



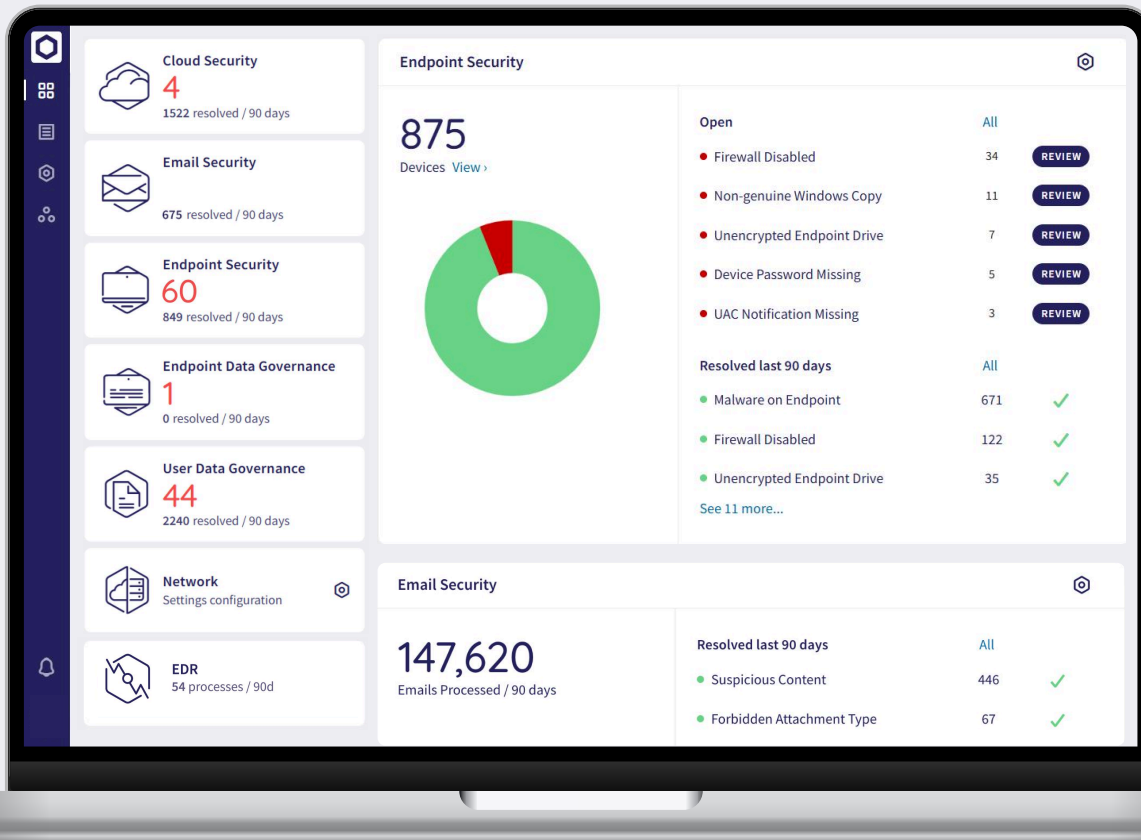
Endpoint Security

Built for small teams with big responsibilities



Safeguard endpoint devices and protect your business with the Coro Endpoint Security module. It automatically identifies and logs all devices, scanning for malware, suspicious activity, and human errors. The Endpoint Security module detects unusual behavior and neutralizes threats before they can cause harm.

Modular Cybersecurity



Coro's Endpoint Security is part of a powerful modular cybersecurity platform. Designed to evolve with your needs, a modular platform ensures effortless security across cloud apps, devices, data, and endpoints while sharing one endpoint agent, one dashboard, and one data engine. Adding modules is done at the click of a button. Chosen modules snap into place, immediately integrating with other modules.



Key Supported Security Incidents

✔ Malware on Endpoint

Detects malware and initiates automatic remediation

✔ Infected Process

Identifies malicious processes and neutralizes the threat

✔ Firewall Disabled

Identifies the disabled firewall and recommends enabling it

✔ Gatekeeper Disabled

Detects unverified app permissions and alerts to restore security settings

✔ Non-Genuine Windows Copy

Identifies non-genuine OS and alerts to potential security risks

✔ System Integrity Protection Disabled

Identifies disabled system protection and alerts to re-enable safeguards

✔ Unencrypted Endpoint Drive

Identifies unencrypted drives and alerts to enable encryption

✔ Forbidden Wi-Fi Connection

Detects unauthorized Wi-Fi connections and blocks access

✔ Development Mode Enabled

Detects active Development mode and flags potential security risks for mitigation

✔ Apple Mobile File Integrity Disabled

Detects the disabled feature and alerts to restore file integrity

✔ Wi-Fi Phishing

Identifies malicious Wi-Fi networks and prevents device connection

✔ Device Password Missing

Detects missing password and prompts to secure the device

✔ UAC Notification Missing

Detects missing user account control alerts and prompts for restoration

✔ VSS Backup Protection

Detects unprotected backups and advises securing them against ransomware

Key Features

✔ Device Posture

Sets device policies according to device vulnerabilities

✔ Quarantine Infected Containers

Automatically quarantines the entire container with malicious files

✔ Secured Shadow Backups

Regular backup snapshots against ransomware

✔ 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

✔ Enhanced EDR Block Mode

Provides endpoint detection and response with Windows Defender Antivirus

✔ Advanced Threat Control

Blocks any processes that exhibit suspicious behavior

✔ Wi-Fi Phishing Detection

Identifies and blocks connections to malicious Wi-Fi networks

✔ Analytics

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

✔ Multilingual Support

Provides additional support for 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

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 small teams with big responsibilities

SCHEDULE A DEMO TODAY

START A FREE TRIAL

