Instalação de softwares de terceiros no Segura™

Política e declaração de ciência de riscos

Segura™

Equipe de Segurança e Inovação - SEGi9

Versão 3



DOCUMENTO PÚBLICO

Resumo Executivo

O Segura™ é entregue como um appliance fechado e endurecido (*hardened*). O sistema operacional e todos os componentes do appliance são homologados e distribuídos pela Segura™ por meio de seus canais oficiais. As atualizações podem ser aplicadas pelo próprio cliente ou pelo parceiro responsável, desde que sigam o processo descrito na documentação oficial.

Não é permitida a instalação de nenhum software de terceiros no appliance Segura™. A instalação viola a EULA e os Termos e Condições de uso, resulta na **perda automática da garantia e do suporte técnico**, inclusive sobre desempenho e segurança, e pode levar à rescisão imediata da licença.

Este documento explica os motivos dessa política, apresenta os controles que o Segura™ já oferece de forma nativa e reúne as recomendações da Segura™ para proteger o ambiente em que o appliance opera.

Ao implantar e operar o Segura™, o cliente declara estar ciente desta política e dos riscos aqui descritos.

Documento público. © Segura™. Todos os direitos reservados.

Sumário

1 Objetivo e escopo **1**

2 Política **1**

2.1 Consequências 2

3 Por que não permitimos **3**

3.1 Alterações no sistema operacional e no kernel . . 3

3.2 Aumento da superfície de ataque 4

3.3 Cadeia de suprimentos (*supply chain*) 4

3.4 Integridade da auditoria e capacidade de suporte . 4

4 Como o Segura™ protege o appliance **5**

5 Recomendações para o ambiente do cliente **6**

5.1 Rede 6

5.2 Identidade e acesso administrativo 6

5.3 Virtualização e nuvem 7

5.4 Atualização e monitoramento 8

5.5 Backup e continuidade 8

6 Declaração de ciência e aceite de riscos **8**

7 Referências **9**

Documento público. © Segura™. Todos os direitos reservados.

1 Objetivo e escopo

Este documento define a política da Segura™ sobre a instalação de softwares de terceiros no appliance Segura™ e serve como declaração de ciência dos riscos associados a essa prática. Ela vale para o cliente e para os parceiros (revendas e integradores) que implantam, operam ou mantêm o appliance.

A política se aplica a todas as formas de implantação em que o appliance é operado pelo cliente: appliance físico, máquina virtual e instância em nuvem pública ou privada. No Segura™ SaaS, a infraestrutura é operada pela própria Segura™ e o cliente não tem acesso ao sistema operacional. Ainda assim, as recomendações de identidade e acesso da seção 5 também se aplicam a esse modelo.

2 Política

Não é permitido instalar, executar ou manter no appliance Segura™ qualquer software, agente, módulo de kernel, pacote, biblioteca ou script que não seja distribuído pela Segura™ por meio de seus canais oficiais de atualização. Também não são permitidos:

- alterar configurações de qualquer componente do Segura™ que não estejam descritas na documentação do produto;
- acessar diretamente o banco de dados ou as áreas internas do produto;
- aplicar correções que não estejam descritas na documentação oficial para falhas ou comportamentos ines-

Documento público. © Segura™. Todos os direitos reservados.

perados. Nesses casos, o cliente deve acionar o Suporte da Segura™ ou o parceiro responsável pelo atendimento.

A restrição inclui, entre outros:

- antivírus e antimalware;
- EDR, XDR e agentes de resposta a incidentes;
- agentes de virtualização (*hypervisor agents*) diferentes dos que já acompanham o appliance;
- agentes de microssegmentação, firewall de host ou controle de tráfego;
- agentes de monitoramento, inventário, gestão de configuração, backup ou prevenção de perda de dados (DLP);
- pacotes de sistema operacional obtidos de repositórios que não sejam os oficiais da Segura™.

Os componentes de terceiros que fazem parte do produto, como os agentes de virtualização já incluídos no appliance, são homologados e distribuídos pela Segura™, são atualizados pelo processo oficial de atualização e não se enquadram nesta restrição. As configurações disponibilizadas pela interface e pelas ferramentas oficiais do produto continuam permitidas.

Qualquer exceção depende de autorização prévia e por escrito da Segura™.

2.1 Consequências

Conforme a EULA (seção “Restrições de Uso”), a instalação de software ou a alteração de configurações não previstas na

Documento público. © Segura™. Todos os direitos reservados.

documentação:

- resulta na perda automática da garantia e do suporte, inclusive sobre o desempenho e a segurança do produto;
- faz com que eventuais falhas sejam consideradas uso indevido, sob total responsabilidade do cliente;
- pode levar à rescisão imediata da licença;
- torna o cliente responsável por restabelecer uma configuração suportada, o que pode exigir a reinstalação do appliance e a restauração de backup.

3 Por que não permitimos

O Segura™ armazena e controla as credenciais privilegiadas de toda a organização. Qualquer componente executado no appliance passa a ter, na prática, acesso àquilo que o appliance protege. Por esse motivo, a Segura™ mantém o menor número possível de componentes no appliance e controla cada um deles.

3.1 Alterações no sistema operacional e no kernel

Agentes de segurança e de infraestrutura costumam carregar módulos de kernel, interceptar chamadas de sistema, inspecionar tráfego e ativar novos serviços. Essas alterações conflitam com o hardening do appliance e com os seus controles nativos, e podem quebrar a aplicação, degradar o desempenho, impedir atualizações ou tornar o ambiente indisponível. Existem casos públicos em que uma única atualização de um agente de segurança deixou milhões de sistemas inoperantes ao mesmo tempo.

Documento público. © Segura™. Todos os direitos reservados.

3.2 Aumento da superfície de ataque

Agentes de terceiros são executados com o mais alto nível de privilégio do sistema e frequentemente mantêm comunicação com servidores externos. Uma vulnerabilidade em um desses agentes pode permitir o controle total do appliance. No caso dos agentes de virtualização, existem vulnerabilidades publicadas que permitem a quem controla o hypervisor executar ações privilegiadas dentro da máquina virtual, e falhas na camada de virtualização que podem ser usadas para alcançar o próprio host.

3.3 Cadeia de suprimentos (*supply chain*)

Cada software adicional traz o seu próprio fornecedor, canal de atualização e dependências, todos fora do controle e da validação da Segura™. Ataques à cadeia de suprimentos, como o caso SolarWinds, mostraram que uma única atualização comprometida basta para atingir todos os clientes de um fornecedor.

3.4 Integridade da auditoria e capacidade de suporte

O Segura™ precisa garantir a integridade dos registros de auditoria e das gravações de sessão. Um software não homologado com acesso privilegiado ao appliance compromete essa garantia. Além disso, o ambiente deixa de corresponder ao que a Segura™ testa e valida, o que impede a reprodução e o diagnóstico de falhas pelo suporte.

Documento público. © Segura™. Todos os direitos reservados.

4 Como o Segura™ protege o appliance

O appliance já incorpora os controles que costumam motivar a instalação de agentes de terceiros:

- **Hardening do sistema operacional:** serviços, portas e componentes são reduzidos ao necessário para o funcionamento do produto.
- **Detecção e resposta nativas:** monitoramento de ameaças e bloqueio automático de tentativas de ataque.
- **Atualizações de segurança:** correções do produto e do sistema operacional são distribuídas pelos canais oficiais da Segura™ e aplicadas pelo cliente ou pelo parceiro, conforme o processo de atualização da documentação oficial.
- **Testes de segurança:** testes de intrusão periódicos realizados por empresas especializadas independentes, além de testes internos contínuos.
- **Integrações de monitoramento:** envio de eventos e logs para soluções de SIEM, monitoramento por SNMP e integração com Zabbix.

Essas integrações atendem às necessidades de monitoramento, auditoria e conformidade sem a instalação de agentes adicionais. Testes de intrusão e varreduras de vulnerabilidade conduzidos pelo cliente dependem de aprovação prévia e formal da Segura™, conforme a EULA. Os resultados são confidenciais e qualquer vulnerabilidade identificada deve ser reportada exclusivamente à Segura™.

Documento público. © Segura™. Todos os direitos reservados.

5 Recomendações para o ambiente do cliente

O Segura™ foi projetado para operar em um modelo de segurança em camadas, e a proteção do ambiente em que ele opera é responsabilidade do cliente, conforme a EULA. A Segura™ recomenda que o cliente adote as práticas abaixo.

5.1 Rede

- Instalar o appliance em um segmento de rede dedicado, com acesso permitido somente às origens e aos serviços necessários, conforme os requisitos de rede da documentação oficial.
- Não expor o appliance diretamente à internet. O acesso externo deve passar por VPN, ZTNA ou pelo módulo de acesso remoto do próprio Segura™.
- Filtrar também o tráfego de saída, liberando apenas os destinos necessários: os sistemas gerenciados, o repositório oficial de atualizações e as integrações em uso.

5.2 Identidade e acesso administrativo

- Exigir autenticação multifator (MFA) de todos os usuários e, obrigatoriamente, dos administradores.
- Integrar o Segura™ ao provedor de identidade corporativo e revisar os acessos periodicamente, removendo de imediato as contas de pessoas desligadas.

Documento público. © Segura™. Todos os direitos reservados.

- Aplicar o princípio do menor privilégio: perfis administrativos restritos a poucas pessoas nomeadas e contas sempre individuais, nunca compartilhadas.
- Administrar o Segura™ somente a partir de estações dedicadas e protegidas, mantidas atualizadas e não utilizadas para e-mail ou navegação geral. Contas administrativas do Segura™ não devem ser usadas em estações de uso comum.
- Manter as credenciais de emergência e as credenciais de console do appliance sob custódia offline, com controle dual, e testá-las periodicamente.

5.3 Virtualização e nuvem

- Proteger a plataforma de virtualização ou a conta de nuvem com o mesmo rigor aplicado ao próprio cofre. Quem administra essa camada controla a máquina virtual do Segura™.
- Restringir e registrar o acesso ao console da máquina virtual e às operações de snapshot, clone e exportação.
- Tratar snapshots e backups como dados sensíveis, com criptografia e acesso restrito.
- Manter o hypervisor e o host atualizados.
- No appliance físico, restringir e registrar o acesso físico ao equipamento.

Documento público. © Segura™. Todos os direitos reservados.

5.4 Atualização e monitoramento

- Manter o Segura™ na versão suportada mais recente e aplicar as atualizações de segurança assim que forem publicadas, seguindo o processo de atualização descrito na documentação oficial.
- Enviar os eventos do Segura™ ao SIEM corporativo e monitorar falhas de autenticação, alterações de configuração, acessos administrativos e indisponibilidade.
- Acompanhar a saúde do appliance pelas integrações de monitoramento nativas.

5.5 Backup e continuidade

- Realizar backups conforme a documentação oficial, com uma cópia criptografada e isolada do ambiente principal.
- Testar a restauração periodicamente.
- Manter um plano de contingência que garanta o acesso às credenciais críticas mesmo com o appliance indisponível.

6 Declaração de ciência e aceite de riscos

Ao implantar, operar ou manter o Segura™, o cliente declara estar ciente de que:

1. não é permitida a instalação de software de terceiros no appliance, nos termos da seção 2;

Documento público. © Segura™. Todos os direitos reservados.

2. a instalação de software não autorizado resulta na perda automática da garantia e do suporte, inclusive sobre desempenho e segurança, e pode levar à rescisão imediata da licença;

3. falhas, indisponibilidades, perdas de dados ou incidentes de segurança decorrentes dessa instalação são considerados uso indevido e são de total responsabilidade do cliente;

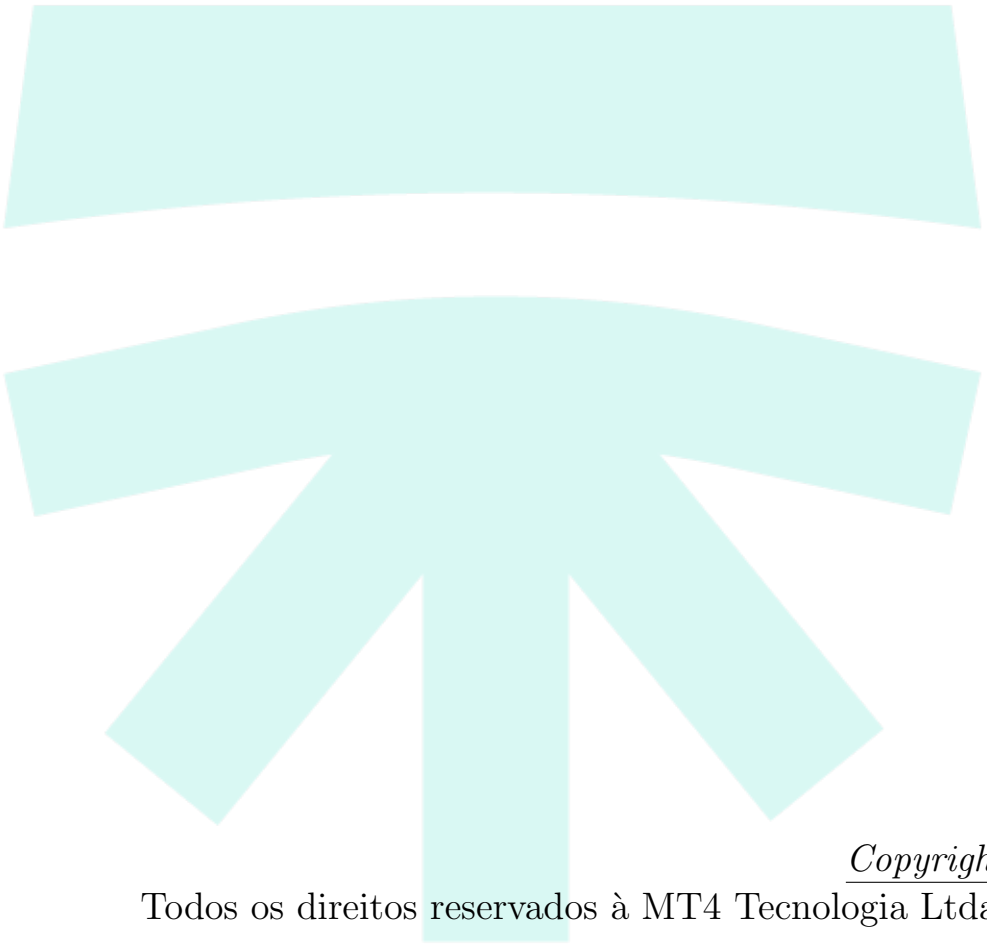
4. a proteção do ambiente em que o appliance opera é de responsabilidade do cliente, e a seção 5 reúne as recomendações da Segura™ para isso.

Este documento não requer assinatura. Ele complementa, e não substitui, a EULA, os Termos e Condições de uso e o contrato comercial. Em caso de conflito, prevalecem esses instrumentos.

7 Referências

- EULA (Contrato de Licença de Usuário Final, SSG 5002)
- Termos e Condições de uso

Documento público. © Segura™. Todos os direitos reservados.



Copyright
Todos os direitos reservados à MT4 Tecnologia Ltda.

Controle do Documento
FSR-1052, versão 3

Contato
Suporte support@segura.security

Documento público. © Segura™. Todos os direitos reservados.