



## Website Healthcare: Protect your e-reputation

**The Problem:** Websites are under attack, as hackers find new ways to make money off the web. The web-security war is where the anti-virus war was ten years ago. At the heart of the matter lies *code injection*, a new cyber-crime proliferation mechanism that introduces malicious code or hyperlinks in compromised websites. The hackers hurt the visitors of the website, by infecting their computers, or performing identity theft. Although the hackers do not harm the website directly, the website can be blacklisted by search engines ruining its online reputation. Who is at risk? Every website is a target, businesses, government and military websites, and web hosting companies (“*Webhost hack wipes out data for 100K sites*”, VAServ Ltd hosting, 06/2009). The incidents are increasing at a rate that hints at a pandemic (“*Malware: Another pandemic of which you need to be aware*”, EDNews, 05/2009).

**Our Mission:** We provide a comprehensive suite of website healthcare services to safeguard a website and its e-reputation. The services can help prevent, detect and recover from an intrusion. Specifically, we can: (a) assess the vulnerability of a website, (b) detect security breaches in the form of *code injection*, and (c) facilitate the recovery of a compromised site and restore its on-line reputation.

**Our services:** Our services are offered on Software as a Service (SaaS) basis, and they are run outside the firewall. There is no software to install, and no need to change anything: just one more powerful security tool in one’s security arsenal. Our services are complementary to, but different from anti-spam, anti-virus, or firewalls.

a. **Health Monitoring (HM)** is a periodic check up of one’s website to detect code injection incidents before the Search Engines blacklist the website or its visitors are hurt.

b. **Vulnerability to Penetration Assessment (VPA)** is an in depth testing of the security level of a website that can prevent web-based intrusions.

c. **Penetration Testing** is an extensive “white-hat attack”: an expert-led, manually-intensive attempt to break into the site, emulating a malicious hacker attack.

d. **Website Recovery** is a service to help remove one’s website from Search Engine blacklists, offered to signed-up customers who do not have the in-house expertise.

e. **Security trustmarks** are provided for our customers’ websites, see below, which are known to increase the visitor’s confidence (research suggests an 11% increase in sales).

**The benefit:** Our services can reduce the operational cost of a company by: (a) **avoiding intrusions** by hackers, (b) **protecting the online reputation of a company** and keeping it off the blacklists of Search Engines, such as Google and Yahoo, and (c) **reducing a company’s IT cost** by reducing the workload and the number of IT professionals needed.

**Our advantage:** We are focused on web security, and because of that, we are in the forefront of technology, while others offer (or claim to offer) similar services as a side-offering. We have developed a number of proprietary, patent-pending algorithms and automatically synthesize and integrate the information from many different tools using Machine Learning and AI techniques with self-adapting capabilities. The novelty of our technology has been recognized by award no. 0839491 from the National Science Foundation.