

Citrix Application Firewall

Comprehensive protection for web applications and web servers

KEY BENEFITS

Delivers PCI-DSS v.1.1 compliance

Protects credit- and debit-card account numbers, enabling your organisation to comply with the Payment Card Industry Data Security Standards.

Protection of sensitive consumer information

Protects data behind Web infrastructure from theft of identity and bank and credit accounts. Eliminates data losses for which government regulations require customer notification.

Protects online revenue sources

Ensures uptime of websites and Web Services by preventing Layer 7 denial of service attacks. Application Learning ensures protection without false positives. Maintains trust relationship between consumer and vendor by preventing cross-site scripting (XSS) attacks.

Point to Point Ltd
Mulberry House
Osborne Road
Wokingham
Berkshire RG40 1TL



T: +44 (0) 118 936 9500
F: +44 (0) 118 936 9501
E: marketing@ptop.co.uk

Citrix Application Firewall™ is a high-performance security appliance solution that blocks all known and unknown attacks against Web applications and infrastructure. Citrix Application Firewall enforces a positive security model that permits only correct application behaviour, without relying on attack signatures. Application Firewall analyses all bi-directional traffic, including SSL-encrypted communications, protecting against 16 classes of Web application vulnerabilities without any modification to applications. Citrix Application Firewall technology is available as an option for Citrix® NetScaler™ or as a stand-alone product offering. The stand-alone Citrix Application Firewall is available on appliances that match a range of performance needs, and is compatible with many load-balancing solutions on the market.

Addressing today's security challenges

Web applications are prone to attacks and exploits from both the internet and within the organisation, because they front databases which contain sensitive and valuable information. Customised and layered Web applications are vulnerable to exploits and hard to protect with fixed signatures or patches. Network-level security infrastructures such as firewalls and intrusion-prevention systems cannot defend against application layer attacks. Web applications and servers are left exposed to a myriad of known and unknown exploits. Citrix Application Firewall comprehensively addresses the challenge of delivering centralised application-layer security for all Web applications.

The positive security model advantage

Citrix Application Firewall enforces a positive security model to ensure correct application behaviour. Instead of relying on attack signatures or pattern-matching techniques, the positive security model understands "good" application behaviour, and blocks as malicious any deviation from proper application activities. It is the only proven approach delivering "zero-day" protection against unpublished exploits.

Powerful business object protection

Citrix Application Firewall prevents in real time the inadvertent disclosure of sensitive application content, which could result in identity theft and fraud. Business object protection modules help to secure both predefined objects such as credit- or debit-card numbers, and administratively defined data objects. By detecting erroneous disclosures and blocking or rewriting content, business object protection modules help to conform to governmental privacy regulations and industry regulations such as the Payment Card Industry Data Security Standard (PCI-DSS).



Tailoring security policies with the Citrix Adaptive Learning Engine

Citrix Application Firewall incorporates a third-generation Adaptive Learning Engine that discovers aspects of application behaviour that might be blocked by the positive security model even if the behaviour is intended by the Web application. Once application behaviour is learned, Application Firewall generates human-readable policy recommendations, which bring to security managers a clearer understanding of actual application behaviour. Tailored security policies may then be applied to each application.

Industry-leading performance

Citrix Application Firewall performance exceeds that of the highest-performing Web servers, and can improve application performance and response time by offloading from Web servers compute- and memory-intensive TCP connection management. Application Firewall-to-server communication uses a small set of persistent TCP connections. Dedicated silicon-based SSL hardware allows for the detection of malicious traffic within encrypted tunnels. SSL encryption and key generation offload can improve overall application performance by relieving servers from these operations. Also included is an option for fully encrypted communication from Application Firewall to the application servers.

Centralised security for all Web applications

Application Firewall can secure an organisation's entire Web application infrastructure, with complete separation of each application's security policies, controls, reporting details and log data.

Flexibility to adapt to changing business requirements

Application Firewall permits flexible, stepwise deployment of Web application protection. The default Web application protection profile defends against the most common dangerous threats, adding full protection against both data theft and layer 4-7 Denial-of-Service attacks. The advanced Web application protection profile adds session-aware protections for advanced Web applications that include authenticated access to sensitive data. Protection is extended to dynamically-generated elements such as cookies, form fields, and session specific URL's. Such protection is mandatory for e-commerce, online financial services, and secure extranet applications, and includes application learning capabilities to help the administrator create managed exceptions and relaxations for the security policy for applications whose intended behaviour might cause violation of the default security policy. Citrix Application Firewall is available on multiple hardware platforms to meet the performance and availability requirements of any organisation — from small enterprises to large data centres. FIPS-140-2 Level 3-compliant models are also available.

Point to Point Ltd
Mulberry House
Osborne Road
Wokingham
Berkshire RG40 1TL



T: +44 (0) 118 936 9500
F: +44 (0) 118 936 9501
E: marketing@ptop.co.uk

