interweb

Generated on 28/10/2026 10:52

KNOWLEDGE BASE · PUBLIC DOCUMENT

What we do about security, DDoS included, and what stays yours

Security

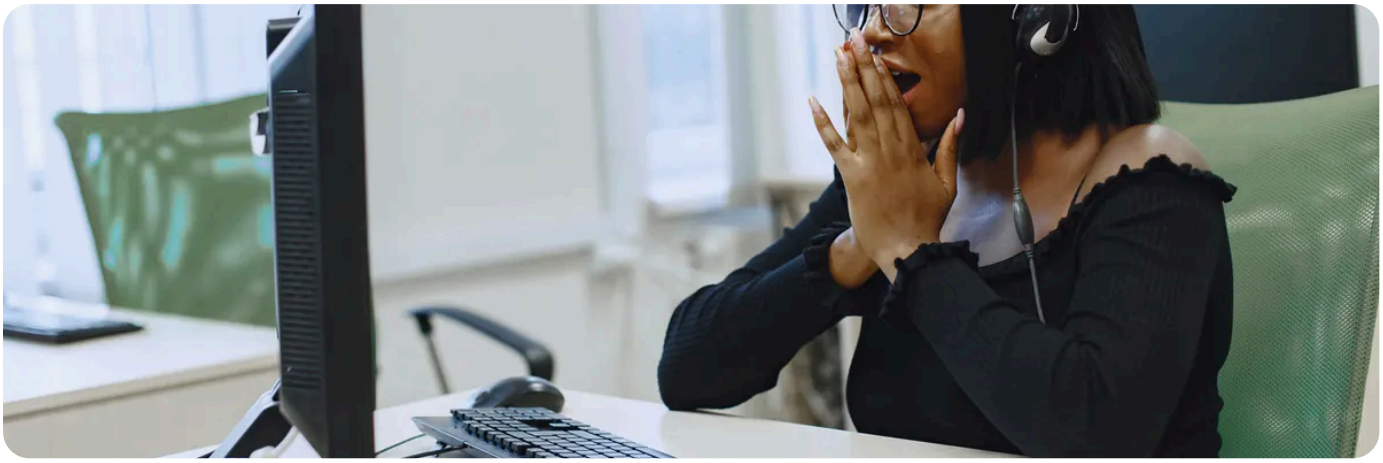
CODE	VERSION	COUNTRY · LANGUAGE
RLX-MZ-KB-330	v2026.09.28	Mozambique · English

Interweb Mozambique
RLX Holdings, S.A. · Group RLX Holdings
Tax ID (NUIT) 401 191 607 · Legal entity no. (NUEL) 105 045 974 · Economic activity code (CAE) 62022

https://www.meu.interweb.co.mz/knowledgebase/330

What we do about security, DDoS included, and what stays yours

Security Created on **September 11, 2026** Updated on **September 28, 2026** 4 min read



This question deserves names and specifics, not marketing. Below is what runs on our servers, what it actually stops, and - the part almost no provider writes down - **what still depends on you**.

What is running, by name

Layer	What it does
CSF/LFD firewall	Filters connections and automatically blocks anyone repeating failed attempts. It is what catches brute force before it lands - and also what occasionally catches a customer on a shared network: **why your IP gets blocked**
ModSecurity	Inspects every web request and refuses the ones shaped like attacks - SQL injection, file-read attempts, requests for *.env* and *.git*. The engine is on, with a commercial, maintained rule set.
Imunify360	Scans account files for malicious code and works alongside the firewall, sharing the list of who is attacking the wider network.
ClamAV antivirus	Server-level file scanning, including what arrives over FTP and by e-mail.
Isolated accounts	Each account runs separately from the others. A compromised neighbour cannot reach your files.
Automatic SSL	Certificate issued and renewed by itself for the account's domains - see **what is an SSL certificate**
JetBackup copies	Restore files, databases or mailboxes, by date - see **how to restore your data**

And denial-of-service attacks (DDoS)?

A DDoS attack does not try to get in: it tries to **drown**. Thousands of fake requests at once, until the server stops answering the real ones. It is different from everything in the table above, and it is stopped somewhere else.

Our servers sit in a European data centre with **volumetric attack filtering at network level** - attack traffic is absorbed before it reaches the machine. For exactly where they are, see **where our servers are**.

What no provider can promise.
No protection is absolute, and anyone saying otherwise is selling. In a very large targeted attack, the network's usual answer is to drop traffic to the address under attack - which protects everyone else and leaves the target unreachable for a few hours. It is unpleasant, and it is the least bad option.

If your site is a likely target.
A site with real adversaries - politics, gaming, betting, or aggressive competitors - gains a great deal from sitting behind a CDN with an emergency mode, which filters requests *before* they reach us. It is the most effective protection there is for this case, and most of it costs nothing.

What we do not claim

We would rather be verifiable than impressive. So we say plainly what we do *not* claim: we hold no ISO 27001 certification, no PCI DSS certification, no dedicated in-house security team, and no public bug bounty programme. If a tender or contract of yours requires one of these in writing, tell us before signing up - see **selling online: PCI and card data**.

The part that is yours - and it is where they get in

This is worth saying without hedging: **the overwhelming majority of hacked sites we see were not broken into through the server**. They were broken into through the application running inside it. The causes repeat:

1. **Out-of-date WordPress, theme or plugin.** It is the first cause by a wide margin. A known hole is exploited by automated scanners within days of being published.
2. **Paid plugins and themes obtained free** from unofficial sites. They frequently come with code added, and that is exactly the price.
3. **Weak or reused passwords.** The same password on the site, the e-mail and some shop that had a breach - and from there nobody has to force anything.
4. **The administrator's own computer.** A laptop with a password stealer on it hands over FTP credentials without anyone noticing.

Against this, the firewall and ModSecurity help but do not replace the basics: update, do not share passwords, turn on **two-factor authentication**, and be suspicious of messages in our name - see **how to tell whether an e-mail really came from us**.

If you suspect it already happened

Do not start by deleting files. Start with **finding out whether the site really was compromised** and then move on to **how to clean up a compromised site**. And tell us: we can read the server log and say how they got in, which stops it happening again through the same door.

Where our work ends and yours begins is written in **how far our support goes**.

NEED A HAND?

Unsure about your site's security? Ask us.

Talk to us →

interweb

Interweb Mozambique

RLX Holdings, S.A. · Group RLX Holdings

TAX ID (NUIT)	401 191 607
LEGAL ENTITY NO. (NUEL)	105 045 974
ECONOMIC ACTIVITY CODE (CAE)	62022
REGISTERED OFFICE	Bairro 7 de Setembro Vilankulo 1304 · CEP 0411-02, Inhambane, Mozambique
CONTACT	info@interweb.co.mz · +258 84 635 1111 · +258 86 635 1111 · www.interweb.co.mz
OPENING HOURS	Monday to Friday - 08 AM to 04 PM Saturday & Sunday - Closed

Online version of this document

RLX-MZ-KB-330 · v2026.09.28 · Generated on 28/10/2026 10:52