Data Sheet

Symantec™ Information Centric Tagging

Protect the Data You Value

The loss of valuable information is a major concern for every organization; and the consequences of a data breach can severely impact brand reputation, endanger customer trust, and cost competitive advantage. It can also result in high fines and penalties for regulatory noncompliance.

According to IT analysis firm IDC, the total volume of data worldwide will increase by 10 times over the next 8 years, driven by the usage of cloud and mobile applications. Organizations must figure out how to protect both their existing data that may be scattered across on-premises repositories, cloud services, and user devices as well as new content they create at an ever-increasing rate. As the total amount of unstructured data grows, so does the risk of losing control over what is truly sensitive.

Along with balancing the need to protect a diverse range of sensitive and valuable information—regardless of whether the data is on-premises, on a user's device, or in the cloud—organizations need to allow collaboration among employees, partners, customers, suppliers, and investors, spanning organizations and locations worldwide.

New security approach

The first step to secure sensitive and valuable data is to identify which data you need to protect. Symantec™ Information Centric Tagging provides an additional layer of user-driven data classification by empowering employees to identify and classify sensitive files and email as they create or handle them. Classification is seamlessly integrated into the user interface of leading productivity applications, such as Microsoft Office® and Outlook®, enabling employees to effortlessly apply a classification tag.

Key features

Data Classification and Labeling
Enables enterprises to classify newly created content, existing files, and emails in a DLP policy-driven or user-driven manner.

Role-Based Taxonomies and Policy
Policy engine allows enterprises to set up different classification taxonomies and policies to be applied to designated users.

Dynamic Watermarking and Tagging
Automatic tagging and watermarking all unstructured data, including emails, documents, and images according to enterprise policy.

Enterprise-Ready Architecture
High scalable architecture with centralized management that integrates with data loss prevention, Encryption and Identity Services.

Comprehensive Audit Trails
Rich Audit trails provide visibility into user and administrator actions enabling regulatory compliance and forensic mandates.

Ease of Use
Intuitive and seamless user experience ensures a smooth roll-out of classification and tagging.

Integrated information detection and protection products

- Symantec Information Centric Tagging
- Symantec Data Loss Prevention
- Symantec Information Centric Encryption
- Symantec Validation and ID Protection Service

Symantec™

Data tagging and classification

Symantec Data Loss Prevention can automate the process of detecting sensitive data with its comprehensive content-aware and context-aware detection capabilities that employ a powerful combination of industry-leading textual, nontextual, and machine-learning-based detection technologies. But to ensure all the right data is properly protected, it is important to rely on more than just data loss prevention. Organizations must also engage the content creators and editors in the decision-making process because their judgment and knowledge is critical to properly identifying and ascribing context to the sensitive data you must protect.

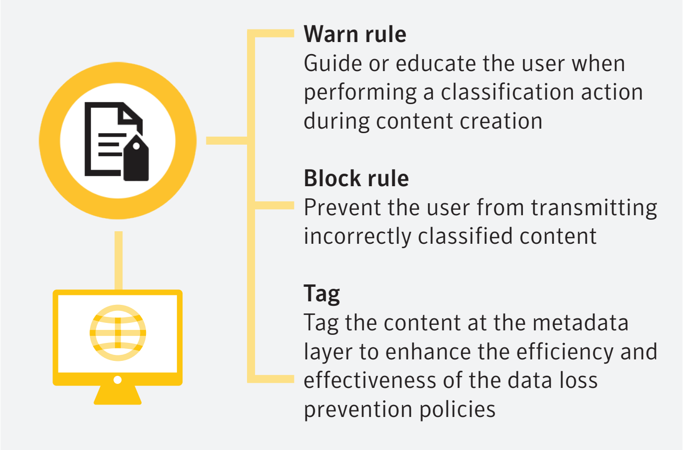
By engaging the users who create and handle the data to determine what's truly sensitive, Information Centric Tagging can help reduce data loss prevention "false negatives" and enhance detection of sensitive data with more accurate outcomes, without requiring administrators to author ever-more complex policies. Once Symantec Data Loss Prevention identifies data that Information Centric Tagging has classified, it can automatically trigger the appropriate response according to your enterprise data loss prevention policies.

Robust data protection everywhere

Information Centric Tagging can engage and encourage users to protect sensitive email messages, documents, and images by triggering educational pop-ups and automatic watermarking. When integrated with Symantec Data Loss Prevention and Symantec Information Centric Encryption, Information Centric Tagging can prevent users from transferring unclassified content and ensure that classified files and messages are automatically encrypted and protected with the application of digital rights and role-based access control that follows the data everywhere—on premises, in the cloud, on user devices—even when shared with external parties. This ensures sensitive data always stays in the correct hands and reduces data loss and noncompliance risks.

In a world that fosters collaboration everywhere, information-centric security must encompass a comprehensive set of capabilities, including sensitive data discovery, classification, user authentication, and encryption. Integrating these capabilities in a manner where the protections follow the data ensures all sensitive information is protected, both inside and outside the organization's network perimeter, and remains accessible only to the intended recipients.

Classification and tagging rules engine



Warn rule
Guide or educate the user when performing a classification action during content creation

Block rule
Prevent the user from transmitting incorrectly classified content

Tag
Tag the content at the metadata layer to enhance the efficiency and effectiveness of the data loss prevention policies

Figure 1 Classification and tagging rules engine

System requirements

Server

- Microsoft Windows® Server 2008 R2 to 2016
  - Microsoft Active Directory® 2003 R2 to 2016
  - Microsoft SQL Server® 2008 R2 to 2016
  - Microsoft Exchange® Server 2010 SP2 or higher and 2013 CU14 (for Outlook Web App on-premises integration)
  - Internet Information Services (IIS) 7.0 or higher
  - Microsoft ASP.NET 3.5 and 4.5

Client

- Microsoft Windows 7, 8, 8.1, and 10 (32-bit and 64-bit)
- Microsoft Office 2010 to 2016 (32-bit and 64-bit)
- Microsoft .NET Framework 4.5

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