

Web Application Firewall

At a Glance, HALOCK's Web Application Firewall solution marries the award-winning Barracuda Web Application Controller with HALOCK's seasoned team of security architects and secure application developers to offer your company the highest level of protection against hackers and web-borne attacks.

This fully-integrated solution secures against all common Web application threats including SQL injection, cross-site scripting attacks, session tampering and buffer overflows.

Additionally, if your company processes credit cards over the web, this solution satisfies section 6.6 of the PCI Data Security Standard version 1.1.



Web-based applications are increasingly at risk from professional hackers who target these applications in order to commit data **theft or fraud**. Being compromised can damage an enterprise's reputation, result in loss of customers and impact the organization's bottom line.

In addition, companies that process online transactions are faced with a host of growing industry regulations such as the Payment Card Industry Data Security Standard (**PCI DSS**).

The combination of these factors creates demand for a more robust and cost-effective risk **protection** solution for online Web applications.

Pricing for this solution includes both the Barracuda technology and HALOCK's professional services.

Our turn-key web application firewall solution is priced starting at approximately \$20k. This includes the hardware, initial configuration, training and deployment.

For additional information, please contact us to discuss your web-based application protection needs.

HALOCKSecurityLabs

www.halock.com | 1.866.781.7799

Solution Details



Protection
By implementing HALOCK's Web Application Firewall solution, you'll be protecting your company from these vulnerabilities

- ▶ Invalid and Non-validated Input
- ▶ Unified Access Control Vulnerabilities
- ▶ Ineffective Authentication and Session Management
- ▶ Cross-Site Scripting (XSS) Attacks
- ▶ Buffer Overflows
- ▶ Injection Flaws
- ▶ Improper Error Handling
- ▶ Insecure Storage
- ▶ Application Denial of Service (DoS)

Delivery
HALOCK engineers will implement your Web App Firewall by following this five phase delivery approach

Technical Assessment

HALOCK engineers will interview key members of your technical staff to gather specific details about the installation site.

Remote Configuration

HALOCK engineers will provision the Barracuda hardware and initialize it for use in your environment.

Local Configuration

Your staff will position the hardware in a secure location, connect it to an externally-accessible network, add AC power and turn the unit on. HALOCK will then complete the configuration remotely via one of many secure channels such as VPN.

Training and Acceptance

HALOCK engineers will host a remote training session for your technical staff via a ninety minute conference call. Your staff will learn how to manage the device and adjust it to actively block and monitor HTTP traffic.

Post Installation Support

Any additional assistance with promoting the device to actively monitor and block HTTP traffic or with other advanced options will be addressed outside of the flat configuration charge.

Related Services

Other HALOCK solutions to keep your company safe, in compliance and free from hackers

- ▶ Incident Response
- ▶ Source Code Analysis
- ▶ Penetration Testing (Ethical Hacking)
- ▶ Ethical Hacker Training

HALOCKSecurityLabs

www.halock.com | 1.866.781.7799