CLOUD WAF ON-DEMAND
Cloud-Based Web Application Firewall (WAF)

Managed Web Application Firewall (WAF)

Security On-Demand’s™ Managed Web Application Firewall Service provides real-time, continuous web application monitoring and active defense to help protect your data. We provide continuous 24x7x365 security monitoring to help detect if web-facing applications are being breached and then immediately take measures to protect and defend.

Web Application Security Challenges

Security On-Demand’s™ Web Application Firewall (WAF) managed firewall service is designed to help you solve issues that are critical to the security of your web applications.

- Web Applications are the number one source of vulnerabilities targeted by hackers
- Vulnerability scanners cannot very well detect application defects
- Identity Theft & Information leakage of insecurely-coded applications
- Targeted Application attacks are typically missed by firewalls, IDS, and IPS devices targeted
- Secure Coding initiatives are a recommended Best Practice, however are usually difficult to implement
- Too much code & too few skilled developers that can fix applications
- Connections between component applications typically insecure

Business Benefits

Security On-Demand™ can help to relieve the burden and liability involved with managing and maintaining business applications, e-commerce sites, intranets and other applications utilizing web-based data architecture.

Our service offering provides the following benefits:

- Lower Cost of Ownership on Solution & Increased ROI - due to leveraging a partner expertise, experience previously developed
- Speeds Time to Deployment
- Relieves Cap Ex Costs - Hardware, Licensing, Support & Monitoring rolled into a single monthly price
- Reduce Product Learning Curve - Product Expertise required to tune, maintain, upgrade, monitor, and manage is minimized
- Relieve Staffing Burden and coverage hours by leveraging our 24x7 Staffing Coverage, 365 Days per year
- Pre-Integrated with other “On-Demand” solutions Including firewall, IPS, IDS, SIM, Reporting, & Logs

Key Features

Our technology is based on the leading industry Web Application Firewall technology featuring:

- Real-time Continuous Monitoring & Web enforcement
- Non-Intrusive-Deploys “Out-of-Band”
- Dynamic Application Profiling
- Inbound & Outbound Traffic Analysis
- Application Security Defect Detection
- Out-of-the box PCI Compliance
- SSL Attack Detection
- Security Dashboard & Alert Console integrates alerts from other security devices.

We ensure Compliance with Section 6.6 of the Payment Card Industry (PCI) Data Security Standard
CLOUD WAF ON-DEMAND
Cloud-Based Web Application Firewall (WAF)

System Architecture
- Non-Intrusive - Deploys “Out-of-Band”
- Positive Security Models - includes Dynamic Profiling which determines what “normal” behavior is for web applications
- Negative Security Model - utilizes signatures, application scanning to identify specific attacks
- Powerful Correlation Engine to determine Event Severity
- Defends against both existing, known vulnerabilities as well as emerging threats
- Addresses “Screen Scrape” threats used for Man-in-the-middle based, targeted attacks

Key Advantages
- Real-time Continuous Monitoring & web enforcement
- Automates compliance with industry standards - such as the Payment Card Industry (PCI) Data Security Standard
- Detects web application defects that vulnerability scanners tend to miss
- Helps to automate regulatory compliance - Section 6.6 requiring a Web Application Firewall or conducting an expensive and time consuming code review
- Helps bridge gap between security & development teams with detailed reports on sources of vulnerabilities
- Data leakage protection of sensitive information

Security Operations Monitoring
- Monitored Protocols: HTTP, HTTPS, (SSL), SML, web Services, SOA and AJAX
- Customized Policies based on PCI Compliance, Hosting, and Audit
- Alerting & Monitoring Response Options: Phone, e-mail, automated blocking
- Severity Mapping: Based on Levels 1-5 for default incident handling priorities
- Blocking Capabilities include: TCP reset, web server agent, user logout, auto-push firewall rule & integrate with other devices