

as a Windows service in this mode, but as a standalone console application.

The Host Component

This small host component is written in C++ and runs as a service on a Windows server. Its role is to take requests from the admin console and respond to those requests. Valid requests include getting information about host component version, and recursive and non-recursive file properties. Note that the host software performs no analysis; it sends raw integrity data (filenames, sizes, hashes, ACLs, and so on) to the admin console, which performs the core analysis.

The Admin Console

The admin console code stores and analyzes resource (file, registry) version information that comes from one or more host processes. A user can instruct the admin console to connect to a host running the iNTEGRITY host software, get resource information, and then compare that data with a local, trusted data store of past resource information to see if anything has changed.

The iNTEGRITY Data Flow Diagrams

The iNTEGRITY data flow diagrams are shown in Figures E-5 and E-6.

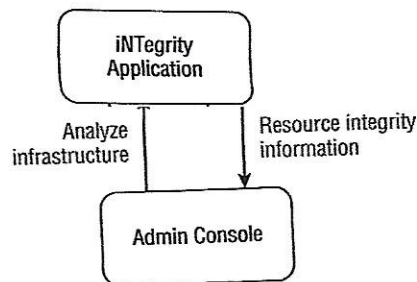


Figure E-5: Context diagram

NOTE The iNTEGRITY example comes from a time when the standard advice was to create a *context diagram*, which can be helpful when an external threat modeling consultant is being used, acting as a forcing function to consider the scope and boundaries of the threat model.