

**Product Hardening and Security Information**

This document describes the hardening and security properties of the SecureSphere technology. The SecureSphere product suite can be licensed in various forms, but consists of the same software and code base. The SecureSphere products are also distinguished by functional roles. The first type is called, MX Management server, this product provides the operator interface (GUI) and provides centralized management of the second type, the Gateway. Gateways receive configuration updates from the MX and perform the analysis and inspection of traffic. A MX is capable of managing multiple Gateway instances.

Imperva has taken steps to ensure that both solutions are secure and hardened. In addition, to meet federal and local government standards, SecureSphere has applied, tested and received national standards certifications. Imperva’s SecureSphere has achieved Common Criteria Certification. SecureSphere appliances have achieved an Assurance Level of EAL2 and conform to the platform evaluation criteria set forth by NIAP. A copy of our certificate can be found in the link below.

<http://www.niap-ccevs.org/cc-scheme/st/st_vid10238-ci.pdf>

Imperva has also taken proactive steps to ensure additional security of its products. These processes include the use of a hardened operating system. Imperva has performed the following measures to protect SecureSphere gateways and the MX Management server from attack:

* Removal of unnecessary services
* Closure of unnecessary ports
* Application of strict permissions on files and internal users
* Application of all patches to internal components
* Addition of an internal firewall to protects the system

Communication between SecureSphere solutions, Gateway and MX, are SSL encrypted. Management access is limited to secure connections only. SecureSphere GUI access also supports client certificates for two-factor authentication and/or Active Directory integration for authentication.

Imperva's internal assurance teams subject SecureSphere to a broad range of security vulnerability, stress and performance tests.  Pentest tools include Paros, Achilles and internally developed test programs to ensure the most secure posture.

Proprietary and Confidential