



Our Services Explained

We have developed a number of proprietary, patent-pending algorithms and automated tools to deliver the state-of-the-art in website security monitoring and testing. Our services are non-intrusive: they are offered on Software as a Service (SaaS) basis, they are run outside the firewall, and there is no software to install.

a. Detection: The **Health Monitoring (HM)** service runs daily to detect code injection. Code injection is a relatively new mechanism for disseminating viruses and performing identity theft by introducing malicious code or hyperlinks in compromised but legitimate websites. Code injection can shatter the reputation of a website, cause it to be blacklisted by search engines, and infect visitors to that site.

Our patent-pending code analysis algorithms allow the service to “watch-over” the website and detect malicious code inserted by hackers into the website. The HM service is fully automated: it immediately sends SMS or email messages pinpointing the malicious code to the appropriate people whenever infection is detected.

b. Prevention: The **Vulnerability to Penetration Assessment (VPA)** service evaluates the security level of the target site. The products used here are a series of sensing routines that are executed over a website as a service offering. The products explore for network and application level vulnerabilities by interrogating exposed website firewall characteristics, website code, back-end database constructs and server vulnerabilities to malicious attacks based on published and emerging susceptibilities. The assessment presents the results of the analysis in report formats that can be used by its customers to “harden” their sites without losing functionality.

Note that this preventive service is: (a) quite in-depth, so that similar services are offered called “penetration testing”, (b) necessary to minimize the chances of being hacked again, and (c) not offered by several competitors in this space. In addition, big security companies and IT consultants offer this service with significantly higher fees, because they do not have the automated tools we have developed, that minimize the need for manual effort.

c. Penetration Testing: The Penetration Testing service is an extensive “White-Hat attack”: an expert-led, manually-intensive attempt to gain unauthorized access to the site, thus emulating a malicious hacker attack. Our highly-skilled engineers use proprietary and industry-standard methods to break into the site. According to standard practices, the engineers leave subtle artifacts as a proof of a successful penetration. At the end, the engineers provide a detailed report and meet directly with the site administrators to tell them how the site was compromised and discuss ways to stop future attacks from breaking in.

d. Website Recovery: The Website Recovery service helps remove our customer’s website from Search Engine blacklists. It is primarily offered to signed-up customers who do not have the in-house expertise. The service includes the clean-up of the website files, and the submission of a request to Google’s blacklisting team. So far, the success of our Website Recovery has been 100%.

e. Security trustmarks are provided for our customers’ websites which are known to increase the visitor’s confidence (research suggests an 11% increase in sales). The security trustmarks indicate level of protection the website is receiving.