COMPLIANCE POLICY APPLICATIONS

Confidential Data Protection Policies

Overview

Sentrion Confidential Data Protection Policies automatically identify content that is tagged for confidentiality, whether the tag is part of a document template, an inherent feature of the document, or has been applied manually. Confidential documents are detected in the email stream and flagged for further action by the Sentrion Policy Engine to protect your company's competitiveness and compliance.

Audience

Any company that needs to prevent inadvertent or intentional disclosure of confidential documents such as trade secrets, source code, draft press releases, legal briefs, or regulated information.

Key Features and Functionality Overview

Every company has its own way of flagging confidential documents—for example, footers and watermarks that indicate a document is for internal use only. Many other types of documents have inherent features that indicate confidentiality, such as a particular entry in the document's Author or Category field, or a programming language header included in the source code for a proprietary product.

It's one thing to have the confidential status of a document noted within the text or structure of the document itself. It's another thing to actually prevent the document from being distributed, whether accidentally or intentionally. But with Confidential Data Protection Policies, your Sentrion appliance can intelligently and automatically scan every email and attachment for the key words, text patterns, and even document structures that indicate confidentiality.

When an email is flagged for confidential content, the message is quarantined and an incident is triggered in the Incident Remediation and Reporting Application. Your security team can then review the message, drill down to see the applicable policies, and take quick action—from escalating the case to the appropriate authority to closing the case and allowing the message to proceed through the email system.

Employees in every department, at every level, routinely deal with confidential documents—from software programmers, to human resources officers, to the sales force. It's not always practical to pass these documents through a formal security review and registration process. But with the Confidential Data Protection Policies Application, you can automatically protect any document that can be identified as confidential by its text or structure, for example:

- Source code
- Internal memos
- HR records
- Proposals
- Client lists
- Draft presentations
- Organizational charts
- PERT charts
- Collaborative documents
- Legal filings

And for organizations that need multi-layered DLP security for all kinds of company-private documents, the Confidential Data Protection Policies Application perfectly complements the document registry and fingerprinting provided by our Protected Content Application, as well our Healthcare, Financial, and other industry-specific policy solutions.