Introducing Endpoint Data Governance

Coro's **Endpoint Data Governance** aims to help administrators establish a strategy for correct and secure handling of data assets by authorized users. Compliance with these strategies includes defining and implementing policies, procedures, and controls for the business in order to ensure the availability, integrity, confidentiality, and privacy of data, based on applicable laws, regulations, and industry standards.

Coro's **Endpoint Data Governance** helps in meeting regulatory requirements. The following are some examples of regulatory requirements that Coro can assist you with:

- HIPAA
- GLB
- GDPR
- SOC2
- SOX

Coro's **Endpoint Data Governance** enables Admin users to remotely scan endpoint devices for storage of:

- PII (personally identifiable information)
- PHI (protected health information)
- PCI (payment card information)
- NPI (non-public information)

Note

Admin users can initiate a sensitive data scan on an endpoint device by selecting **Remote scan for sensitive data** from a device's action menu on the **Devices** page.

Threat types

Coro's **Endpoint Data Governance** provides the means to reduce the risk of data breaches and to protect sensitive information from unauthorized access and misuse. A number of threats can place an organization's data at risk and it is important to be aware of them and take measures to limit their impact:

- **Cyber attacks**: Cybercriminals can use a variety of methods to access sensitive information, such as hacking into systems, phishing scams, and malware.