



## Unified Threat Management



Elitecore Product

[www.cyberoam.com](http://www.cyberoam.com)  
Contact: [info@cyberoam.com](mailto:info@cyberoam.com)



## Internet threats take many forms

- Viruses, Worms, Trojans
- Spam
- Intrusions
- Indiscriminate Surfing
- Spyware
- Phishing and Pharming
- Bandwidth abuse

Today's typical Internet threat takes a blended attack form, targeting individual users to gain control over networks and data. Successful defense depends on preemptive, blended action with a high level of granular, user-identity based controls.

## Granular Solution to Complex Threats

### Granular Controls

Given the increasingly user-based nature of attacks, fine granular controls are a necessity to contain future threats. Granularity need not be compromised to attain unified security.

### Blended Solution

Enterprises that have deployed individual security solutions face the daunting task of managing and upgrading multiple solutions constantly while leaving loopholes in enterprise defense. For proactive security, they are turning to blended, coordinated solutions over a single platform.

Cyberoam offers intelligent threat management with blended security supported by user-identity controls. This leaves no loop holes in the network nor does it involve expensive, difficult-to-manage duplications that raise the cost of purchase, processor load and multiple, time-consuming policy setting.

Cyberoam is the unified threat management solution that offers integrated Internet security with fine granularity through its unique user-identity based policies.

Cyberoam delivers dependable network protection to corporates and educational institutions through easy to deploy and manage appliances and software.

Cyberoam's unique user-based management offers granular controls for flexibility and ease-of-use that offset the high levels of complexity involved in a unified threat management solution.



## Features

Cyberoam offers a well-coordinated defense through tightly integrated best-of-breed solutions over a single interface. The result is a complete, dependable shield that Internet threats find extremely difficult to penetrate.

- Identity based Firewall
- VPN - Virtual Private Network
- Gateway Level Anti-Virus
- Gateway Level Anti-Spam
- IDP—Intrusion Detection and Prevention
- Content Filtering
- Bandwidth Management
- Multi-Link Manager
- Intelligent Reporting

## Identity Based Advantages

Cyberoam is the only UTM that embeds user identity in firewall rule matching criteria, which offers instant visibility and proactive controls over security breaches.

### Eliminates Dependence on IP Address

Unlike traditional firewalls, Cyberoam's identity-based firewall does not require IP address to identify the user. This empowers administrators to control user access irrespective of login IP address.

### Complete Security in Dynamic IP Environments

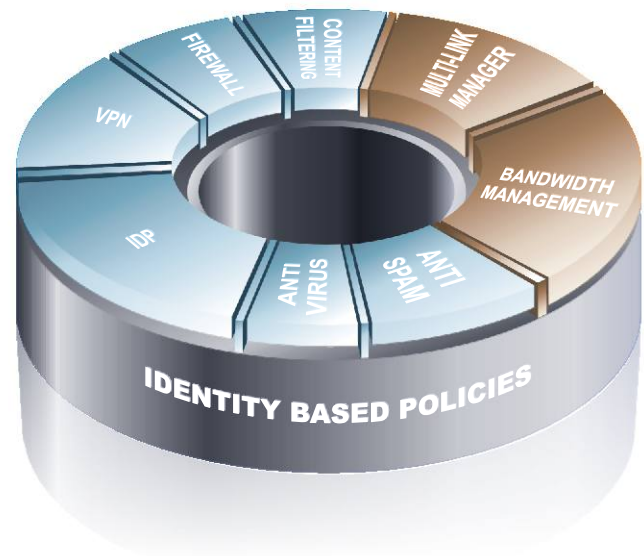
Cyberoam provides complete security in dynamic IP environments like DHCP and Wi-Fi where the user cannot be identified through IP addresses.

### One Step Policy Creation

Cyberoam's identity-based security links all the UTM features, offering a single point of entry to effectively apply policies for multiple security features - Anti-virus, Anti-spam, IDP, Web and Application filtering, Bandwidth management and Multiple link management, to the user directly, from within the firewall rule. This delivers truly unified controls in addition to ease of use and in troubleshooting.

### Dynamic Policy Setting

Cyberoam offers a clear view of usage and threat patterns. This offers extreme flexibility to change the security policies dynamically to meet the changing requirements of different users.

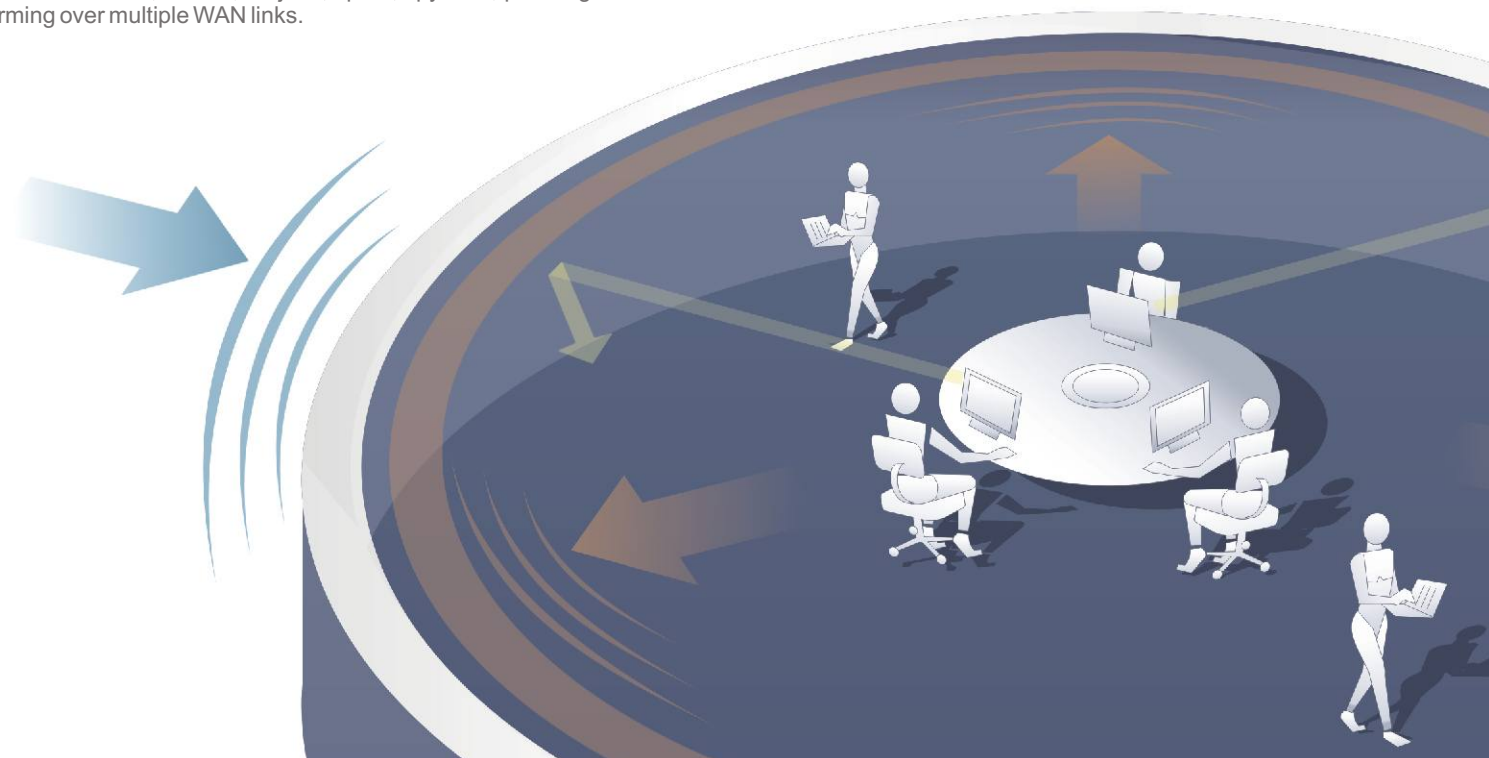


## Twin Shield Security

Cyberoam's twin shield security offers double-layered protection that controls indiscriminate surfing and defends against external threats. It reduces threats to the minimum, leaving the enterprise free to focus on its business.

Cyberoam's innershield controls indiscriminate surfing, preventing virus, worm, Trojan, spyware, phishing sites from becoming aware of your network.

Cyberoam's external shield provides dependable gateway-level protection from viruses, worms, Trojans, spam, spyware, phishing and pharming over multiple WAN links.



## Identity based Firewall

*Cyberoam's identity-based firewall delivers instant visibility and consolidated security*

### Embeds User Identity

Cyberoam embeds user identity in firewall rule matching criteria, which eliminates IP address as an intermediate component to identify the user, offering instant visibility and proactive controls over security breaches.

### Gateway Level Protection

Cyberoam firewall delivers effective protection with stateful and deep-packet inspection, analyzing packet headers and payloads. Cyberoam firewall protects networks from Denial of Service (DoS) and flooding attacks and prevents IP spoofing.

### Reduces Threat Incidence

Through the Cyberoam firewall's dynamic NAT (Network Address Translation), internal networks remain hidden from prying external eyes, protecting the enterprise from unauthorized external access. Internal protection prevents unauthorized access to subnets, work groups within the enterprise network.

### Blended Protection

User Identity binds the security features to create a single, consolidated Cyberoam security unit enabling the administrator to change security policies dynamically while accounting for user movement- joiner, leaver, rise in hierarchy and more through easy to configure policies.

## VPN - Virtual Private Network

*Secure communication is the basis for enhancing business on the move*

### Secure Communication

Cyberoam IPSec VPN delivers secure, encrypted tunnels with high performance and low bandwidth requirements. Using advanced algorithms and authentication methods, Cyberoam provides secure Net-to-Net, Host-to-Net and Host-to-Host connectivity.

Enterprises receive the benefits of secure connectivity without fear of eavesdropping, data tampering and concerns over safety of host, end-point and data integrity with Cyberoam, making sure that no modifications were made to the data in transit.

### Flexible, Low-cost Connectivity

Cyberoam VPN works in transport and tunneling mode, securing IP packets and wrapping an existing IP packet inside another. This offers enterprises the flexibility of turning to any ISP for connectivity and keeps costs low by doing away with expensive, dedicated leased lines.

## Gateway Level Anti-Virus

*Powerful, Real-time Anti-Virus Protection*

Cyberoam offers gateway level protection from virus, worms and malicious code through leading third party anti-virus solution, stopping threats before attack. Using cutting-edge technologies and user-friendly management tools, it offers a highly versatile security solution.

Gateway-level scanning and blocking of HTTP, FTP, SMTP, POP3 and IMAP traffic offers a powerful coordinated web and email defense. 24 x 7 virus monitoring ensures rapid response to new viruses.

### Up-to-date Protection

Anti-Virus checks viruses against its vast and regularly updated virus signature database. It ensures rapid response to new threats, high detection rates, thorough scanning, easy installation and configuration, offering near instant virus protection.

## Gateway Level Anti-Spam

*Customizable, Intelligent Spam Solution*

Cyberoam offers leading third-party anti-spam solution through advanced technology that eliminates the need for integration with existing mail servers. Anti-spam detects spam in incoming mail transmitted by SMTP, enforces black, RBL (Realtime Blackhole Lists) and white lists, performs text identification of spam and comes with regular, frequent updates with frequency of 2 hours.

It is highly scalable with the ability to analyze large messaging volumes at high throughput rates. The solution reduces spyware, phishing and adware attempts, controls porn spam while enhancing enterprise productivity by preventing mail systems from being submerged by spam.

### Multi-tier Filtration

Multi-tier monitoring techniques are implemented to check the body of the message and attachments for words and phrases typical of spam in addition to sender, recipient addresses, sender's IP, size and format. Incoming mail is compared against sample spam signatures. Anti-Spam analyses graphics and detects atypical spammer tricks like HTML tags, invisible text and more.

### Flexible Options

Based on configuration, Anti-Spam offers flexible options to deliver spam to the original address, quarantine, delete or redirect to a pre-defined address.

### Easy Administration

A built-in administration module based on a web interface allows administrators to modify program settings from any node in the network to change parameters for automatic spam database updates or add new signatures directly to the database.

### Advanced Controls

Anti-spam delivers maximum spam detection with low false positives through relevant, continuous and real-time spam detection.

## IDP—Intrusion Detection and Prevention

Cyberoam IDP protects against threats, blocking Internet attacks before they impact the network. It blocks intrusion attempts, DoS attacks, malicious code transmission, backdoor activity and blended threats without degrading network performance.

### Comprehensive Protection

Cyberoam IDP offers blended protection through multiple analysis, stateful detection and prevention techniques, resist false positives and evasion techniques with accuracy. It offers application and network-layer protection, enabling comprehensive zero-day defense-readiness to enterprises against viruses, worms, Trojans, spyware, keyloggers and more.

### Granular User-based Identification and Protection

Cyberoam's user-based policies deliver granular protection in addition to identifying attackers within the network and alerting administrators, enabling real-time corrective action. Visibility into applications by user, with period and extent of usage, enables easy zoning in on rogue users and systems.

### Online Updates

Updates are delivered online, allowing automatic updation and application of protection policies to vulnerabilities before exploit.

### Bridge-mode Deployment

Cyberoam can also be deployed in bridge mode, remaining invisible to the network as well as external intruders.

## Content Filtering

*Indiscriminate surfing is the leading factor attracting Internet threats*

### Comprehensive Site Database

Cyberoam delivers dependable content filtering through WebCat, the comprehensive database of millions of region-specific popular sites across the globe, grouped in 60+ categories, delivering great value-for-money and dependability.

### Granular Controls

Cyberoam breaks free of static IP-based and blanket policies with its granular, user- identity based policy capability to apply pre-defined surfing policies to any user, anywhere in the network.

With Cyberoam's high-flexibility and customization, enterprises can define and apply user, group, application-based policies assigned by hierarchy, department or any combination. Cyberoam restricts access to certain sites during specific time of the day.

### IM-P2P Traffic

Cyberoam's surfing security extends beyond standard HTTP traffic to include IM (instant messaging), P2P (peer-to-peer) exchanges, delivering great flexibility to match the dynamic application and threat scenario.

## Bandwidth Management

*Bandwidth management controls threat to enterprise productivity*

Cyberoam offers a high degree of customization in assigning bandwidth with the facility to define own groups, subgroups and departments for policy setting and updation over the easy-to-use GUI.

### Control over Bandwidth Choking

Cyberoam delivers a powerful productivity tool, reducing bandwidth choking through control over threat-induced flooding attacks and indiscriminate surfing of bandwidth guzzlers like audio-video downloads, gaming, tickers, ads, etc.

### Protecting Mission-Critical Applications

Committed and burstable bandwidth can be assigned to bandwidth-sensitive applications like VoIP in real-time with no solution configurations. Cyberoam implements policies assigning bandwidth based on time and mission criticality. Cyberoam's Traffic Discovery brings suspicious traffic to IT managers' notice in real-time, allowing them to take immediate corrective action, preventing network choking and spread of attack.

### Bandwidth Scheduling

Priorities can be established based on users, groups and applications with precise bandwidth allocation based on usage and time of the day.

### Data Transfer Quota

Policies can be assigned limiting data transfer on user and cyclic time-basis.

### Capacity Planning

Detailed bandwidth usage reports allow enterprises to plan capacity enhancements and make optimum use of resources.

## Multi-Link Manager

*Optimum use of multiple links for dependable connectivity and cost savings*

Cyberoam Multi-Link Manager controls traffic over multiple WAN links with a single Cyberoam installation. It delivers comprehensive traffic management capability, optimizing links, offering high-speed connectivity while maximizing ROI, turning small lines into reliable higher bandwidth offerings.

### Load Balancing

Multi-Link Manager maximizes reliability of enterprise connectivity by managing outbound Internet traffic over multiple ISP links. It load balances on a weighted round robin basis in policy-based ratios for users and applications, offering a dynamic traffic management system.

### Gateway Failover

Multi-Link Manager monitors link availability of multiple WAN connections and transfers traffic from a failed link to a working link, delivering dependable, seamless connectivity. It ensures continuous application availability so that mission-critical applications do not suffer, enhancing productivity and reducing maintenance costs.

## Intelligent Reporting

*Current traffic and analytical reports enable real-time, continually enhanced protection*

While Cyberoam's Traffic Discovery brings suspicious traffic patterns to the IT managers' notice as they happen, its intelligent reporting offers a range of analytical reports that show trends in Internet usage. This enables IT managers to identify emerging applications, pattern changes in usage and fine tune enterprise policies accordingly, supporting the creation of advanced levels of security and productivity.

## Benefits

Cyberoam offers all-encompassing benefits to enterprises.

### Technical Benefits

- Immediate deployment
- Zero network configuration
- Single management interface
- Real-time protection against all Internet threats

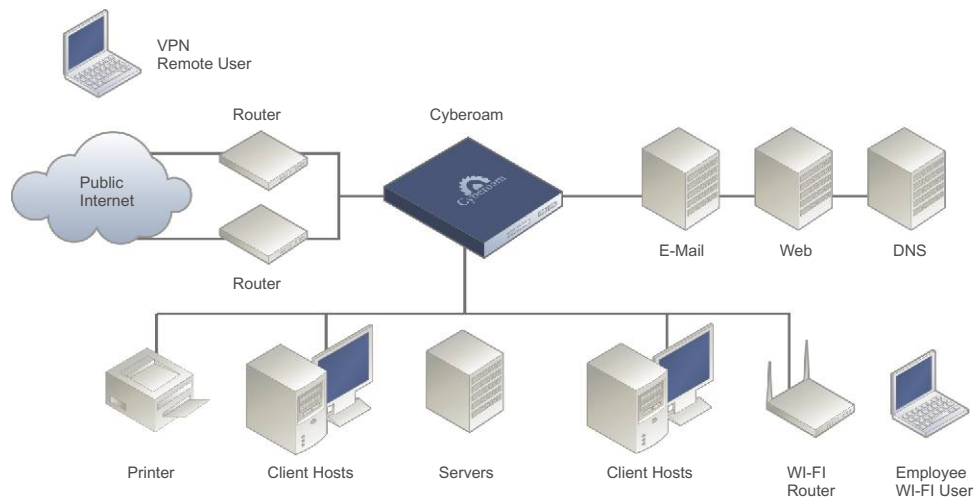
### Financial Benefits

- Low capital expense
- Low operating expense

### Business Benefits

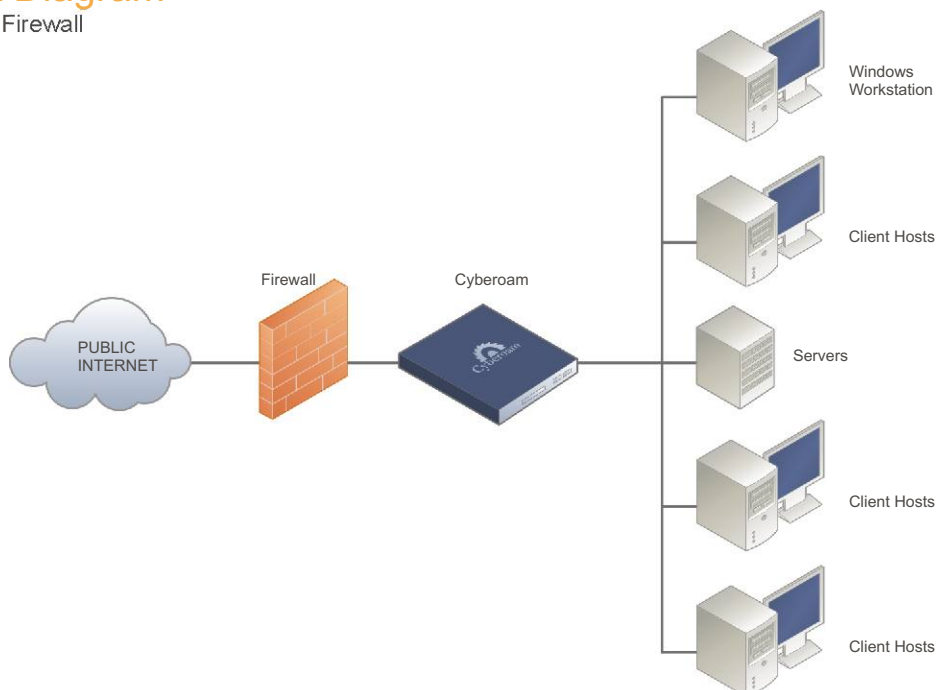
- Safe business environment
- Control over legal liability
- Enhanced productivity

## Network Diagram



## Network Diagram

With Existing Firewall





[www.elitecore.com](http://www.elitecore.com) | [www.cyberoam.com](http://www.cyberoam.com)

**U.S.A**

600 Meadowland Parkway,  
Suite 270, Secaucus,  
New Jersey 07094, U.S.A.  
Tel: 201-484-7581  
Fax: 201-777-2113

**Corporate**

904, Silicon Tower,  
B/h Pariseema Building,  
Off C.G.Road,  
Ahmedabad-380 006. INDIA.  
Tel: +91-79-26405600  
Fax: +91-79-26407640

**Contact**

[info@cyberoam.com](mailto:info@cyberoam.com)