

## Securing You



In today's Information age, need for continuous internet connectivity cannot be denied. As an individual user or as an employee in your organization, blended threats are waiting to attack YOU by identifying one vulnerable moment when your defenses are low. These can be viruses, malware, spam, Trojans and insider attacks like data theft and leakage. Securing YOU – the User, thus becomes critical! How do you ensure continuous security against sophisticated IT security threats?

Cyberoam's identity-based security solutions can secure your every move at work, at home and while you travel – from the network gateway to the endpoints. It binds security with your identity and works as your private security guard, even when you are away from work or at home. Its endpoint security protects your sensitive data by securing your endpoints, storage devices and controlling applications.

  
**Cyberoam**<sup>®</sup>  
Securing You

 Elitecore Product

# Cyberoam Identity-based Unified Threat Management

Cyberoam Unified Threat Management appliances offer comprehensive security to small, medium and large enterprises through multiple security features integrated over a single platform. It is the first UTM that embeds user identity in the firewall rule matching criteria, offering instant visibility and proactive controls over security breaches and eliminating dependence on IP Addresses.

Cyberoam's unique Layer 8 technology treats USER as the 8th layer in the network stack. Also known as the Human layer, it penetrates through each of Cyberoam's security modules, allowing organizations to create user identity-based security policies. This offers them complete visibility and control over user activities, showing who is doing what anywhere in the network and enables them to take network security decisions based on usernames and not just IP addresses.

Cyberoam's identity-based security offers a high degree of granularity, making policy-setting an efficient process down to the user level that can be extended to any combination of group, job function or application. The IP-independent nature of Cyberoam allows users to carry their own access rights and policies anywhere in the network, even in dynamic IP environments like DHCP and Wi-Fi.

Cyberoam's Layer 8 technology adds speed to the whole security set-up by offering administrators instant visibility into source of attacks, enabling them to identify attacker/victims by username and achieve immediate remediation to any security breach condition.



**Small Offices**

15wi, 15i, 25wi, 25ia, 35wi, 35ia



**SME**

50ia, 100ia, 200i, 300i



**Enterprises**

500ia, 750ia, 1000ia, 1500ia

## Cyberoam's Identity-Based Security Advantages

- Identifies and controls users through identification, policy-setting and reporting by username.
- Offers security even in dynamic IP environments like DHCP and Wi-Fi.
- Allows binding of user identity with IP address, MAC Id, Session Id to prevent unauthorized network access.
- Allows real-time threat control through identity-based reporting on usage and threat patterns of individual users.
- Facilitates regulatory compliance for HIPAA, PCI-DSS, GLBA, CIPA, etc. with on-appliance reporting of "who" is accessing "what", shortening audit and reporting cycles.

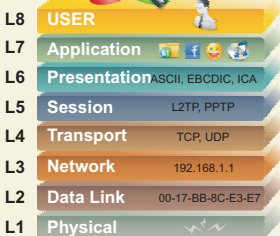
## Cyberoam's Future-ready Architecture

Cyberoam's Multi-core technology offers high security without compromising on performance by allowing parallel processing of multiple security features, therefore allowing effective management of dynamic, content-based threats such as Web 2.0 applications, Voice over IP, streaming media, IM and P2P.

Cyberoam UTM's Extensible Security Architecture (ESA) is built on an extensible platform that can organically grow with future security needs of the organization. Such an approach has the agility to prolong the life and performance of the legacy UTM appliance by supporting future feature enhancements, for which the development can be done very rapidly and with minimum deployment effort.



### User Identity-based Security Policy Controls



**Cyberoam's Layer 8 Technology treats "User Identity" as the 8th Layer in the protocol stack**

Cyberoam UTM offers security across Layer 2-Layer 8 using Identity-based policies

## Cyberoam UTM Features Assure Security, Connectivity and Productivity

Cyberoam UTM offers security without compromising on connectivity and productivity. It offers a combination of best-of-breed assembly of solutions over a single interface, resulting in a complete, dependable shield that network threats find extremely difficult to penetrate.




### Security

- Network Security**
  - Firewall
  - Intrusion Prevention System
  - Wireless security
- Content Security**
  - Anti-Virus/Anti-Spyware
  - Anti-Spam
  - HTTPS/SSL Content Security
- Administrative Security**
  - Next-Gen UI
  - iView- Logging & Reporting



### Connectivity

- Business Continuity**
  - Multiple Link Management
  - High Availability
- Network Availability**
  - VPN
  - 3G/WiMAX Connectivity
- Future-ready Connectivity**
  - "IPv6 Ready" Gold Logo



### Productivity

- Employee Productivity**
  - Content Filtering
  - Instant Messaging Archiving & Controls
- IT Resource Optimization**
  - Bandwidth Management
  - Traffic Discovery
  - Application Layer 7 Management
- Administrator Productivity**
  - Next-Gen UI

### Technical Benefits

- Real time protection against all Internet-based Threats, including blended and internal threats
- Rapid deployment
- Minimal configuration
- Next-generation GUI enhances security with its easy navigation and custom controls

### Financial Benefits

- Low capital expense
- Low operational expense
- Higher ROI

### Business Benefits

- Safe business environment
- Control over legal liability
- Enhanced productivity
- Meets regulatory compliance requirements

## Cyberoam Central Console (CCC) - Centralized Management

Cyberoam Central Console (CCC) is a centralized security management appliance that allows enterprises and MSSPs to manage multiple, dispersed Cyberoam UTM installations across remote or branch offices and clients respectively. CCC lowers the operating cost of upgrading and maintaining security across distributed networks.

### Security Management – Instant Enforcement of Security Policies

CCC simplifies security management by enabling centralized policy creation and implementation, subscription and signature updates for Cyberoam UTM appliances deployed at branch offices and client offices for all UTM features like Firewall, Intrusion Prevention System, Anti-Virus scanning, and more. It allows real-time protection against zero-hour threats in enterprises and reduces response time against newly identified threats across multiple customer networks of MSSPs.

### Flexibility of Management

CCC provides MSSPs and Enterprises the flexibility to group Cyberoam UTM appliances deployed across various offices based on geography, Cyberoam UTM models, firmware version, organization (for MSSP) and service subscription for their quick management. Web 2.0-based GUI offers dynamic views for easy management, search and sorting of appliances.

Enterprises and MSSPs have the flexibility to create customizable and multiple dashboards for group of appliances that helps in quick monitoring and action.

### Security against Misuse of Administrator Privileges

CCC enables enterprises and MSSPs to set role-based administration for CCC appliance as well as individual Cyberoam UTM appliance and for groups of Cyberoam UTM appliances.

### Audit Logs & Alerts

The CCC Log Viewer offers logs and views of administrator actions on CCC as well as dispersed UTM appliances. Email alerts can be set based on expiry of subscription modules, excess disk usage, IPS and virus threat counts, unhealthy surfing hits and other parameters.



**CCC Series :** CCC15, CCC50, CCC100, CCC200, CCC500 and CCC1000



## Cyberoam iView - Intelligent Logging and Reporting Solution

The Cyberoam iView appliance series offers visibility into activity within the organization for high levels of security, data confidentiality and regulatory compliance. It provides an organization-wide security picture on a single dashboard through centralized reporting of multiple devices across geographical locations. This enables organizations to apply or correct security policies from a central location, enhancing security.

### Log Management

It allows effortless, identity-based log management in near real-time. Organizations can match user identity-based information contained in logs with their rights and privileges to reveal discrepancies in user activities.

### Security Management

A quick glance at the iView dashboard, its drill-down reports and identity-based logging and reporting enables organizations to instantly locate network attacks, their source and destination, allowing rapid action.

### Compliance Management

iView eliminates compliance complexities with a one-step access to critical information with multiple reports

on a single dashboard that can be drilled down to get the third-level of information. Organizations can easily monitor access and security violations in the network, accelerating incident response and facilitating compliance.

### Forensic Analysis

iView helps organizations reconstruct the sequence of events that occurred at the time of security breach through iView logs and reports. They can reduce the cost of investigation and analysis and minimize network downtime while gathering historical information.

## Cyberoam SSL VPN Appliance

Cyberoam SSL VPN is available as a dedicated appliance, as a virtual VMware-based appliance and as a software installer on client machines, allowing organizations a much greater choice in addressing their individual connectivity requirements. It meets the performance goals of organizations by running on a hardened, Gateway operating system, being scalable to unlimited users and supporting Active-Active N+1 clustering with load balancing for transporting critical databases and large files as per demand necessity. It also runs smoothly on hardened Linux-based platform, Virtualization platforms such as VMware and custom hardware.

### SSL VPN Appliances:

CR-SSL-800, CR-SSL-1200, CR-SSL-2400

## Cyberoam Endpoint Data Protection

Cyberoam Endpoint Data Protection protects endpoints from data leakage with Identity and group-based policy controls, encryption, shadow copies, logging, reporting and archiving. It offers data protection and asset management in four easy-to-deploy and use modules - Data Protection & Encryption, Device Management, Application Control and Asset Management. These modules enable organizations to limit access only to trusted devices, applications and recipients while sharing data and also reduce IT burden with reduced support calls for malware attacks recovery and more.



Data Protection & Encryption



Device Management



Application Control



Asset Management

## Awards & Certifications



### Elitecore Technologies

600 West Cummings Park, Suite 1550 & 1650,  
Woburn MA 01801, USA, Tel: +1-847-235-4684

### India

904, 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



sales@cyberoam.com | www.cyberoam.com

® Registered Trademark of Elitecore Technologies Pvt. Ltd.