Management overview of Corporate installation for the Locklizard Viewer

The Locklizard Safeguard PDF Viewer is an application dedicated to processing DRM protected PDF documents that have been encrypted into a proprietary (PDC) format.

The authenticity of the application code is secured in a number of ways. Locklizard use standard code signing technology so that installers may be confident that the application they are installing has been released by Locklizard and has not been infected with malware or other code to perform unauthorized exploits of the computer(s) it is installed on. We avoid plug-in methods because they are open to compromise from other plug-ins, may cause conflict with other plug-ins, cannot be validated, and require the same level of administrator privileges as any other type of installation without returning useful control benefits. We also incorporate a number of features to prevent code attack, code alteration and memory handling in order to prevent run-time alterations that might prejudice the operation of the code.

The Safeguard Viewer will only 'open' documents prepared in the Locklizard proprietary format, which is recognized by the file extension of .pdc. Files that are given that extension, but do not pass cryptographic control tests will be rejected (this includes .pdc files that have been altered in any way). The Viewer does not have any 'Save' or 'Save As' features, so it does not have the ability to create new or 'fake' documents as part of its operation.

In order to support corporate IT installers, Locklizard provide an MSI install as well as the conventional .exe package. And there are a number of important features to support push type installation models:

- silent options;
- ability to install user license during the application install;
- ability to forbid automatic updates so updates can be coordinated as part of the desktop update cycle;
- no need to carry out local installation steps as a sys admin.

For technical installation details please see the Safeguard Viewer product manual.

The Safeguard Viewer also does not allow the inclusion of JavaScript as a part of the initial pdf format and does not implement features that would allow the execution of JavaScript when the Viewer runs. This automatically prevents typical attacks mounted through PDF documents.

There are occasions where the Viewer needs an Internet connection, either on Port 80 or 443, to connect to the Administration Server of the secure document publisher (this may be a site on the corporate network for internal control systems). The first is when the Viewer account is registered with

the publisher, when licensing data for the machine on which the Viewer is installed is transferred (the external IP and Mac and a 'random' number) so that subsequent license verification can check that only the duly licensed machine (associated with a 'user' account) is being used. This registration is logged by the publisher's licensing server.

The Viewer will also contact the publisher's licensing server when a document is opened for the first time. This is to verify that the document has been licensed for use by that publisher, and if approved, information required to decrypt the document is then transferred secretly from the server to a local control file keyed to the licensed machine. These connections are mandatory for the operation of the system.

A publisher may also have specified that a license has to be checked again on a periodic basis, varying from every time a document is opened, to never after the first time. Often internal control systems validate every use to ensure that the user is part of the internal network. Server connections will be required accordingly. The same goes if the making of a limited number of printed copies is allowed (but not if infinite copies are allowed). The publisher may, if using our Enterprise edition, monitor these events (in other words the server will log the fact of the inquiry being made for a view or print associated to the licensed machine).