

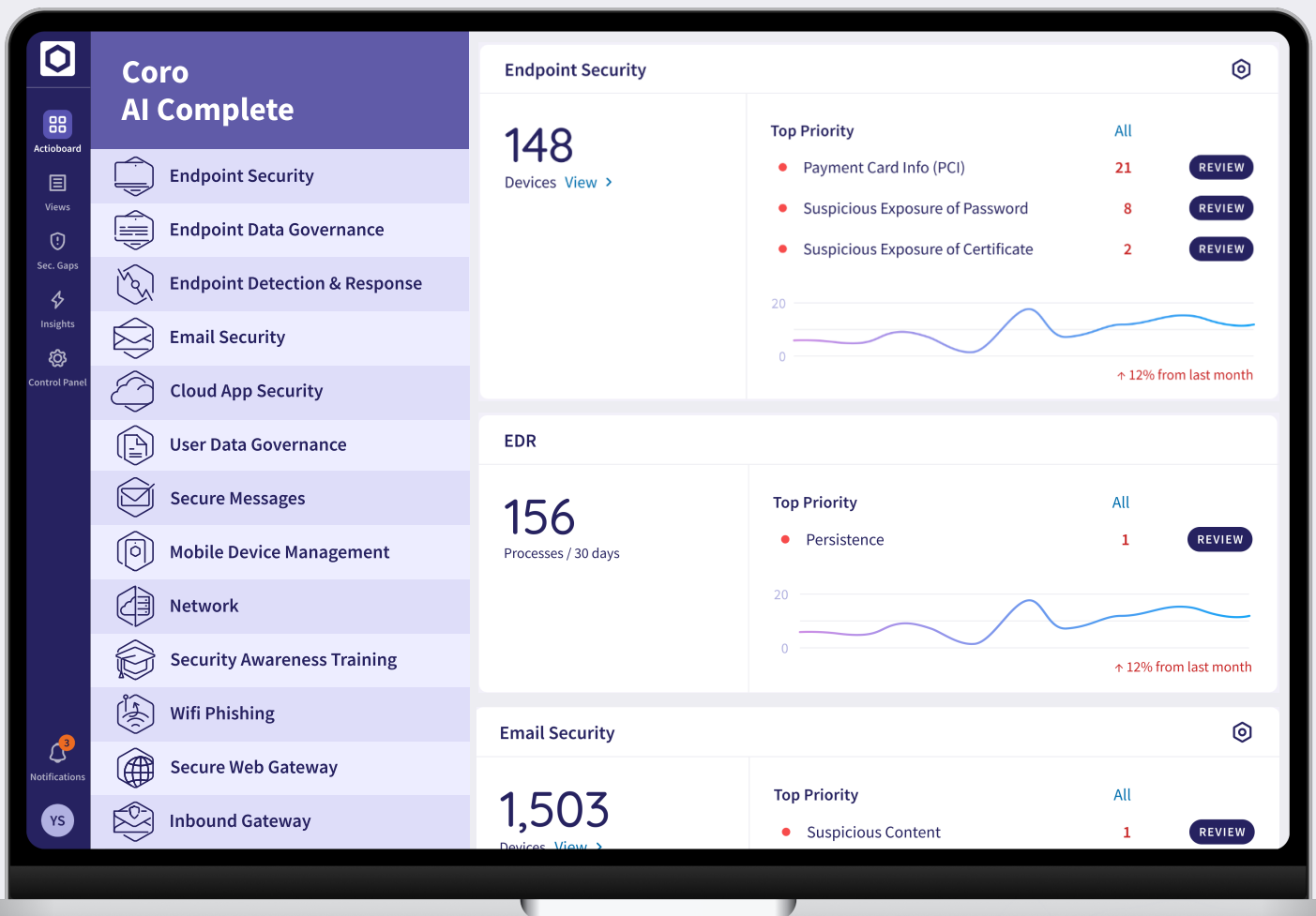


AI Complete

Cybersecurity Made Easy



Protect your business with a fully integrated security platform that combines Coro's full range of modules from email security to data governance, cloud and network to security awareness training. Coro AI Complete brings unlimited access to all Coro security modules and allows IT teams to deploy one, easy to use platform that covers all of their cybersecurity needs.



 **One Dashboard**  **One AI Agent**  **One Data Engine**



info@coro.net | coro.net

Key Features

Coro AI Complete



- ✓ **Coro AI Assistant**
Generates AI-powered summaries of key trends and recommendations with prompts and product-doc links
- ✓ **Device Posture**
Sets device policies according to device vulnerabilities
- ✓ **Telemetry Tab**
Collects and organize forensic details from devices
- ✓ **Process Graph**
Visualizes process lineage and parent-child relationships to trace threats
- ✓ **Allowlist / Blocklist**
Creates allowlists and blocklists for files, folders, and processes to reduce tickets triggered by unknown activities
- ✓ **Coro Mobile App**
Enables Zero Trust Network Access (ZTNA) or Virtual Private Network (VPN) protection and DNS filtering on iOS and Android
- ✓ **Secure Messages**
Encrypts sensitive emails and offers a secure platform to access encrypted messages
- ✓ **Real-Time URL Protection**
Rewrites and inspects email links at click time, blocking malicious sites and hidden redirect destinations
- ✓ **Zero Trust Network Access**
Applies granular, identity-based access control, ensuring that only authorized users or devices can access specific resources
- ✓ **Trusted Networks**
Automatically disables Secure Access Service Edge (SASE) on office networks to improve on-site latency and performance, with protection re-enabled when offsite
- ✓ **Device Management**
Remotely wipes data from compromised mobile devices, marks them for disenrollment to remove profiles and policies, and removes mobile devices that are inactive or disenrolled
- ✓ **Lost Mode**
Locks supervised mobile devices, shows custom contact info, and tracks location when powered on
- ✓ **Application Policy**
Defines and enforces rules for app use, including install / remove restrictions, blocking in-app purchases, and locking system defaults
- ✓ **Remote App Installation**
Installs required apps on employee mobile devices directly from the console
- ✓ **Coro Insights**
Provides key security insights, including top vulnerable users and workspaces and ticket trends, with filtered ticket logs for fast review
- ✓ **Multi Factor Authentication**
Prevents unauthorized access to company resources by requiring users to provide a second form of verification when establishing a VPN connection via the Coro Agent
- ✓ **Security Awareness Training**
Trains users to identify phishing and social engineering threats through real-world simulations
- ✓ **Cloud Applications**
Connects, monitors and controls a range of cloud apps: Microsoft Office 365, Google Workspace, Slack, Dropbox, Box, & Salesforce
- ✓ **Outbound Gateway**
Enables real-time monitoring and blocking of outbound emails that violate an organization's sensitive data policies
- ✓ **Wi-Fi Phishing**
Identifies malicious Wi-Fi networks and prevents device connection
- ✓ **Scheduled Malware Scans**
Schedules daily, weekly, or off-hours malware scans on Windows, macOS, and Linux agents
- ✓ **Third Party Applications**
Lists and manages third-party apps connected to MS 365 and Google Workspace, offering control and visibility into app usage within the organization
- ✓ **Secure Web Gateway**
Admins can activate domain name system (DNS) filtering and create allowlists and blocklists to control what domains are not able to be accessed while on the network
- ✓ **Inbound Gateway**
Provides real-time detection and protection for incoming emails from all 3rd party providers at the delivery level
- ✓ **Impossible Traveller**
Detects login attempts from distant locations in unrealistically short intervals, helping identify potential credential compromise or unauthorized access
- ✓ **API-Based Cloud Email Protection**
Integrates directly with API-based email providers with no installation or hardware require
- ✓ **Sensitive Data Detection**
Leverages country-specific infotypes, including Germany, Canada, France, Italy, USA, New Zealand, Australia, and the Netherlands to detect and alert on sensitive data

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

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.

Cybersecurity Made Easy

TRY OUR INTERACTIVE DEMO

REQUEST A QUOTE

