



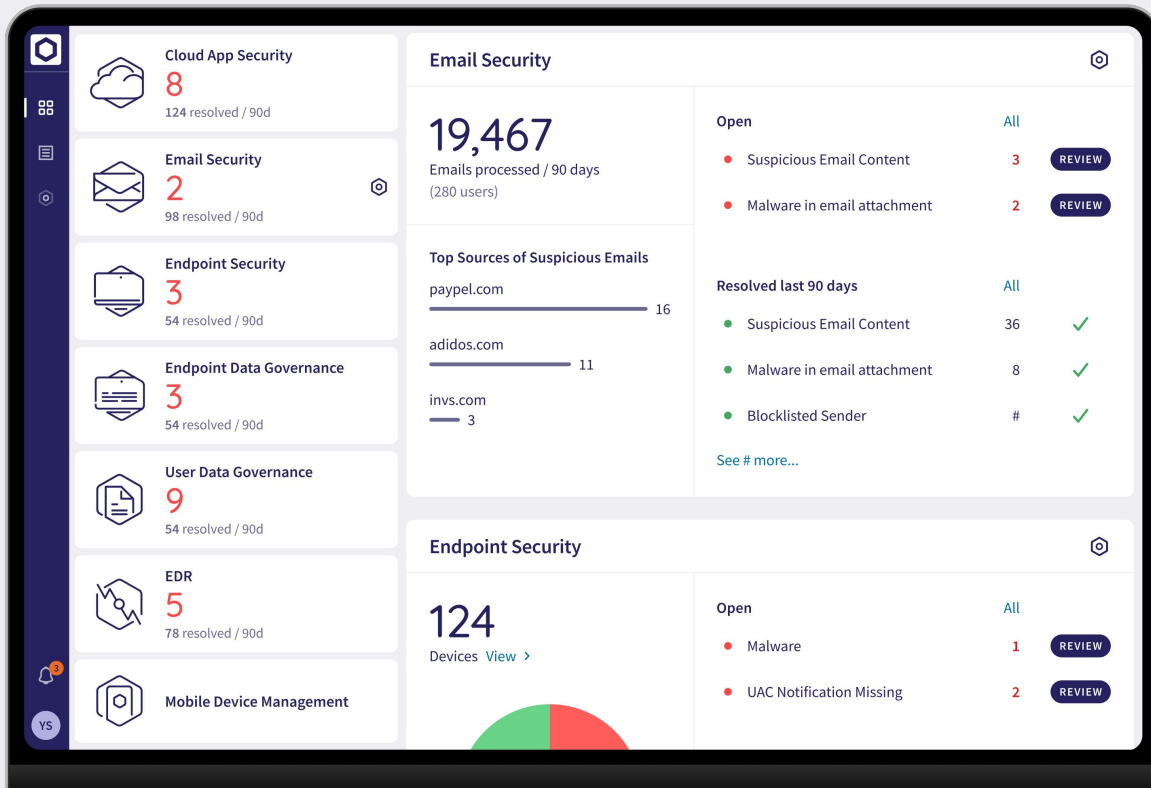
Kyaniteblue

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



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.



Kyanite Blue Ltd | david.whitton@kyanite.blue | 07777498343

Key Supported Security Incidents

- | | | | |
|--|--|--|---|
|  Spam
Filters unsolicited bulk emails |  Brand/User Impersonation
Detects attempts to impersonate trusted brands or individuals |  Suspicious Metadata
Flags emails with abnormal or altered metadata |  Missing Required Authentication
Identifies emails lacking proper authentication |
|  Email Phishing
Detects phishing attacks that attempt to steal credentials or sensitive data |  Domain Impersonation
Identifies and stops spoofed domains mimicking legitimate organizations |  Crowd Blocked
Automatically protects emails from senders on the global blocklist |  Blocklisted Sender
Prevents known malicious senders from reaching users |
|  Malware & Ransomware in Email Attachments
Detects and removes malicious files embedded in attachments |  Suspicious Content
Scans for risky or deceptive text, attachments, and links |  Forbidden Attachment Type
Blocks unsafe file types, such as executables or scripts |  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 |  Inbound Gateway*
Provides real-time detection and protection for incoming emails from all 3rd party providers at the delivery level |  Inbound Gateway Setup Monitoring
Verifies that inbound gateway is configured correctly and alerts when the configuration is incorrect |  Role-Based Access Control
Role-based access by user roles, departments, or groups |
|  Quarantine / Warn Modes
Isolates suspicious emails or flags them with alerts for review |  Allow / Block Lists
Defines trusted senders or blocks specific domains to control access |  Dedicated “Quarantine” Folder
Stores flagged emails in a separate folder for user review |  Attachment Quarantine Management
Isolates suspicious attachments for secure analysis or removal |
|  Secure Messages*
Encrypts sensitive emails and offers a secure platform to access encrypted messages |  Reporting
Customizable dashboards, scheduled reporting and real-time alerts |  User Feedback
Provides tools for users to report phishing or misclassified emails |  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

Get in touch to learn more.

