SiteWALL

Web Application Firewall

Simplifying Web Application Security

Datasheet

May 2024

PAGE NTRA

SiteWALL Web Application Firewall

Secure Applications, Safeguard Critical Data and Ensure Resource Availability

Cloud-Based Solutions for Enhancing Application Security

In the current digital era, web applications are critical for the prosperity of major companies, playing a central role in generating revenue, enhancing brand identity, and deepening customer engagement. Despite their importance, these applications are increasingly targeted by global cybercriminals seeking to breach IT systems and access vital corporate data. The shift towards rapid, agile development often leads to premature releases of applications, making them prone to cyber threats. This situation is compounded by the rising frequency and sophistication of cyberattacks on web applications and servers, highlighting the inadequacy of traditional perimeter security measures and underscoring the urgent need for robust, flexible, and scalable web security solutions to prevent data breaches and service disruptions.

Next Generation Protection Tools

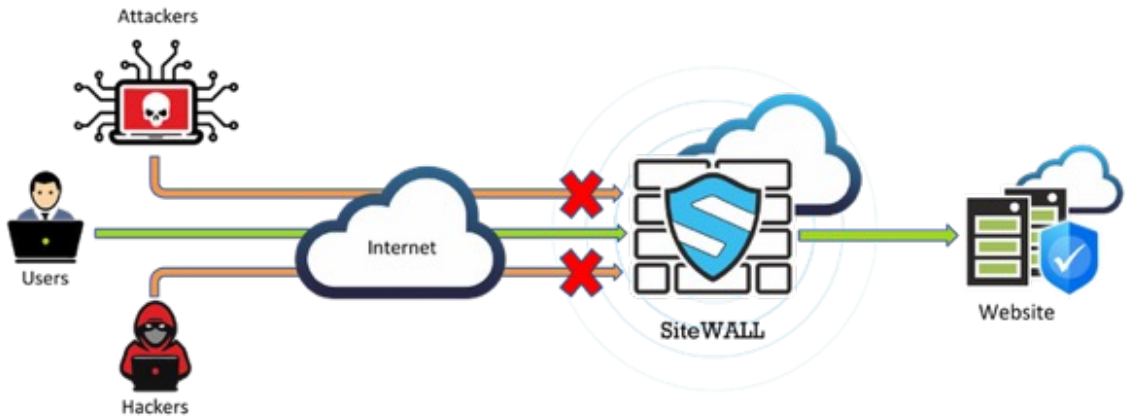
SiteWALL Web Application Firewall, an AI/ML-based next-generation solution by PageNTRA Infosec Pvt. Ltd. delivers unmatched defense for enterprises against sophisticated online threats. Expertly crafted to protect websites and applications in varied settings, including cloud and on-premises, it effectively combats a wide range of application-layer hacking tactics. The solution includes comprehensive services like L7 DDoS, advanced bots, malware protection, and API protection. Utilizing advanced AI technology, **SiteWALL** WAF adeptly transforms numerous security incidents into concise, actionable reports, enhancing SOC efficiency and lowering risk. Its seamless integration with leading SIEM systems and the strategic deployment of security measures at the network edge solidify its status as a top-tier tool for protecting vital digital assets against ever-evolving cyber threats.

Effortless Deployment for Universal Protection Across All Your Web Applications

The **SiteWALL** multi-tier threat engine conducts real-time profiling of all incoming traffic, effectively distinguishing between legitimate and malicious clients well before they reach a web application. This automated security process not only enhances web security but also reduces the utilization of web server resources and minimizes bandwidth consumption. Furthermore, it decreases the reliance on in-house security experts and eliminates the potential inaccuracies associated with manual controls.

It's no surprise that **SiteWALL** WAF customers opt for deploying the solution in blocking mode right from the outset. This is because it allows legitimate traffic to pass through with zero false positives. **SiteWALL** is designed to enhance the security of any web application's attack surface, regardless of its location, while still maintaining efficiency and effectiveness.

SiteWALL WAF offers flexible and comprehensive protection for all web applications, whether they are hosted on-premises or in the cloud. It adopts a streamlined approach that removes the need for excess and underutilized capacity, ensuring cost-effective and efficient security.



Key Features

- AI/ML Powered Next Gen - Web Application Firewall
- Built-in Redundancy
- L7 DDoS Protection
- API Protection
- Malware Scanning.
- Bot Protection
- OWASP Top 10 Risks
- Vulnerability scanning & Management.
- Virtual Patching
- Website Defacement Detection.
- Web-Shell Detection
- Website Cloning Detection.
- Integrated Threat Intel
- Attack Analysis with Dynamic Detection.
- SIEM Integration

Advanced Application Security Protection

SiteWALL WAF goes beyond providing protection against just the OWASP Top 10 security threats, which include vulnerabilities like cross-site scripting, illegal resource access, and remote file inclusion. It actively blocks these attacks in real time. In addition to guarding against these threats, SiteWALL, with its multi-tier threat engine, leverages various mitigation capabilities tailored to different types of attacks, whether it's countering a DDoS attack or thwarting a bot attempting a SQL injection against your API and web applications.

SiteWALL's research team is at the forefront of cybersecurity, actively identifying emerging threats to ensure our clients have the most current protection in the rapidly evolving cyberattack landscape. These experts diligently monitor external sources for new vulnerabilities and work to mitigate the risks associated with third-party code.

The **SiteWALL** research team meticulously analyzes traffic through **SiteWALL**'s threat intelligence system, swiftly identifying and neutralizing new threats. This proactive approach results in daily updates of security signatures to defend against the latest threats, providing our customers with robust, maintenance-free security solutions.

User-Friendly and Scalable with Ease

SiteWALL WAF distinguishes itself with an intuitive and easy-to-use web interface, simplifying policy configuration without the need for manual intervention. By harnessing AI and ML, it skillfully customizes security rules, ensuring robust defense in diverse settings and automating policy updates. This approach makes **SiteWALL** stand out from other WAFs, which typically demand considerable dev-ops or administrative input. Its inherent learning abilities and user-friendly interface promote quick and efficient inline block mode deployment, reducing administrative efforts. Moreover, the WAF's interactive dashboard provides detailed traffic analysis and a comprehensive view of your organization's security situation, centralizing management and integrating advanced features like API security and DDoS protection.

Comprehensive Vulnerability Management with Virtual Patching

SiteWALL significantly boosts the ability of security teams to quickly detect and address key web application vulnerabilities. Combining the detection and defense capabilities of **SiteWALL** WAF with extensive vulnerability scanning and automated patching, it reduces false positives and strengthens the security of all web applications, including legacy and unpatched ones. Regularly updated rule sets provide a solid defense against various threats.

Additionally, **SiteWALL** offers comprehensive assessments and actionable insights into web application security postures and risk scores, along with a detailed executive summary that includes risk assessments, technical vulnerability analysis, and tailored security recommendations.

This all-in-one approach simplifies vulnerability management and threat mitigation, reducing the complexity and cost of operations by integrating these functions into a single interface.

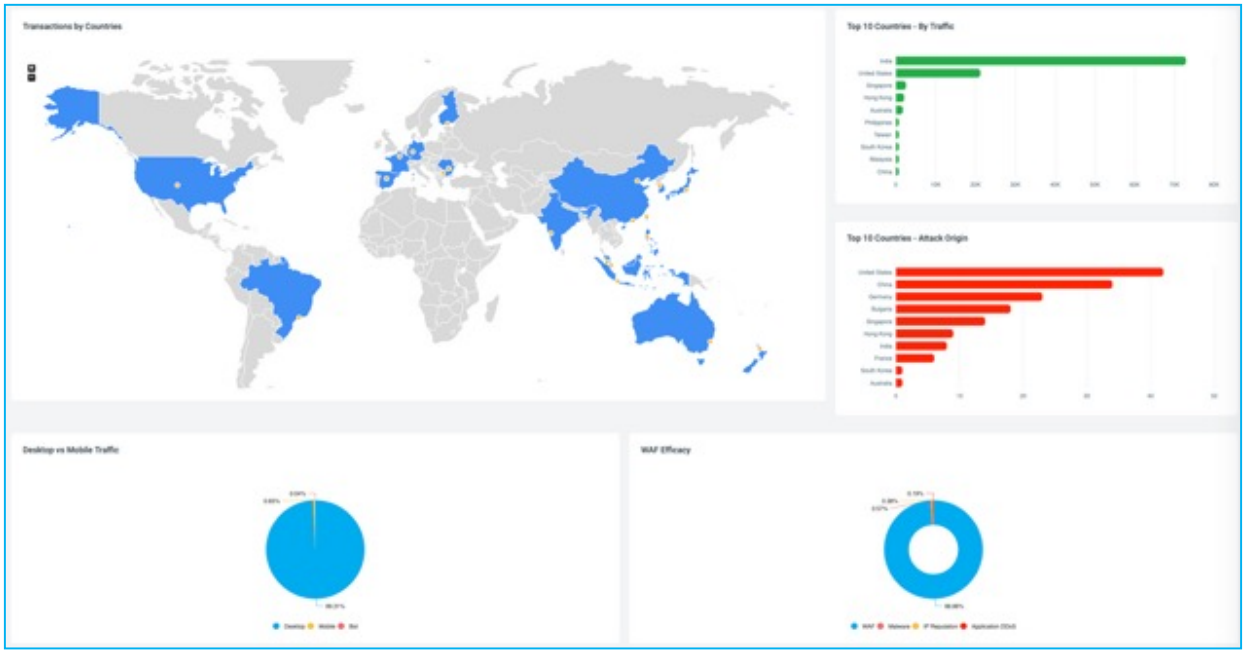
Simplified Compliance

SiteWALL Web Application Firewall (WAF) plays a crucial role in enhancing compliance and security. It acts as a robust barrier against attacks on web applications, which could compromise sensitive data. With the increasing reliance on web applications by a variety of organizations, such as web application developers, social media platforms, and digital banks, the role of WAFs becomes increasingly critical.

SiteWALL WAF not only meets compliance standards like PCI DSS 6.6 but also implements specific access controls based on geographic and network criteria. Its capability to protect sensitive customer and payment information makes it a key component in an organization's security strategy in today's interconnected digital environment. To meet various regulatory compliance requirements, **SiteWALL** offers 180 days of log storage for organizations.

Security Analytics

As the attack surface broadens and cyber threats grow more sophisticated, security teams worldwide are inundated with alerts, many of which lack context. With the migration of applications to the cloud adding new challenges, teams need tools to sift through the noise and focus on genuine threats. **SiteWALL** employs machine learning algorithms to discern attack patterns across all application assets, aggregating them into security incidents and assigning severity levels. This intelligent approach helps distinguish actual threats from informational alerts and false positives, enabling SOC analysts to swiftly concentrate on the most critical issues.



Key Benefits

Application Security
Shield your applications and APIs from application-layer attacks with automated policies designed to adapt to the evolving threat landscape.

Effortless Deployment
Accelerate your path to enhanced security by swiftly onboarding applications with guidance from **SiteWALL**'s seasoned professionals.

Cloud-Based Solution with Built-In Redundancy for Uninterrupted Business Operations
Utilize **SiteWALL**'s redundant service architecture to ensure uninterrupted application security and availability.

Affordable Initial Investment and Cost-Effective Long-Term Ownership
SiteWALL Cloud Services provide Customers with affordable access to critical security solutions, thereby maximizing their return on investment.

Enhanced Staffing Support, Immediate Access to WAF Experts, and Collective Knowledge Resources.
Customer teams can form collaborative partnerships with **SiteWALL**'s security experts, who are consistently available and equipped with up-to-the-minute threat intelligence from **SiteWALL**'s R&D teams.

Robust Layer 7 DDoS defense
SiteWALL WAF services provide automated Layer 7 DDoS protection, featuring rate limiting with zero manual intervention.

SiteWALL Web Application Firewall

Learn more about **SiteWALL** Web Application Firewall online at https://www.sitewall.net

Reach Us Out

Simplifying Web Application Security

PageNTRA Infosec Pvt Ltd
L-383, Dreams – The Mall, LBS Marg,
Bhandup-West Mumbai – 400078

contact@pagentra.com

www.sitewall.net
www.pagentra.com