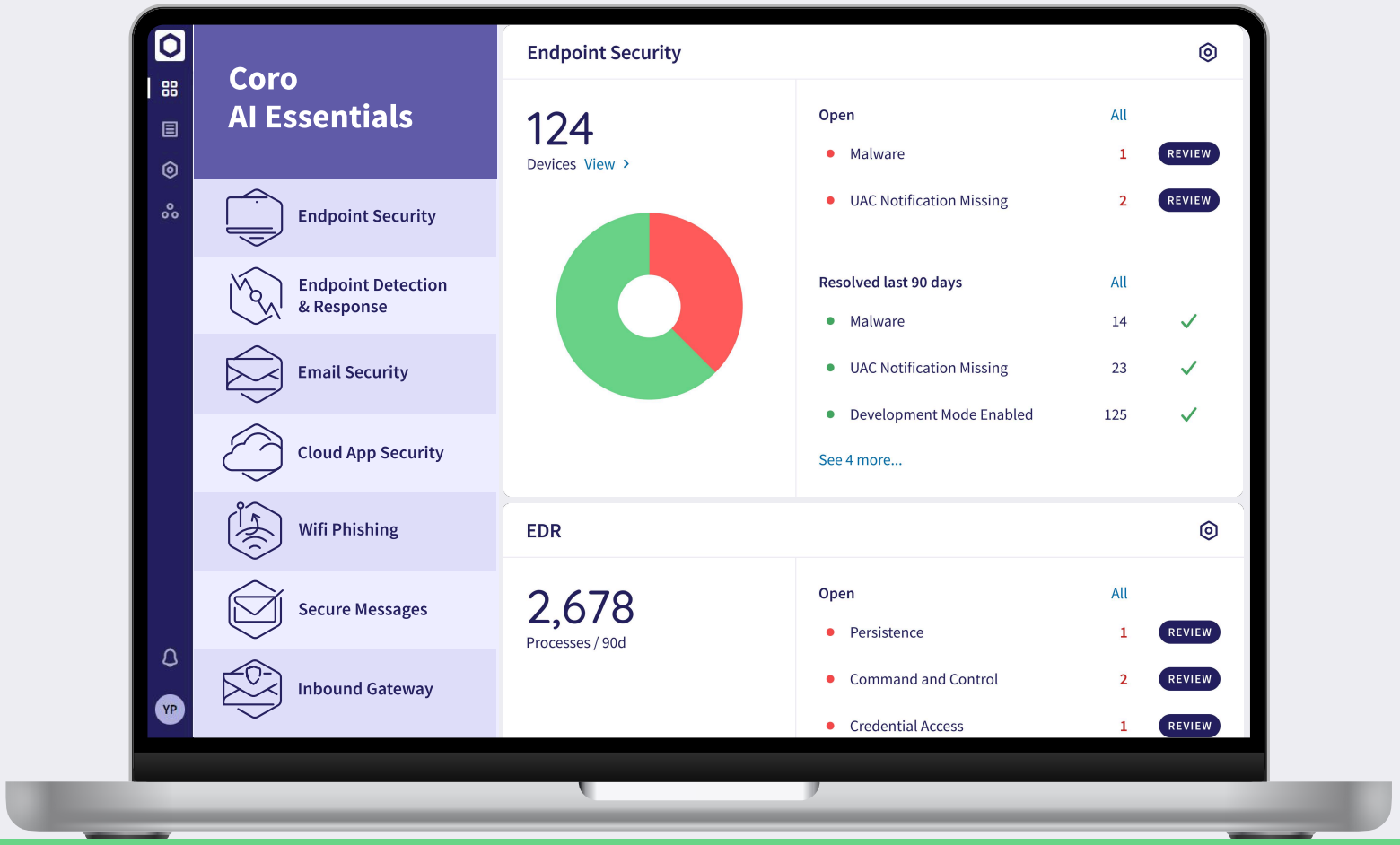
CORO

AI Essentials

Built for small IT teams with big responsibilities

Coro AI Essentials combines the essential security tools you need to protect your business. The Endpoint Security module detects and logs devices, scanning for malware and suspicious activity. Coro's EDR provides real-time protection, identifying and neutralizing threats across devices. The Email Security module defends against data leaks and social engineering, automatically monitoring, flagging, and remediating advanced threats. The Cloud App Security module ensures secure access and malware protection for cloud apps and drives.



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

Key Features

Coro AI Essentials

Device Posture
Sets device policies according to device vulnerabilities

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

Cloud Applications
Connects, monitors and controls a range of cloud apps: Microsoft Office 365, Google Workspace, Slack, Dropbox, Box, and Salesforce

Quarantine Infected Containers
Automatically quarantines the entire container with malicious files

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

API-Based Cloud Email Protection
Integrates directly with API-based email providers with no installation or hardware required

Full Log View
Provides detailed logs for advanced investigations

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

Third Party Applications Tab
Lists and manages third-party apps connected to MS 365 and Google Workspace, offering control and visibility into app usage within the organization

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

Quarantine / Warn Modes
Isolates suspicious emails or flags them with alerts for review

Advanced Threat Control
Blocks any processes that exhibit suspicious behavior

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

Inbound Gateway Setup Monitoring
Verifies that inbound gateway is configured correctly and alerts when the configuration is incorrect

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

App Connection & Permission Status
Validates cloud app connections and permissions, with health status displayed

Dedicated "Quarantine" Folder
Stores detected malicious emails and files in the "Suspected folder" and creates a ticket for the event

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

Access Permissions
Allows admins to set permissions for specific groups, specific users, or all users, with access restricted by country or IP

Protected Users & Groups Sync
Provides automatic daily synchronization of protected users and groups with manual triggering by admins

Secured Shadow Backups
Regular backup snapshots against ransomware

Attachment Quarantine Management
Isolates suspicious attachments for secure analysis or removal

User Feedback
Provides tools for users to report phishing or misclassified emails

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

Inbound Gateway
Provides real-time detection and protection for incoming emails from all 3rd party providers at the delivery level

Secure Messages
Encrypts sensitive emails and offers a secure platform to access encrypted messages

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, 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.

Cybersecurity for IT small teams with big responsibilities

TRY OUR INTERACTIVE DEMO

REQUEST A QUOTE

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