



Endpoint Security

Built for small IT 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
- ✓ **Non-Genuine Windows Copy**
Identifies non-genuine OS and alerts to potential security risks
- ✓ **Forbidden Wi-Fi Connection**
Detects unauthorized Wi-Fi connections and blocks access
- ✓ **Wi-Fi Phishing**
Identifies malicious Wi-Fi networks and prevents device connection
- ✓ **Infected Process**
Identifies malicious processes and neutralizes the threat
- ✓ **System Integrity Protection Disabled**
Identifies disabled system protection and alerts to re-enable safeguards
- ✓ **Development Mode Enabled**
Detects active Development mode and flags potential security risks for mitigation
- ✓ **Device Password Missing**
Detects missing password and prompts to secure the device
- ✓ **Firewall Disabled**
Identifies the disabled firewall and recommends enabling it
- ✓ **Unencrypted Endpoint Drive**
Identifies unencrypted drives and alerts to enable encryption
- ✓ **Apple Mobile File Integrity Disabled**
Detects the disabled feature and alerts to restore file integrity
- ✓ **UAC Notification Missing**
Detects missing user account control alerts and prompts for restoration
- ✓ **Gatekeeper Disabled**
Detects unverified app permissions and alerts to restore security settings
- ✓ **VSS Backup Protection**
Detects unprotected backups and advises securing them against ransomware

Key Features

- ✓ **Device Posture**
Sets device policies according to device vulnerabilities
- ✓ **Allowlist/Blocklist**
Creates allowlists and blocklists for files, folders, and processes to reduce tickets triggered by unknown activities
- ✓ **Advanced Threat Control**
Blocks any processes that exhibit suspicious behavior
- ✓ **Quarantine Infected Containers**
Automatically quarantines the entire container with malicious files
- ✓ **Initial Malware & Ransomware Scan**
Performs a device scan upon installation
- ✓ **Analytics**
Dashboards, scheduled reporting for audits and executive summaries, real-time alerts
- ✓ **Secured Shadow Backups**
Regular backup snapshots against ransomware
- ✓ **Wi-Fi Phishing Detection**
Identifies and blocks connections to malicious Wi-Fi networks
- ✓ **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 IT teams with big responsibilities

[TRY OUR INTERACTIVE DEMO](#)

[START A FREE TRIAL](#)

