

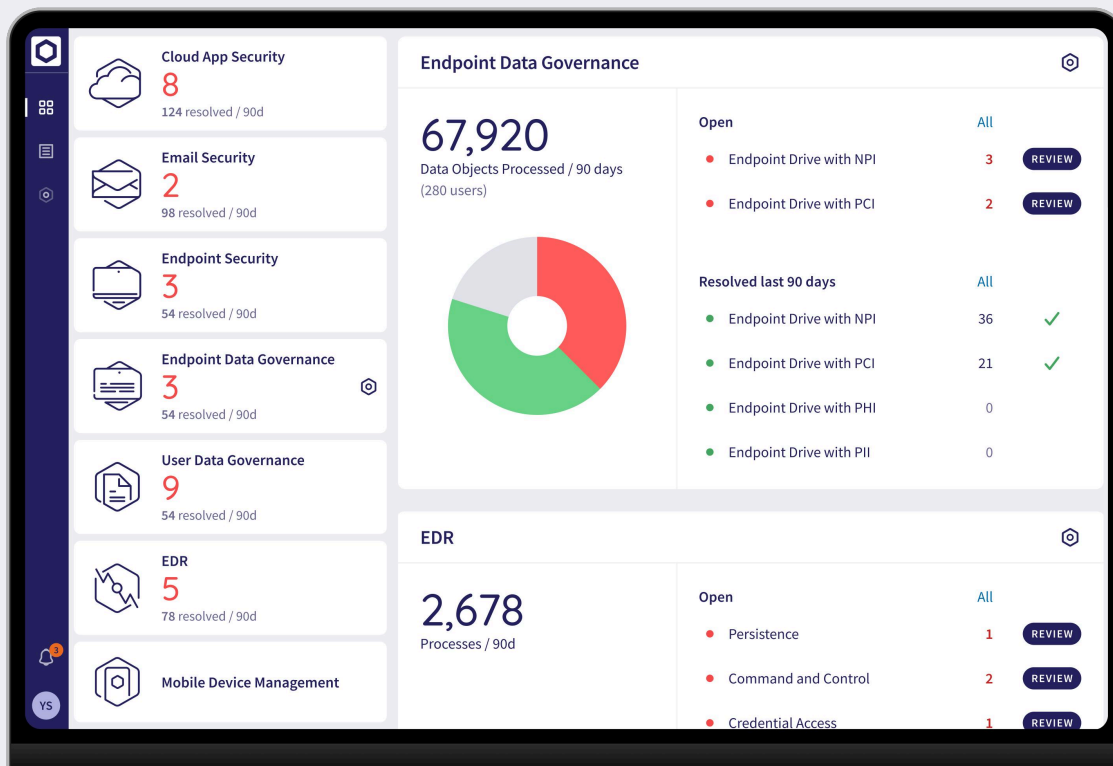


# Endpoint Data Governance

Built for small IT teams with big responsibilities

**Coro Endpoint Data Governance module protects sensitive and critical data on endpoint devices.** It actively monitors how data on these devices is stored, detecting and preventing unauthorized use, accidental loss, risky data sharing, or violations of data protection policies. Endpoint Data Governance comes pre-configured with baseline security policies and ensures endpoint devices comply with data protection policies from day one.

## Modular Cybersecurity







**Coro's Endpoint Data Governance module is part of a powerful modular cybersecurity platform.**


Designed to evolve with your needs, a modular platform ensures effortless security across cloud apps, devices, data, and endpoints while sharing one endpoint agent, one dashboard, and one data engine. Adding modules is done at the click of a button. Chosen modules snap into place, immediately integrating with other modules.








## Key Supported Security Incidents

- **Endpoint Drive with NPI**  
Detects unauthorized exposure of NPI (Non-Public Information) on an endpoint device, such as personal financial data
- **Endpoint Drive with PCI**  
Detects unauthorized exposure of PCI (Payment Card Industry) data on an endpoint device, including credit card or payment-related information
- **Endpoint Drive with PHI**  
Detects unauthorized exposure of PHI (Protected Health Information) on an endpoint device, such as medical records or health-related data
- **Endpoint Drive with PII**  
Detects unauthorized exposure of PII (Personally Identifiable Information) on an endpoint device, such as names, addresses, or social security numbers

## Key Features

- **Regulatory Data Configuration**  
Enables the configuration of various sensitive data types, such as PHI, PCI, PII, and NPI, ensuring compliance with data protection laws
- **Scheduled Scans**  
Admins can schedule automated scans on endpoint devices to check for sensitive data stored on storage drives, ensuring continuous protection & early detection of potential risks
- **Manual Scanning**  
Provides the ability to perform on-demand scans from the Coro Console of endpoint devices to check for sensitive data exposure (e.g., PHI, PCI, PII, NPI) and mitigate risks in real-time
- **Multilingual Support**  
Provides additional support for Spanish and Italian

## Why Coro?

- **High Threat Detection and Protection Rate**  
Achieved AAA rating from SE Labs
- **Easy to Maintain**  
95% of the workload offloaded from people to machines
- **Quick Deployment**  
Simple and quick installation, no hardware required
- **Fast Learning Curve**  
Minimal training, simplified onboarding, user-friendly interface
- **High ROI**  
No hardware costs, zero maintenance overhead, affordable pricing
- **High Customer Satisfaction**  
95% likelihood to recommend - as rated by G2

# Cybersecurity for small IT teams with big responsibilities

TRY OUR INTERACTIVE DEMO

START A FREE TRIAL

## About Coro

**Coro, the leading cybersecurity platform for small and mid-size businesses**, empowers organizations to easily defend against malware, ransomware, phishing, data leakage, network threats, insider threats and email threats across devices, users, networks and cloud applications. Coro's platform automatically detects and remediates the many security threats that today's distributed businesses face, without IT teams having to worry, investigate, or fix issues themselves. Coro has been named a leader in G2-Grid for EDR/MDR, received Triple-A grading (AAA) from SE LABS, and was named on Deloitte's Fast 500.

