

SHARED RESPONSIBILITY FOR ON-PREMISES

WHITEPAPER

July 2025

© 2025 Software AG. All rights reserved.

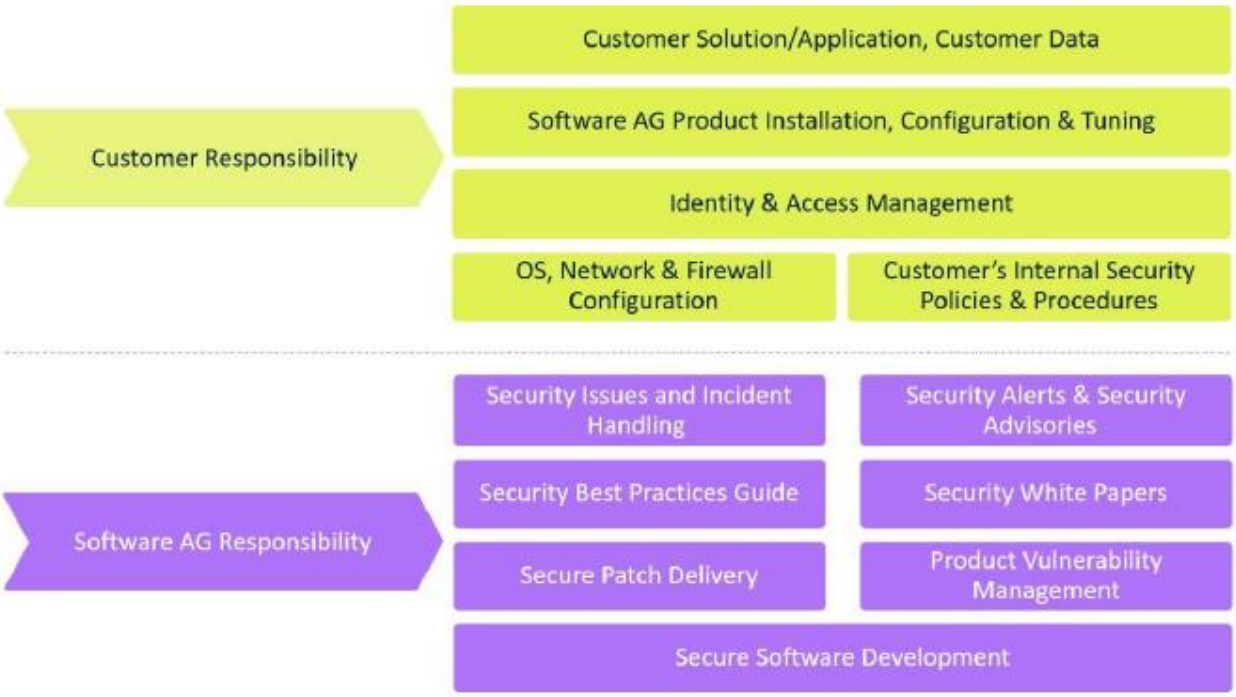
softwareAG
A SOFTWARE GMBH BRAND

1 Introduction

In the digital world with the raising vulnerabilities every day, there remains confusion about the split of responsibility between product vendors and their customers. This document provides a shared responsibility model that dictates and defines certain responsibilities for Software AG and its customers to ensure accountability.

Each party (Software AG and the on-premises customer) is accountable for different aspects and must work together to ensure full coverage. In this model, ownership is clearly defined, with each party maintaining complete control over those assets, processes, and functions they own.

The following chart shows the shared responsibility model and depicts how the various responsibilities are shared and controlled by Software AG and its customers.



© 2025 Software GmbH. All rights reserved.

2 Software AG Responsibility

Software AG is responsible for delivering secure products and its shared responsibilities are:

2.1 Secure Software Development & Release

Software AG has established a secure software development methodology for creating software that incorporates security into every phase of the software development life cycle and software releases.

The security practices adopted to deliver secure software are defined by the processes such as Compliance Assessment, Security Training, Secure Design and Implementation, Supply Chain Security Assessment, Automated security assessment, Security Penetration Testing, and Secure Quality Release Standards.

The integrity of the software delivered to the on-prem customer is ensured by following the process:

- Only authenticated users can download from Software Download Center.
- On downloading the SAG installer, SUM, the customer can check the integrity by SHA checksum provided.
- The integrity of the build modules or product artifacts downloaded by the Installer or SUM is internally verified before the install/update process.

2.2 Security best practices guide

The Product Security Best Practices document provides a set of best practices to ensure that the deployment of the product in the customer environment is configured most securely.

2.3 Security White Papers

Software AG periodically updates and shares new security policies, standards, and processes adopted to the customer through the security whitepapers and security technical documents published on Empower.

2.4 Security Alerts & Advisories

Software AG keeps the customers informed about every aspect of security pertaining to the organization and its complete range of products through the Alerts and Advisories subscription.

On subscription, customers receive “early warnings or alerts” updating them on the availability of fixes for the vulnerabilities reported in Software AG products. Customers are recommended to

© 2025 Software GmbH. All rights reserved.

subscribe for Security advisory notifications, so that they get informed about the latest updates as soon as they are published.

2.5 Security issues & incident handling

For reported security issues, Software AG is responsible for identifying and fixing the security vulnerabilities in the application. Patch updates comprise a collection of updates, fixes, or enhancements for software, delivered in the form of a single installable package.

2.6 Product vulnerability management

Software AG internally uses CVSS3.X scoring system for assigning priorities to ensure that the security flaws are handled with adequate priority. The security fixes are released with limited information along with standard fix packs to avoid disclosing sensitive information to the public.

The internal policy and processes ensure backporting and forward porting of security defects to all the affected versions within the internally defined scope.

3 On-Premises Customer Responsibilities

For on-premises product deployments, the customer is solely responsible for security on-premises and all aspects of the product-installed systems.

3.1 Secure Platform, Application, Identity & Access Management

The customer is responsible for managing access to applications, platform security updates, and configuring access to Software AG product applications/ services, by configuring access such as Single Sign-On access, adding/ deleting users, reviewing, implementing logical access security measures.

- Responsible for managing the appropriate access (credentials, roles) for their users.
- Integrating with their Identity Provider for Single Sign-On (SSO) and/or Multi-factor Authentication (MFA).
- Responsible for adding or removing users.
- Managing the appropriate access (credentials, roles) for their users.
- Performing periodic reviews of their access and configuration.

© 2025 Software GmbH. All rights reserved.

3.2 Infrastructure

The customer handles the infrastructure that runs all the services offered by the Software AG products and must ensure to protect the same. This infrastructure is composed of hardware, software, operating system (including updates and security patches), networking, firewall, and application server.

3.3 Customer Data Management

Data is increasingly seen as an essential corporate asset that can be used to make informed business decisions. Managing data includes the process of acquiring, validating, storing, protecting, and processing the data collected by the customer organization.

The customer is responsible for the security and integrity of data stored and processed in on-premises facilities, infrastructure, and environment. Any data stored or processed by the Software AG product in customer environments is under customer control.

To protect from any perils, the customer should adhere to the regulatory controls that the companies need to abide by and adopt applicable data protection and privacy laws.

3.4 Custom solution/application Integration

By default, integrations are not imposed by Software AG. If the customer integrates any applications (like importing/exporting data to/from other application/layered services) with Software AG product, it would be its full responsibility to do so, starting from establishing the integration, data interchange, and so on.

Customers should carefully choose the services they interact with to make sure that the third-party services do not compromise your security.

3.5 Backup and data storage

As for the maintenance and operations, the on-premises customer has full control over their data management, its security and is responsible for backup and storage of the software data.

3.6 Software AG product installation & Patch management

In customer-controlled environments, the customer is responsible for monitoring product patch notifications and installing them when they are available in the Software AG Download Centre. This includes taking appropriate actions as required in the installation guide.

Customers must always ensure that the building is kept updated to the latest version. On installation, customers are recommended to tune the security configuration as proposed in the product security best practices guide.

© 2025 Software GmbH. All rights reserved.

4 Feedback

If you have feedback or questions on this whitepaper, please send an email to devsecurity@softwareag.com

© 2025 Software GmbH. All rights reserved.