



DATA SECURITY, POWERED BY CORO

Cybersecurity, Simplified

Data Security & 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 built for SMEs with lean IT teams. Simply choose the Coro cybersecurity suite that combines the right modules to fit 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 address your most pressing security needs.

CORO AI 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 App Security
- Secure Messages
- Inbound Email Gateway
- Wifi Phishing

CORO AI ENDPOINT

Log all endpoint activity, analyze data anomalies, and automate resolution of most security incidents.

Included Modules:

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

CORO AI COMPLETE

Get Coro's full range of security modules for comprehensive coverage and automatic incident resolution.

Included Modules:

- Endpoint Security
- Endpoint Detection & Response (EDR)
- Endpoint Data Governance
- Wifi Phishing
- Email Security
- Inbound Email Gateway
- Secure Messages
- User Data Governance
- Cloud App Security
- Network Security
- Secure Web Gateway
- Mobile Device Management
- Security Awareness Training

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 suites bundle multiple modules together into affordable cybersecurity solutions.



Endpoint Security

CAPABILITIES:

- **Device Posture:** Sets device policies according to device vulnerabilities
- **Allow/Block Lists:** Creates allowlists and blocklists for files, folders, and processes to reduce tickets triggered by unknown activities
- **Advanced Threat Control:** Blocks any processes that exhibit suspicious behavior
- **Scheduled Malware Scans:** Schedules daily, weekly, or off-hours malware scans on Windows, macOS, and Linux agents
- **Multilingual Support:** Provides additional support for Spanish, Italian and French

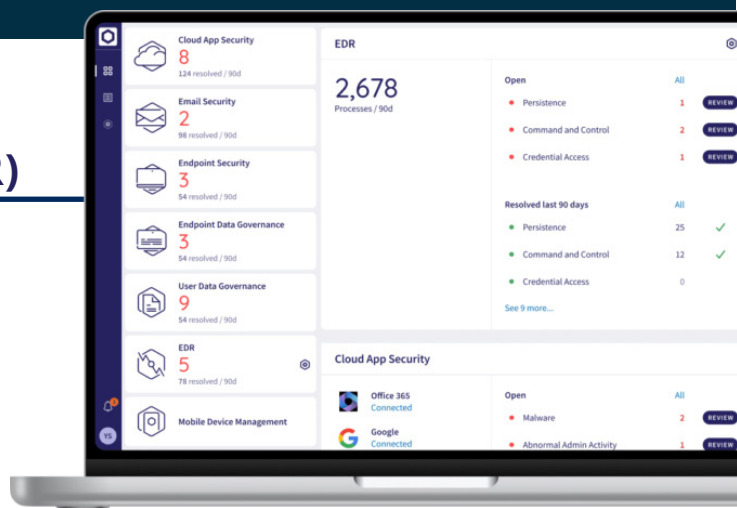
Safeguard endpoint devices and protect your business with the **Coro Endpoint Security** module. It automatically identifies and logs all devices, scanning for malware, suspicious activity, and human errors. The Endpoint Security module detects unusual behavior and neutralizes threats before they can cause harm.

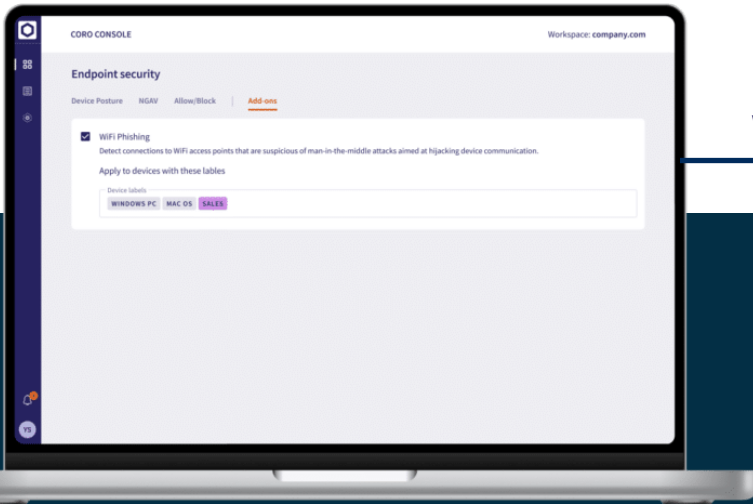
Endpoint Detection & Response (EDR)

CAPABILITIES:

- **Telemetry Tab:** Collects and organizes forensic details from devices
- **Process Graph:** Visualizes process lineage and parent-child relationships to trace threats
- **Process Tab:** Displays an aggregated view of all executed processes

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.





Wifi Phishing

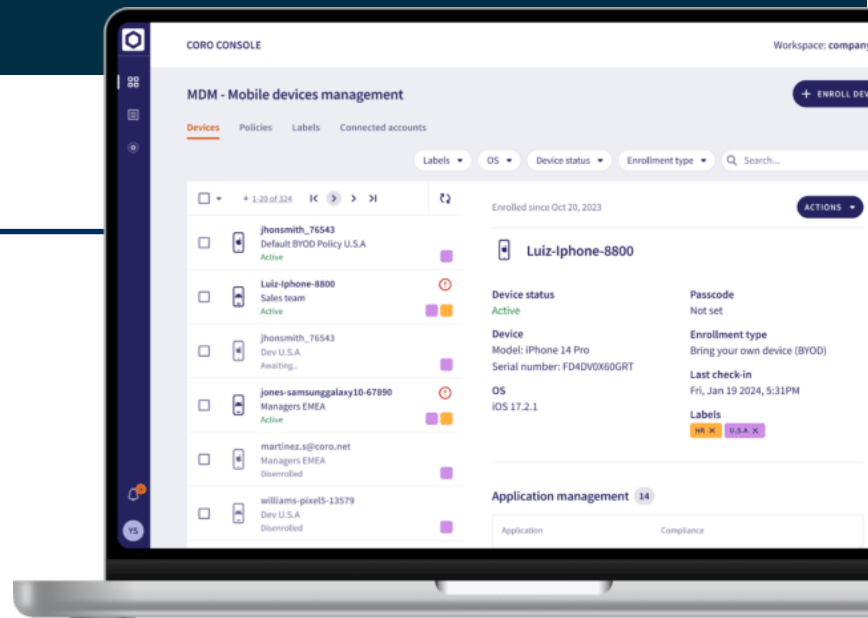
PROTECTS:

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

The **Coro 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.

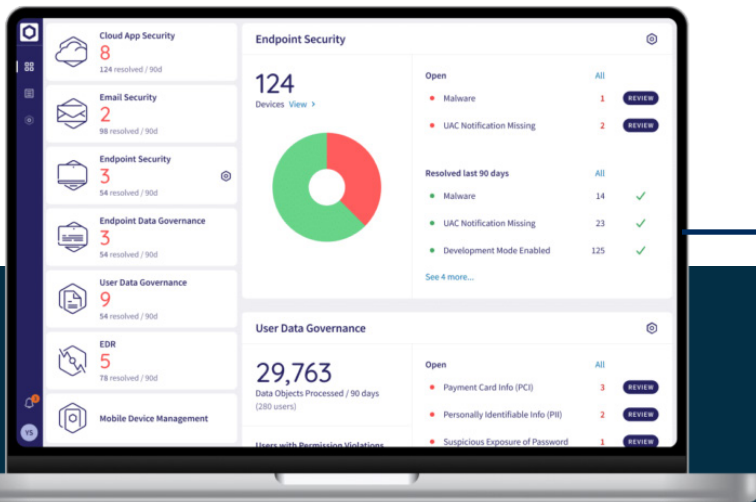
Mobile Device Management

Coro's **Mobile Device Management (MDM)** module simplifies the management and security of company-owned and Bring Your Own Device (BYOD) work-related mobile devices. It enables IT teams to enforce app policies, manage apps, and ensure company policy compliance. The module gives visibility into mobile devices, ensuring efficient device management across the organization.



CAPABILITIES:

- **iOS and iPadOS Device Enrollment:** Enrolls devices via DEP or through MAID
- **Application Policy:** Defines and enforces rules for app use, including install/remove restrictions, blocking in-app purchases, and locking system defaults
- **Lost Mode:** Locks supervised devices, shows custom contact info, and tracks location when powered on
- **Remote App Installation:** Installs required apps on employee devices directly from the console
- **Device Management:** Remotely wipes data from compromised devices, marks devices for disenrollment to remove profiles and policies, and removes devices that are inactive or disenrolled
- **Multilingual Support:** Provides additional support for Spanish, Italian and French



Email Security

CAPABILITIES:

- **Outbound Gateway:** Enables real-time monitoring and blocking of outbound emails that violate an organization's sensitive data policies
- **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
- **Allow/Block Lists:** Defines trusted senders or blocks specific domains to control access
- **Multilingual Support:** Provides additional support for Spanish, Italian and French

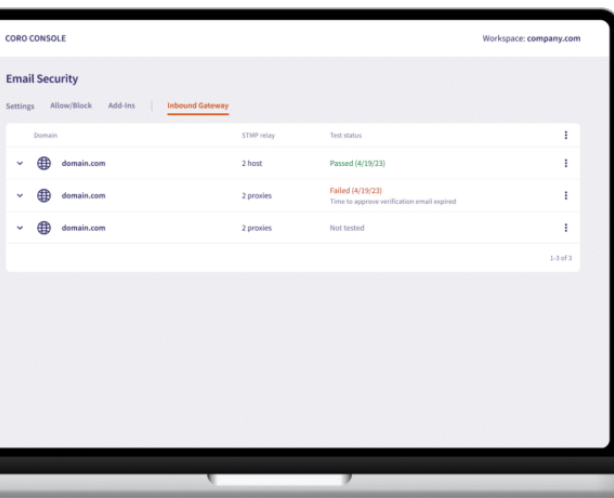
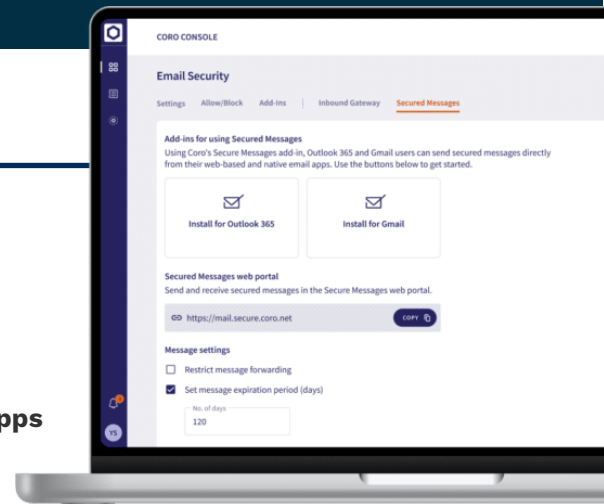
Experience advanced email protection that safeguards your business against data leaks and social engineering attacks with ease. Powered by Coro's intelligent engine and Large Language Models (LLMs), the **Coro Email Security** module automatically monitors, detects, flags, prioritizes, quarantines, and remediates the most advanced threats. Leveraging advanced LLMs increases phishing attack detection accuracy and strengthens the system's capabilities.

Secure Messages

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

WORKS WITH:

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

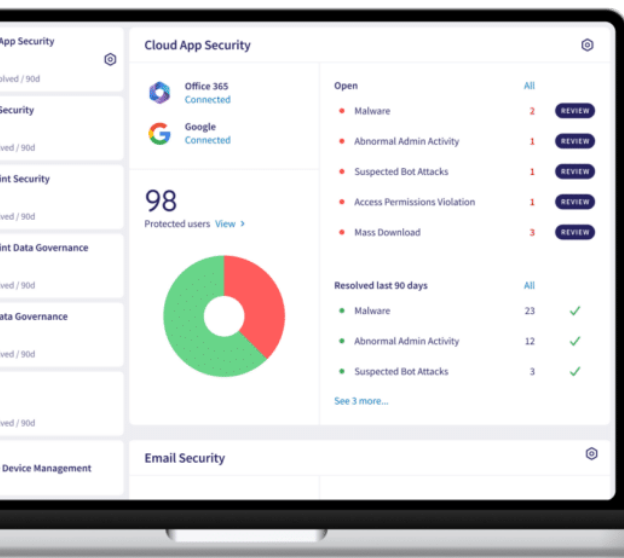


Inbound Gateway

The Coro 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



Cloud App Security

CAPABILITIES:

- **Cloud Applications:** Connects, monitors and controls a range of cloud apps: Microsoft Office 365, Google Workspace, Slack, Dropbox, Box, and Salesforce
- **Access Permissions:** Allows admins to set permissions for specific groups, specific users, or all users, with access restricted by country or IP
- **Impossible Traveler:** Detects login attempts from distant locations in unrealistically short intervals, helping identify potential credential compromise or unauthorized access
- **Dedicated “Quarantine” Folder:** Stores detected malicious files in the “Suspected folder” and creates a ticket for the event
- **Third Party Applications Tab:** Lists and manages third-party apps connected to MS 365 and Google Workspace, offering control and visibility into app usage within the organization

Coro’s **Cloud App Security** module provides advanced malware detection and robust remediation capabilities to protect users, their cloud drives and apps. By securely connecting cloud applications, Coro ensures monitored, protected, and controlled user access, enabling businesses to safeguard data and apps against a wide variety of threats.

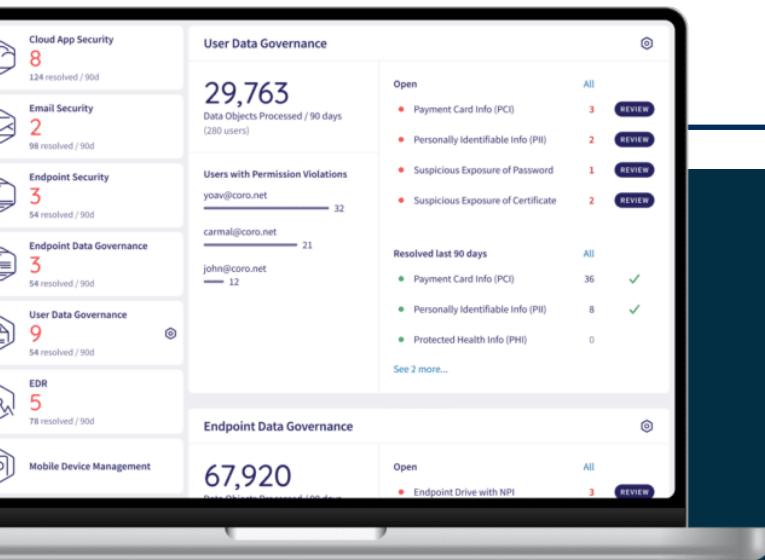
Endpoint Data Governance

Coro’s **Endpoint Data Governance** module protects sensitive and critical data on endpoint devices. It monitors how data on these devices is stored, detecting and preventing unauthorized use, accidental loss, risky data sharing, or violations of data protection policies. Endpoint Data Governance comes pre-configured with baseline security policies and ensures endpoint devices comply with data protection policies from day one.

CAPABILITIES:

- **Regulatory Data Configuration:** Enables the configuration of various sensitive data types, such as PHI, PCI, PII, and NPI, ensuring compliance with data protection laws
- **Manual Scanning:** Provides the ability to perform on-demand scans from the Coro Console of endpoint devices to check for sensitive data exposure (e.g., PHI, PCI, PII, NPI) and mitigate risks in real-time
- **Scheduled Scans:** Admins can schedule automated scans on endpoint devices to check for sensitive data stored on storage drives, ensuring continuous protection and early detection of potential risks





User Data Governance

CAPABILITIES:

- **Outbound Gateway:** Enables real-time monitoring and blocking of outbound emails that violate an organization's sensitive data policies
- **Regulatory Data Configuration:** Enables the configuration of various sensitive data types, such as PHI, PCI, PII, and NPI, ensuring compliance with data protection laws
- **Continuous Monitoring:** Monitors and scans unusual data-sharing activities that might expose sensitive data (PHI, PCI, PII, NPI) via email or file-sharing
- **Access Permissions:** Allows administrators to control user access to sensitive data by setting specific permissions for individuals, groups, or domains
- **Exclusions:** Allows administrators to exclude emails from sensitive data scans based on specified keywords in the subject line

The Coro **User Data Governance** module enables businesses to detect unauthorized sharing or access of sensitive data. Through continuous monitoring of user behavior and data exposure, it ensures that sensitive data such as personal details, health records, and payment information is only accessible to authorized individuals and compliant with data protection regulations such as GDPR, HIPAA, and PCI-DSS.

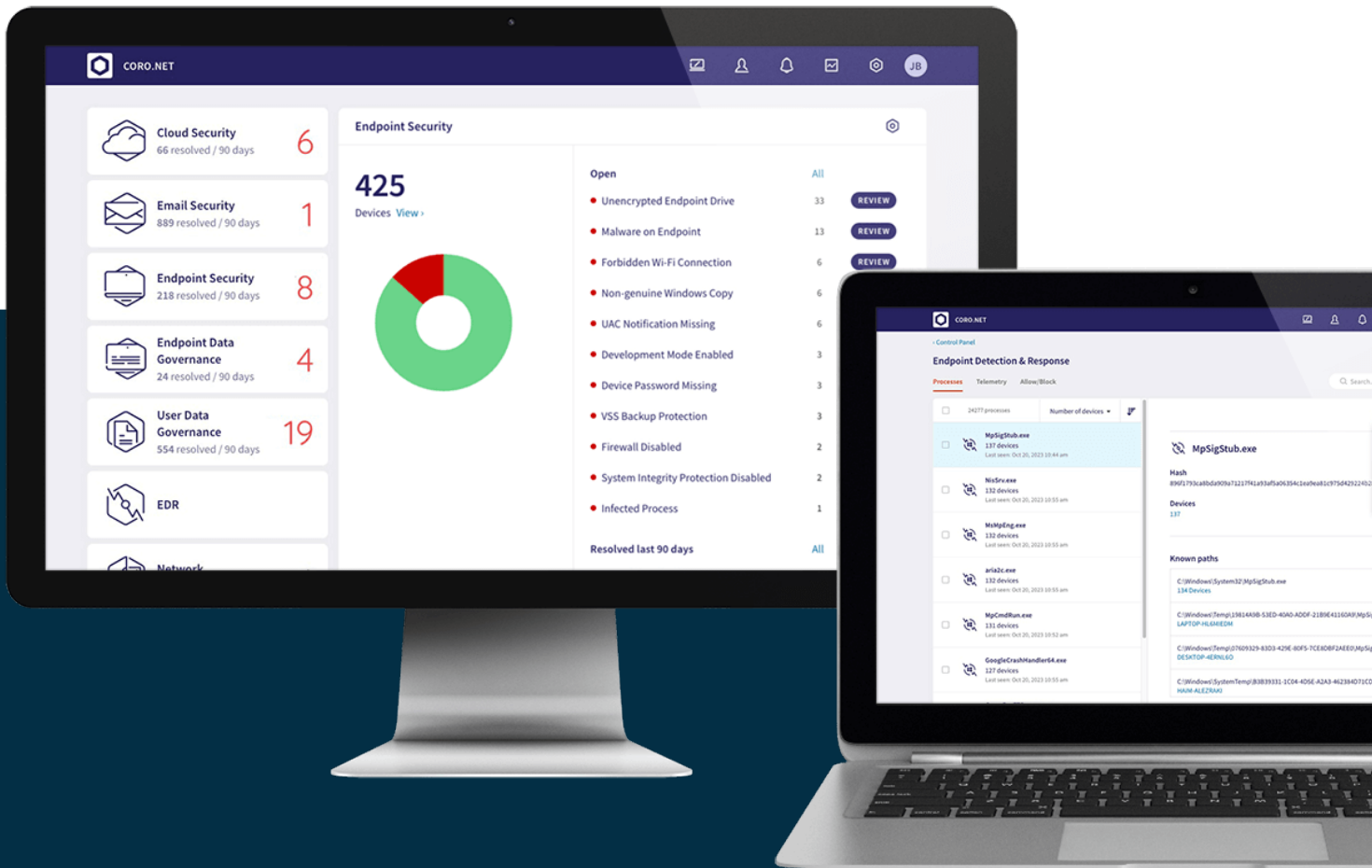
Security Awareness Training

Coro's **Security Awareness Training (SAT)** module empowers leadership, employees and contractors with the knowledge and tools to recognize phishing and social engineering attacks. SAT reduces human error and strengthens your cybersecurity posture through real-world phishing simulations and high-quality security awareness training. Using SAT shows that your business has proactively implemented security awareness measures, mitigating legal, financial, insurance, and reputational risks while safeguarding your organization and leadership.

CAPABILITIES:

- **Phishing Simulations:** Simulates phishing attacks to assess vulnerabilities and raise awareness
- **Adaptive Training:** Uses adaptive training to personalize learning based on security risks and user behavior
- **Training Courses:** Delivers focused courses on best-practice cybersecurity via videos and quizzes
- **Reporting:** Delivers powerful analytics including simulations engagement, phishing failure and training completion rates





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 deceptively 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.

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

TALK TO AN EXPERT