



Secured eControl

Receive real-time warnings when your email or Microsoft Office files contain traces of deleted text, hidden comments, passwords and more

Detects sensitive information and safeguards against non-compliance

Receive real-time warnings when your email or Microsoft Office files contain traces of deleted text, hidden comments, passwords and more. Secured eControl provides the necessary safeguards to ensure total data protection compliance through enforced email encryption, metadata removal, secure PDF creation, etc. With Secured eControl, you can force the use of encryption on emails containing sensitive information such as credit card numbers, social security numbers or patient records. The entire email and all of its attachments will then be encrypted before it leaves the endpoint, and will be protected until it reaches the intended destination. It is also possible to deny the sending of information completely.

Key Features

- Document & email content analysis
- Integration with Microsoft® Office
- Metadata removal and management
- Redact sensitive information
- Tamper-proof, secure PDFs

Benefits

Enforce the use of email encryption on sensitive information

Secured eControl has the ability to trigger the use of email encryption if a user tries to send sensitive information such as credit card numbers, social security numbers or patient records. The information would then either be encrypted before leaving the endpoint, or blocked completely. Policies and triggers for this are controlled from a central location and pushed out to all clients.

Confidential Data Discovery & Removal

When leveraged with the Workshare Policy Manager, content detection alerts notify

you when intellectual property or sensitive information such as financial data or passwords are within your email or Microsoft Office documents and provide the tools to remove or redact the information. Data discovery will even identify improperly redacted text

Email Protection

Receive an alert before your email is sent whenever an email or its attachment breaches a security policy. To prevent you from accidentally emailing confidential information, this feature can block or prompt you to remove sensitive data. The security policies are easily customized and include the ability to specify different actions when a document is emailed internally or externally, such as enforcing email encryption.

You can customize 25 metadata cleaning options with different options for recipients within your organization and outside

The text redaction tools blacks out sensitive information and permanently delete the content from your document

Seamlessly Removes Hidden Data in Word, Excel, PowerPoint

Remove data located in hidden cells in Excel spreadsheets, cleanse confidential information stored in PowerPoint speaker notes, and ensure that modifications or deletions in Word documents logged by the 'track changes' mode cannot be read by third-parties. You can customize 25 metadata cleaning options with different options for recipients within your organization and outside.

Batch Metadata Cleaning

Select a number of files and run batch metadata cleaning to remove the metadata from all of the files.

Document Classification

Easily restrict access to sensitive business documents by setting document classifications. The classification controls the distribution of documents by email and will alert you to the potentially sensitive nature of the document you are attempting to email and can prevent documents from being emailed to specific internal or external users.

Auto Zip Attachments

Automatically zip attachments when the file size exceeds a specific limit.

Preview Cleaned Attachments

When cleaning email attachments you can now preview the cleaned attachment before sending your email.

Extend the Office 2007 Document Inspector

Extend the Office 2007 Document Inspector to provide configurable policies to protect your confidential data, including policy-enforced document rights

Redact Sensitive Information

Now you can redact (black out) selected content in Microsoft Word (DOC and DOCX) documents so that it is no longer discernible. The text redaction tools blacks out sensitive information and permanently delete the content from your document.

Multiple Metadata Removal Options

You can easily remove hidden metadata with this one-click metadata removal option, or an organization can set an automated policy to make metadata removal transparent to the user.

Metadata Discovery in Protected Documents

Receive alerts for password-protected documents, zipped documents, and documents with restricted editing rights that contain metadata.



Microsoft Partner

Gold Independent Software Vendor (ISV)

Cryptzone solutions mitigate information security risks in the key areas of Policy Compliance, Content Security, Secure Access and Endpoint Security.

International Headquarters

Cryptzone Group AB
Drakegatan 7,
SE-412 50 Gothenburg,
Sweden

www.cryptzone.com
info@cryptzone.com

Regional Offices

Sweden
Tel: +46 (0)31 773 86 00

United States
Tel: +1.949.279.6177

United Kingdom
Tel: +44 (0)370 013 1600

Partner information:

For more information go to
www.cryptzone.com/partners