FORTIWEB AND IMMUNIWEB AI
Web Application Security Testing and Agile Virtual Patching

Virtual patching is a great method to protect web applications until they can be permanently fixed by developers. High-Tech Bridge and Fortinet now offer an integrated solution that audits web applications and web services (REST/SOAP) for vulnerabilities with High-Tech Bridge ImmuniWeb AI and then reliably protects them with FortiWeb virtual patching. Once a vulnerability is discovered, it is protected by FortiWeb instead of issuing disruptive emergency patches, or worse, waiting weeks or months for developers to deploy a new release while the application sits unprotected.

FortiWeb virtual patching uses a combination of sophisticated tools such as URLs, parameters, signatures, and HTTP methods to create a granular rule that addresses each specific vulnerability discovered by ImmuniWeb AI. A zero false-positives SLA is provided by ImmuniWeb AI to every customer, guaranteeing safe and reliable virtual patching that will not impact web application firewall (WAF) performance or website availability.

While virtual patching will not replace the traditional application development process, it can create a secure bridge between the time a vulnerability is discovered and the time a software release is issued to address it. In cases where it may not be possible or practical to change the application code, such as with legacy, inherited, and third-party applications, FortiWeb virtual patching can provide a permanent security solution for vulnerabilities.

ImmuniWeb AI uses its award-winning machine learning and AI technology for intelligent automation and acceleration of application security testing. The technology is enhanced with scalable and cost-effective manual testing when required, reliably detecting even the most intricate vulnerabilities and flaws in business logic. FortiWeb complements ImmuniWeb AI with granular application protection rules that take the imported vulnerability results and provide immediate mitigation with the same level of accuracy. This granular virtual patching is able to maintain application security until development teams are able to fully deploy permanent fixes in the application code. It can also extend the windows between security patches to minimize disruptions to the organization and its users.

BENEFITS

Using FortiWeb with High-Tech Bridge ImmuniWeb AI gives organizations:

- An enhanced solution that exceeds PCI DSS 6.5/6.6/11.3 and GDPR Art. 25/Art. 35.
- Absolute visibility across sophisticated web application vulnerabilities, weaknesses, and privacy issues.
- Prevention of data breaches and targeted attacks via corporate web applications.
- Minimized risk of exposure to threats between the time a threat is discovered until it is fixed by developers.
- Less disruptions due to emergency fixes and test cycles by virtually patching vulnerabilities until they can be permanently fixed.
- Protection for legacy, inherited, and third-party applications where development fixes are not an option or are impractical.
- More stability in application security patches as developers have more time to properly fix code vs. issuing emergency patches that have not had time to be fully tested.
- More accurate FortiWeb reporting and identification of attempts to exploit vulnerabilities discovered by ImmuniWeb AI.
- Additional flexibility and granular management of FortiWeb WAF policies based on ImmuniWeb AI audit results.
FIGURE 1: ONCE IMMUNIWEB AI AUDIT RESULTS ARE IMPORTED TO FORTIWEB, THEN FORTIWEB VIRTUAL PATCHING AUTOMATICALLY CREATES NEW WAF RULESETS TO PROTECT AGAINST NEWLY DISCOVERED VULNERABILITIES AND WEAKNESSES.