at the same time—is all too common in many deployments. Security leaders are understandably eager to protect sensitive data across the network, endpoints, data at rest, data in use, and point solutions such as email.

But identifying, locating, and classifying important data takes substantial effort. And the work involved in deciding how to enforce DLP policies (block, quarantine, delete, encrypt, and so on) is almost always underestimated. Most organizations stop at the "crown jewels," leaving large gaps in protection.

DLP poses many integration hurdles

Another hurdle for DLP deployments, especially network-based deployments, is integrating them with point solutions for authentication and endpoint security.

For one, a network-centered DLP approach is usually better at preventing insider negligence than malicious data theft. A motivated troublemaker will find many ways around normal DLP safeguards—

remote desktop protocols (RDP), proxy services, VMs, to name a few. Network-based DLP deployments can be easily defeated simply by encrypting the data, neutering the ability of most DLPs to inspect traffic.

Some organizations add SSL inspection to their DLP deployment, though most shy away from the added complexity. SSL inspection is notorious for bringing traffic inspection to a crawl and slowing down the network. So any SSL inspection must be done in a way that helps analyze suspect traffic faster rather than getting in the way. This is no easy feat, even for seasoned IT security pros.

And most DLP tools require frequent tuning—which means on-hand expertise. Without such tuning, IT teams quickly get bogged down in false positives or, even worse, block legitimate traffic.

The budget, expertise, and support behind a lengthy configuration, integration, and roll-out process required can make network-based DLP projects feel like a four letter word. False starts, lack of business alignment, and limited understanding of the context for creating and sharing company data are just some of the problems of deploying or expanding DLP in your organization.

Your DLP tools aren't going away anytime soon. But you can complement them with technology that helps lessen the burden of constant tuning to adapt to new users, data sources, and changes to the network.

A BETTER SOLUTION WITHOUT ALL THE DLP TROUBLE

Building an effective information protection program means tackling the privileged user problem. Often, safeguarding your organization from security risks means protecting trusted employees from themselves.

Getting the benefits of DLP without all the heartache requires automated protection and advanced controls to reduce your attack surface—finding the sensitive data users create and protecting it before it leaves their control.

What to look for in an information protection solution
The most effective solutions will protect corporate data without complicating your environment. The following sections describe what capabilities can enhance your DLP deployments.

Automated discovery and identification of sensitive content
By automatically finding and identifying corporate data with personally identifiable information (PII) and other high-value content, an enhanced solution simplifies the task of determining the "who, what, where, and when" throughout your environment.

The most effective solutions also help classify sensitive data automatically and move it to a more secure location when needed. Rather than relying on a manual document inventory, look for information protection that does this automatically and visualizing results with a heat map of your file stores.

Continuous monitoring
Your data is constantly changing as files are created, moved, and saved. To ensure that the proper controls are in place, your information protection solution must be able to track and enforce security policies for these files across all of your managed data stores—including Microsoft SharePoint and file stores in remote offices.

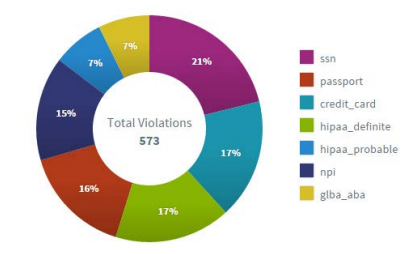
Automated, dynamically applied encryption
A modern information protection solution automatically encrypts sensitive information on the fly based on your IT policies. Users shouldn't need to take any special actions to encrypt sensitive documents and messages. Instead, your solution should be able to deeply analyze the content and automatically encrypt it when it finds any of the following:

- Regulated information such as social security numbers, credit card numbers, account numbers, medical information and specific messages, such as CEO memos and patent information
- Destination or sender fields such as a specific business partner or supplier
- Message attributes such as attachment type

DATA DISCOVER PROFILER

Learn more about what's at risk within your organization. Get started today with Proofpoint's complimentary Data Discover Profiler tool

With Data Discover Profiler, you can quickly scan your organization's file servers and see where sensitive data is stored and who has access to it. The software takes a minute to install and runs automatically. Within minutes, you get a visual overview of where your most sensitive data exists and how to protect it. The tool provides a complete profile of your risk, ranging from breaches (both external and internal) to compliance violations.



On average, only 18% of organizations employ tools that automatically discover data desirable for exfiltration - PHI, PII, PCI, etc.

Osterman Research, March 2015, Dealing with Data Breaches and Data Loss Prevention

Encryption policies should trigger with both full and partial matching of your document fingerprints regardless of whether the data resides in the original file format.

CONCLUSION

Sprawling data and a growing numbers of users needing access to sensitive information continues to challenge today's enterprises. Employees now create more than 80% of a typical company's data—about 2 terabytes per user every year. That's why you need a people- and data-centered approach to securing your data.

To reduce your attack surface and compliance risk, look for integrated solutions that:

- Simplify and automate discovery of sensitive data
- Offer transparent control of outgoing communications
- Continuously monitor your data sources

These key ingredients mean stolen credentials cause far less damage—even with this access, outsiders can't take your sensitive data or intellectual property.

The Proofpoint Information Protection Suite secures offers all three of these capabilities to secure most sensitive data. It stops data leaks before they happen by identifying, fingerprinting, classifying, and encrypting critical data and messages.

To learn more about how the Proofpoint Information Protection Suite can enhance your DLP efforts, visit http://proofpoint.com/us/solutions/products/data-discover

ABOUT PROOFPOINT
Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.

©Proofpoint, Inc. Proofpoint is a trademark of Proofpoint, Inc. in the United States and other countries.
All other trademarks contained herein are property of their respective owners.