SecureSphere Platform Security

Overview

This document describes the significant security measures taken by Imperva to protect the platform common to the SecureSphere Web Application Security, File Security and Database Security product lines. The information provided in this document is applicable to SecureSphere version 8.5 and above.

Architecture of the SecureSphere Platform

The component designated as SecureSphere Platform is the core system of all the SecureSphere data security products. The platform is composed of Hardware or Virtual Appliances which host a Linux based embedded Operating System. This infrastructure is common to the SecureSphere Management Server and the SecureSphere Gateways. The Management Server also includes an embedded Oracle database server and a Java based Web Application Container.

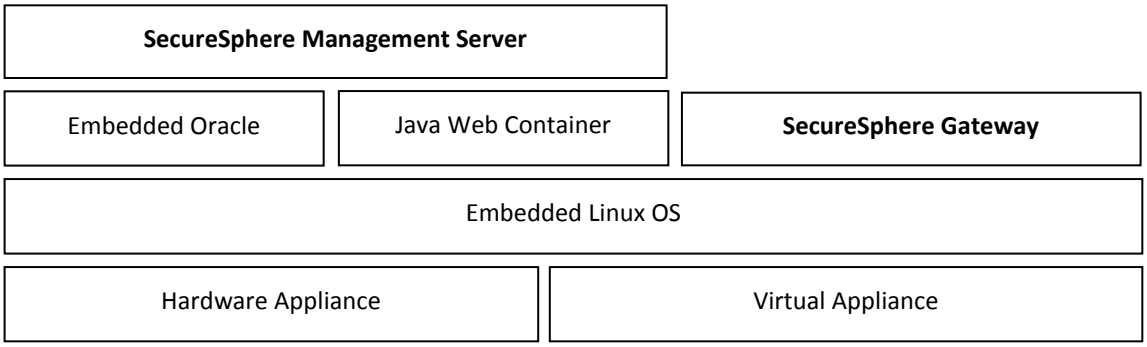

Figure 1 – SecureSphere Platform Architecture Stack

Operating System Hardening

Packaging

The SecureSphere Linux OS is derived from the CentOS Open Source project. While CentOS is normally packaged to run as a fully functional Linux server, Imperva has created a custom stripped-down version of the OS to safely run the SecureSphere functions and no others. As such, the SecureSphere Linux OS is unable to provide the usual desktop or server services of Linux machines.

Note: The SecureSphere appliances are network devices and must be administered as such by the IT and Security operations teams. Patch and other software updates are provided by Imperva, OS level configuration changes must be done following the guidelines of Imperva Support.

Network Access

The SecureSphere appliances offer minimal network access, all Linux network services are shutdown by default or protected by host-based firewall policies called 'portguard'. The only TCP ports that remain open are: 22 for remote SSH login, 8083 for management server access and 443 for management to gateway communications. SSH access by the root user is prohibited, for remote access a named account creation is required during the installation process. Access to the gateway communication port is restricted via login/password which can be changed by a CLI administrator.

On our Management Server appliances, access to the Web administration interface on port 8083 is also restricted by login/password initially defined at installation time. Access to the embedded Oracle server is local only, the embedded Oracle server cannot be accessed from the network, and data on this server cannot be modified by any other means than through the SecureSphere GUI or CLI.

All SecureSphere appliances provide an alternate network management NIC which enables an out-of-band deployment of the device. Such deployment is recommended when the network communications between the SecureSphere devices must be isolated from the management network. OOB deployment is documented in the SecureSphere Administration Guide.

User Accounts and Passwords

The OS or CLI user accounts are created locally on each SecureSphere appliance. CLI accounts are not of common use for day-to-day operations and should be limited to SecureSphere administrators who must perform sensitive platform level configuration changes. All the most common SecureSphere management functions are performed through the Management Server web interface which relies on a separate user repository and connects to external authentication systems such as Radius or LDAP.

By default SecureSphere enforces a strong password policy on every user account including password complexity requirement, validity period, and brute-force protection via temporary lockout. The details of the password policy are described in the SecureSphere Administration Guide.

Encrypted Communications

SecureSphere uses FIPS-certified encryption modules to perform cryptographic operations within the cryptographic boundary. The cryptographic modules used by SecureSphere are compiled and operated in FIPS mode and perform the appropriate self-tests at initialization. The details of the FIPS and encryption considerations are documented in the SecureSphere Administration Guide.

Oracle Database

The SecureSphere Management Server (MX) embeds a local Oracle database server, the following measures are taken to strengthen the security of this components:

- All network access to Oracle is prevented by the host-based firewall of the OS i.e. Only connections coming from the loopback interface are allowed.
- All administration and management services are disabled, the only possible way to interact or configure with the Oracle database if via the command-line through an OS administrator account.
- All default accounts, logins, schemas are disabled or removed.
- The Oracle version is frequently updated through SecureSphere version upgrades or patch updates.
- Every vulnerability and CVE reported by Oracle is analyzed by an Imperva Security Researcher who determines if the vulnerability is applicable to SecureSphere (see Vulnerability Assessment below)
- The Oracle server is installed but disabled on any appliance which does not require it.

Vulnerability Assessment

Internal Penetration Testing

During the development cycle of every SecureSphere version, Imperva performs a security scan of all the platform components. The scan includes a port scan to verify that no unexpected service is reachable remotely, a web vulnerability assessment scan and an OS scan following the DISA STIG guidelines. Every finding reported by the scanners is manually verified by an Imperva Application Defense Center expert. During this analysis, the Imperva ADC expert determines whether the finding has any actual impact on the security of the platform, and provides guidelines for software correction prior to the release of the product.

External Penetration Testing

At least once a year, Imperva contracts an external security firm to perform a penetration testing of our SecureSphere appliances. Findings are reviewed and inserted into our product development plans similarly to those of the Internal Penetration Testing effort.

Third-Parties Vulnerability Tracking

Our Imperva ADC team monitors every published security advisory on a weekly basis for all external facing SecureSphere components. Each relevant vulnerability is analyzed and documented by an ADC expert who qualifies the requirement for remediation via a software patch or through a subsequent SecureSphere product release.

Note: 3rd-party components of the SecureSphere platform may be reported as vulnerable by a scanner, it does not mean that SecureSphere is vulnerable! It is with a deep understanding of the configuration of each package, program and library that our experts review and determine if the security of SecureSphere is impacted or not. In such cases, our Imperva Support teams are available to answer any questions regarding a reported platform vulnerability.

Certifications

ICSA Web Application Firewall

In 2012, Imperva received ICSA Web Application Firewall Certification for SecureSphere Web Application Firewall. As part of the ICSA Labs' WAF Certification process, analysts evaluated SecureSphere in six categories: documentation, administration, vulnerability testing, persistence, functional security and logging. In addition, SecureSphere was subjected to a battery of sophisticated attacks and penetration attempts.

Common Criteria EAL 2+

In 2009, Imperva achieved Common Criteria Certification at Evaluation Assurance Level 2 (EAL 2). The certification of SecureSphere version 9 is estimated to complete by end of January 2013. Common Criteria certification, or ISO 15408, is recognized as the gold standard by which U.S. government organizations, international government entities, and global enterprises evaluate and select IT security products. Internationally, Common Criteria validation is accepted through the Common Criteria Recognition Arrangement (CCRA) and products with certification carry an unbiased, third-party validation of their functional capabilities and an assurance that they meet strict IT security, reliability, and quality standards.