Unified Threat Management

Comprehensive Network Security

Cyberoam

Emerging Internet threats External and Internal

- Viruses, Worms, Trojans
- Malware
- Spam
- Intrusions
- Spyware
- Phishing and Pharming
- Data Leakage
- Bandwidth Abuse

There's no escaping it: Enterprises, large and small are facing Internet threats not just from the external world, but from within too. While external threats are taking a targeted, blended form of attack, internal threats are creating security loopholes that leave the enterprise vulnerable to attacks. Faced with such a rapidly evolving threat environment, enterprises require multiple security features to ensure comprehensive network protection.

Enterprises that have deployed multiple security solutions face the daunting task of managing and upgrading these solutions constantly. At the same time they add to their capital and operating expenses.

Unified Threat Management

The complexity involved in managing multiple security solutions has led to unified security with multiple security features over a single platform – Unified Threat Management.

With the rise in targeted external attacks and insider threats, Unified Threat Management solutions have proven to be most effective when they extend security to encompass user identity to identify any threat whether it comes from inside or outside.

Cyberoam - Comprehensive Network Security

Cyberoam offers intelligent threat management with user identity-based controls. This approach 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.

Identity-Based Security
The Advantage

Cyberoam is the only UTM that embeds user identity in the firewall rule matching criteria, offering instant visibility and proactive controls over security breaches. It offers LDAP, Active Directory and RADIUS authentication too.

Eliminates Dependence on IP Address

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

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. This delivers truly unified controls in addition to ease-of-use and troubleshooting.

Dynamic Policy Setting

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

Regulatory Compliance

Through user identification and controls as well as Compliance templates and reports, Cyberoam enables enterprises to meet regulatory compliance and standards. With instant visibility into 'Who is accessing What in the enterprise', Cyberoam helps shorten audit and reporting cycles.

Twin Shield Security

Cyberoam's twin shield security offers double-layered protection that protects against internal and external threats.

Cyberoam's inner shield controls internal threats, including data leakage as well as indiscriminate surfing, that leaves enterpises vulnerable to spyware, phishing, pharming and more.

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

Net Facts - External Threats

- 63 % of companies report virus and worm attacks
- Trojan attacks have occurred in 58 % of companies
- 60% of spam-sending bots also send email-borne malware
- Image spam accounts for almost 35 % of worldwide spam mail and 70% of bandwidth taken by spam.
- An average of 343,000 newly activated zombies are reported everyday
- More than 48% of corporate PCs are infected by some type of spyware

Source: wired.com, Commtouch Software Ltd.

View latest threat outbreaks at Cyberoam Security Center
http://csc.cyberoam.com

Stateful Inspection Firewall

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

Embeds User Identity

Cyberoam embeds user identity in the firewall rule matching criteria, which eliminates the IP address as an intermediate component to identify the user, offering instant visibility and proactive controls over security breaches - even in dynamic IP environments. User identity binds the security features to create a single, consolidated security unit enabling the administrator to change security policies dynamically while accounting for user movement - joiner, leaver, rise in hierarchy and more.

Unified Management

Cyberoam enables management of multiple security features from a single entry point, while defining the firewall policy. This offers a unified approach to the overall security policy. It also enables easy configuration and trouble shooting.

Gateway Level Protection

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

Reduces Threat Incidence

Through the 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 and work groups within the enterprise network.

Enterprise Grade Security

Cyberoam meets enterprise level security requirement through features like Active-Active High Availability, support for Virtual LAN, Dynamic Routing, Multicast Forwarding and more to ensure comprehensive security with business continuity.

Virtual Private Network - VPN

Secure communication is the basis for enhancing business on the move

Secure Communication

Industry standard IPSec, L2TP and PPTP VPN provide enterprises with secure connectivity with low bandwidth requirements, without fear of eavesdropping, data tampering or concerns over the safety of host, end-point and data integrity. The dual VPNC - (Virtual Private Network Consortium) certification - Basic and AES Interop assures Cyberoam's VPN interoperability in multi-vendor IPSec VPN environments. Cyberoam provides secure Site- to-Site, Host-to-Net and Host-to-Host connectivity.

Secure, Low-cost Connectivity

Cyberoam's 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. Also, PPTP VPN eliminates the need for additional client on individual user machines , reducing complexity and additional expense.

VPN High Availability

Cyberoam provides automatic failover of VPN connectivity for IPSec and L2TP connections, ensuring continuous VPN connectivity across multiple ISP gateways. In doing so, it supports business continuity and employee mobility by allowing branch offices and road warriors to establish an alternate VPN connection to the secondary gateway when the current WAN link fails. A group of VPN connections with defined connection priorities facilitates effective failover management.

Gateway Anti-Virus & Anti-Spyware

Powerful, Real-time Anti-Virus and Anti-Spyware Protection

Cyberoam offers gateway level protection from virus, worms and malicious code through its Anti-Virus and Anti-Spyware solution, stopping threats before an attack. 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. In addition, it offers a self-service quarantine area.

Up-to-date Protection

Cyberoam's Anti-Virus feature checks viruses against its vast and regularly updated virus signature database. It's virus signature database is regularly updated to provide complete protection. Cyberoam's Anti-Virus engine supports a wide-range of file formats including password-protected attachments.

Gateway Anti-Spam

Customizable, Intelligent Anti-Spam Solution

Zero hour Defense

Cyberoam's Anti-Spam feature delivers zero-hour protection though RPD™* (Recurrent Pattern Detection) technology which provides industry's highest and best spam and threat detection capabilities. The content agnostic RPD™ technology detects and blocks emerging spam outbreaks including image, PDF, Excel spam and more with the least amount of false positives.

It is highly scalable with the ability to analyze large messaging volumes at high throughput rates. The solution reduces spyware, phishing and adware attempts and controls spam involving pornography while enhancing enterprise productivity. In addition, Cyberoam has the ability to configure White Lists and Black Lists based on user-identity, which facilitates granular mail management controls.

Early Outbreak Detection

With proactive virus detection technology, Cyberoam identifies massive e-mail borne virus outbreaks as soon as they emerge, effectively closing the early-hour vulnerability gap during which millions of users can be infected. It does so by providing a critical first layer of defense by intelligently blocking suspicious e-mails during the early stage of a virus outbreak.

Multi-tier Filtration

Cyberoam's granular policies use sender or recipient name, IP address, mime header and message size as their scanning parameters. This ensures that policies are fine tuned as per business and compliance needs. Cyberoam supports the full protocol spectrum which consists of SMTP, POP3 and IMAP, offering comprehensive protection.

Flexible Options

Based on configuration, Cyberoam's Anti-Spam offers flexible options to deliver spam to the original address, delete or redirect to a pre-defined address e.g. Administrator, department head or others. In addition, Cyberoam provides user-wise self-service quarantine area where mails identified as spam can be quarantined. This gives the flexibility to the administrator and the users to self manage their quarantined e-mails. This also reduces the risk of losing legitimate business communication messages.

*Commtouch Software Ltd.

Net Facts - Internal Threats

- 50 % of security problems originate from internal threats
- IM Threats are growing 50% per month
- One in three instant message users have received spim - spam over IM
- 51% of executives say they do personal surfing during business hours
- Financial losses from unauthorized access to data and theft of proprietary information has gone up

Source: CSO Metrics, Yankee group

Intrusion Detection and Prevention - IDP

Cyberoam's IDP protects against threats by blocking Internet attacks before they impact the network. With its unique identity based policy and reporting support, it provides advanced Intrusion Detection and Prevention, cutting down false positives drastically. Cyberoam IDP blocks intrusion attempts, DoS attacks, malicious code transmission, backdoor activity and blended threats without degrading network performance.

Comprehensive Protection

With one of the largest signature databases, Cyberoam's IDP instantly detects potentially malicious traffic based on policy settings, bringing intelligence into the IDP mechanism. It offers blended protection through multiple analysis, stateful detection and individual user identity-based policies rather than blanket policies, providing application and network-layer protection.

Identity-based Protection

Cyberoam's user identity-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 IT administrators to zone in on rogue users and systems.

Custom IDP Signatures

Cyberoam's IDP supports custom signatures, allowing enterprises to create their own signatures, delivering zero-hour protection against emerging threats. The IDP signature database includes HTTP proxy signatures that prevent masking of user surfing through an anonymous open proxy.

Online Updates

Updates are delivered online, allowing automatic updates for protection against vulnerabilities before they are exploited.

Content Filtering

Indiscriminate surfing is the leading factor attracting Internet threats

Comprehensive Site Database

Cyberoam delivers dependable content filtering through WebCat, Cyberoam's web categorization engine. With a comprehensive database of millions of region-specific popular sites across the globe, grouped in 68+ categories, it delivers great value-for-money and dependability. The comprehensive database ensures the safety and security of minors online, supporting CIPA compliance for schools and libraries.

HTTPS URL Filtering

Cyberoam can also control access to websites hosted over HTTPS by categorizing the domain names using the comprehensive website database. This feature helps the administrator to block access to unauthorized or unsafe websites like anonymous proxies and malware hosting websites, hosted over HTTPS.

Granular Controls

Cyberoam breaks free from 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. Enterprises can define and apply user, group and application-based policies by hierarchy, department or any combination with access restriction to certain sites during specific time of the day.

IM-P2P Traffic

Cyberoam's surfing security extends beyond standard Web traffic to include IMs (instant messaging) like Yahoo, MSN, Skype as well as P2P (peer-to-peer) exchanges. It offers a complete view and user based controls to match the dynamic 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 groups, subgroups and departments for policy setting over an easy-to-use GUI.

Preventing Bandwidth Congestion

Cyberoam delivers a powerful productivity tool, reducing bandwidth congestion through control over bandwidth of non-critical applications and recreational traffic like audio-video downloads, gaming, tickers, ads, etc.

Prioritizing Bandwidth-Critical Applications

Committed and burstable bandwidth can be assigned to bandwidth-sensitive applications like ERP in real-time. Cyberoam implements policies by assigning bandwidth based on time and business criticality.

Bandwidth Scheduling

Cyberoam is unique in allowing administrators to schedule and regulate bandwidth on time basis to users and host groups. This enables precise bandwidth allocation based on usage and time of the day, with a defined data transfer.

Capacity Planning

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

Multiple Link Management

Optimum use of multiple links for dependable connectivity

Cyberoam Multi-Link Management controls traffic over multiple WAN links with a single Cyberoam installation. It delivers comprehensive traffic management capability, optimizing links and offering high-speed connectivity while maximizing ROI.

Load Balancing

Multi-Link Management maximizes reliability of enterprise connectivity by managing outbound Internet traffic over multiple ISP links. It load balances traffic based on a weighted round robin distribution, offering a dynamic traffic management system.

Gateway Failover

Multi Link Manager monitors link availability of multiple WAN connections and transfers traffic from a failed to an operational link, delivering seamless connectivity for business continuity.

Comprehensive Reporting

Traffic and analytical reports to identify pattern changes in usage

Comprehensive Analytical Reports

Cyberoam's analytical reports enable IT managers to identify pattern changes in Internet usage and fine tune enterprise policies accordingly, supporting the creation of advanced levels of security and productivity.

Compliance Reports

Cyberoam reporting includes 45 compliance reports aiding SOX, HIPAA, PCI-DSS, FISMA, GLBA and CIPA compliance. Reports enable corporations and educational institutions to meet regulatory compliance needs and also reduces audit time.

Network and Application Monitoring

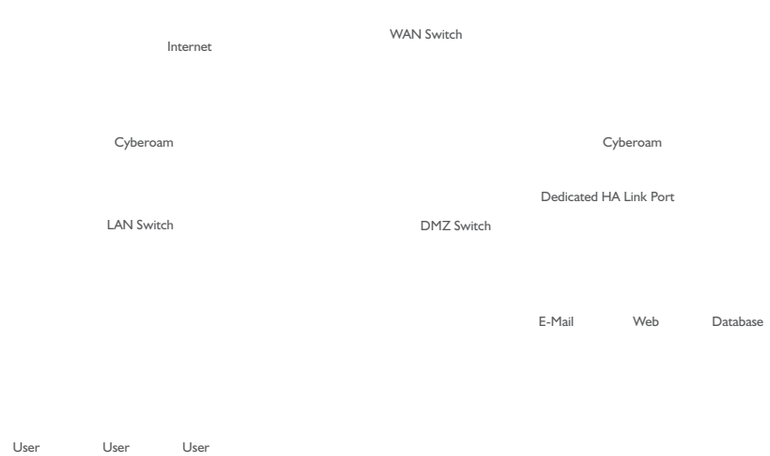
Cyberoam's network and application monitoring provides details of data transfer, application used through Traffic Discovery reports. This brings suspicious traffic patterns to the IT manager's notice enabling immediate corrective actions.

Cyberoam Deployment Scenarios

Gateway Mode

Bridge Mode
With Existing Firewall

High Availability
Active - Active



eLITECORE®
TECHNOLOGIES LTD.

www.elitecore.com I www.cyberoam.com

North America

Cyberoam

Elitecore Technologies

29 Water Street
Newburyport, MA 01950
USA
Tel: +1-978-465-8400
Fax: +1-978-293-0200

India

Elitecore Technologies

904, Silicon Tower,
B/h Pariseema Building,
Off C.G.Road,
Ahmedabad-380 006. INDIA.
Tel: +91-79-66065606
Fax: +91-79-26407640

Contact

info@cyberoam.com

Version:1.0-954-Feb,08