Coro protection

Coro provides unified modular security for business workspaces, safeguarding against malware, ransomware, phishing attacks, and human error. Coro achieves this by actively monitoring access, activity, and protection across:

- Cloud applications
- Email accounts
- Users
- Devices
- Sensitive data

Coro runs on an intelligent model that leverages heuristic analysis techniques to identify risk and threats to an organization's data infrastructure by 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% for manual review by administrators. All actions are backed up with a detailed activity and event log.

Modular protection

Coro utilizes a modular approach to providing cybersecurity protection for customers. Each **module** is its own standalone cybersecurity feature (for example, security for email), and can be activated separately, or in addition, to all other modules in the Coro platform.