Telemetry

The **Telemetry** page collects and aggregates various types of monitored forensic information from devices, which users can use to conduct malware-related investigations more efficiently.

> **Note**
>
> If a device loses network connectivity or the Coro agent is inactive, Coro EDR preserves your telemetry data. This saved data becomes accessible once the device re-establishes connection or the Coro agent resumes operation.

Telemetry is built from:

- **macOS logs**: macOS uses the application console to collect logs generated by your macOS device. Account activity logs collected in the application console are crucial for diagnosing device issues and potentially malicious user account activity.
- **Windows event logs**: The Windows event log is a comprehensive and chronological record of system, security, and application notifications stored by the Windows operating system, which network administrators use to diagnose system problems and predict future issues.

  For *Windows* devices, when **Tamper Protection** is enabled, Coro EDR safeguards against malicious attempts to disable the Windows Event Viewer, which is critical for gathering Windows event log telemetry data.

  When a malicious process disables the Windows Event Viewer, The Coro agent immediately restarts the service, and the following notification appears: