



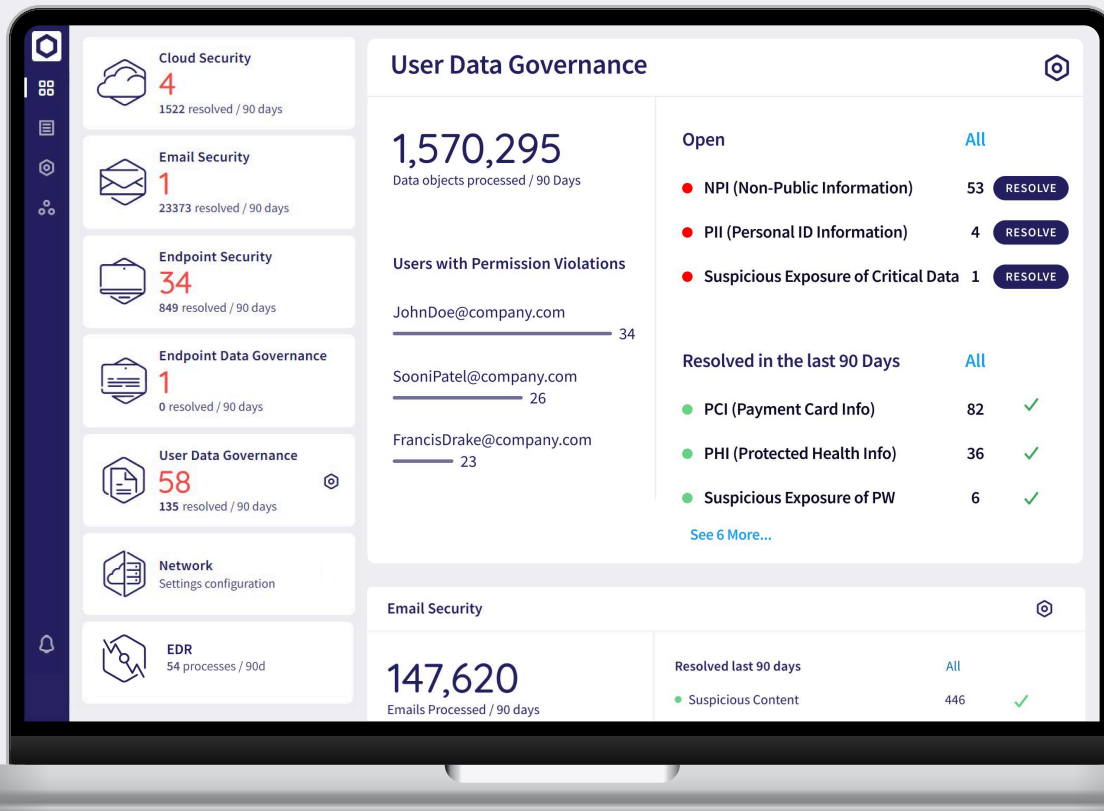
User Data Governance

Built for small teams with big responsibilities



The **Coro User Data Governance module** enables businesses to detect unauthorized sharing or access of sensitive data. Through continuous monitoring of user behavior and data exposure, it ensures that sensitive data such as personal details, health records, and payment information is only accessible to authorized individuals and compliant with data protection regulations such as GDPR, HIPAA, and PCI-DSS.







Modular Cybersecurity








Coro's User 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

- 
NPI, PII, PHI, and PCI
 Detects when a user shares or emails information containing NPI, PII, PHI, or PCI
- 
Critical Data Exposure
 Identifies potential exposure of critical data with defined keywords
- 
Password Exposure
 Detects potential exposure of passwords
- 
Suspicious Certificate Exposure
 Identifies potential exposure of monitored security certificates (.crt or .pem)
- 
File Type Exposure
 Detects potential exposure of specific file types (e.g., attachments or shared content)
- 
Source Code Exposure
 Identifies potential exposure of source code files (e.g., .md, .yaml, .sh)

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
- 
Continuous Monitoring
 Monitors and scans unusual data-sharing activities that might expose sensitive data (PHI, PCI, PII, NPI) via email or file-sharing
- 
Access Permissions
 Allows admins to control user access to sensitive data by setting specific permissions for individuals, groups, or domains
- 
Exclusions
 Allows admins to exclude emails from sensitive data scans based on specified keywords in the subject line
- 
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 teams with big responsibilities

SCHEDULE A DEMO TODAY

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.

