



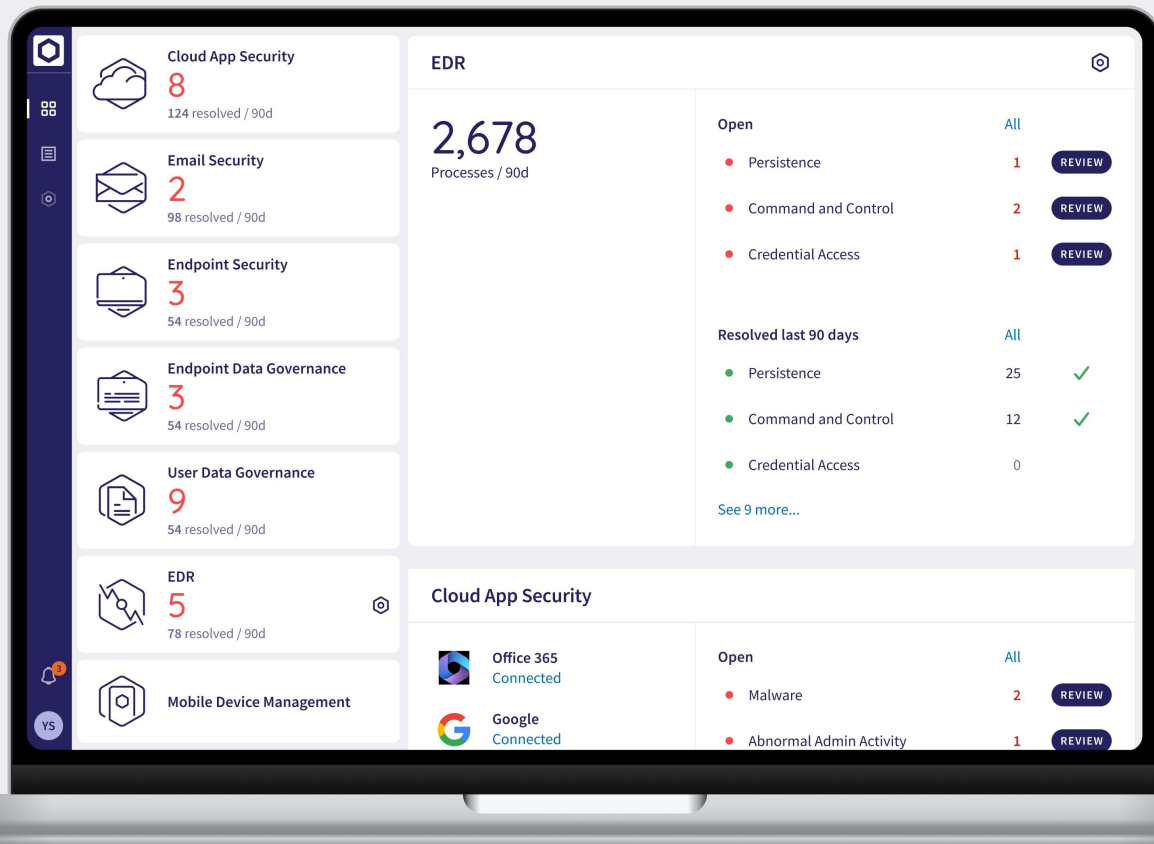
Kyaniteblue

Endpoint Detection & Response

Built for small IT teams with big responsibilities

Coro's Endpoint Detection & Response (EDR) module provides proactive, real-time protection for interconnected endpoint devices and the broader network against sophisticated cyber threats. Leveraging behavior-based detection and continuous monitoring, Coro EDR identifies threats in real time, preventing them from going unnoticed for extended periods.

Modular Cybersecurity



Coro's EDR 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

-  **Remote Access Tool Attack**
 Detects unauthorized use of remote access tools
-  **Suspicious Usage of a LOLBin**
 Detects misuse of legitimate system tools for malicious purposes
-  **Brute Force Attempt Using a Non-Existent Username**
 Flags login attempts with fake usernames
-  **Repeated Brute Force Attempts Using Wrong Passwords**
 Flags repeated failed login attempts with incorrect passwords
-  **Malicious UAC Bypass**
 Detects attempts to bypass system privilege controls
-  **Execution of a Renamed Tool**
 Flags renamed tools used to evade detection
-  **Unauthorized System Discovery Activity**
 Detects commands used to identify users or system privileges
-  **Malicious File Download and/or Execution**
 Flags downloads or execution of malicious files using 'curl'
-  **Malicious PowerShell Download from External Source**
 Detects PowerShell commands downloading malicious files
-  **Malicious Base64-Encoded PowerShell Command Usage**
 Flags encoded PowerShell commands used to hide malicious scripts
-  **Malicious Scheduled Task Creation / Execution**
 Detects creation or execution of tasks for malicious purposes
-  **Modification of User Accounts in Elevated Groups**
 Flags suspicious changes to privileged user accounts
-  **Password Spray Attack Involving 200 Login Attempts**
 Detects bulk login attempts targeting user credentials
-  **Password Spray Attack Involving 100 Login Attempts**
 Detects smaller-scale login attempts targeting credentials

Key Features

-  **Process Graph**
 Visualizes process lineage and parent-child relationships to aid in investigating malicious activity
-  **Quick Actions**
 Offers remote options like isolating, shutting down, rebooting devices, or blocking processes
-  **Telemetry Tab**
 Collects and organizes forensic details from devices like account events, scheduled tasks, registry keys, and related process command lines
-  **Full Log View**
 Provides detailed logs for advanced investigations
-  **Process Tab**
 Provides an aggregated overview of executed processes, enabling quick analysis and insights
-  **30-Day Data Storage**
 Aggregates and stores data for 30 days to support investigations
-  **Allow/Block List**
 Blocks unsafe processes from running, preventing malware infections and breaches. Allows specified processes and folder paths, reducing telemetry for trusted tools and software
-  **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

Get in touch to learn more.

