

Data Loss Prevention : Minimum Effort, Maximum ROI

The DLP Problem

As the traditional perimeter is vanishing, with enterprises are connecting to their customers and partners, data leakage is becoming an expensive, burdensome problem. Employees, whether innocent or malicious, can easily send a Webmail or instant message with confidential information. Information can be posted on social networks and blogs instantaneously. Customer's private information, such as Social Security and credit card numbers, is protected by government regulations and leakage creates legal liabilities and can damage a company's brand and reputation. Further, leaks of sensitive company information risk financial loss.



Web 2.0 communications such as...social networking sites and blogs carry an even greater risk for data leakage and brand damage than email, because anyone can potentially access them.



- Katie Gotzen, Frost & Sullivan

How Current Solutions Fail

Several companies have begun offering point solutions to prevent data leakage. These products often require extensive implementation and consulting services. They are also just another point solution to be added to an already-crowded network gateway. Not surprisingly, less than 5% enterprises have deployed data leakage prevention (DLP) solutions today.

Enforce Compliance with Zscaler

The Two Types of Data Leakage Violations

Zscaler provides full inspection of all HTTP/HTTPS traffic leaving the organization. Specifically, our technology inspects two types of violations:

- Regulatory compliance by state or federal governments, or other standards bodies, often pertains to personal or private consumer information. Examples include regulations such as HIPAA, GLBA, PCI, or SOX.
- Company sensitive information may include sales data, pricing information, or intellectual property such as source code.

Granular Policy & Flexible Dictionaries

Zscaler's DLP solution uses a patent-pending engine and can reduce implementation from months to hours. Because of Zscaler's in-the-cloud architecture, customers do not have to deploy DLP boxes at every Internet gateway. Policy definition is intuitive but powerful, offering granular control over specific users, locations, and applications (Webmail, social networks, etc). Enterprises can define custom dictionaries and engines in addition to the pre-defined lexicons and categories provided by Zscaler.

Data Loss Prevention : Minimum Effort, Maximum ROI



Depending on how many records are at stake, individual breach costs may run into millions or even billions of dollars and organizations still aren't prepared to protect their environments.

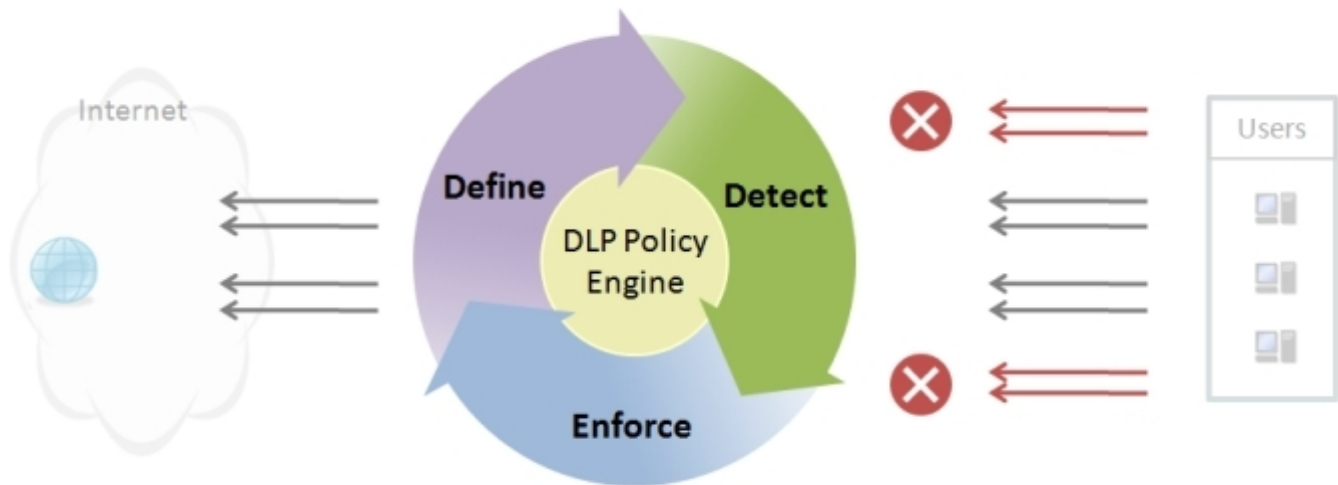


- Khalid Kark, Forrester

Our Technology

Proprietary Algorithms, Pattern Matching

- Sophisticated algorithms detect the leakage of credit card and Social Security numbers without false positives.
- Advanced self-learning algorithms create dictionaries for the leakage of source code, financial statements, and Protected Health Information (PHI).
- Pattern matching engines evaluate data based on weighted scores. Dictionaries of key words and phrases are assigned different weights. Data is evaluated based on these weighted scores.



Solution Benefits

Accurate Detection, Easy of Deployment

Zscaler provides an integrated DLP solution for security and control. Our technologies allow us to have the highest accuracy of detection while minimizing false positive and latency. Finally, deployment takes hours rather than weeks or months.

Contact Us

Zscaler, Inc.

Visit: www.zscaler.com Email: info@zscaler.com