Keeping Data in Bound: The Case for a Unified Data Loss Prevention Policy

Strong data-layer security can improve enterprise security and enable new workflows

WHITE PAPER

Symantec

As mobility and cloud computing continue to expand, so does the network perimeter that defense agencies need to protect. Data loss prevention (DLP) used to be simple, at least in theory: Protect the local network, and all data within that network perimeter will be secure. But it's no longer that simple. Today, the perimeter has expanded to wherever users are, from the frontlines to the Pentagon. In essence, data is the new perimeter.

In this new era of network and data growth, the Department of Defense (DOD) must create a unified DLP policy. For large departments such as the DOD, this means a multi-faceted approach covering several technological domains, including cloud applications, endpoints, data repositories, emails, and web communications.

In adopting cloud, mobility, and related technologies, agencies have argued that users need to access data whenever they need it, wherever they are, and through whatever device they are using. The same requirements apply to DLP.

Agencies need the ability to enforce a DLP policy, however users access data. Otherwise, agencies either risk exposing valuable and sensitive data to adversaries, or restrict data access so severely that modern mobility and cloud technologies become all but useless.

> We need to figure out what it means to implement data protections that will allow us to rollback that perimeter protection. We need to start shifting to data security from where we are today, but…we can't just abandon our boundary at this point because we still need that boundary to protect us.
>
> **— Robert Vietmeyer**
> Associate Director for Cloud Computing and Agile Development, Enterprise Services & Integration Directorate, Office of the DOD CIO (2017 Defense Systems Summit)

Components of a Unified DLP Policy

A DLP policy should follow data wherever it goes. As a result, DOD agencies need to ensure that they have a unified strategy that weaves the different technological components together to ensure complete security. Here are some key attributes the DOD should look for to protect data in different areas of the enterprise.

CLOUD

Agencies need to uncover data loss blind spots that exist in both sanctioned and unsanctioned cloud apps. They also need to ensure that DLP systems work with the most popular cloud productivity apps, including Office 365, Box, and Dropbox. Agencies should also look for detect-as-a-service technologies that can identify anomalies in network behavior.

EXTERNAL

Agencies require real-time permission management, allowing them to protect information when it is stored with third parties outside the enterprise. Agencies also need to protect sensitive data found in the cloud, in on-premises file stores, SharePoint, removable USB, or data tagged by users. Finally, agencies call for security measures such as identity controls, encryption/decryption, and digital rights management to follow users wherever they go.

IN TRANSIT

Data must be controlled whenever it leaves an organization, even when it is accessed from unmanaged locations or devices. One option is to define a user's level of access through digital rights management technology, applied not at the network level, but the data level. Another option is to monitor user access for any behaviors that might compromise security—and to revoke access as appropriate.

ENDPOINTS

As agencies create DLP policies, they need to ensure that endpoints remain protected, wherever they are. Agencies need to scan local hard drives, allowing deep visibility into sensitive files that users store on their laptop and desktops, along with the ability to quarantine files, local or remote, as necessary. These tools should also help users, providing them with alerts to incidents with on-screen popups or email notifications.

STORAGE

Even data at rest must be protected. DLP technologies can scan network file shares, databases, and other enterprise data repositories for confidential data. This includes local file systems on Windows, Linux, AIX and Solaris servers, among others. DLP technologies also clean up and secure any files that have been exposed, and remediate them to ensure they are secure. Newer systems can even educate users about policy violations by leaving a market text file in the file's original location to explain why it was quarantined.

Implementing a unified DLP policy ensures that data remains protected and secure no matter its state—in transition, in use, or at rest. As a result, the agency remains more secure as a whole. Unified DLP is not just about providing a layer of protection over valuable data but also about creating a safeguard against other threats and risk factors entering the overall enterprise. As the network continues to expand, the DOD will want to look at a unified DLP approach as a key component of their overall security strategy.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

Symantec

350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com

19A174397_WP_Unified_DLP_EN