Coro Modular Cybersecurity Platform for the MSP:

A Proposal For EDR and Endpoint Security

Contact: Joe Polak
Email: joe@coro.net

Coro Cybersecurity

550 West Van Buren
Suite 1300
Chicago, IL 60607
866-950-5165
joe@coro.net

Aug 22, 2024

Amit Kumar, Managing Director
MMA Infosec
ak@mmainfosec.com

Dear MMA,

At Coro, we deeply value the opportunity to partner with forward-thinking organizations like MMA. We understand your unique challenges and are committed to delivering tailored solutions that not only address your immediate needs but also contribute to your long-term success.

In this proposal, we have outlined our Endpoint Security and EDR modules and provided a general overview of the entire platform and all of its modules.

We are excited about the potential of working together and are confident that our expertise, combined with our commitment to excellence, will make a meaningful difference for MMA and its customers.

Best regards,

Joe Polak
Director of Sales, EMEA
Coro Cybersecurity, Ltd

Table of Contents

About Coro

Coro is an industry leader in flexible and adaptable modular cybersecurity focused on AI-based, automated technologies for lean IT teams, offering a full range of enterprise-grade security modules available separately or jointly. By adopting a modular, flexible, and scalable approach to cybersecurity, Coro is able to meet your current security needs where they are today, scaling with you as your needs change.

Coro's modular security platform is designed for IT teams:

- with little or no security expertise,
- who are responsible for more than just security,
- who don't have the resources to juggle a range of complex applications

With presence in the US, the UK and the Middle East markets, and more than 5,000 customers globally relying on the Coro platform to keep them secure and compliant, Coro has made a name for itself in the investor community as well. Coro has raised over $200 million from Energy Impact Partners, Balderton Capital, JVP, and Ashton Kutcher's Sound Ventures. Thanks to our core belief in every company's right to enterprise-grade security, Coro is transforming the way companies invest in cybersecurity.

Coro's core mission is to transform the way companies invest in cybersecurity by bringing enterprise-grade security to companies of all sizes and across all industries through a unique matching of the platform with companies' specific security needs and budgets.

Coro has been named a leader in G2-Grid for EDR/MDR, and has received Triple A grading (AAA) from the testing institute SE LABS. We have also won awards for Best Performer by customer reviews. In early 2024 Coro was named a Global InfoSec Award Winner during the RSA Conference. Most recently, the company was ranked in the top 5 security products by G2.

How Coro Works

Powered by artificial intelligence and machine learning, behavioral analysis, data-driven algorithms, and by incorporating industry best practices, Coro resolves challenges around lack of resources, complexity, and siloed security.

Coro:

- Orchestrates and processes multiple signals across a business's environment to determine threats.
- Employs AI to automatically remediate 95% of security threats, eliminating the need for human intervention.
- Adaptively balances between team awareness and alert fatigue by automating ticket prioritization and only alerting on a select few tickets that require inspection or post-remediation review.
- Derives curated threat intelligence and event logs, served up in our user-friendly dashboard and our single-source interface.
- Protects all devices and endpoints through ongoing monitoring, powerful next-gen antivirus and EDR, all done through a single Endpoint Agent.

Coro Architecture

Coro runs on an intelligent model that leverages heuristic analysis techniques to identify risks and threats to an organization's data infrastructure by the following:

- **Best practices**: based on industry recommendations and the requirements of most regulations.
- **Data-driven algorithms**: supporting continuous processing and analysis of multiple data sources simultaneously.
- **Adaptive AI techniques**: leveraged to identify anomalies based specifically on how each unique business operates.

Using these techniques, Coro can accurately distinguish between normal and unusual user behaviors.

Coro automatically remediates 95% of all observed threats, with less than 5% requiring the administrators' manual review. All actions are backed up with a detailed activity and event log.

A full Coro deployment consists of the following components:

Coro platform architecture

- The Coro service is a Software-as-a-Service (SaaS) cloud component hosted on AWS that forms the core backend of the Coro platform. It is responsible for all data processing, analysis, reporting, and communication with other components, such as endpoint devices and the various cloud apps that Coro can work with.
- The Coro Console is a secure web-based user interface that enables administrators to configure and monitor your Workspaces. The console connects to the backend Coro service through an API, which is also exposed for you—typically MSPs — wanting to extend the functionality to your own services.
- Endpoint devices and the Coro Agent monitor and protect devices using Windows, Windows for servers, and macOS. Once the Coro endpoint protection Agent is installed, each device is monitored by the Coro service. When enabled, the single Coro Agent also includes our VPN services to extend your Virtual Office to all connected devices. The Coro VPN is also available on Android and iOS devices through the Coro Android and iOS mobile apps.
- Coro also provides an email add-on, designed to enable end users to report on emails that appear suspicious, and to request release of emails that may have been mistakenly quarantined.

The Modules

Our modular approach is flexible and scalable by design, ensuring that as security needs change, you can easily expand your security stack. Adding modules is done at the click of a button. Chosen modules snap into place, immediately integrate with other modules and start working. Our modules cover user, endpoint, email, network, cloud, and data protection, all using a single dashboard, a single endpoint agent, and a single data engine.

The following table describes all of the modules offered by Coro:

Modules	Description
Endpoint Security	1) Protection against real-time malware and ransomware with NGAV 2) Management of critical device security features, including drive scans, agent updates, activity monitoring, customizable enforcement settings, firewall management, and UAC notifications
EDR	Management of processes and device access to network, telemetry, and post-breach analysis
Endpoint Data Governance	Scanning endpoints for sensitive data based on the workspace configurations; includes exposure of PHI/PCI/PII/NPI and business sensitive data.
Cloud Security	Advanced malware and ransomware detection and remediation in cloud drives, including access violations, malware in the cloud, and mass data download/deletion. Admins configure geo/network fencing. Consolidated data analysis optimizes incident detection's real-timeness.
Email Security	Protection against domain impersonation, or any email with the intention to mislead the recipient, and against malware in email attachments.
User Data Governance	Anomaly analysis of exposure of sensitive data (via both: email and file sharing) based on workspace configurations; includes exposure of PHI/PCI/PII/NPI and business sensitive data.
WiFi Phishing	Endpoint protection from dangerous or risky wifi connections
MDM	Monitor supervised and BYOD handheld devices, iOS and Android

Modules	Description
Network	Remote office cluster security including virtual office, virtual office firewall, and site-to-site tunnels.
Secure web gateway	Implementation of DNS filtering, including allow/block lists

Scope of Included Functionality

Combining the Endpoint security and EDR modules provides comprehensive protection for your endpoints. It identifies vulnerabilities, provides automatic remediation in most cases, and provides investigation capabilities to prevent the spreading and recurrence of any incident, breach, or attack. Together and separately, these modules enable alignment with multiple regulatory frameworks, standards, and requirements.

Overarching features and functionality

The Endpoint security and EDR modules both rely on the same endpoint agent for data and share the same device information, process information, and allow/block lists.

Since all of this information is shared across modules, you can easily onboard them both without any complex or multiple configurations.

Coro protects servers and personal devices from:

- Infection of and execution on servers and personal devices
- Spread of malware and ransomware within your organization
- Data loss due to zero-day ransomware
- Post-breach exposure of sensitive resources to breached endpoint devices

Following are the features that are shared between these modules:

Feature	Description
One easily-installable agent	Easily configurable endpoint security with one single agent for all endpoint-related services.
Continuous monitoring	24/7 monitoring and recording of endpoint activity.
30-day data storage	Data is aggregated and stored for 30 days, for investigation and analysis.
Actionboard	The Coro Action Board provides an overview of a you' security posture, and is the first thing the user sees when logging in. It displays a bird's eye view of security modules in the customer's subscription. Each widget represents a module the customer is

Feature	Description
	subscribed to, and displays the number of tickets awaiting review (in red), and the number of resolved tickets over the last 90 days. Clicking on any widget directs the user to that module's unique, detailed, dashboard. Dashboards are specific to each module, displaying the security posture of this particular module and providing details including: ● overall security posture ● additional status indicators, depending on the specific module ● ticket types and number of occurrences of each type ● quick access to the Ticket log, filtered by type, for quick issue resolution
Allow/block list	Disable Suspected unsafe files, folders and processes (= prevent from running in the future) and add to the list for tracking and management. Allow files that are safe to be accessed. Suspected processes can be blocked (meaning, prevented from running in the future) by the administrator by adding them to the blocked list for tracking and management. Bulk lists of processes can be imported using csv files for more efficient management. Prevent telemetry data collection of individual or a list of processes, files and folders by allowlisting separately or using a csv file.
Tickets	The Coro ticketing system automatically generates a ticket for each incident detected by the Coro service and links all subsequent detections to the same incident. These tickets provide crucial information and visibility into detections such as device information, related processes and telemetry, as well as information about the type of attack and the relevant actions that the administrator can take. Actions that can be taken include approving a file, deleting a file, quarantining a user account, closing a ticket, contacting a user, or suspending a user from specific (or all) cloud apps. Advanced filter options enable a quick and easy search-and-sort functionality: ● By object/domain ● By vulnerability type ● By date or date range ● Free text Endpoint security ticket types and EDR ticket types are fully detailed in our documentation.

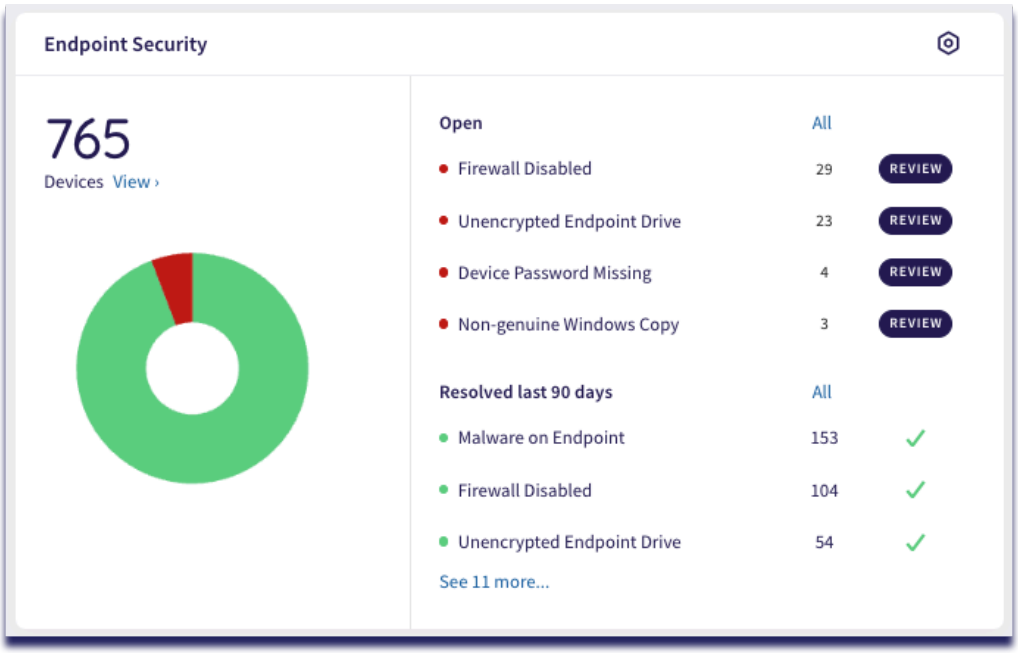
Feature	Description
Ticket retention	Tickets are available for 7 years.
Quick actions	A set of actions that can be applied to devices or tickets for remote managed remediation. Quick actions are fully detailed in our product documentation.
Activity Log	All activity performed by the Coro service and by any of the business's administrators is recorded in the Activity log. Administrators can refer to the log to review and reverse automated remediations, reopen tickets, review and assess history, track user activity, and investigate breaches and ensure compliance with regulatory requirements.
Administration	Administrator permissions can be configured for user groups, specific users or domains, or all users. Violations of set policies are reported through generated tickets in the Actionboard.
Integrations	Coro offers the ability to seamlessly integrate with other existing tools to ensure that you can benefit from all of the advantages of the Coro Platform while continuing to use your other business management tools. You can integrate via: ● out-of-the box integrations (connectors) - These integrations can be managed from the **Connectors** tab in the Coro Console. ● with our open APIs By integrating Coro with a SIEM or PSA, businesses can benefit from greater operational efficiencies and optimize their own internal processes: ● **Advantage of integrating with a SIEM:** SIEM integration offers organizations enhanced visibility into their security posture, quicker incident response, and improved ability to protect against evolving cyber threats. ● **Advantage of integrating with a PSA:** Integration with PSAs helps organizations (particularly MSPs and Channel Partners) make their billing more efficient. It does this by allowing them to automate invoice creation, track billable hours and streamline client payments.
Reports	View and download a summary report offering a detailed overview of the security status and activities within a workspace. See View a summary report in our product documentation for more details.

Feature	Description
Supported endpoint operating systems	Coro endpoint-related protection provides support for these operating systems: • Windows • Windows servers • macOS

Endpoint security features and functionality

Coro Endpoint Security is a robust solution that utilizes the Coro Agent to automatically recognize and monitor any endpoint devices that have the Coro Agent installed on them. The Coro endpoint agent collects data from connected endpoints and sends it to the platform for analysis, to provide comprehensive security coverage, improve the organization's security posture, and identify, alert, and respond to incidents.

Coro Endpoint Security records and logs all endpoint activity, analyzing all activity related to data movement to detect anomalies, including suspicious files, processes and human error, and will automatically remediate 95% of security incidents found.



Coro provides both antivirus and next-generation antivirus support, referred to as advanced threat protection (ATP), which guards against various forms of malware, including ransomware

and other malicious threats. Coro actively scans all protected devices for malware files and suspicious processes.

Device posture policies and NGAV settings can be configured to determine how Coro monitors, collects and inspects security-related data from the connected devices according to these policies. Administrators can easily tailor your device posture policies to your specific needs.

All monitored devices are listed with key details such as opened and resolved tickets, system information, user activity, and more. Devices can be managed individually or as a group, and relevant actions can be applied to resolve issues.

Coro classifies endpoint security-specific ticket types that are generated to alert administrators about incidents and vulnerabilities. Each ticket refers to one or more related findings. The tickets are tracked, managed, and resolved in the ticket log.

It then allows security teams to take immediate actions that are related to a specific ticket or device, from within the platform to remove the threat or prevent further damage from an infected/breached device or a harmful process. The action menu dynamically adapts based on the device's configuration, security posture, or if the device is online or offline.

Managing suspicious files, folders, and processes in the Allow/Block list, gives administrators more control over what Coro monitors by disabling those that are considered unsafe and allowing those that are verified as safe to be accessed. This helps reduce possible false positive detections of files/folders/processes considered safe by your organization. Exclude folders from being scanned by the Coro Agent in order to improve the Agent's performance. Block malicious processes from executing.

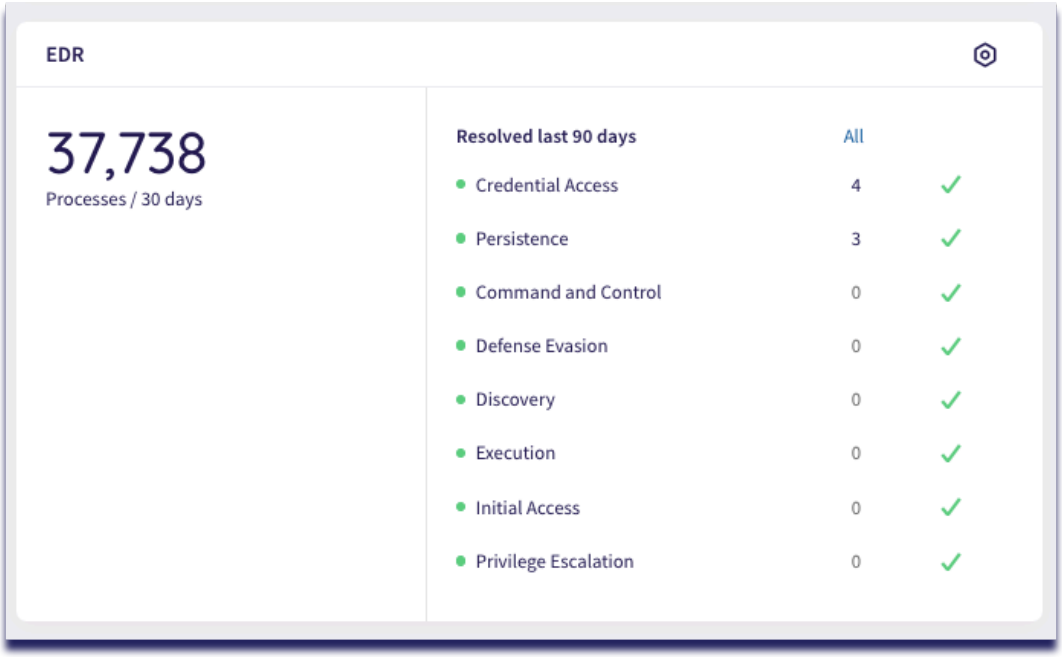
Following are the features unique to this module:

Feature	Description
Device posture	Set trust policies for devices in your workspace. These settings define the requirements a device must meet to access applications. According to these policies, Coro collects and inspects security-related data from connected devices.
Anti-virus / NGAV	Actively scans all protected devices for malware files and processes to guard against various forms of malware, including ransomware and other malicious threats.
Auto-remediation	Automated remediation contains security events and remediates 95% of security incidents found.
Remote disk encryption	Remote disk encryption for endpoint devices using Bitdefender for Windows and ? for Mac. When you encrypt an endpoint remotely, the encryption key is

Feature	Description
	automatically stored in the device details. Device posture can be set to alert about an unencrypted drive and filter vulnerabilities for it.
Device Backup	Enforces backup snapshots of files every four hours and blocks processes that exhibit risks to the backup using VSS to allow quick recovery and minimize business impact.
USB lockdown	Determines what USB devices are authorized to be connected to endpoint devices and block unauthorized USB devices.

EDR features and functionality

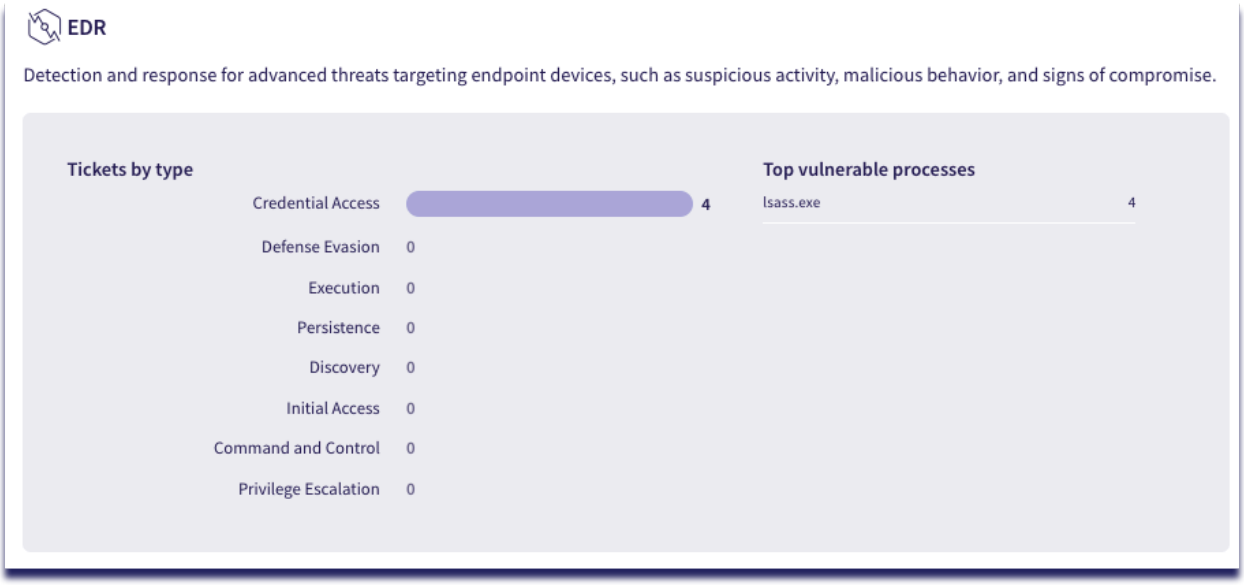
The Coro endpoint agent collects data from connected endpoints and sends it to the platform for analysis. It combines it with additional data from the additional modules to which you subscribe to provide comprehensive security coverage, improve the organization's security posture, and identify and alert on incidents.



The data is presented in clear and easy-to-understand tabs, and easy-to-use filters, links and log views that allow you to follow the data and review the information easily and clearly, facilitating incident investigation.

The system alerts admins of potential risks by generating tickets that indicate a possible attack. Tickets provide visibility and crucial information about detections and the type of attack, reducing the time needed for investigation and analysis and assisting in remediation and prevention decision-making.

It then allows security teams to take immediate actions, such as isolate devices from the network, shut down or reboot the device or block a suspected process, from within the platform to prevent further damage from an infected/breached device or a harmful process. Administrators can isolate devices from the network to prevent malicious activity from spreading. An isolated device cannot communicate with any resource on the network or the internet. The Coro process remains functional in order to communicate with the Coro server.



Following are the features unique to this module:

Feature	Description
Process tab	It provides an aggregated view of all collected information on processes executed within the organization, allowing users to drill down quickly into a process. The types of information provided are fully detailed in our documentation.
Telemetry tab	Collects and aggregates various types of monitored forensic information from devices, which users can review efficiently for malware-related investigations. Lists information about account events, scheduled tasks, registry keys and related process's command line.

Feature	Description
	Displays process-related information, and associated devices.
EDR quick actions	Each process listed on the Process tab or item in the Telemetry tab has a set of actions that can be applied for remote-managed remediation: • Isolate device • Shutdown device • Reboot device • Block process
Full log view	For deeper investigations in advanced cases.

The Coro Agent

The agent detects and prevents the creation of malicious processes on the customer's endpoint devices or servers, reducing the risk of infection and damage. Once installed, the Agent monitors devices and delivers data to the Coro service. Through data collected by the Coro Agent, tickets get populated with rich contextual insights and remediation instructions.

The Coro Agent delivers data to the Coro service on an ongoing basis. However, the Agent is fully autonomous and continues to function even if communication with the Coro service is interrupted. The Agent's autonomous status ensures continuous protection for endpoint devices.

The Coro Agent continuously communicates with the Coro service, enabling the service to:

- Monitor your devices and your connections to other objects in your network.
- Provide shadow backups for data recovery, ensuring fast recovery in case of a breach.
- Collect and aggregate relevant data.
- Identify potential threats including malware and ransomware files and processes.
- Block suspicious processes when identified on any of your devices.
- Add processes to 'allowed' and 'blocked' lists based on its analysis of the user's day-to-day business behaviors.
- Enforce device security policies by opening tickets and alerting on unencrypted drives, missing passwords, disabled firewalls, etc.
- Notify of suspected infected devices.

When an admin user logs into the Coro Console, a dedicated download link for the corresponding Coro Agent specific to that workspace is sent to them. This ensures that endpoint devices establish secure communication exclusively with the designated workspace, preventing unauthorized access. For MSPs who are typically subscribed to multiple Coro workspaces, each workspace provides its own unique Agent installer.

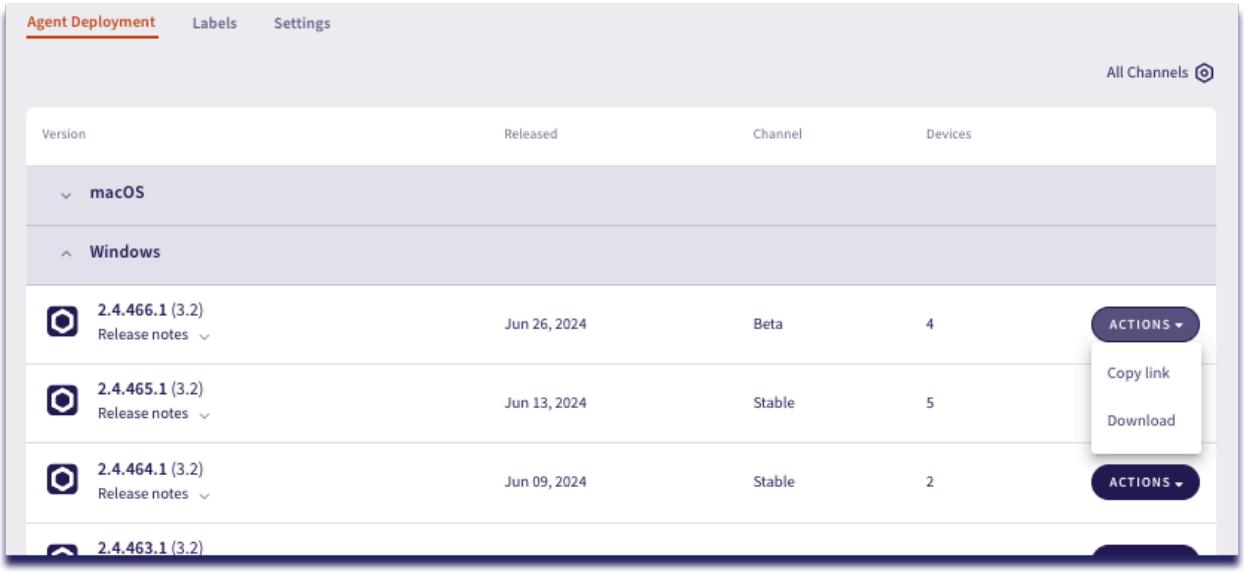
Our Deployment Processes

Coro understands how important reliability and stability are in ensuring the security of your endpoints. That is why we have built our Endpoint Agent with business continuity at its core. In order to ensure stability, the Coro Endpoint Agent undergoes regular and rigorous testing before being pushed to production.

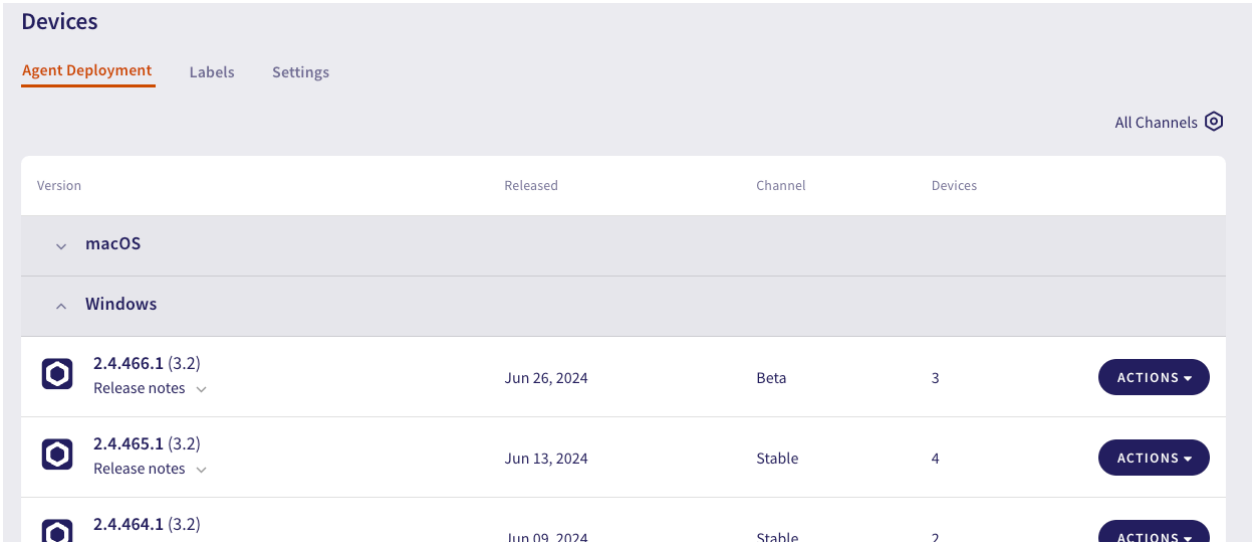
Our dedication to the highest security standard is steeped in robust CI/CD development, rolling deployment, and feature flagging processes and is coupled with ongoing customer feedback loops.

The Coro Agent undergoes a rigorous QA and beta testing process before commercial deployment. Updates to the Agent are held to an uncompromising vetting protocol before they are released, minimizing the risk of service disruptions.

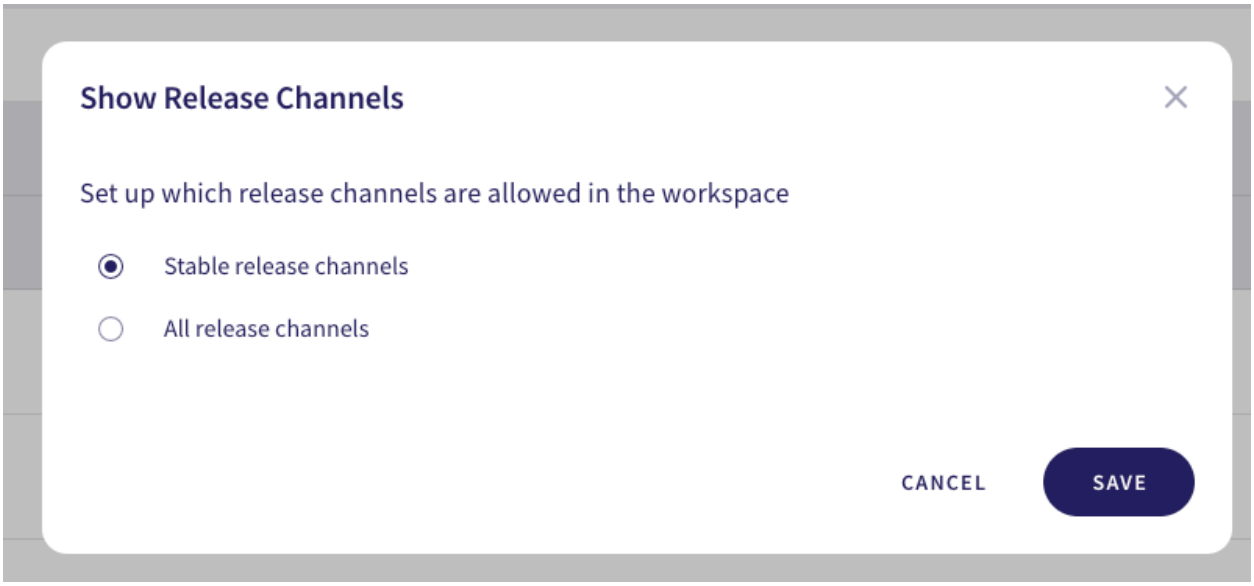
Our customers and partners have full control of the endpoint agent and the way that it is deployed and managed for all of their devices. Administrators can download the agent and deploy it via their own RMM, they can copy a link to the agent and have their users independently install the agent for different devices, they can choose to experiment with our beta agent, and they can also choose to enable automatic agent updates (with only our stable versions) by Coro for all or only a specified group of devices.



Administrators can deploy the Beta Agent available to them if they want to evaluate and test new features. Those interested in our Beta Agent don't have to worry about added threat exposure to their endpoints caused by automatic mass deployment updates, as automatic updates to endpoint devices are only activated for our Stable Agent releases.

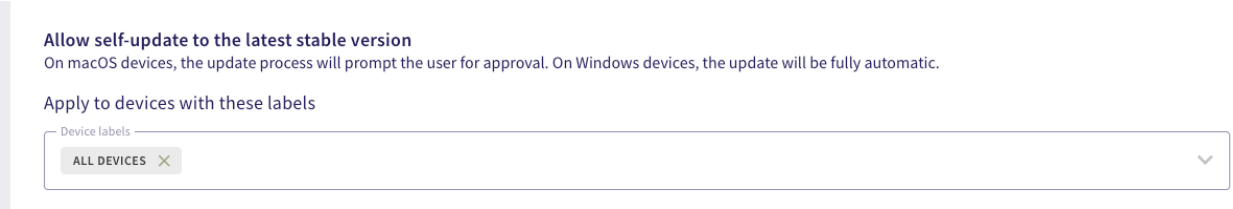


At the same time, customers can ignore this option and stick to only the stable agent when released.



Furthermore, our Stable Agent, which is rolled out only when it has passed all exit criteria and we have the utmost confidence in it, can be subscribed to for automatic updates. Similarly, our customers also choose to:

- unsubscribe to automatic updates, giving them full control of what endpoints they wish to update and when
- only enable automatic updates for a specified group of devices



To further ensure the safety of our Agent, we deploy in small increments to contain unexpected issues. We use a gradual rollout methodology to monitor updates and quickly remediate any issues, should they occur, while minimizing impact. Our feature flagging protocols streamline our development cycle, allowing us to deliver at a quick pace, fix bugs and make updates without the need for redeployment.

We embrace open communication with our customers, updating them about upcoming releases and ensuring they are prepared and supported throughout the process. We

proactively engage in customer feedback loops, adjusting our product roadmap based on what we hear from our partners to ensure we support their business needs.

You can also see more information about our Endpoint Agent on our docs portal.

The Workspace

Coro offers monitoring, remediation, and recovery techniques, including real-time, automatic remediation of suspicious files, malware, and ransomware processes and undesired applications; guarded shadow backups for recovery from zero-day ransomware attacks; unlimited allow and blocklisting for files, processes, and applications, consolidated across all workspace assets such as email, endpoint devices, and cloud drives; and endpoint detection and response (EDR) module for post-breach process analysis and device control, combined with antivirus (AV) and next-generation antivirus (NGAV) technology by Bitdefender and Coro.

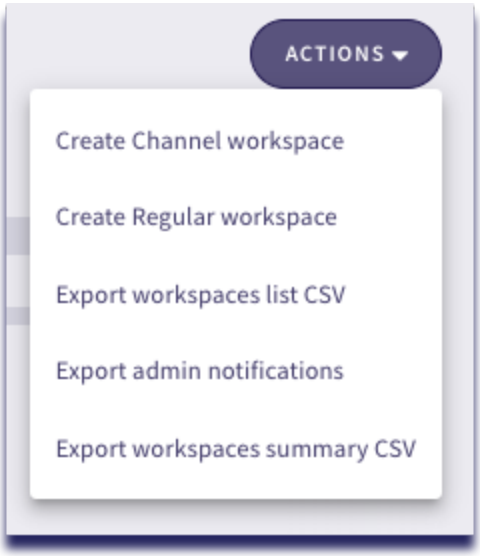
When onboarding to Coro, we provide a dedicated workspace exclusively for your organization. This workspace operates as a separate tenant, ensuring that your organization's data and permissions are completely distinct and secure. Workspaces can be configured to reside in the United States, Canada and Germany, depending on the customer's needs and the regulations with which they must comply.

Multiple Workspaces

MSP customers and partners can have more than one workspace, enabling them to manage their own customers. Each workspace is treated as independent.

Each independent workspace can be configured to reside in the United States, Canada and Germany, depending on the customer's needs and the regulations with which they must comply. The Coro service offers the following types of workspace:

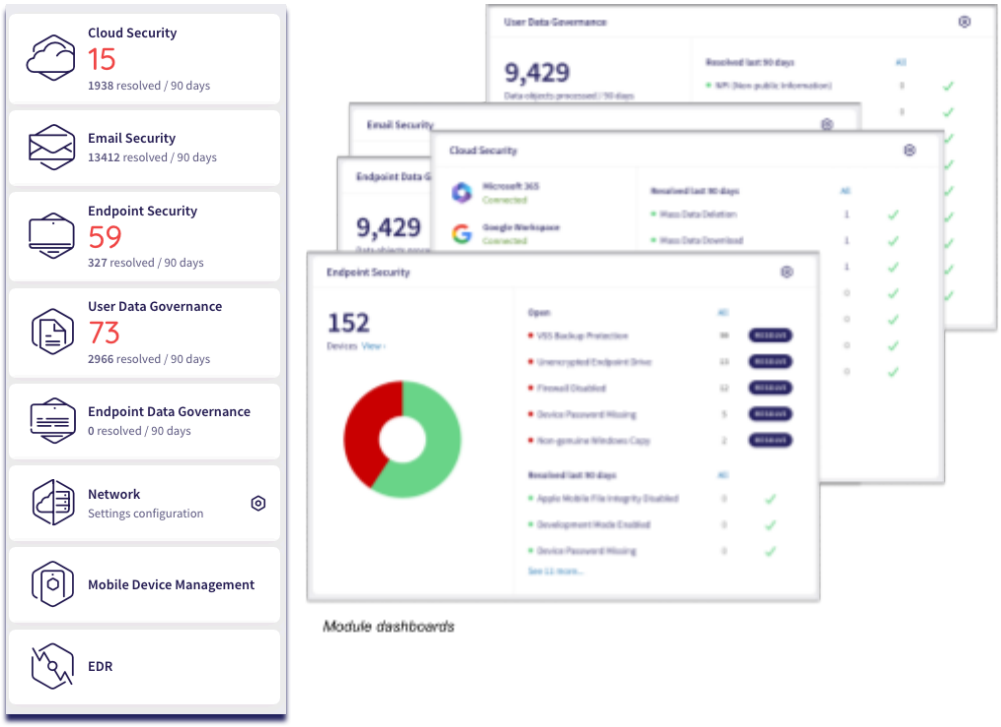
- Regular – workspaces assigned to direct customers
- Child – workspaces belonging to the customers of an MSP
- Channel – the MSP's workspace, which functions as the parent/container of all of their child workspaces



The Coro Console, via which the workspace is displayed, is the IT administrator's window into the security posture of the entire business. Admins manage the business' security posture from the Coro Console, providing visibility across devices, users, and applications.

Additional Features for the MSP

Coro is dedicated to supporting all of our partners, enabling them to easily manage their customer base with simple management tools.



Module dashboards

- Coro enables our partners to white label their workspaces, sharing their branding across the workspaces of their customers and enabling them to promote brand presence and recognition.

- Admins can add comments to tickets. This is advantageous for both Coro customers, Coro managed services team members and the MSP's managed services when communicating ticket analysis and recommended actions. Comments can also provide general information.

- The Managed Service page allows admin users with sufficient permissions to configure managed service contact details and define how to manage remediation issues. The Managed Service settings page appears in the Control Panel when a workspace subscription includes at least one module with the corresponding managed service add-on enabled. Managed Service settings are applied individually to each workspace. Child workspaces do not inherit managed service settings from channel workspaces. This enables MSPs to subscribe to our managed services without exposing that subscription to their own customers. For more information about workspace type, see managing workspaces.

Managed Services

Our Managed Services offer continuous monitoring of all tickets produced by the modules you have chosen, manual remediation where relevant, and in-depth threat investigation. Coro's Managed Services are led by trained professionals, serving as the perfect solution for customers lacking the internal resources to actively monitor and manage their Coro workspace on their own.

Our Managed Services team offers around-the-clock tracking of the Coro workspace, including:

- Monitoring of the Coro modules based on your needs and current subscription
- Managing tickets for all applicable security modules
- Responding to suspected security incidents as they arise
- Resolving incidents when applicable
- Investigating threats that require in-depth analysis
- Communicating all relevant information promptly
- Delivering timely information and best practices for customers to make swift and informed decisions

Coro's Managed Services work with the Coro platform for a holistic security solution that:

- Provides 24/7 coverage of your Coro workspaces
- Saves time on mitigation, remediation, and investigation of security tickets
- Saves money on growing your team to handle the security workload
- Provides visibility and context for security threats
- Offers actionable resolution tactics
- Minimizes IT team burnout