# Endpoint data governance

## Why does Coro only detect a small number of sensitive data occurrences within a file when a file scan is run?

The purpose of file scans (on endpoint device drives and in general) is to identify files containing sensitive information so that admin users are notified of potential risks and can take appropriate measures to protect the sensitive information in question, by either:

- Adjusting data governance permissions
- Taking measures prescribed by their organization's data governance policy

It is not necessary to detect all occurrences of each type of sensitive information within a given file for that, so Coro limits the number of such detected occurrences to optimize performance and (in the case of endpoint devices) improve end-user experience.

## What social security number (SSN) pattern does Coro detect?

Coro recognizes US social security numbers (SSNs). Coro additionally detects SSNs on a predefined list of keywords if the SSN is in an unrecognized format.

## Under what circumstances will Coro automatically close Data Loss Prevention (DLP) tickets?

Tickets containing sensitive information, but that do not require manual review by admin users, are automatically closed.

Such tickets are included in the Coro console ticket log for audit, monitoring, analysis, and to satisfy regulatory compliance requirements. They are typically triggered automatically by events such as the detection of sensitive information in an email, file, or file sharing. Some examples of this type of ticket include:

- **Personal Identifiable Information (PII)**: IP and MAC address.
- **Nonpublic Personal Information (NPI)**: Monthly payment (financial content) and email address.
- **Protected Health Information (PHI)**: Medical Records Number (MRN).