

# Application Security

[Return to Glossary](#)

**Application Security** is the [Business Process](#) of developing, adding, and testing security features within applications to prevent security [Vulnerabilities](#) against cyberthreats such as unauthorized access and modification.

Application Security describes security measures in the [Application](#) that aim to prevent data or code within the Application from being stolen or hijacked. It encompasses the security considerations that happen during application development and design, but it also involves systems and approaches to protect Applications after deployment.

**Application Security** may include [Hardware \(H/W\)](#), [Software \(SW\)](#), and [Business Processes](#) that identify or minimize security [Vulnerabilities](#). A [router](#) that prevents anyone from viewing a computer's [Internet Protocol Address \(IP Address\)](#) from the [Internet](#) is a form of hardware **Application Security**. But security measures at the [application](#) (**Note:** NOT to be confused with OSI [Application Layer](#) or the [TCP/IP Conceptual Model](#) Application Level) are also typically built into the software, such as an [Application firewall](#) that strictly defines what activities are allowed and prohibited. Business Processes can entail things like an **Application Security** routine that includes protocols such as regular testing.

Source: <https://www.vmware.com/topics/glossary/content/application-security>

From:

<https://www.omgwiki.org/dido/> - **DIDO Wiki**

Permanent link:

[https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:xapend:xapend.a\\_glossary:a:applicationsecurity](https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:xapend:xapend.a_glossary:a:applicationsecurity)

Last update: **2022/01/19 11:12**

