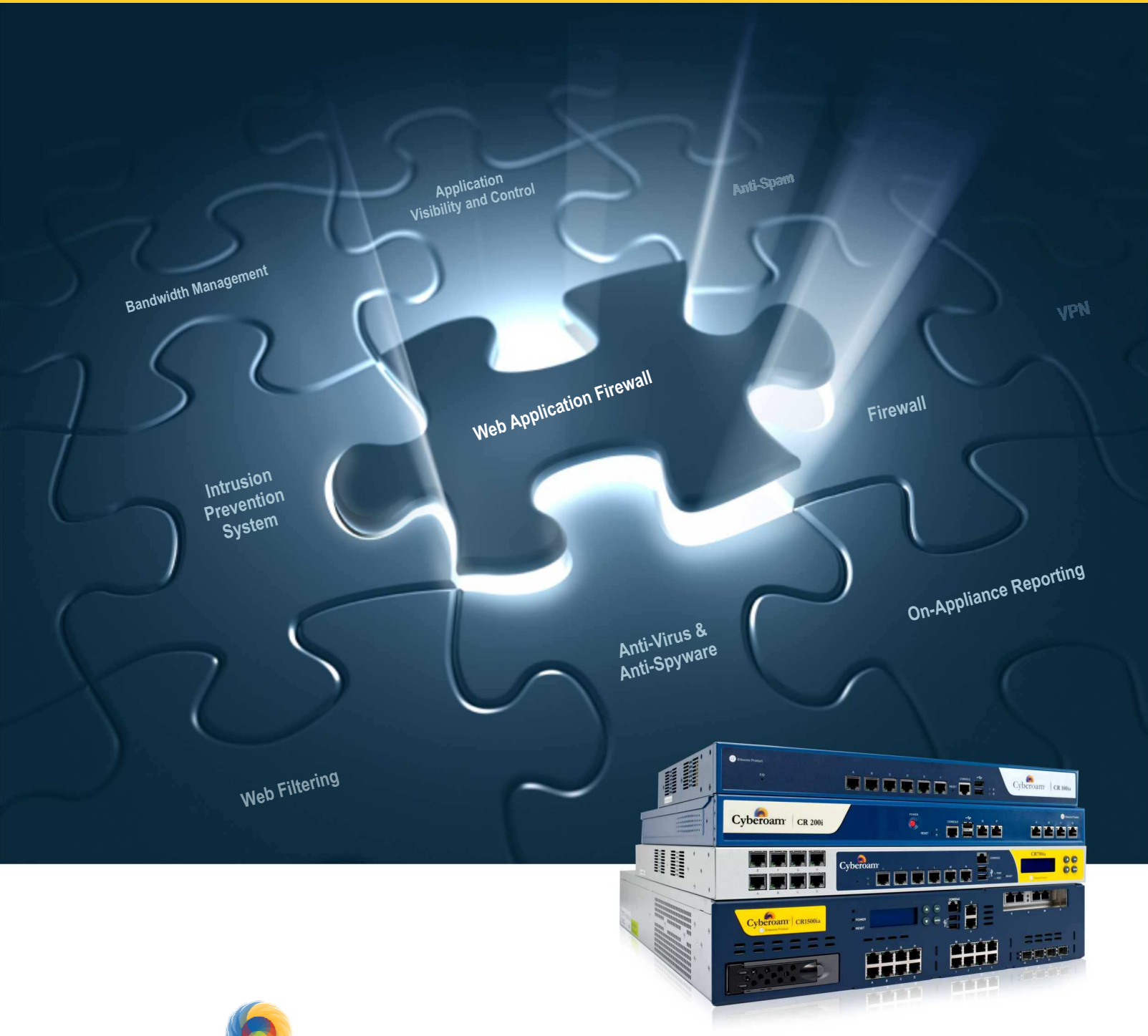
Web Application Firewall Subscription on Cyberoam UTM appliances

Protecting Web Applications from hackers



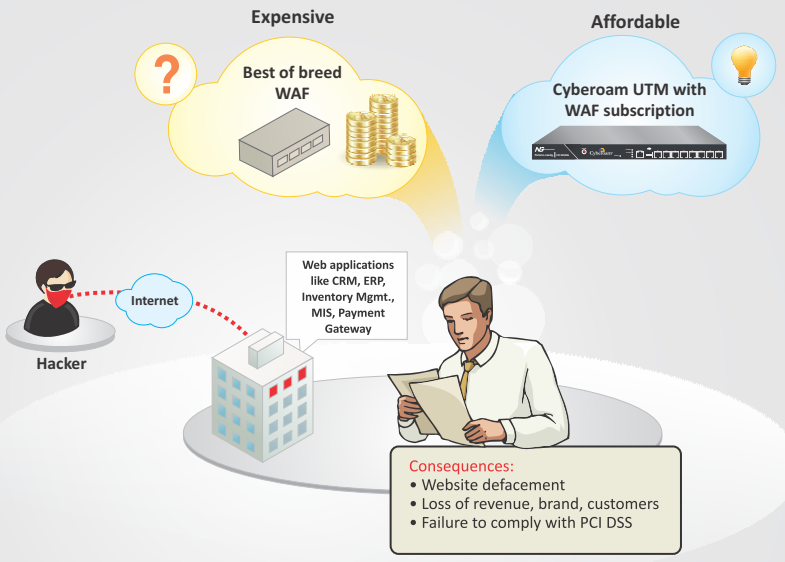
Cyberoam
Securing You

www.cyberoam.com

Introduction

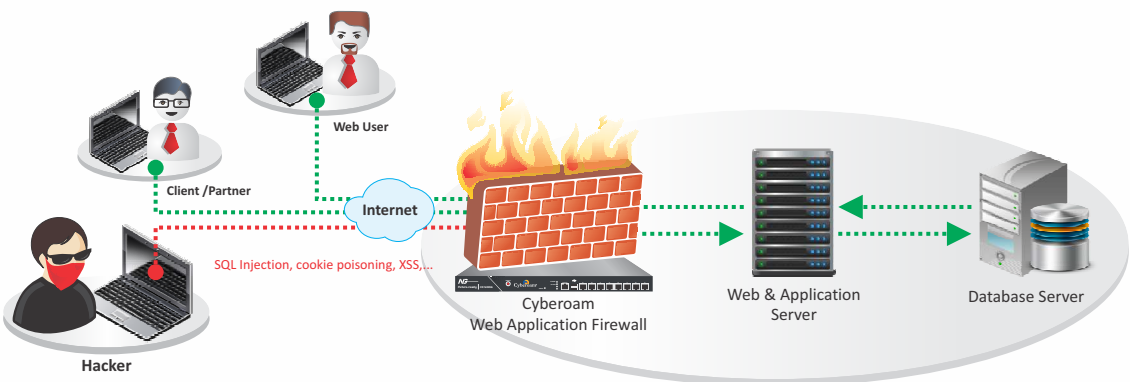
Today, organizations host critical web-based applications like CRM, ERP, inventory management, online banking and E-commerce applications, and more, that serve business information to employees, partners and customers. However, hackers are increasingly exploiting vulnerabilities present in these web-applications to break into organizations' IT networks and reach the database server where all corporate data resides. This can result into loss of business and customer data, IPR theft, downtime, and more, leading to loss of reputation, business and customers. Unfortunately, no organization is today left out from web-application attacks, including Governments, banks, retail, manufacturing organizations, and more.

With Cyberoam's Web Application Firewall available as a subscription on its UTM appliances, SMBs no longer need to make a choice between the need and luxury of securing their applications using a Web Application Firewall. So far, lack of a simpler and better WAF option deferred their investment in a Web Application Firewall. In enterprises, Cyberoam WAF removes the need of spending a fortune in securing critical web applications by offering the Web Application Firewall subscription at a minimal extra cost, which comes along with a host of other security features of a Unified Threat Management. Cyberoam WAF can be easily deployed in an organization's security infrastructure without requiring any change to existing Web applications.



Cyberoam's Web Application Firewall

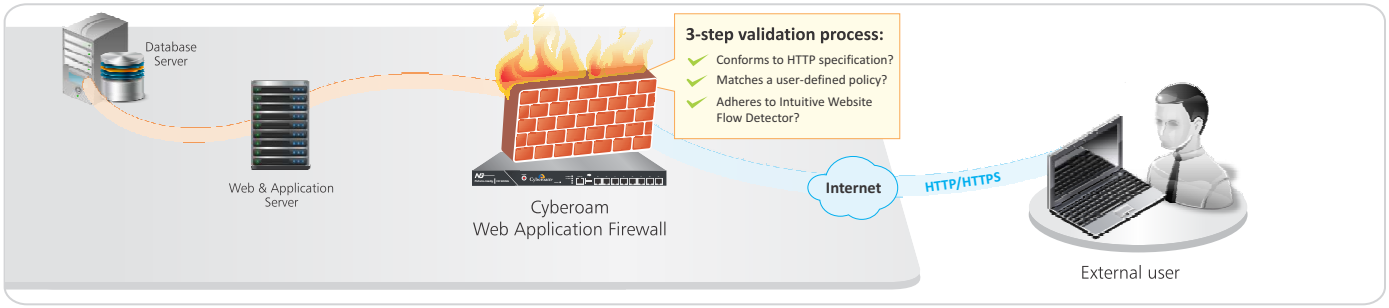
Cyberoam Web Application Firewall is available as a subscription on Cyberoam UTM appliances. It follows the positive security model based on its Intuitive Website Flow Detector to secure websites and Web-based applications against attacks like SQL injection, cross-site scripting (XSS), URL parameter tampering, session hijacking, buffer overflows, and more, including the OWASP Top 10 Web application vulnerabilities.

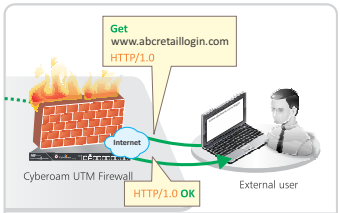


Cyberoam Web Application Firewall Protection against Web-based Application Attacks

Cyberoam Web Application Firewall is deployed to intercept the traffic to and from the web servers to provide an added layer of security against attacks before they can reach the web applications. Its Intuitive Website Flow Detector intelligently "self-learns" the legitimate behavior and response of web applications. Based on the Intuitive Website Flow Detector, the Web Application Firewall ensures the sanctity of web applications in response to server requests, protecting them against web application attacks. Cyberoam Web Application Firewall looks at every request and response within the HTTP/HTTPS/Web Service layers. It is effective at repelling attacks from a wide range of commercial and open-source automated vulnerability scanners (e.g. Nessus, WebInspect), as well as hand-crafted attacks.

How Cyberoam Web Application Firewall Works?

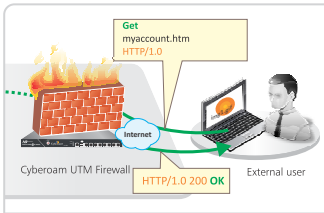




1 HTTP Protocol Specification

Supports HTTP protocol specification versions 1.0/1.1

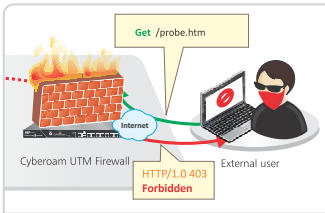
```
<html>
  <head>
    <title>Home Page</title>
  </head>
  <body>
    <a href="myaccount.htm">Page 2</a>
    <img src="images/img1.gif" />
  </body>
</html>
```



2 Intuitive Website Flow Detector

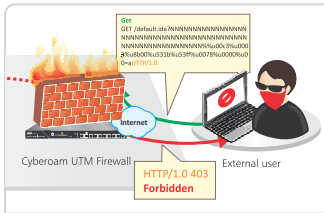
Request is legitimate and adheres to the Intuitive Website Flow Detector's "self-learning" in the past, when such a request was last made to the Web server.

```
<html>
  <head>
    <title>Page 2 </title>
  </head>
  <body>
    <a href="myservices.htm" >Page 3</a>
    <img src="images/img2.gif"/>
  </body>
</html>
```



3 User-defined policies

The server request was not found valid under the Intuitive Website Flow Detector's knowledge from the past – the requested URL cannot be the entry point and it is, hence, blocked from reaching the Web server and the browser receives an HTTP 403 Forbidden response code. No other information is exposed as decided under the User Defined Policy.



Code Red Attack (or any variant)

The request doesn't pass any of the 3 validation steps. Web server is thus protected from present/future URL-based HTTP attacks.

Features:

Positive protection model without Signature Tables

The Cyberoam Web Application Firewall enforces a positive security model through Intuitive Website Flow Detector to automatically identify and block all application-layer attacks without relying on signature tables or pattern-matching techniques. The Web Application Firewall considers defined Web application behavior as "good". Any deviation is considered "bad", or malicious, and is blocked accordingly. This provides security against zero-day attacks and eliminates the need to manually populate and update signature tables. The Intuitive Website Flow Detector automatically adapts to changes in the website.

Comprehensive business logic protection

The Cyberoam WAF protects against attacks like SQL injection,cross-site scripting (XSS),and cookie-poisoning that seek to exploit business logic behind Web applications, ensuring they are used exactly as intended.

HTTPS (SSL) encryption Offloading

Attackers cannot bypass the Cyberoam WAF protection measures through an HTTPS (SSL) connection, mostly used in the financial services, healthcare, e-commerce, and other industries that process sensitive data. The WAF not only secures encrypted connections, but also reduces latency of SSL traffic with its SSL offloading capabilities.

Instant Web server hardening

The Cyberoam WAF instantly shields any Web environment (IIS, Apache, WebSphere®, etc.) against the more than 14,000 common server mis-configurations and an ever-expanding universe of known 3rd-party software vulnerabilities.

Reverse proxy for incoming HTTP/HTTPS traffic

The Cyberoam WAF follows a reverse proxy model for all incoming HTTP and HTTPS traffic which provides an added level of security by virtualizing the application infrastructure. All incoming Web application requests from the Web client terminate at the WAF. Valid requests are submitted to the back-end Web server, hiding the existence and characteristics of originating servers.

URL , Cookie, and Form hardening

Application-defined URL query string parameters, cookies, and HTML form field values (including hidden fields, radio buttons, checkboxes, and select options) are protected by the Cyberoam WAF. Attempts to escalate user privileges through cookie-poisoning, gain access to other accounts through URL query string parameter tampering, and other types of browser data manipulation are automatically identified and blocked.

Monitoring and reporting

Cyberoam Web Application Firewall provides alerts and logs that help organizations with information on types of attacks, source of attacks, action taken on them, and more that help comply with the PCI DSS requirements.

Additional Features:

- Block/alert known bad IP addresses
- Customizable user messages for blocked requests
- Rate-based connection safeguards

Business Benefits

- Offers instant protection without requiring changes to existing Web applications when deployed.
- Prevents intruders from manipulating web content
- Protects data inside the organization from being hacked by exploiting Web application vulnerabilities
- Secures corporate brands, trade secrets, and Intellectual Property
- Maintains customer confidence in your website's security, especially for banks, e-commerce, and more.
- Ensures sensitive information about the environment doesn't go out to hackers by sending customizable error messages to users.
- Easy to use with no special training required for administrators
- Low maintenance as it automatically adapts to website / web-application changes
- Promotes integrity and availability of Web applications
- Helps comply with mandatory PCI requirements

WAF subscription available on following Cyberoam UTM Appliances :

Cyberoam NG series Appliances :

CR25iNG, CR25wiNG, CR25iNG-6P, CR25wiNG-6P, CR35iNG, CR35wiNG, CR50iNG, CR100iNG, CR200iNG, CR200iNG-XP, CR300iNG, CR300iNG-XP, CR2500iNG

Cyberoam ia series Appliances :

CR50ia, CR100ia, CR200i, CR300i, CR500ia, CR750ia, CR1000ia, CR1500ia

Cyberoam
Securing You

sales@cyberoam.com | www.cyberoam.com

Awards & Certifications

2008 - Emerging Vendor of the Year

Cyberoam Technologies
505 Thornall Street, Suite # 304, Edison,
New Jersey 08837, USA, Tel: 201 -301-2851

India
901, Silicon Tower, Behind Pariseema Building, Off, C.G.Road,
Ahmedabad 380 006, INDIA, Tel: +91-79-66065606

Toll Free Numbers
USA : +1-800-686-2360 | **India :** 1-800-301-00013
APAC/MEA : +1-877-777-0368 | **Europe :** +44-808-120-3958

Business Benefits

- Offers instant protection without requiring changes to existing Web applications when deployed.
- Prevents intruders from manipulating web content
- Protects data inside the organization from being hacked by exploiting Web application vulnerabilities
- Secures corporate brands, trade secrets, and Intellectual Property
- Maintains customer confidence in your website's security, especially for banks, e-commerce, and more.
- Ensures sensitive information about the environment doesn't go out to hackers by sending customizable error messages to users.
- Easy to use with no special training required for administrators
- Low maintenance as it automatically adapts to website / web-application changes
- Promotes integrity and availability of Web applications
- Helps comply with mandatory PCI requirements

WAF subscription available on following Cyberoam UTM Appliances :

Cyberoam NG series Appliances :

CR25iNG, CR25wiNG, CR25iNG-6P, CR25wiNG-6P, CR35iNG, CR35wiNG, CR50iNG, CR100iNG, CR200iNG, CR200iNG-XP, CR300iNG, CR300iNG-XP, CR2500iNG

Cyberoam ia series Appliances :

CR50ia, CR100ia, CR200i, CR300i, CR500ia, CR750ia, CR1000ia, CR1500ia

Cyberoam
Securing You

sales@cyberoam.com | www.cyberoam.com

Awards & Certifications

2008 - Emerging Vendor of the Year

Cyberoam Technologies
505 Thornall Street, Suite # 304, Edison,
New Jersey 08837, USA, Tel: 201 -301-2851

India
901, Silicon Tower, Behind Pariseema Building, Off, C.G.Road,
Ahmedabad 380 006, INDIA, Tel: +91-79-66065606

Toll Free Numbers
USA : +1-800-686-2360 | **India :** 1-800-301-00013
APAC/MEA : +1-877-777-0368 | **Europe :** +44-808-120-3958