

NotAPOS

SECURITY WHITEPAPER

v4.20.69 - Classification: Definitely Public

Executive Summary

At NotAPOS, security is our second-most important value, right after synergy and slightly above 'shipping the feature Brett tweeted about.'

This whitepaper outlines our defense-in-depth strategy, which consists of:

- one (1) Cloudflare Worker
- a Slack channel called #security-stuff
- Brett's gut feeling

We have never had a breach. We have also never had a customer.

Statistically speaking, we are one of the most secure companies on Earth.

Our Threat Model

We have identified the following adversaries:

- | | |
|--------------------------------|--------------------|
| - Karens | HIGH |
| - Aftermarket LCD cartels | HIGH |
| - Brett's ex | CRITICAL |
| - Nation-states | low |
| - OWASP Top 10 | we don't read it |
| - Customers requesting refunds | EXISTENTIAL |

TRUST ME BRO

- our entire encryption strategy

Signed,

Brett (CISO, also CEO, also founder, also ate the last bagel)

Compliance & Certifications

- SOC 2 Type II (self-attested, in a Google Doc)
- ISO 9001 (printed at home, slightly crooked)
- HIPAA (we googled what it stands for)
- PCI-DSS (we wrote 'compliant' on a sticky note)
- GDPR (we have a cookie banner that does nothing)
- FedRAMP (we asked nicely)
- ISO 27001 (Brett did the audit himself, in the mirror)
- Actual audit by an actual auditor