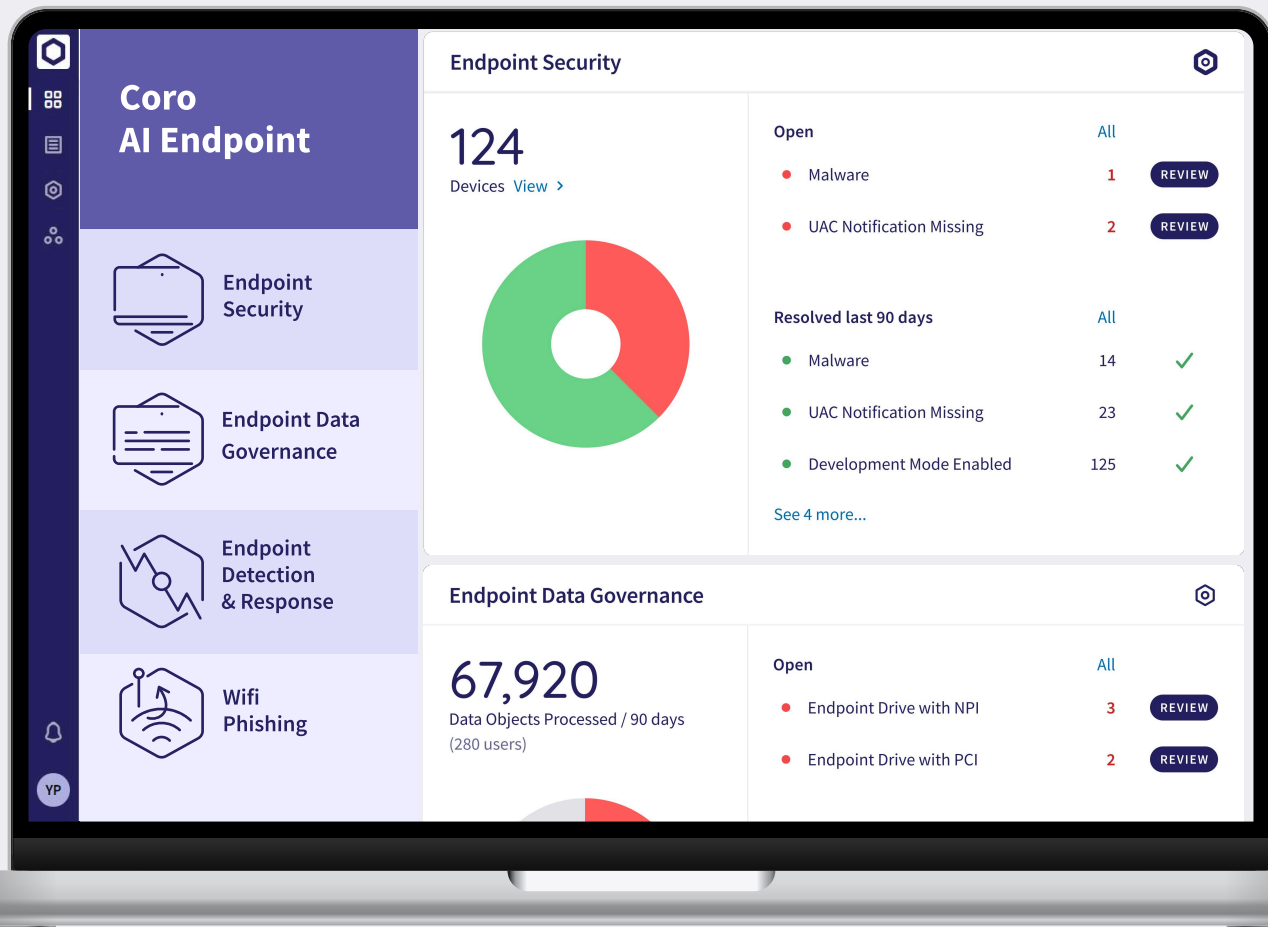# CORO

AI Endpoint

Built for small IT teams with big responsibilities

Coro AI Endpoint combines powerful modules to safeguard endpoint devices and protect your business. The Endpoint Security module automatically detects and logs devices, scanning for malware and suspicious activity. Coro's EDR module offers proactive, real-time protection by identifying and neutralizing threats across interconnected devices. The Endpoint Data Governance module ensures compliance with data protection policies, monitoring sensitive data on devices and preventing unauthorized use or loss.

Coro AI Endpoint

- Endpoint Security
- Endpoint Data Governance
- Endpoint Detection & Response
- Wifi Phishing

Endpoint Security

124
Devices View >

Open		All
● Malware	1	REVIEW
● UAC Notification Missing	2	REVIEW

Resolved last 90 days		All
● Malware	14	✓
● UAC Notification Missing	23	✓
● Development Mode Enabled	125	✓

See 4 more...

Endpoint Data Governance

67,920
Data Objects Processed / 90 days
(280 users)

Open		All
● Endpoint Drive with NPI	3	REVIEW
● Endpoint Drive with PCI	2	REVIEW

One Dashboard   One AI Agent   One Data Engine

CORO

Key Features

Coro AI Endpoint

Device Posture
Sets device policies according to device vulnerabilities

Process Graph
Visualizes process lineage and parent-child relationships to aid in investigating malicious activity

Quarantine Infected Containers
Automatically quarantines the entire container with malicious files

Wi-Fi Phishing Detection
Identifies and blocks connections to malicious Wi-Fi networks

Secured Shadow Backups
Regular backup snapshots against ransomware

Telemetry Tab
Collects and organizes forensic details from devices like account events, scheduled tasks, registry keys, and related process command lines

Allowlist/Blocklist
Creates allowlists and blocklists for files, folders, and processes to reduce tickets triggered by unknown activities

Initial Malware & Ransomware Scan
Performs a device scan upon installation

Quick Actions
Offers remote options like isolating, shutting down, rebooting devices, or blocking processes

Advanced Threat Control
Blocks any processes that exhibit suspicious behavior

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 and early detection of potential risks

Process Tab
Provides an aggregated overview of executed processes, enabling quick analysis and insights

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

Full Log View
Provides detailed logs for advanced investigations

Analytics
Dashboards, scheduled reporting for audits and executive summaries, real-time alerts

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

REQUEST A QUOTE

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.

500™
Technology **Fast 500**
2024 NORTH AMERICA
30 YEARS OF INNOVATION
Deloitte.

SE LABS
AAA
NOVEMBER 2024
ENTERPRISE ADVANCED SECURITY

SUMMER 2025
Easiest To Use

THE CHANNEL CO.
CRN
★★★★★
PARTNER PROGRAM GUIDE
WINNER 2025

2025
WINNER
★ ★ ★
CYBER SECURITY
EXCELLENCE AWARDS

CORO