

Trustwave DataControl

DLP

Data Loss
Prevention

ENC

Encryption

For businesses that need to locate and protect specific types of sensitive data within a complex infrastructure.

Trustwave's DataControl integrates Data Loss Prevention (DLP) Discover and Encryption (ENC) Smart Tag™ technology to enable companies to discover and protect sensitive data within their organization.

Losing control of sensitive information can lead to fines, damage to brand and reputation, loss of competitive advantage, and expensive breach notification costs. Organizations are turning to data loss prevention (DLP) solutions to locate sensitive information in order to prevent it from leaving their environments or to ensure it is protected.

Discover Once, Protect Forever

To address these concerns over locating and protecting sensitive data, Trustwave DataControl integrates two critical capabilities into a single solution: content awareness via DLP Discover to identify data and Smart Tag-enabled persistent file encryption to protect data. This combination enables an organization to enable a "Discover Once, Protect Forever" capability for its sensitive information.

Data Discovery: Understand Content to Reduce Risk

Content-aware scanning, an integral part of Trustwave DataControl, provides a powerful, workstation-based capability for administrators and content owners to identify and remediate information risk. Using content inspection and classification methods to identify sensitive information, DataControl highlights faulty business processes, areas of non-compliance and risks to company proprietary information.

With Trustwave DataControl, administrators can scan servers, file shares, laptops, desktops and removable drives to identify sensitive information across their environment. Patient records, personal information, credit card numbers and financial documents are all examples of content that Trustwave's content discovery can identify.

While content-aware data loss prevention solutions are excellent at locating data, this technology has not traditionally focused on protecting data post-detection. Many organizations are forced to take manual steps to ensure their data is protected once it is identified; this process can be expensive and difficult to manage.

The integration of content-aware discovery with persistent file encryption offers the optimum level of protection for data within and outside a company's network.

Smart Tag™ Technology Enables Document Control

With Trustwave's persistent file encryption, once sensitive data is discovered by the scan, it can then be automatically encrypted based on customizable security policies. For example, if documents containing credit card information are discovered, the policy might dictate that only members of the "Business Analyst" group should have access to the document. This is enforced by the innovative Smart Tag technology which encrypts the document itself and assigns this policy to the document.

An integral part of Trustwave DataControl, Smart Tag technology keeps data encrypted and protected wherever it goes, inside or outside of a company network. Smart Tags are transparent bundles of security controls that are attached directly and to each file. They make sure that security policies— such as those related to encryption, access control, classification – are consistently enforced, regardless of where the data resides. Thus, security policy can be enforced at the data level, anywhere a file moves.

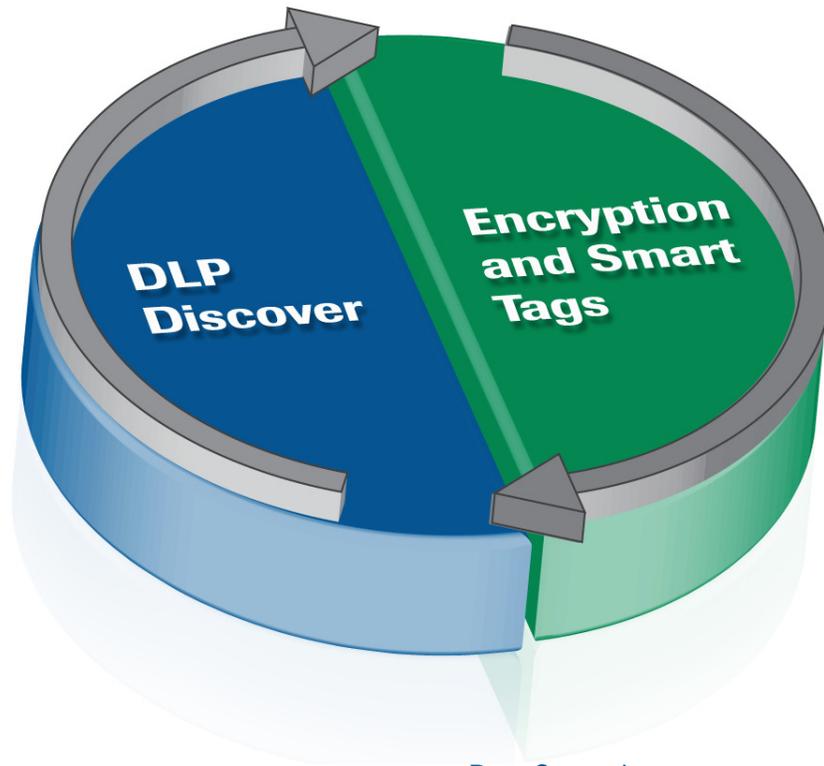
About Trustwave®

Trustwave is a leading provider of information security and compliance management solutions to large and small businesses throughout the world. Trustwave analyzes, protects and validates an organization's data management infrastructure - from the network to the application layer - to ensure the protection of information and compliance with industry standards and regulations such as the PCI DSS and ISO 27002, among others. Financial institutions, large and small retailers, global electronic exchanges, educational institutions, business service firms and government agencies rely on Trustwave. The company's solutions include on-demand compliance management, managed security services, digital certificates and 24x7 multilingual support. Trustwave is headquartered in Chicago with offices throughout North America, South America, Europe, the Middle East, Africa, Asia and Australia.

Trustwave DataControl: Completing the Cycle of Protection

This combination of content discovery and policy-based encryption provides significant advantages to the resource-strapped organization:

- Easier compliance to regulations such as PCI DSS, HIPAA and state data privacy laws and obtain audit-ready reports.
- Scheduled or on-demand scans of file shares, folders, laptops, desktops and USB devices for sensitive data that might break compliance with regulations such as HIPAA, PCI DSS and others
- Automatically encrypt data upon detection, reducing the need for expensive manual intervention
- Ensure only authorized persons have access to the documents, regardless of where the data travels or is stored
- Encrypt data in place, not just move or quarantine the data to a secure folder, which may disrupt business workflow and productivity
- Protect data from all applications—not just Microsoft® Office or Adobe® Acrobat® –without any changes to those applications
- Reduce risk across the organization; even if data were to leak, it remains encrypted and thus protected



DataControl

DLP Discover identifies sensitive data while Smart Tags remain with that data as it travels from device to device. DataControl integrates these complementary solutions to complete the cycle of protection.