



Protected Content (Fingerprinting)

Overview

Sentrion Protected Content uses sophisticated document fingerprinting techniques to identify and block sensitive content before it leaves your enterprise. It can also be combined with an encryption solution to allow content to reach its destination in encrypted form, and it can flag content for reporting in the Incident Reporting and Remediation Application.

Audience

Companies that generate confidential documents—such as financial reports, trade secrets, customer profiles, patient records, and other sensitive information—and need a way to prevent these documents from being disclosed outside the organization.

Key Features and Functionality Overview

Unlike the structured fields of a database, most company-private information is captured in unstructured documents—functional specifications, customer contracts, legal filings, employee evaluations, draft financial reports, and so on. Because these documents are structured around human thought rather than computer logic, you might think there's no practical way, short of human review of all outgoing emails, to prevent information leakage.

Think again. The Sentrion Protected Content Application automatically detects confidential documents and even document excerpts in the body and attachments of all outbound emails. Sensitive documents are registered in the system, then when it identifies sensitive content from the registry, the Policy Engine takes appropriate action based on custom policies—for example:

- Block and quarantine the message
- Log the event in the system log
- Create an incident in the Incident Reporting and Remediation Application workflow
- Return the message to the sender with a notification of the policy that was violated
- Deliver the message to an authorized recipient using Voltage or S/MIME Encryption

The Protected Content Application works by analyzing brief, overlapping “chunks” of text in registered documents. It then calculates a unique hash (code) based on the content of each chunk—creating a database of structured entries that represent each unstructured document.

The same analysis is applied to the body and attachments of each outbound email, and the resulting hashes are compared with the hashes in the database of registered documents. If there's a match, the application knows that a confidential document or even a small excerpt is being sent through the system—similar to the way a fingerprint can identify a criminal.

Not that your employees purposely leak data. On the contrary, most data leakage is the result of an honest mistake. For example, an employee planning to work at home over the weekend might send documents to a personal, web-based email account. An unintended recipient may be on an email distribution list. A sender might not notice that the email program's auto-complete function has entered the wrong person in the “To” field. Things happen.

The point is, whether intentional or accidental, why risk the leakage of confidential information when the financial, legal, or competitive health of your company is at stake? Before an incident can even occur, with Sentrion Protected Content you already have the fingerprints.