6 Common Misconceptions About Application Shielding

White Paper

Sam Pickles, CTO

RedShield Security, LTD

6 COMMON MISCONCEPTIONS ABOUT APPLICATION SHIELDING

Application Shielding is a new tool for many organizations and is the subject of several commonly held beliefs which may prevent a security team from fully embracing shielding as a strategic option.

The biggest misconceptions we hear at RedShield are:

Misconception #1: Fixing code is always better/more robust/more secure

When vulnerabilities are discovered, fixing the application code is often the ideal strategy; provided all of the following are true:

- The priority of vulnerability mitigation is quickly agreed at management level, and communicated to engineers. Impact to other activities is accepted.
- You have access to the application code
- Developers are immediately available to fix vulnerabilities and rebuild the application, ahead of other priorities
- Fixing the code is not too big or expensive a job
- Fixing the vulnerable component will not break the system
- The developers are sufficiently skilled in security engineering to resolve all issues

This will probably be true for some of your applications; and these will most likely already be fixed.
For applications with open vulnerabilities, look at other options – remember that hackers don't care whether you are planning to fix a system next quarter.

Most organizations which depend solely on fixing code to mitigate vulnerabilities do not have the all of the above factors in their favor, and continuously have a list of open vulnerabilities which are not yet fixed. Taking the IT industry as an example, the average time between discovering a vulnerability and fixing it, is **893 days**. In our view, this is an unnecessary risk, when shielding can often mitigate vulnerabilities in hours.

RedShield advocates doing both – Shield First, then Fix.

Misconception #2: Shields can simply be bypassed using special techniques

Application Shielding is a rapidly advancing field in security engineering. Virtually all security controls have flaws discovered in them from time to time; including those within application frameworks, databases, operating systems etc. and in the case of shield policies, discovered bypass techniques have been rare and addressed swiftly.

RedShield operates a bug bounty and we encourage researchers to submit any weaknesses discovered within shield objects to us, allowing us to strengthen the shields and advance the field of Application Shielding. If you have techniques which allow a well-tuned shield policy to be bypassed, we look forward to putting your name on our honors board and rewarding your efforts!

Misconception #3: Our vulnerabilities are too complex or unique for shielding

Application Shielding is a form of software development. Most shielding projects require customization of our shield library, or the creation of new shield objects to suit. Shield objects can be programmed to transform application content, track application and session state, detect illegal inputs or outputs, illegal changes to client side contents, and a huge range of unwanted activity and perform many other functional tasks. Within these capabilities, RedShield can mitigate most web penetration testing results which are shared with us, including complex application logic flaws; and this capability is continuously growing.

There are certainly some vulnerabilities which cannot yet be fully or partially mitigated by shielding; and in such cases, RedShield will provide recommendations on other options.

Misconception #4: Shield layers might introduce new vulnerabilities

It is true that any security layer could have unknown vulnerabilities within it, but this also applies to any system components including operating systems, databases, web app containers etc.

The risk of leaving known, discoverable, exploitable vulnerabilities open is far worse, and in the imperfect world of IT security and risk management, we advocate choosing the shortest path to the lowest measurable risk.

Misconception #5: Relying on shielding, makes developers less motivated to improve security

The development of secure systems requires several key supporting factors:

- Ability of the engineering team to deliver secure code
    - Size and seniority of developer team
    - Skills, time and tools available to find and fix vulnerabilities at each stage
    - Security as a priority within the product goals

- Level of management support
    - Secure software costs more and takes longer to develop
    - Security competes with functionality, performance, scalability and delivery deadlines

Shielding doesn't negatively impact these factors - it is a strategy to reduce overall risk, but should not cause standards to drop elsewhere. The same can be said for cyber liability insurance – addressing your organization's overall risk by multiple methods doesn't reduce the need to get security right at all levels.

Misconception #6: New vulnerabilities found in shielded apps means a failure of shielding

To the contrary, effective shielding depends on vulnerability intelligence – an ongoing partnership between the shield engineering team and penetration testers. Testers and application teams must advise the shielding team when new vulnerabilities are discovered, and authorize the changes to the policy through agreed escalation paths and change control. This can usually be done quickly, as an emergency if necessary; which is one of the advantages of shielding vs fixing code.

There are some vulnerabilities which are automatically detected by vulnerability scanning, however engaging with a professional penetration tester for more advanced testing is always strongly recommended and this will lead to the best possible shield policy.

RedShield has partnerships with many penetration testing companies and is always happy to provide recommendations and options.

Consider an Advanced Shielding Plan

An Advanced Shielding Plan from RedShield enables application launch without risk acceptance or function disable and creates the time needed for code remediation. With base security policies in place often in hours, shield first then fix all starts with a no-obligation Advanced Shielding Plan from RedShield.

Contact: Sales@RedShield.co