

CA DLP

CA DLP (Data Loss Prevention) is data protection done right.

CA DLP leverages identity to analyze end-user activity in real time and understand data with a high level of precision. This helps organizations to protect more types of sensitive information, more effectively. CA DLP helps protect the entire enterprise by minimizing inadvertent and malicious data loss while helping firms to comply with various data protection regulations.

Product Overview

CA DLP is designed to dynamically monitor a wide range of data activities while providing a range of response actions to help the organization achieve the appropriate mix of business continuity and risk remediation. It provides a configurable level of control to critical areas throughout the enterprise — at the endpoint, on the network, on the message server and for stored data.

CA DLP helps organizations realize quick time-to-value by leveraging a single set of policies, a unified platform and a rapid implementation service program.

Business Value

A great investor once said that it takes twenty years to build a reputation but only five minutes to destroy one. When IT departments protect a firm's sensitive data from loss or misuse, they are simultaneously protecting a firm's brand and reputation.

Every company has sensitive data that is critical to the organization — from financial data and customer records to patents and product formulas. While the proper use of this information is essential to the operations of the company, it also needs to be protected from various forms of misuse and loss.

CA DLP enables organizations to better protect and control this critical data where it is stored or used, thereby reducing the risks associated with uncontrolled information and helping address regulatory and corporate privacy directives.

Features

CA DLP is designed to deliver a broad range of features to help your organization meet its data loss prevention and data protection goals.

- **COMPLETE PROTECTION COVERAGE:** Because of differing requirements and priorities, CA DLP is designed to protect data where needed — at the endpoint, on the message server, on the network and for stored data.
- **IDENTIFY VARIOUS CONTENT TYPES:** Customers have many data types that require protection. CA DLP can accommodate all of them — from personally identifiable information, to non-public information, to intellectual property.
- **FLEXIBLE, PRE-BUILT POLICIES:** CA DLP's configurable pre-built policies leverage industry best-practices to more accurately identify and protect sensitive data. The detection techniques employed in our policies are unmatched.
- **ENTERPRISE SCALABILITY AND RESILIENCE:** CA DLP can be deployed to thousands of desktops and can scan terabytes of data. When connectivity to the central server is unavailable, the distributed components are designed to continue to detect and protect data.
- **SECURE REVIEW:** CA DLP is designed to control sensitive data during the review workflow and to limit access to reviewers with specific permissions.
- **APPROPRIATE ENFORCEMENT ACTIONS:** There may be no need to involve management when end-users can *self-remediate* their own activity. Actions include block, warn, quarantine, redirect, move, delete, replace, capture and alert.
- **INTEGRATION TO CA MESSAGE MANAGER:** This integration merges CA DLP's content inspection, real-time email control and capture and secure review capabilities with CA's archive solution for managing and optimizing message retention. This integration offers an end-to-end solution designed to help meet regulatory and security requirements while also lowering configuration and maintenance costs.

What's New in CA DLP r12?

CA DLP r12 is the latest release of this CA Security product. This release includes many new and enhanced capabilities designed to offer more protection of your sensitive data and to simplify system support. Endpoint detection capabilities are enhanced with the ability to better protect against writing sensitive data to CDs or DVDs and to control screen printing. Discovery capabilities are extended with the ability to scan files that reside locally on laptops and desktops and to scan into structured ODBC databases. This release enhances network detection by integrating with ICAP to analyze content traveling thru HTTPS (SSL). The solution also offers tight integrations to complementary CA solutions including CA Enterprise Log Manager and CA Message Manager.

Benefits

CA DLP is designed to offer many benefits to your organization including:

- Limiting costly and embarrassing data loss events that plague many companies today. Preserve your company's brand equity and your customer's trust in you by reducing the risk of high-profile data leaks.
- Better adherence to government and industry information protection regulations while helping to prevent end-users from violating your firm's general corporate security and behavioral policies.
- More quickly expanding the solution deployment as your needs and requirements grow. Centralized administration enables data protection policies to be more easily deployed to additional control points.

Delivery Approach

CA Services provides a rapid implementation service for CA DLP delivered by CA internal staff and a network of established partners chosen to help you achieve a successful deployment and realize the desired business results as quickly as possible. Through our proven nine-stage deployment methodology, best practices and expertise, CA can help you achieve faster time-to-value for your CA DLP implementation.

Why CA

CA DLP is one of several robust security solutions from CA that helps you protect your IT assets across a wide range of platforms and environments. As such, it contributes to your ability to optimize the performance, reliability and efficiency of your overall IT environment. The next step is to tightly integrate the control and management of distinct functions such as operations, storage, lifecycle and service management, along with IT security.

Copyright © 2009 CA. All rights reserved. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. This document is for your informational purposes only. To the extent permitted by applicable law, CA provides this document "As Is" without warranty of any kind, including, without limitation, any implied warranties of merchantability or fitness for a particular purpose, or noninfringement. In no event will CA be liable for any loss or damage, direct or indirect, from the use of this document, including, without limitation, lost profits, lost investment, business interruption, goodwill or lost data, even if CA is expressly advised in advance of the possibility of such damages. CA does not provide legal advice. Neither this document nor any CA software product referenced herein shall serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, policy, standard, requirement, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. The reader should consult with competent legal counsel regarding any Laws referenced herein. MPECA_DLP_PS

