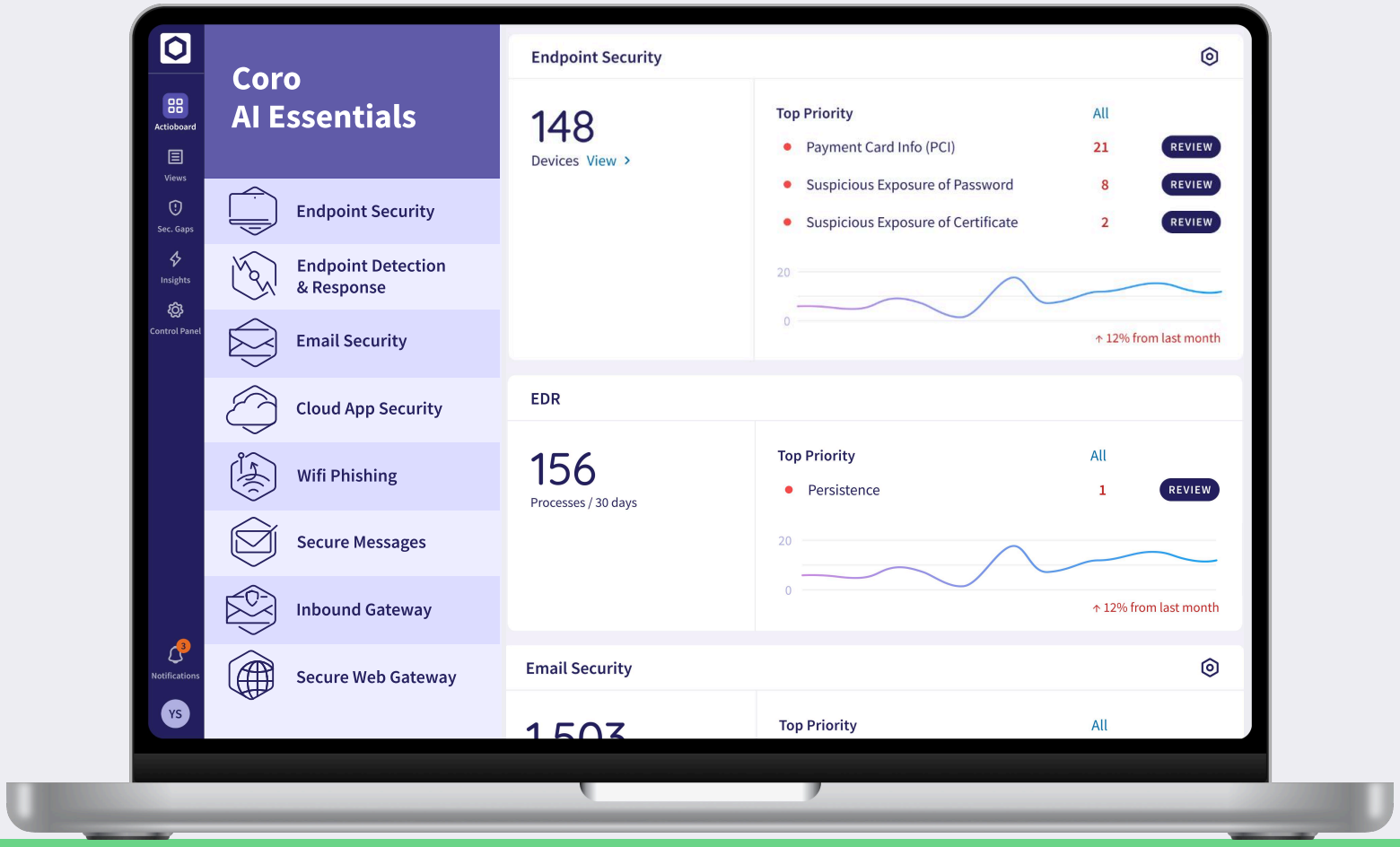
CORO

AI Essentials

Cybersecurity Made Easy

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
- **Quarantine / Warn Modes**
  Isolates suspicious emails or flags them with alerts for review
- **Remote Agent Uninstallation**
  Remotely triggers uninstallation of Windows agents from the Console
- **Auto-Forward Protection Policy**
  Deletes unauthorized auto-forward rules to external addresses
- **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
- **Outbound Gateway**
  Enables real-time monitoring and blocking of outbound emails that violate an organization's sensitive data policies
- **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
- **Initial Malware & Ransomware Scan**
  Performs a device scan upon installation
- **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
- **Scheduled Malware Scans**
  Schedules daily, weekly, or off-hours malware scans on Windows, macOS, and Linux agents
- **Threat Detection Policies**
  Adds new threat detection policies and actions for admins, including alerts for abnormal admin activity, mass data actions, bot attacks, and identity compromise
- **Impossible Traveller**
  Detect login attempts from distant locations in unrealistically short intervals, helping identify potential credential compromise or unauthorized access
- **Secured Shadow Backups**
  Regular backup snapshots against ransomware
- **User Feedback**
  Provides tools for users to report phishing or misclassified emails
- **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
- **Phishing Sensitivity**
  Reduces alert volume by configuring phishing sensitivity levels (high, medium, or low)
- **End-User Phishing Report**
  Provides users with regular reports of emails that Coro quarantined before reaching their inbox
- **Add and Manage User Labels in the SWG Tab**
  Enables admins to create and manage user labels in the SWG tab, simplifying user categorization and DNS filtering, even without VPN connection

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

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

SE LABS AAA MAY 2025
ENTERPRISE ADVANCED SECURITY

SUMMER 2025
Easiest To Use

THE CHANNEL CO. CRN PARTNER PROGRAM GUIDE WINNER 2025

2025 WINNER CYBER SECURITY EXCELLENCE AWARDS