Web applications are at the center of business online and handle critical aspects of day-to-day operations. For many organizations, the implications of an attack on business-critical systems are tremendous: loss of revenue, sensitive data stolen, dissatisfied customers, and much time and money spent to remedy the situation.

Critical business applications are constantly threatened by common threats like SQL injection and XSS, as well as new, unknown zero day threats. ServerDefender VP’s (SDVP) host-based application security provides powerful, granular security. By customizing policies to your application’s needs, you can ensure your business stays protected and online.
Security Advantages

Monitoring
Interactive Log Viewer provides data on hack attempts in real-time. Sorting, filtering, and searching for specific events or parameters is quick and easy. Each logged event is interactive, providing powerful forensic tools. Possible actions that can be taken include: creating an exception, comparing against IIS logs, and blocking the offending IP permanently.

Reporting
Daily reports summarize key site traffic trends and anomalies. Reports can be configured to email nightly, weekly, monthly - or as much as you need them. This makes monitoring your app’s security or reporting to clients simple. But more importantly, it means you no longer must constantly access a server to check on things.

Granular Controls
No two pages or forms on a web app have the same security requirements. Thus, it's important to have the ability to perform custom configurations. Sophisticated controls let you shrink wrap security to perfectly fit a web app. SDVP’s sliders configure security at a high-level, but Expert View controls specify rules for individual forms and URLs, providing maximum control and stringent security.

Alerting
Configure email alerts to be sent when an event meets specific criteria. From each email alert, view threat details, and choose to block the offending IP address. This allows for rapid response times and stops hackers dead in their tracks.

Zero Day Protection
Zero-day attacks are brand new threats. These occur when a vulnerability exists that developers have no knowledge of and there is no patch for them. Detecting zero-day attacks is impossible for security systems that use signature lists. SDVP has stronger zero-day protection because it doesn’t rely on signature lists.

Threat Detection
Analyses, detects and responds to suspicious activity, accurately differentiating between trusted and untrusted behavior to thwart hacker attacks.

Threat Blocking
Before traffic can make it to IIS, it must first pass through SDVP. This allows SDVP to stop any malicious traffic before it has a chance to harm to your site or application.

We Protect
SharePoint  Exchange  Microsoft .NET
DOTNETNUKE  WordPress  Joomla

Compliances
HIPAA  PCI DSS

Security Features: Under the Hood

No Signatures
Most Web application firewalls use a database of attack signatures (known attacks) to detect and stop threats. This makes it easy for unknown threats to bypass the security controls. SDVP goes further by not using signatures, and instead looks for patterns necessary to execute attacks. This makes SDVP better equipped to handle new attacks.

Algorithm Based
SDVP uses an algorithm-based security model rather than the traditional signature-based model. Since there are a finite number of attack types, we programmed SDVP to understand the key aspects of each type of attack. This allows SDVP to detect the different categories with precision and prevent unknown attacks, catching the attacks that a signature based approach would miss.

Session-based User Scoring
Sometimes well-intentioned users accidentally do bad things. That doesn’t make them malicious. SDVP tracks a users session and scores them based on their behavior. When it sees too many malicious actions, SDVP temporarily blocks the user – then escalates to a permanent block if the activity continues.

Minimal Performance Impact
The performance of your Web server is critical to keeping your business up and running. That’s why SDVP is built to have a minimal impact on your server’s performance. Running SDVP uses about the same resources as turning on SSL.
Secures Against

**OWASP Top 10**

SDVP’s security controls were based on the OWASP Top 10 web vulnerabilities: the most prevalent security threats on the web. This makes SDVP well suited to handle the most commonly seen threats.

**Attack Categories & Security Controls**

SDVP defends against the most prevalent security threats on the web.

- SQL Injection
- Input Validation Error
- XSS
- HTTP Request Smuggling
- Buffer Overflow
- Cookie Tampering
- IP Blocking
- Directory Browsing
- Unauthorized Resource Request
- Unauthorized File Upload
- Unauthorized HTTP Method
- Unauthorized URL Request
- Country Blocked
- 5xx Error
- HTTP response splitting
- User-agent Blocking
- Missing referrer
- Session expiration
- Suspicious 404

**The Port80 Difference**

**A Different Approach to Security**

Using a database of attack signatures may be a good business model, but it doesn’t make for a good security model. Port80 Software is in the business of security. To us, that means providing real security. Our approach protects against known and unknown threats. We don’t use signatures. Instead, we use an algorithm-based approach that eliminates the need for constant updating – so you can always be secure.

**Cost Effective**

Web application firewall appliances can cost tens, if not hundreds of thousands of dollars. SDVP offers the functionality of an appliance WAF, but at a fraction of the cost (up to 40% savings versus competing products), making it ideal for small and medium sized businesses as well as larger enterprises.

**Requirements**

- WindowsServer 2003 with IIS6
- Windows Server 2008 with IIS7
- Windows Server 2008 R2 with IIS7.7
- Windows Server 2012 with IIS8