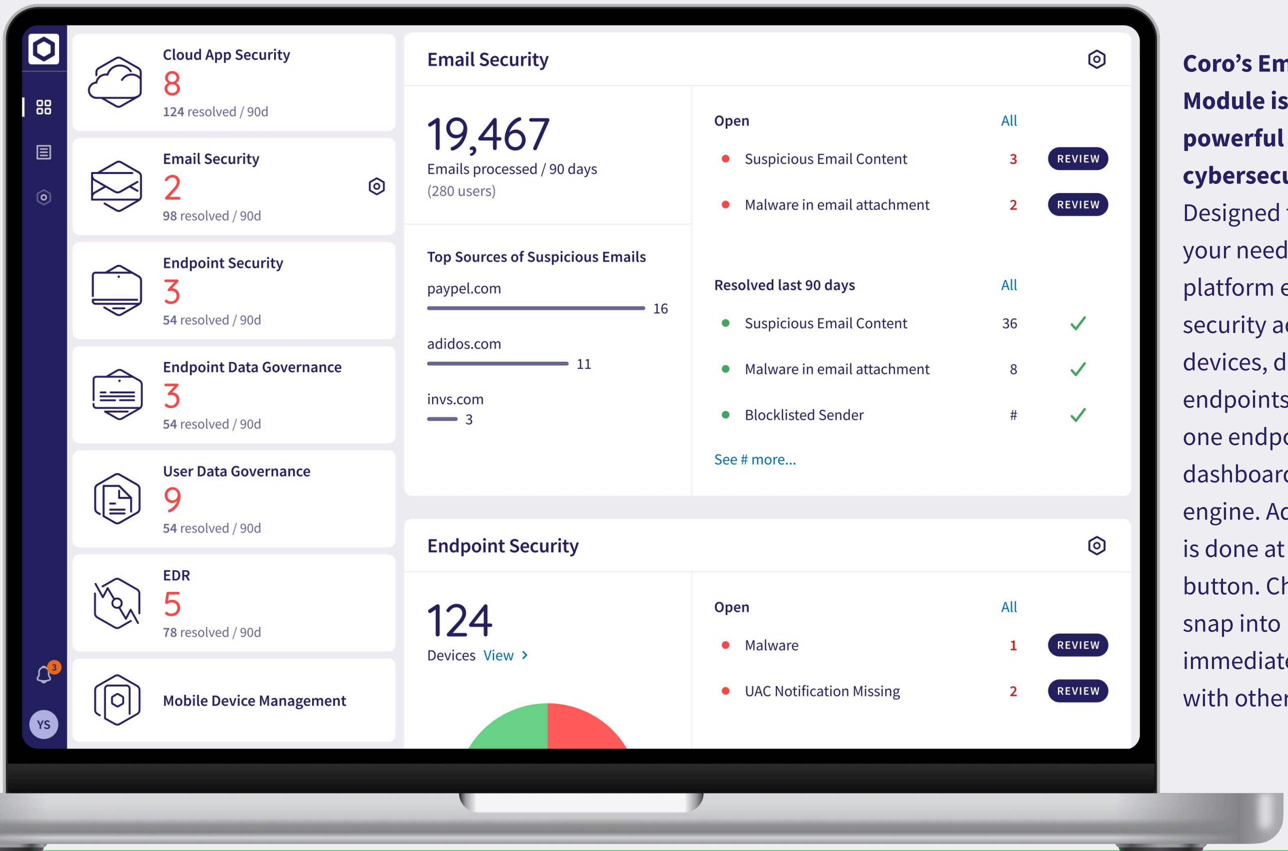
CORO

# Email Security

## Built for small IT teams with big responsibilities

**Experience advanced email protection and safeguard your business against data leaks and social engineering attacks with ease.** Powered by Coro's intelligent engine and Large Language Models (LLMs), the Email Security module automatically monitors, detects, flags, prioritizes, quarantines, and remediates the most advanced threats. Leveraging advanced LLMs increases phishing attack detection accuracy and strengthens the system's capabilities. The module comes pre-configured with baseline security policies built on industry best practices, providing robust protection from day one.

## Modular Cybersecurity



Cloud App Security
8
124 resolved / 90d

Email Security
2
98 resolved / 90d

Endpoint Security
3
54 resolved / 90d

Endpoint Data Governance
3
54 resolved / 90d

User Data Governance
9
54 resolved / 90d

EDR
5
78 resolved / 90d

Mobile Device Management

Email Security

19,467
Emails processed / 90 days
(280 users)

Top Sources of Suspicious Emails

| | |
|---|---|
| paypel.com | 16 |
| adidos.com | 11 |
| invs.com | 3 |

Open — All

| | | |
|---|---|---|
| ● Suspicious Email Content | 3 | REVIEW |
| ● Malware in email attachment | 2 | REVIEW |

Resolved last 90 days — All

| | | |
|---|---|---|
| ● Suspicious Email Content | 36 | ✓ |
| ● Malware in email attachment | 8 | ✓ |
| ● Blocklisted Sender | # | ✓ |

See # more...

Endpoint Security

124
Devices View ›

Open — All

| | | |
|---|---|---|
| ● Malware | 1 | REVIEW |
| ● UAC Notification Missing | 2 | REVIEW |

**Coro's Email Security Module 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

- **Spam**
  Filters unsolicited bulk emails
- **Email Phishing**
  Detects phishing attacks that attempt to steal credentials or sensitive data
- **Malware & Ransomware in Email Attachments**
  Detects and removes malicious files embedded in attachments
- **Brand/User Impersonation**
  Detects attempts to impersonate trusted brands or individuals
- **Domain Impersonation**
  Identifies and stops spoofed domains mimicking legitimate organizations
- **Suspicious Content**
  Scans for risky or deceptive text, attachments, and links
- **Suspicious Metadata**
  Flags emails with abnormal or altered metadata
- **Crowd Blocked**
  Automatically protects emails from senders on the global blocklist
- **Forbidden Attachment Type**
  Blocks unsafe file types, such as executables or scripts
- **Missing Required Authentication**
  Identifies emails lacking proper authentication
- **Blocklisted Sender**
  Prevents known malicious senders from reaching users
- **User Reported**
  Enables end-users to report emails as Phishing

## Key Features

- **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
- **Secure Messages***
  Encrypts sensitive emails and offers a secure platform to access encrypted messages
- **Inbound Gateway***
  Provides real-time detection and protection for incoming emails from all 3rd party providers at the delivery level
- **Allow / Block Lists**
  Defines trusted senders or blocks specific domains to control access
- **Reporting**
  Customizable dashboards, scheduled reporting and real-time alerts
- **Inbound Gateway Setup Monitoring**
  Verifies that inbound gateway is configured correctly and alerts when the configuration is incorrect
- **Dedicated “Quarantine” Folder**
  Stores flagged emails in a separate folder for user review
- **User Feedback**
  Provides tools for users to report phishing or misclassified emails
- **Role-Based Access Control**
  Role-based access by user roles, departments, or groups
- **Attachment Quarantine Management**
  Isolates suspicious attachments for secure analysis or removal
- **Multilingual Support**
  Provides additional support for Spanish and Italian

*Add-on

## 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

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

SE LABS AAA NOVEMBER 2024 ENTERPRISE ADVANCED SECURITY

SPRING 2025 Grid Leader

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

2025 WINNER ★★★ CYBER SECURITY EXCELLENCE AWARDS