What Steel Security Is

What Steel Security Is

Welcome to Steel Security

What Steel Security Does

Steel Security is a high-signal WordPress security auditing and hardening plugin designed to surface real risks quickly and help you address them safely.

Instead of overwhelming you with noise, Steel Security focuses on identifying meaningful security issues such as exposed files, misconfigurations, and unsafe defaults — then provides clear, actionable guidance to resolve them.

Steel Security is built for real-world environments where uptime matters, and where security changes must be applied carefully and reversibly.

Why Steel Security Is Different

Most security plugins try to do everything — malware scanning, firewalls, monitoring — often at the cost of clarity and performance.

Steel Security takes a different approach:

- Focus on **high-value, high-signal findings**
- Separate **Scan** (what's wrong) from **Hardening** (what you can safely change)
- Provide **clear explanations**, not just alerts
- Support **safe, reversible changes**
- Respect **real-world hosting environments** (Apache, IIS, Nginx, shared hosting)

This makes Steel Security especially useful for developers, agencies, and site owners who want control and clarity.

What Steel Security Does Not Do

Steel Security is not a malware scanner or firewall.

It does not attempt to:

- continuously scan files for malware signatures

- block traffic or act as a web application firewall
- replace server-level security tools

Instead, it focuses on identifying and resolving **structural security risks** that are often overlooked but highly impactful.

Core Concepts

Understanding Steel Security starts with two key ideas:

Scan

The Scan identifies potential risks in your WordPress installation.

These include:

- exposed sensitive files
- debug configurations
- insecure defaults
- leftover artifacts (backups, dumps, test files)

Each finding includes context so you understand both the risk and the recommended response.

Hardening

Hardening allows you to apply protective changes to reduce risk.

These changes are:

- **targeted** (only what is needed)
- **safe** (designed to avoid breaking your site)
- **reversible** (you can roll them back if needed)

Examples include:

- blocking PHP execution in uploads
- disabling directory listing
- applying security headers
- tightening configuration exposure

When to Use Steel Security

Steel Security is most valuable when:

- launching or auditing a new site
- taking over an existing site
- preparing for production or client handoff
- performing routine security reviews
- cleaning up after migrations or backups

It is also useful as an ongoing check to ensure nothing unsafe has been introduced over time.

Steel Security Pro

Steel Security includes both a free core plugin and a Pro upgrade.

The Pro version expands functionality with additional:

- advanced checks and findings
- enhanced hardening controls
- deeper insights and guidance
- licensing and multi-site management capabilities

If you are managing multiple sites or require more advanced control, Pro is recommended.

What to Do Next

If you're just getting started:

1. Install and activate the Steel Security plugin
2. Run your first scan
3. Review the highest-risk findings
4. Apply hardening where appropriate
5. Re-scan to confirm improvements

From there, explore the rest of the documentation to deepen your understanding and refine your security posture.

Related

- Installing the Steel Security Plugin
- Activating Steel Security
- Running Your First Scan
- Understanding the Dashboard