Third-party software installation on Segura™

Policy and risk acknowledgement

Segura™

Security and Innovation Team - SEGi9

Version 3



PUBLIC DOCUMENT

Executive Summary

Segura™ is delivered as a closed, hardened appliance. The operating system and every component of the appliance are approved and distributed by Segura™ through its official channels. Updates may be applied by the customer or by the responsible partner, provided they follow the process described in the official documentation.

Installing any third-party software on the Segura™ appliance is not permitted. Doing so violates the EULA and the Terms and Conditions of use, **automatically voids the warranty and support**, including over performance and security, and may lead to immediate termination of the license.

This document explains the reasons for this policy, presents the controls Segura™ already provides natively, and sets out Segura™'s recommendations for protecting the environment in which the appliance runs.

By deploying and operating Segura™, the customer acknowledges this policy and the risks described here.

Public document. © Segura™. All rights reserved.

Contents

1 Purpose and scope 1

2 Policy 1

2.1 Consequences 2

3 Why we do not allow it 3

3.1 Changes to the operating system and kernel . . . 3

3.2 Larger attack surface 3

3.3 Supply chain 4

3.4 Audit integrity and supportability 4

4 How Segura™ protects the appliance 4

5 Recommendations for the customer environment 5

5.1 Network 6

5.2 Identity and administrative access 6

5.3 Virtualization and cloud 7

5.4 Updates and monitoring 7

5.5 Backup and continuity 8

6 Risk acknowledgement 8

7 References 9

Public document. © Segura™. All rights reserved.

1 Purpose and scope

This document defines Segura™'s policy on installing third-party software on the Segura™ appliance and serves as an acknowledgement of the risks associated with that practice. It applies to customers and to the partners (resellers and integrators) who deploy, operate or maintain the appliance.

The policy applies to every deployment in which the customer operates the appliance: physical appliance, virtual machine, and public or private cloud instance. In Segura™ SaaS, the infrastructure is operated by Segura™ and the customer has no access to the operating system. Even so, the identity and access recommendations in section 5 also apply to that model.

2 Policy

No software, agent, kernel module, package, library or script that is not distributed by Segura™ through its official update channels may be installed, run or kept on the Segura™ appliance. The following are not permitted either:

- changing settings of any Segura™ component that are not described in the product documentation;
- accessing the product database or internal areas directly;
- applying fixes for failures or unexpected behavior that are not described in the official documentation. In those cases, the customer must contact Segura™ Support or the partner responsible for support.

Public document. © Segura™. All rights reserved.

This restriction includes, among others:

- antivirus and anti-malware;
- EDR, XDR and incident response agents;
- hypervisor agents other than those already shipped with the appliance;
- microsegmentation, host firewall or traffic control agents;
- monitoring, inventory, configuration management, backup or data loss prevention (DLP) agents;
- operating system packages obtained from repositories other than Segura™'s official ones.

Third-party components that are part of the product, such as the hypervisor agents already included in the appliance, are approved and distributed by Segura™, are updated through the official update process and are not covered by this restriction. Settings exposed through the product's interface and official tools remain permitted.

Any exception requires prior written authorization from Segura™.

2.1 Consequences

Under the EULA ("Usage Restrictions" section), installing software or changing settings not covered by the documentation:

- automatically voids the warranty and support, including over the performance and security of the product;

Public document. © Segura™. All rights reserved.

- causes any resulting failure to be considered improper use, under the customer's total responsibility;
- may lead to immediate termination of the license;
- makes the customer responsible for restoring a supported configuration, which may require reinstalling the appliance and restoring from backup.

3 Why we do not allow it

Segura™ stores and controls the privileged credentials of the entire organization. Any component running on the appliance effectively gains access to what the appliance protects. For this reason, Segura™ keeps the number of components on the appliance as small as possible and controls each one of them.

3.1 Changes to the operating system and kernel

Security and infrastructure agents commonly load kernel modules, intercept system calls, inspect traffic and enable new services. These changes conflict with the appliance hardening and its native controls, and can break the application, degrade performance, prevent updates or make the environment unavailable. There are public cases in which a single update of a security agent took millions of systems offline at the same time.

3.2 Larger attack surface

Third-party agents run with the highest privilege level on the system and often communicate with external servers. A vulner-

Public document. © Segura™. All rights reserved.

ability in one of these agents can allow full control of the appliance. For hypervisor agents, there are published vulnerabilities that let whoever controls the hypervisor perform privileged actions inside the virtual machine, and flaws in the virtualization layer that can be used to reach the host itself.

3.3 Supply chain

Every additional piece of software brings its own vendor, update channel and dependencies, all outside Segura™'s control and validation. Supply chain attacks such as the SolarWinds case showed that a single compromised update is enough to reach every customer of a vendor.

3.4 Audit integrity and supportability

Segura™ must guarantee the integrity of audit records and session recordings. Unapproved software with privileged access to the appliance undermines that guarantee. In addition, the environment no longer matches what Segura™ tests and validates, which prevents support from reproducing and diagnosing failures.

4 How Segura™ protects the appliance

The appliance already includes the controls that usually motivate installing third-party agents:

- **Operating system hardening:** services, ports and components are reduced to what the product needs to run.

Public document. © Segura™. All rights reserved.

- **Native detection and response:** threat monitoring and automatic blocking of attack attempts.
- **Security updates:** product and operating system fixes are distributed through Segura™'s official channels and applied by the customer or partner, following the update process in the official documentation.
- **Security testing:** periodic penetration tests by independent specialized firms, plus continuous internal testing.
- **Monitoring integrations:** event and log forwarding to SIEM solutions, SNMP monitoring and Zabbix integration.

These integrations meet monitoring, audit and compliance needs without installing additional agents. Penetration tests and vulnerability scans conducted by the customer require Segura™'s prior and formal approval, under the EULA. Their results are confidential, and any vulnerability identified must be reported exclusively to Segura™.

5 Recommendations for the customer environment

Segura™ is designed to operate on a layered security model, and protecting the environment in which it runs is the customer's responsibility under the EULA. Segura™ recommends that customers adopt the practices below.

Public document. © Segura™. All rights reserved.

5.1 Network

- Place the appliance in a dedicated network segment, allowing access only from the sources and to the services required, as listed in the network requirements of the official documentation.
- Do not expose the appliance directly to the internet. External access must go through a VPN, ZTNA or Segura™'s own remote access module.
- Filter outbound traffic as well, allowing only the destinations required: managed systems, the official update repository and the integrations in use.

5.2 Identity and administrative access

- Require multi-factor authentication (MFA) for all users, and always for administrators.
- Integrate Segura™ with the corporate identity provider and review access periodically, removing accounts of departed staff immediately.
- Apply least privilege: administrative profiles limited to a few named people, and accounts that are always individual, never shared.
- Administer Segura™ only from dedicated, protected workstations that are kept up to date and are not used for e-mail or general browsing. Segura™ administrative accounts must not be used on general-purpose workstations.

Public document. © Segura™. All rights reserved.

- Keep emergency credentials and appliance console credentials in offline custody under dual control, and test them periodically.

5.3 Virtualization and cloud

- Protect the virtualization platform or cloud account with the same rigor applied to the vault itself. Whoever administers that layer controls the Segura™ virtual machine.
- Restrict and log access to the virtual machine console and to snapshot, clone and export operations.
- Treat snapshots and backups as sensitive data, with encryption and restricted access.
- Keep the hypervisor and the host up to date.
- For physical appliances, restrict and log physical access to the equipment.

5.4 Updates and monitoring

- Keep Segura™ on the latest supported version and apply security updates as soon as they are published, following the update process described in the official documentation.
- Forward Segura™ events to the corporate SIEM and monitor authentication failures, configuration changes, administrative access and unavailability.
- Track appliance health through the native monitoring integrations.

Public document. © Segura™. All rights reserved.

5.5 Backup and continuity

- Perform backups as described in the official documentation, with an encrypted copy kept isolated from the main environment.
- Test restoration periodically.
- Maintain a contingency plan that ensures access to critical credentials even when the appliance is unavailable.

6 Risk acknowledgement

By deploying, operating or maintaining Segura™, the customer acknowledges that:

1. installing third-party software on the appliance is not permitted, as set out in section 2;
2. installing unauthorized software automatically voids the warranty and support, including over performance and security, and may lead to immediate termination of the license;
3. failures, unavailability, data loss or security incidents resulting from such installation are considered improper use and are the customer's total responsibility;
4. protecting the environment in which the appliance runs is the customer's responsibility, and section 5 sets out Segura™'s recommendations for doing so.

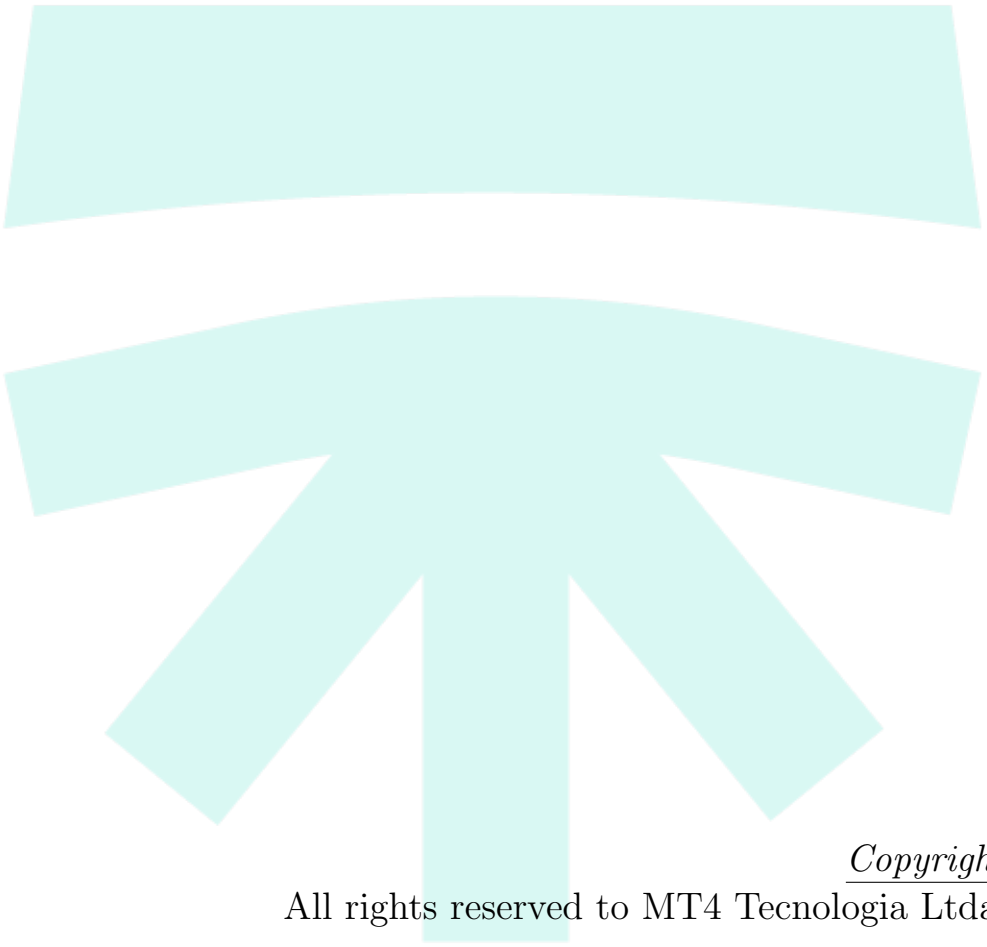
Public document. © Segura™. All rights reserved.

This document does not require a signature. It complements, and does not replace, the EULA, the Terms and Conditions of use and the commercial agreement. In case of conflict, those instruments prevail.

7 References

- EULA (End-User License Agreement, SSG 5002)
- Terms and Conditions

Public document. © Segura™. All rights reserved.



Copyright
All rights reserved to MT4 Tecnologia Ltda.

Document Control
FSR-1052, version 3

Contact
Support support@segura.security

Public document. © Segura™. All rights reserved.