Gerado a 28/10/2026 05:55

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

O que fazemos pela segurança, DDoS incluído, e o que fica do seu lado

Segurança

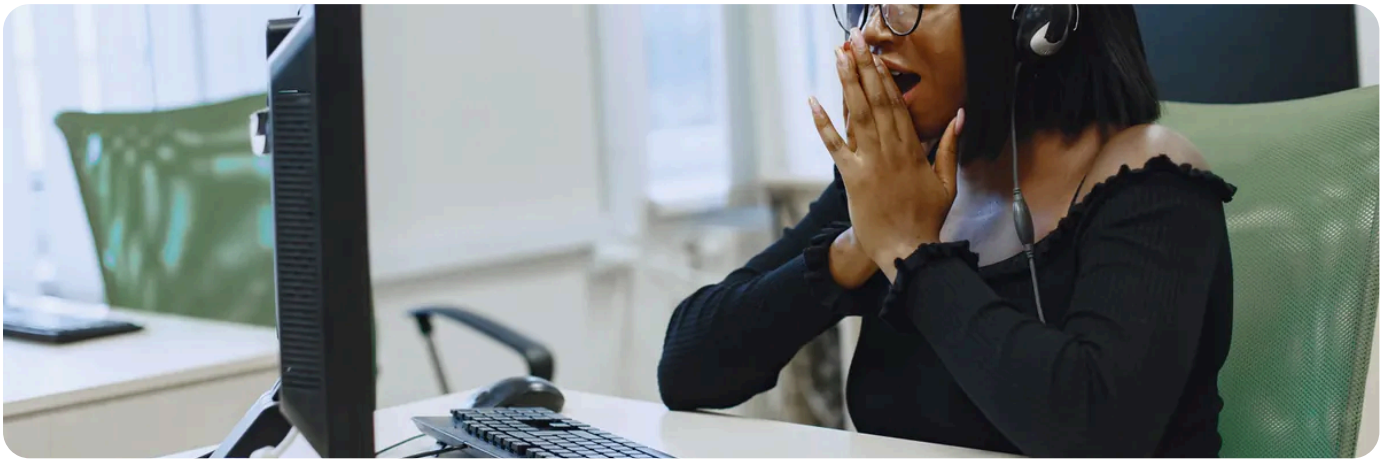
CÓDIGO	VERSÃO	PAÍS · IDIOMA
RLX-BR-KB-1074	v2026.10.18	Brasil · Português (Brasil)

MozOut Brasil
RLX Holdings (Pty) Ltd. · Grupo RLX Holdings
N.º fiscal (SARS) 943 907 6234 · N.º de registo (CIPC) 2025/667953/07

https://www.my.mozout.com/knowledgebase/1074

O que fazemos pela segurança, DDoS incluído, e o que fica do seu lado

Segurança Criado em **11 de setembro de 2026** Atualizado em **18 de outubro de 2026** 4 min de leitura



Esta é uma pergunta que merece números e nomes, e não publicidade. Abaixo está o que roda nos nossos servidores, o que isso trava de fato, e - a parte que quase nenhum fornecedor escreve - **o que continua dependendo de si**.

O que está rodando, pelo nome

Camada	O que faz
Firewall CSF/LFD	Filtra as conexões e bloqueia automaticamente quem repete tentativas falhadas. É o que apanha a força bruta antes de ela acertar - e também o que por vezes apanha um cliente numa rede compartilhada: **por que o seu IP é bloqueado**
ModSecurity	Inspeciona cada requisição web e recusa as que têm forma de ataque - injeção de SQL, tentativas de leitura de arquivos, pedidos a *.env* e a *.git*. O motor está ligado, com um conjunto de regras comercial e atualizado.
Imunify360	Analisa os arquivos das contas à procura de código malicioso e trabalha em conjunto com o firewall, compartilhando a lista de quem está atacando a rede inteira.
Antivírus ClamAV	Verificação de arquivos ao nível do servidor, incluindo o que entra por FTP e por e-mail.
Contas isoladas	Cada conta roda separada das outras. Um site vizinho comprometido não alcança os seus arquivos.
SSL automático	Certificado emitido e renovado sozinho para os domínios da conta - ver **o que é um certificado SSL**
Cópias com o JetBackup	Restauração de arquivos, bancos de dados ou caixas de e-mail, por data - ver **como repor os seus dados**

E os ataques de negação de serviço (DDoS)?

Um ataque DDoS não tenta entrar: tenta **afogar**. Milhares de pedidos falsos ao mesmo tempo, até o servidor deixar de responder a quem é verdadeiro. É diferente de tudo o que está na tabela acima, e trava-se em outro lugar.

Os nossos servidores estão num centro de dados europeu com **filtragem de ataques volumétricos ao nível da rede** - o tráfego de ataque é absorvido antes de chegar à máquina. Sobre onde ficam exatamente, ver **onde ficam os nossos servidores**.

O que nenhum fornecedor pode prometer.
Nenhuma proteção é absoluta, e quem disser o contrário está vendendo. Num ataque muito grande e dirigido, a resposta habitual da rede é deixar cair o tráfego para o endereço atacado - o que protege todos os outros e deixa o alvo indisponível durante algumas horas. É desagradável, e é a opção menos má.

Se o seu site é alvo provável.
Um site com adversidade real - política, jogos, casas de apostas, ou concorrência agressiva - ganha muito em ficar atrás de uma CDN com modo de emergência, que filtra os pedidos *antes* de eles chegarem cá. É a proteção mais eficaz que existe para este caso e a maior parte custa zero.

O que não dizemos ter

Preferimos ser verificáveis a ser impressionantes. Por isso deixamos claro o que *não* reivindicamos: não temos certificação ISO 27001, nem certificação PCI DSS, nem equipe de segurança interna dedicada, nem programa público de recompensas por falhas. Se algum concurso ou contrato seu exige um destes pontos por escrito, diga-nos antes de contratar - ver **vender online: PCI e dados de cartão**.

A parte que é sua - e é por onde entram

Vale a pena dizer isto sem rodeios: **a esmagadora maioria dos sites invadidos que vemos não foi invadida pelo servidor**. Foi pela aplicação que corre dentro dele. As causas repetem-se:

1. **WordPress, tema ou plugin desatualizado.** É a primeira causa, com folga. Uma falha conhecida é explorada por varredores automáticos poucos dias depois de ser publicada.
2. **Plugins e temas pagos obtidos de graça** em sites não oficiais. Vêm frequentemente com código acrescentado, e o preço é exatamente esse.
3. **Senhas fracas ou repetidas.** A mesma senha no site, no e-mail e numa loja qualquer que teve um vazamento - e a partir daí entra-se sem forçar nada.
4. **O computador de quem administra.** Um notebook com um ladrão de senhas instalado entrega as credenciais de FTP sem que ninguém dê por isso.

Contra isto, o firewall e o ModSecurity ajudam mas não substituem o básico: atualizar, não compartilhar senhas, ativar a verificação em duas etapas, e desconfiar de mensagens em nosso nome - ver **como saber se um e-mail é mesmo nosso**.

Se desconfia que já aconteceu

Não comece por apagar arquivos. Comece por **saber se o site foi mesmo comprometido** e siga depois para **como limpar um site comprometido**. E avise-nos: conseguimos ver o registro do servidor e dizer-lhe por onde entraram, o que evita que volte a acontecer pela mesma porta.

Onde acaba o nosso trabalho e começa o seu está escrito em **até onde vai o nosso apoio**.

PRECISA DE AJUDA?

Tem dúvidas sobre a segurança do seu site? Pergunte-nos.

Falar conosco →

MozOut

MozOut Brasil

RLX Holdings (Pty) Ltd. · Grupo RLX Holdings

N.º FISCAL (SARS)	943 907 6234
N.º DE REGISTO (CIPC)	2025/667953/07
SEDE	72 York Road, Kensington Joanesburgo 2094, Gauteng, África do Sul
CONTACTOS	info@mozout.com · +27 78 823 3325 · www.mozout.com
HORÁRIO	2ª. à 6ª. Feira - 08 à 16 Horas Sábado & Domingo - Fechado

RLX-BR-KB-1074 · v2026.10.18 · Gerado a 28/10/2026 05:55

Versão online deste documento