DATA SECURITY, POWERED BY CORO

Cybersecurity, Simplified

Data Security and Endpoint Protection

Coro data security and endpoint protection solutions fit perfectly with Adaptiv Networks' multi-layered network protection, offering you added peace of mind that comes with a comprehensive cybersecurity strategy. With no complicated integrations, and no technical challenges, Coro solutions are designed for SMEs with lean IT teams. Simply choose the right Coro bundle that fit your business.

Coro and Adaptiv, Partners in Cybersecurity

Adaptiv SD-WAN and SASE solutions work as a firewall to protect against threats moving through your network, but what about threats that are lurking in data that's stored in your cloud servers, emails or employee endpoint devices?

Coro adds protection for data, email and endpoints that complements Adaptiv's network security to help you build a comprehensive cybersecurity posture. With no complicated integrations, and no technical challenges, Coro is ideal for SMEs with lean IT teams. Simply choose the Coro cybersecurity suite that fits your business needs.

Why Coro?

Building a cybersecurity stack has always meant buying multiple, segmented tools from multiple vendors, training employees on each one, and dealing with multiple interfaces and endpoint agents. Until now. Coro is one platform with many modules. Get all the security you need now, with the ability to switch on any module you need in the future..

ONE INTERFACE

All modules feed into one, easy-to-use dashboard, in which you can quickly view and even respond to statuses, events, and logs.

ONE ENDPOINT AGENT

Device posture, NGAV, EDR, VPN, firewall, and data governance are all on one easy-to-manage endpoint agent, eliminating agent conflicts.

ONE DATA ENGINE

Modules inform each other through a shared data engine, eliminating the need for integration and improving security posture.

Simplifying Cybersecurity: Coro Suites That Cover Your Needs in Each Domain

Buying cybersecurity can be daunting, we get it. How do you ensure you're getting the most security possible for your budget? That's why we offer three affordable Coro Suites that include the right combination of modules to addresss your most pressing security needs.

Coro Essentials

Get essential coverage for endpoints, email, and cloud apps, automating resolution of most security incidents.

Included Modules:

- Endpoint Security
- Endpoint Detection & Response (EDR)
- Email Security
- Cloud Security

Endpoint Protection

Log all endpoint activity, analyze data anomalies, and automate resolution for 95% of security incidents found.

Included Modules:

- Endpoint Security
- Endpoint Data Governance
- Endpoint Detection & Response (EDR)
- Wifi Phishing

Email Protection

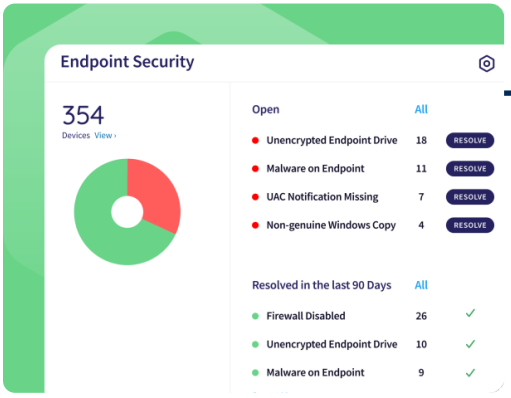
Automatically scan and remediate emails threats, drastically reducing email security management time.

Included Modules:

- Endpoint Security
- Endpoint Detection & Response (EDR)
- Email Security
- Cloud Security

Explore Coro Cybersecurity Modules

Coro modules are self-contained security components that can be turned on or off within the Coro platform. Each module performs as well as, or better than, legacy solutions in its security domain. Our Coro bundles combine multiple modules into affordable cybersecurity solutions.



Endpoint Security

Endpoint Security is the core endpoint module in Coro.

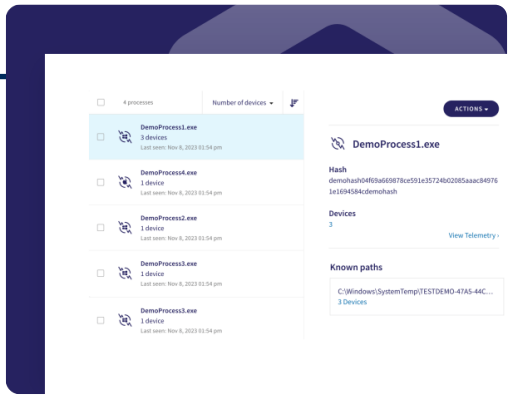
Capabilities:

- Device Posture: Apply policies to users or groups and determine the remediation action for vulnerabilities.
- Next-gen Antivirus: Advanced threat protection (ATP) analyzes both static files and running processes for anomalies.
- Allow/Block Lists: Create lists of files, folders, and processes to allow or block on your protected endpoints.

Endpoint Detection & Response

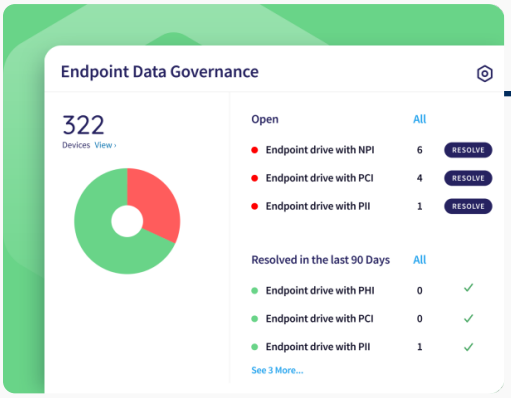
The Endpoint Detection and Response (EDR) module extends your ability to handle incidents as they occur. You can remediate quickly to prevent further damage from known and unknown threat sources and to conduct post-breach analysis.

It continuously monitors endpoint devices and presents these findings in clear, easy-to-manage tabs from the Coro dashboard. Filter through the data as needed, and receive remediation guidance and immediate response actions.



Capabilities:

- Enhanced malicious software detection
- Proactive isolation of infected devices
- Automatic remediation across endpoints



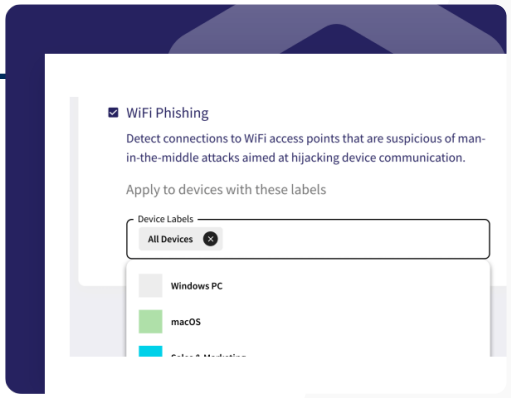
Endpoint Data Governance

The Endpoint Data Governance module protects sensitive data from unauthorized access, use, disclosure, modification, or destruction across endpoints.

To help ensure compliance with these regulatory standards, Coro lets you remotely scan endpoints for:

- PII (personally identifiable information)
- PHI (protected health information)
- PCI (payment card information)
- NPI (non-public information)

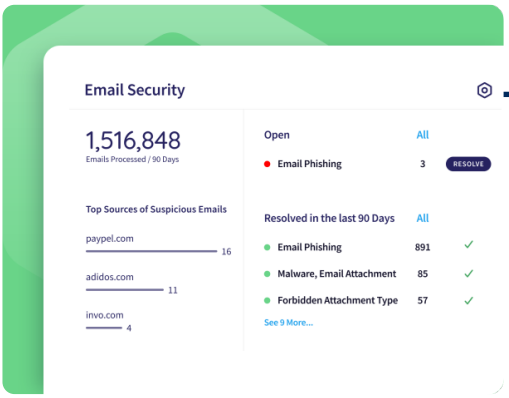
Wifi Phishing



The WiFi Phishing add-on guards endpoints outside the LAN (local area network) by preventing connections to suspicious WiFi access points. It works by detecting connections to WiFi access points that are suspicious of man-in-the-middle attacks aimed at hijacking device communication.

Protects:

- All devices in your workspace
- Specific groups of devices
- Remote/traveling employees



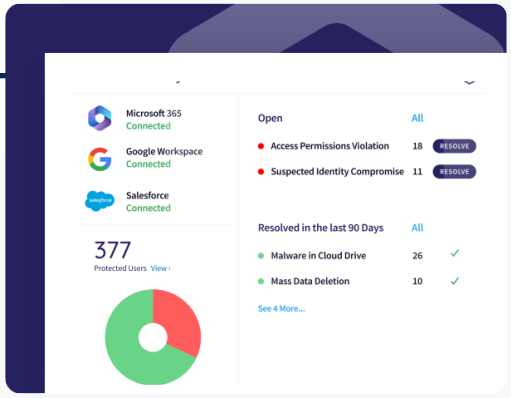
Email Security

Email Security is the core email module in Coro.

Capabilities:

- Malware Scanning: Identify and quarantine emails with potential malware or ransomware attachments.
- Email Phishing Protection: Prevent threats from domain impersonation, spoofing, and other misleading phishing attempts.
- Allow/Block Lists: Create and maintain a list of individual senders or sending domains to allow or block from your business inboxes.

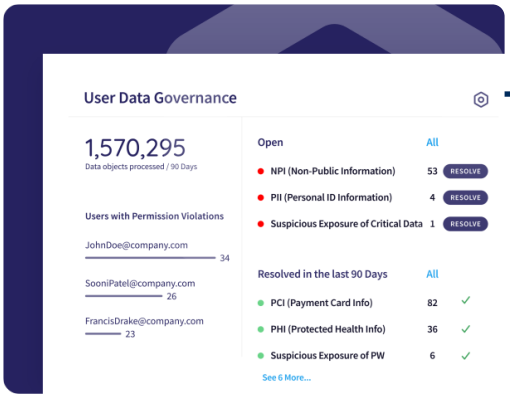
Cloud App Security



Cloud Security is one of the core SASE modules in Coro.
With it, you can stop abnormal admin activity, access violations, ID compromise, malware, and mass data changes in the following cloud apps: Microsoft Office 365, Google Workspace, Slack, Dropbox, Box, and Salesforce.

Blocks:

- Abnormal admin activity
- Malware in cloud drive
- Suspected identity compromise
- Access permissions violation
- Suspected bot attacks
- Mass download
- Mass deletion



User Data Governance

The User Data Governance module helps administrators establish a data handling strategy. Make sure data is only being accessed by by authorized users and maintain compliance to strict regulatory standards.

This module scans emails for unauthorized disclosure of sensitive sensitive data like:

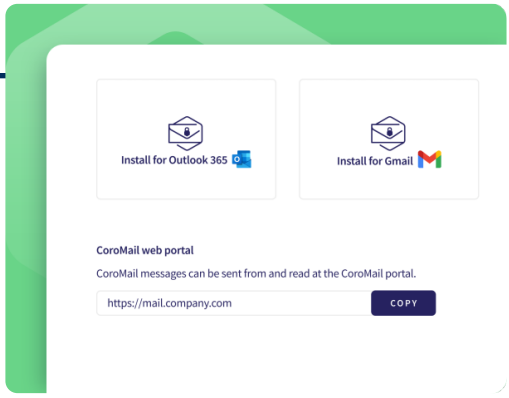
- PII (personally identifiable information)
- PHI (protected health information)
- PCI (payment card information)
- NPI (non-public information)
- Passwords
- Source code
- Certificates
- Custom keywords

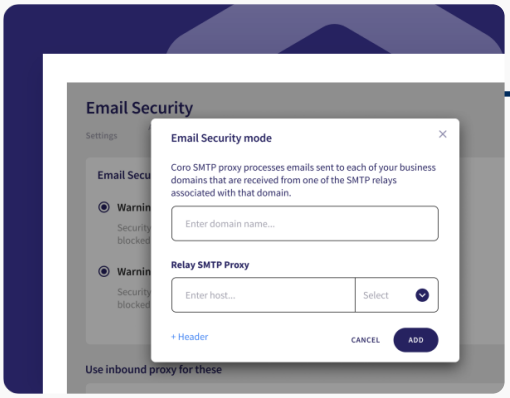
Secure Messaging Encryption

The Secure Messages add-on lets you encrypt outbound emails. With this module, you can use a private key to ensure only the intended recipients to access emails.

Works with:

- Microsoft O365
- Google Workspaces
- Desktop email
- Mobile email apps



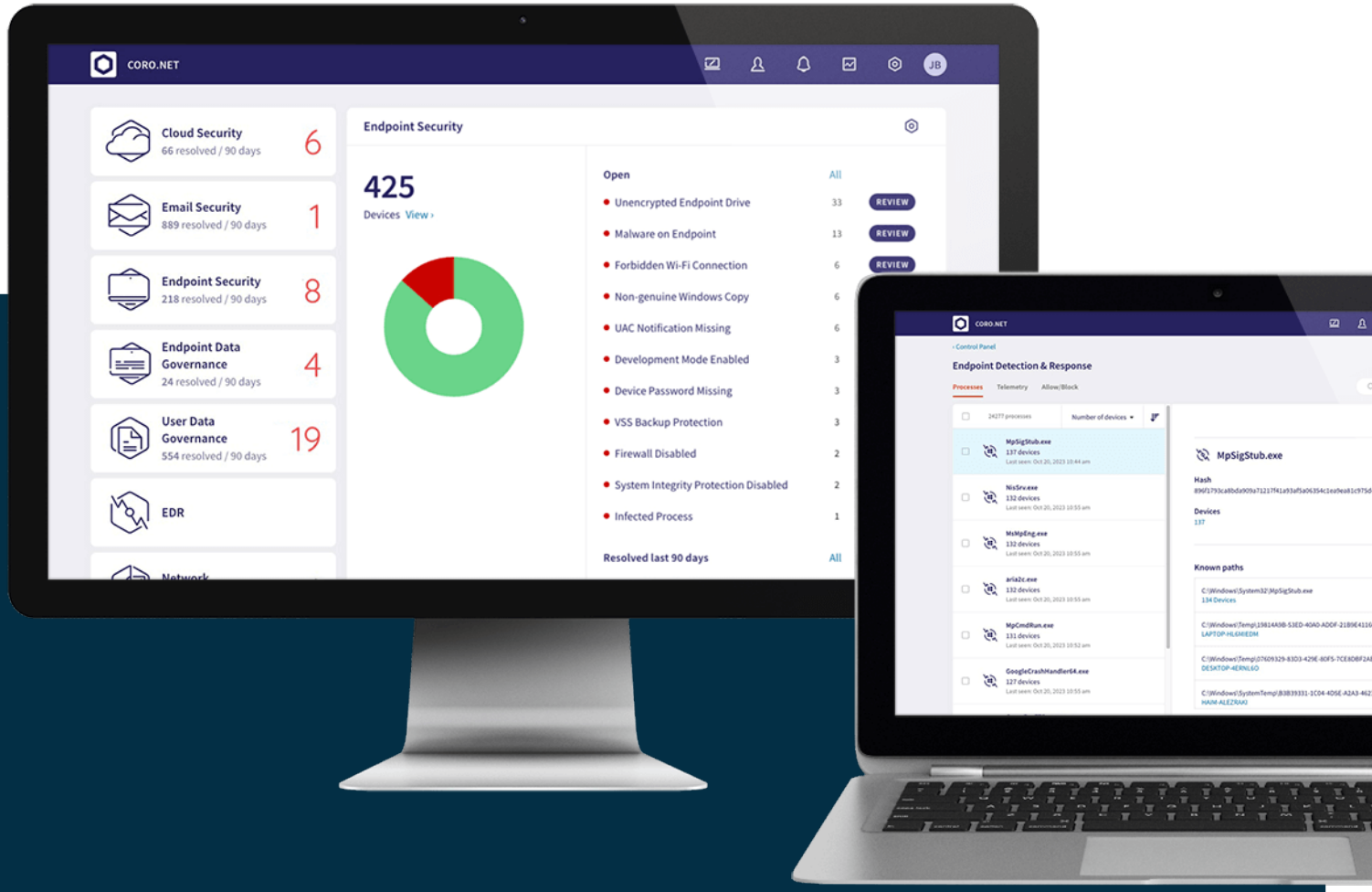


Inbound Gateway

The Inbound Gateway add-on is a proxy that provides real-time detection and protection for incoming emails. It lets you intercept inbound emails and inspect them, allowing only threat-free or trusted emails to reach recipients.

You can choose between the following for suspicious emails:

- Warning Only: Emails are not blocked but are marked with explanatory warnings for the recipients
- Block: Emails are blocked and can only be released from quarantine by workspace administrators
- Allow/Block Lists: Create and maintain a list of individual senders or sending domains to allow or block from your business inboxes.



Peace of Mind is Within Your Reach

Connect your business to Coro with a click. Enjoy immediate detection of threats and vulnerabilities for your entire business. Talk to an expert about your needs.

Try Coro for Free for the Next 30 Days

- See how much time you could save with Coro guarding your business:
- Instantly handle 95%+ of email threats
- Monitor cloud security from a single dashboard
- Protect devices across the threat landscape
- Prevent data loss with a deceivingly simple solution
- No Credit Card Required. Easy to upgrade to our unified platform any time during or after your trial

Adaptiv Networks Solutions

Smart, secure business networks that deliver superior cloud performance with the simplicity of a managed service.

CLICK HERE TO TALK TO AN EXPERT

adaptiv-networks.com | sales@adaptiv-networks.com