



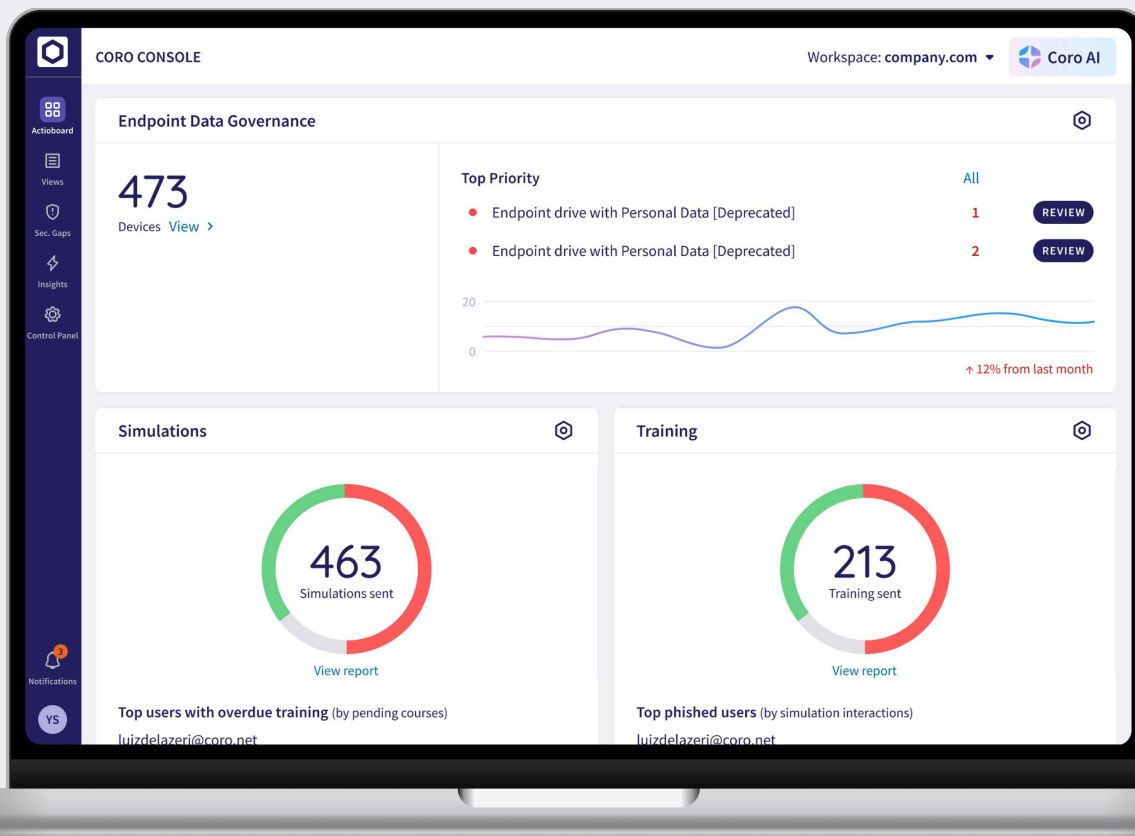
Endpoint Data Governance

Cybersecurity Made Easy



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.

Unified Cybersecurity



Endpoint Data Governance is part of a unified and powerful cybersecurity platform.

- ✓ One dashboard
- ✓ One endpoint agent
- ✓ One AI-driven data engine
- ✓ No integration
- ✓ No headaches

Coro is designed to make your life easier; A single security platform with all the capabilities you need.



Key Supported Security Incidents

- **Endpoint Drive with Non-Public Data**
Detects unauthorized exposure of non-public data on an endpoint device, such as personal financial data
- **Endpoint Drive with Credit Card Data**
Detects unauthorized exposure of credit card data on an endpoint device, including payment-related information
- **Endpoint Drive with Health Data**
Detects unauthorized exposure of health data on an endpoint device including medical records
- **Endpoint Drive with Personal Data**
Detects unauthorized exposure of personal data 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 credit card, health, non-public and personal data, 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., credit card, health, non-public and personal data) and mitigate risks in real-time
- **Sensitive Data Detection**
Leverages country-specific infotypes, including Germany, Canada, France, UAE, Italy, USA, Australia, and the Netherlands to detect and alert on sensitive data
- **Unified Ticketing for All Data Types**
Automatically consolidates all sensitive data type detections from endpoint into one unified ticket
- **Multilingual Support**
Provides additional support for French, 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 Made Easy

TRY OUR INTERACTIVE DEMO

START A FREE TRIAL



About Coro

Coro is the easy cybersecurity company. We designed a platform that every lean IT team will master. While other solutions scare people into buying complicated, confusing products, we lead with elegant simplicity. Coro is fast to deploy, easy to use, and designed not to waste your time. Once you install Coro, you'll hardly think about us. That's the point. Coro automatically detects and fixes security problems, so IT teams don't have to spend time investigating or troubleshooting. We're also one of the fastest-growing tech companies in North America, just ask Deloitte.

