



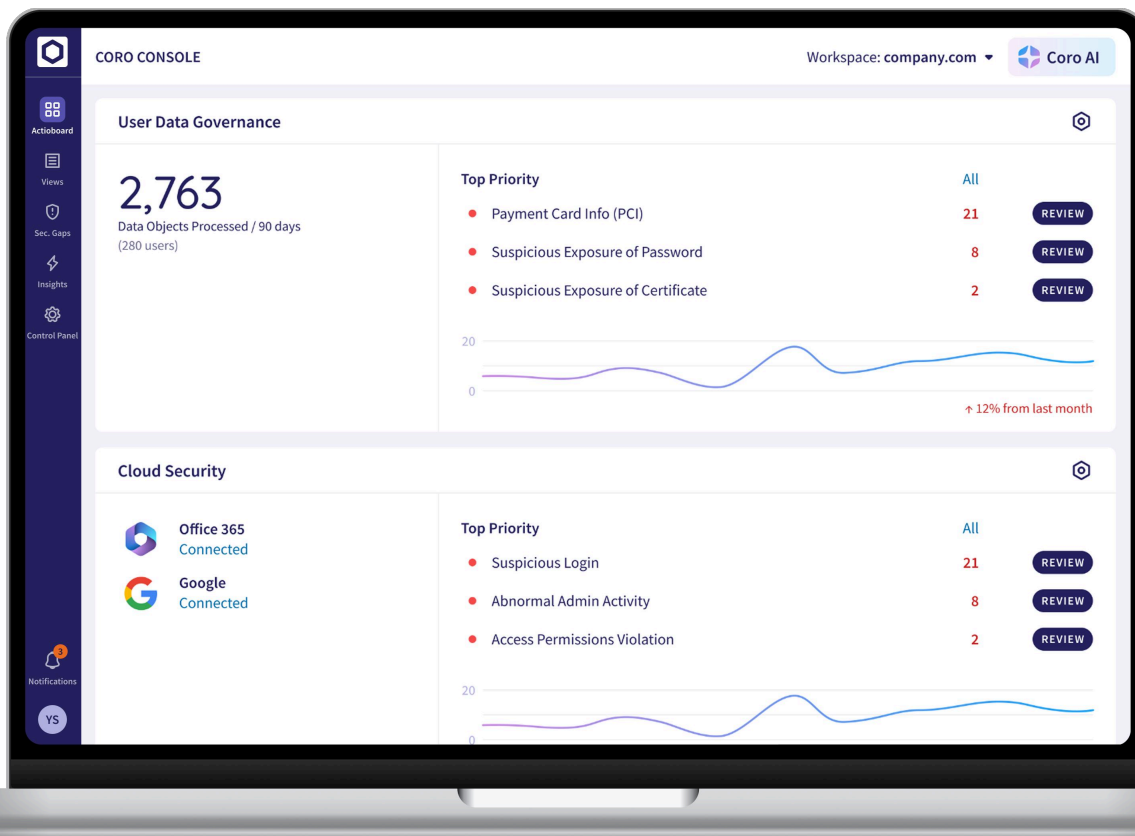
User Data Governance

Cybersecurity Made Easy



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.

Unified Cybersecurity



User 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

- **Privacy Sensitive Data**
Detects when a user shares or emails information containing credit card, health, non-public and personal data
- **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 credit card, health, non-public and personal data, ensuring compliance with data protection laws
- **Outbound Gateway**
Enables real-time monitoring and blocking of outbound emails that violate an organization's sensitive data policies
- **Sensitive Data Detection**
Leverages country-specific infotypes, including Germany, Canada, France, 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 email and cloud activity into one unified ticket
- **Exclusions**
Allows admins to exclude emails from sensitive data scans based on specified keywords in the subject line
- **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
- **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.

