Sophos **security and data protection**

SOPHOS

Data Loss Prevention

Sophos offers a unique and simple solution for data loss prevention (DLP). We integrate content scanning into the threat detection engine and include a comprehensive set of sensitive data type definitions to enable immediate protection of your sensitive data. This DLP functionality is included in our Sophos Endpoint and Email Appliance products, providing you simple and effective protection for your data within your existing security budget.

Free DLP with your threat protection

Traditional data loss prevention solutions are expensive, complex, cumbersome to implement and difficult to administer. Sophos changes all that by being the first vendor to offer sophisticated, effective, tightly integrated, data loss prevention on the endpoint and email gateway at no additional cost.

Consider the advantages this provides:

- Zero additional investment to protect your valuable sensitive data from accidental or malicious disclosure via removable devices or media, internet applications, or email all within your existing security budget.
- Ultimate simplicity with no additional software to install or administer and the same DLP engine and data definitions on the endpoint and gateway.
- Maximum transparency and performance with DLP content scanning integrated into the threat detection engine.

Simplified compliance

Sophos takes the guesswork out of DLP by including a comprehensive set of sensitive data type definitions created and maintained by SophosLabs. You simply select the data you want to protect from the hundreds of region specific data types provided, and know that your sensitive data is protected from accidental or even intentional disclosure, literally enabling point-and-click compliance.

SophosLabs pre-packaged content control lists:

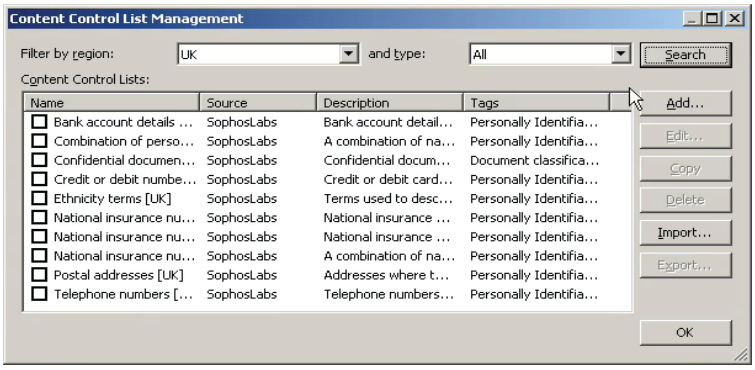
Contain hundreds of pre-defined Personally Identifiable Information (PII) and other sensitive data types such as credit cards, bank accounts, government ID numbers, addresses, phone numbers, and more.

- Cover 11 regional localizations of PII data types.
- Accessible via a simple point-and-click DLP policy wizard.
- Customizable with your own PII or senstive data types that are unique to your industry or organization.
- Consistent across endpoint and email appliances with the ability to easily export customizations from the Sophos Enterprise Manager and import to the email appliance DLP engine.
- Enable immediate compliance with PCI and policy and regulations governing the protection of sensitive information.

Key benefits

- Integrated with all Sophos Endpoint and Email Appliance products
- Included at no extra charge - protect your data within your existing security budget
- Simple setup: be up-and-running in minutes
- Transparent high performance single scan engine for threats and content
- Immediate compliance with data protection regulations
- No additional software client installation required
- Hundreds of included PII and sensitive data definitions maintained by SophosLabs
- Customize the included content control lists and easily keep them consistent between endpoint and gateway
- Easy point-and-click policy configuration
- Prevent loss of data through removable devices and media, web and IM applications, and email
- Flexible policy settings for individual endpoints, groups or email users
- Log, warn, block or encrypt sensitive information that triggers a DLP policy rule
- True file type analysis prevents file type masquerading
- Easily associate email encryption policy with sensitive data that must leave the organization

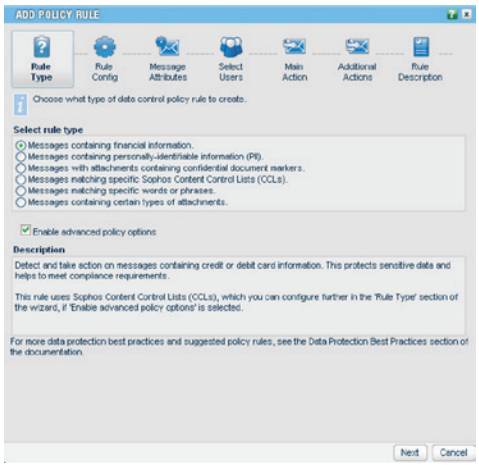
Content Control List Management



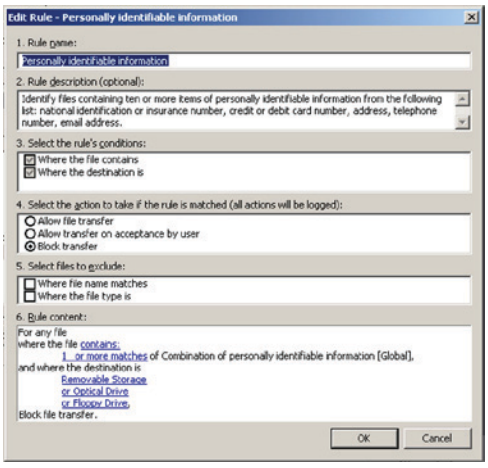
Easy, powerful DLP policy configuration

Flexible point-and-click policy wizards enable easy DLP rule definitions:

- **Scope:** Data control policies can be defined by endpoint, groups, email sender, recipient, or content. Policies may contain multiple rules.
- **Criteria:** Define rules on file types (e.g., XLS) or content. File type scanning utilizes Sophos true file type technology to prevent file type masquerading. Content scanning leverages the pre-packaged content control lists (CCL's) which include hundreds of pre-defined data definitions across several localizations provided and maintained by SophosLabs.
- **Triggers:** Evaluation of DLP policy is triggered in any of these cases: copying content to a removable storage device (e.g., USB stick or external harddrive), copying/ burning content to a CD/DVD, uploading content to web browsers or IM clients, or sending via email.
- **Actions:** On the endpoint, the options include logging the event, logging and warning the user with a prompt to proceed, or logging and blocking the transaction. On the email appliance, the options include logging, quarantine, blocking or encrypting the content before sending.



Sophos Email Appliance DLP Wizard



Sophos Endpoint Rule Configuration

To evaluate Sophos Endpoint or Email Appliances with DLP, visit www.sophos.com/products/eval/.

Specifications

Included data types

- Credit card numbers and qualifying terms
- Debit card numbers and qualifying terms
- Bank routing numbers and qualifying terms
- International bank account numbers
- National insurance numbers
- Social insurance numbers
- Fiscal code numbers
- Tax file numbers and qualifying terms
- Postal addresses
- Telephone numbers
- Email addresses
- Passport details and qualifying phrases
- Confidential document markers
- Ethnicity terms
- Sensitive content markers

Supported localizations

- United States of America
- United Kingdom
- France
- Germany
- Ireland
- Spain
- Australia
- Canada
- Japan
- China
- Global

ds/091130

SOPHOS
WWW.SOPHOS.COM