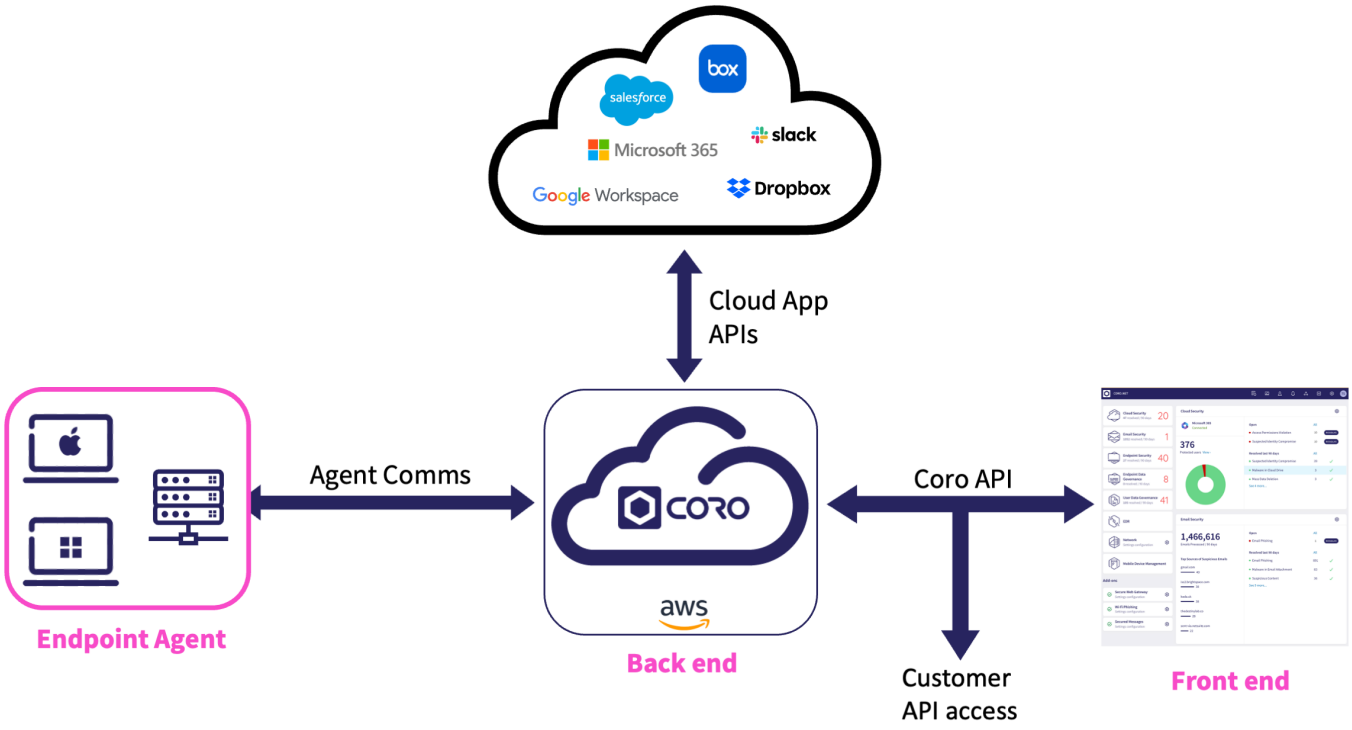
Introducing the Coro Agent

The Coro Agent provides protection for Windows and macOS endpoint devices.

The Coro Agent communicates with the Coro Backend service by providing monitoring data from devices and receiving instructions in cases where automated remediation is not enforced. The Coro Agent is autonomous and functions independently of whether or not connectivity to the Coro service is available at the time.

The Coro console (Frontend) connects to the Backend via a private API and controls information and commands transferred to and from cloud apps and Coro Agents to the Backend. These three components form the basis of the Coro cybersecurity platform.



The Coro Agent operates similarly to other antivirus applications: it compares the hashes of downloaded files to public databases of previously checked viruses; if they match, Coro quarantines the file. Additionally, the Coro Agent can identify system vulnerabilities. For example, it verifies that the computer is protected by a password and that **Developer Mode** remains disabled, see **Device posture configuration overview**.

Ensuring device protection is critical, especially as compliance requirements often mandate encrypting all internal and external device drives used within an organization. The Coro Agent, through policy definition in the Coro Console, actively aids organizations in monitoring, protecting, and ensuring compliance for the endpoint devices utilized by their employees.