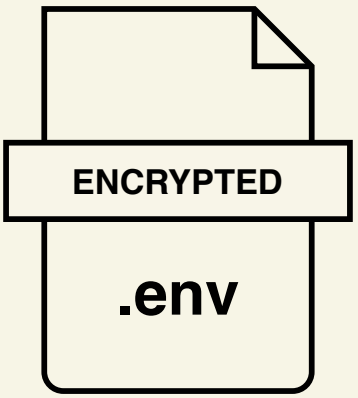
Are your *env* files safe?

Probably not.

They're plaintext.
They're everywhere.

On developer laptops.
In production.

Pushed to Git. Shared on Slack. And opened who knows where.



And a leaked secret? It can cost a company $4 million dollars [†]. And the risk is only growing.

With LLMs reading and refactoring code, leaks don't require human error anymore.

You've locked down everything else– infra, databases, and networks.

But your env files?
Still plaintext.
Still invisible.

That changes now.
Dotenv Enterprise encrypts your env files at rest, protects them in transit, and audits them everywhere. All without changing your workflow or doing integration work.

Same files. Same workflow. Zero integrations. But now they're safe.

www.DOTENV-ENTERPRISE.com

[†] https://resources.github.com/enterprise/understanding-secret-leak-exposure/

.ENV