Cyberoam

Unified Threat Management

Product Comparison

# Cyberoam UTM (CR Series)

# Vs.

# SonicWALL UTM (TZ , Pro , NSA Series)

SonicWALL Anti Spam service charges per mailbox rather than flat pricing

Hwww.cyberoam.com

## Cyberoam Certifications

**Westcoast Labs Checkmark Certification:**

**UTM Level 5**

**Categories:**

- Enterprise Firewall
- VPN
- Anti-Virus and Anti Spyware Gateway
- Premium Level Anti-Spam
- IPS
- URL Filtering

**ICSA Certification**

**Category:**

Corporate Firewall with Active- Active High Availability

## Awards

**Winner of 2008/2009 ZDNet Award**

**Category:**

- IT Leader
- Asia's Most Promising Asian TechnoVisionaries

## Product Review

- PC Pro Recommended UTM
- Techworld Recommended UTM

- **SC Magazine** : Cyberoam UTM Overall Rating: ★★★★★ **- 5 Stars**
- **SC Magazine** : Best Buy

## Cyberoam UTM is Certified by Virtual Private Network Consortium (VPNC) :

- Basic Interop
- AES Interop
- SSL Portal
- SSL Firefox
- SSL Java Script
- SSL Basic Network Extension
- SSL Advanced Network Extension

## Cyberoam in Numbers

| | |
|---|---|
| World wide Presence | Deployed in 90+ countries |
| Number of Anti Virus Signatures | 2 Million |
| Virus Detection Rate | 100% |
| Spam Detection Rate | 98% |
| False Positive Rate | 1 in One Million |
| Number of URL categories | 82+ |

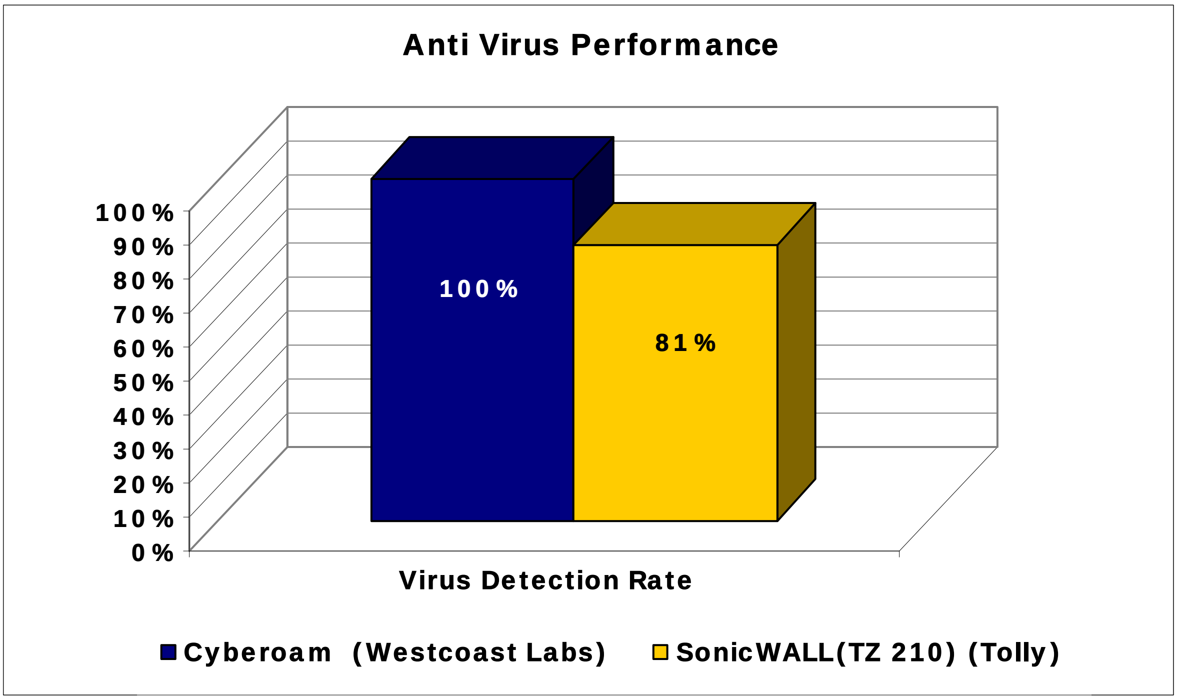
## Cyberoam's Anti Virus vs. SonicWALL Anti Virus:

Cyberoam has an OEM with Kaspersky Lab for Gateway Anti Virus, which is one of the industries leading Anti Virus Solution.

SonicWALL has a proprietary gateway anti virus engine.

In 2009, public test of different anti-virus vendors all out to see how they really compare took place.

While Kaspersky topped with 100%, SonicWALL was dragging its feet with 81% detection rate.



Cyberoam also has a User based Self Service Quarantine area for virus which SonicWALL does not have.

## Cyberoam's Real-Time RPD™ Anti Spam Technology

Cyberoam's RPD™ technology focuses on detecting recurrent message patterns in outbreaks. Message patterns are extracted from the message envelope, headers, and body. Patterns are extracted in real time from the message hashes being continuously sent to the detection centers.

Cyberoam has a User based Self Service Quarantine area, so that no business mails are lost to security.

**Anti Spam Statistics**:

1. Cyberoam's Spam Detection Rate is industry's best: **98%**
2. Cyberoam's False Positive Rate is : **1 in 1 Million**

### SonicWALL: Poor Anti SPAM

The anti spam service being launched is now an admission by SonicWALL about the lack of Anti Spam features on its appliances.

The anti spam engine is still a combination of many engines such as Adversarial Bayesian, image inference analysis etc which have their limitations and should be now considered obsolete with respect to the RPD and IP reputation services being used in

Cyberoam.

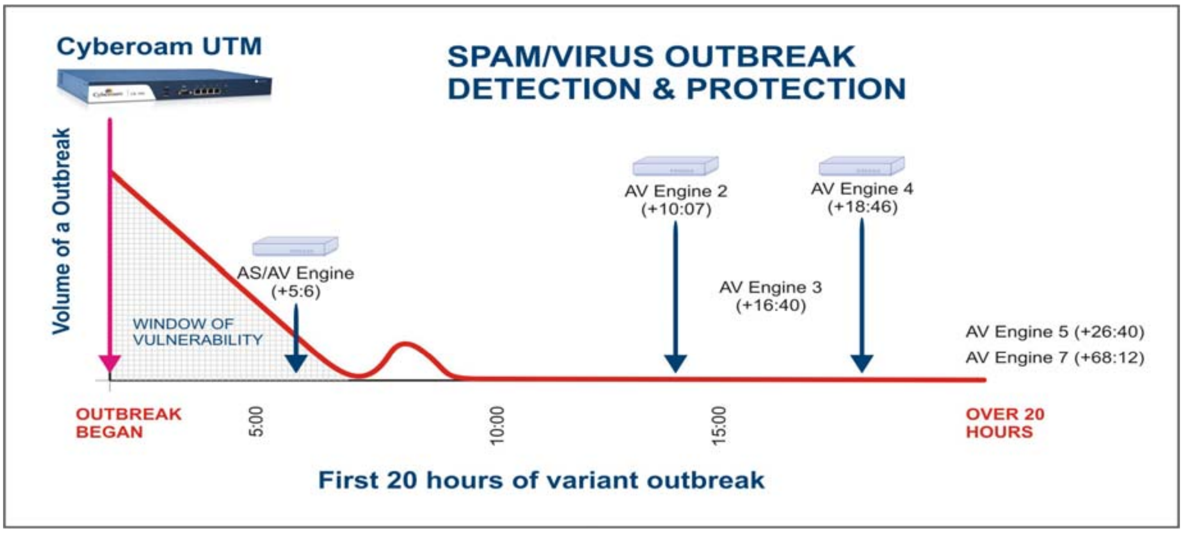
The worst thing about this Anti Spam service is that it is actually a service that is charged per mailbox rather than flat pricing that is the norm today.

Another fact to be considered is that the Anti Spam engines reside on the cloud rather than the appliance and most of the processing is done on the network, so appliance is just a medium for the service rather than a subscription

Given below is comparison chart for anti spam service.

| | SonicWALL | Cyberoam |
|---|---|---|
| Checkmark certification | No | Yes (Premium Level) |
| Language and Content independent anti spam engine | No | Yes |
| Protocol support | SMTP | SMTP, POP3, IMAP |
| Detection rate | 98% | 98% |

## Cyberoam Minimizes the Window of Vulnerability



Cyberoam provides proactive protection against new email-borne virus outbreaks, hours before the signatures are released. It has empowered with the proactive virus detection technology which detects and blocks the new outbreaks immediately and accurately.

It provides a critical first layer of defense by intelligently blocking suspicious mails during the earliest stage of a virus outbreak.

## Bandwidth Management vs. Bandwidth Control

Cyberoam gives Bandwidth Management that is a full fledge user–based policy level management designed to provide:

1. Guaranteed or burst-able bandwidth
2. Flexible, prioritized, bidirectional rules
3. Rules for Users, Groups, IP addresses
4. Web Category based bandwidth management
5. Transparency for end users
6. Detailed and comprehensive bandwidth reports

SonicWALL UTM on the other hand provided preconfigured options from **Firewall > QoS Mapping** option. The options are not self explanatory.

## Cyberoam's User-based Multiple IPS Policies

User-based flexible multiple policies are supported by Cyberoam UTM only and not by SonicWALL.

SonicWALL does not support Custom IPS signatures.

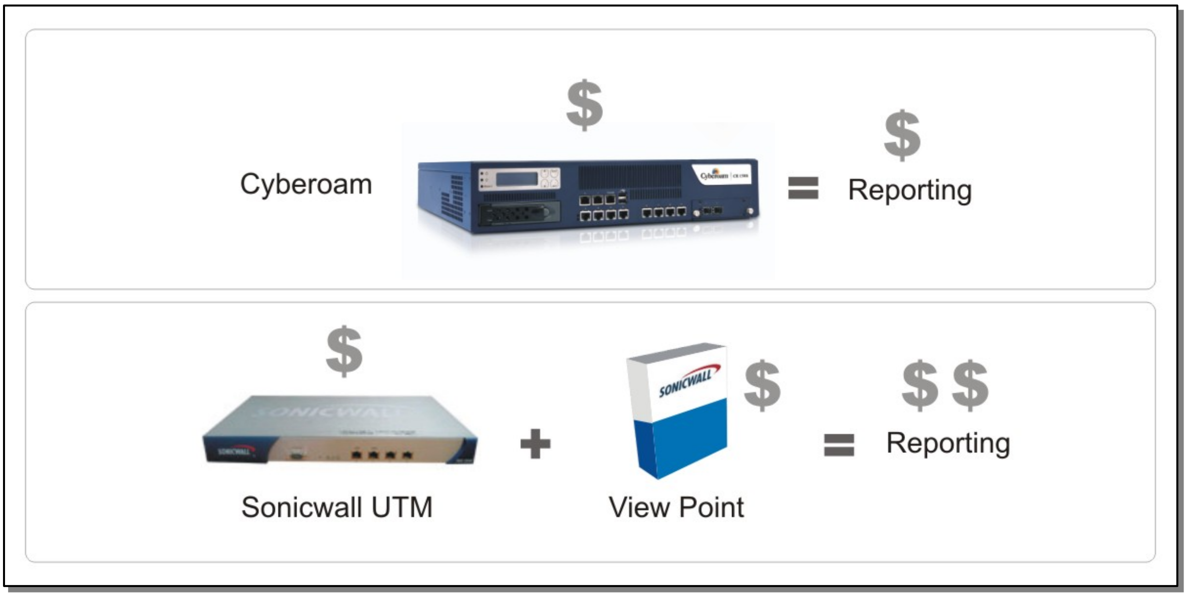
## Cyberoam Reporting – Free + User Friendly

In SonicWALL, the customer needs to purchase and deploy ViewPoint software to get detailed reporting. This is a steep escalation in terms of Capital Expenditure and Operational Expenditure.

Cyberoam's On-Appliance **Plug-and-Play** reporting provides detailed reports.

Some unique Cyberoam Reports include:

1. User-wise reports of all types (Web Filtering, Internet Surfing, IPS)
2. User-wise Data Transfer
3. User-wise Search Keywords (reports of web searches)
4. Web Surfing Trends reports as per: User, Organization, Site, Category(graphical reports)
5. Compliance reporting comprising of: HIPAA, GLBA, SOX, PCI, FISMA



## Cyberoam iView - Open Source Logging and Reporting Solution

Taking a step ahead of competitors, Cyberoam also provides external reporting for Cyberoam as well other products with the help of Cyberoam iView.

Cyberoam iView is an open source logging and reporting solution that provides organizations with visibility into their networks across multiple devices for high levels of security, data confidentiality while meeting the requirements of regulatory compliance.
Enabling centralized reporting from multiple devices across geographical locations, Cyberoam iView offers a single view of the entire network activity with the help of 1000+ unique reports.

Refer to www.cyberoam-iview.org for further details.

## Head-to-Head Comparison:

| Points to Ponder | SonicWALL UTM | Cyberoam UTM |
|---|---|---|
| **Enhanced Firewall Decision Matrix:**<br>Firewall is a primary security component in network security.<br>A normal decision matrix in a firewall stops at the IP address of a machine.<br>In the blended threat scenario, social engineering is used to target the weakest link – end user. So a user's identity becomes an important decision and control parameter in the firewall matrix. | SonicWALL UTM does not use identity as a parameter in the firewall decision matrix. | Cyberoam extends the firewall's rule matching criteria to include schedule and the user's identity.<br>Similarly, the firewall actions are extended to include complete policy based control over all the security solutions like, content filtering, IPS, Internet access management, bandwidth management and anti-virus and anti-spam scan. |
| **State-of-Art Identity-based Access Management:**<br>IAM is a combination of Identity, time scheduling and access management. This is a powerful control mechanism which reaches down to all the security features in a UTM. Identity and time schedule are the two dimensions used to define a user's real time identity in a security solution. | SonicWALL UTM does not use Identity as a parameter in the firewall decision matrix. | Cyberoam's Identity-based access management feature provides unparalleled flexibility, security and control to the network administrator over the end user.<br>Cyberoam also facilitates the user to implement combination of security parameters as IP Address, Identity, and MAC Address, firewall decision matrix. |
| **Centralized point of UTM Management:**<br>Aggregation of security solutions is not enough. A UTM should be easily manageable. This makes it user friendly and the learning curve of the end user remains low. | SonicWALL UTM does not have this flexibility and ease of use. | Cyberoam is manageable through its single firewall page. It is designed to provide a central management of all member security packages of the UTM. In a few clicks, you can have custom policy to meet any security demand. |

| Points to Ponder | SonicWALL UTM | Cyberoam UTM |
|---|---|---|
| **Enhanced Application Firewall**<br>Application firewall monitors, controls and blocks applications and services (input, output, or system service calls) which do not meet the configured policy of the firewall.<br>To secure the organization's network from blended internal and external threats, company needs application firewall | Supports application firewall | Application Firewall is part of IPS with 3500+ Signatures<br>Application based Bandwidth Management is part of product roadmap deliverable in April. |
| **World Wide Honey Pot Back Bone**<br>Requirement to secure the network from blended Internet threats is rising day by day.<br>Network security companies need access to malware and spam outbreaks instantaneously<br>To achieve this there is a need of world wide honey pot network. | SonicWALL machines world wide acts as security agents. | Cyberoam has installation in 90 different countries and all Cyberoam appliances update the information about new virus and spam attacks to central office. |

| Points to Ponder | SonicWALL UTM | Cyberoam UTM |
|---|---|---|
| **Purpose built Hardware**<br>Purpose built hardware strengthens and speeds up the security software installed on it.<br>A SOHO appliance and enterprise appliance might have different security needs and the hardware should reflect the business purpose of security. | SonicWALL supports VPN accelerators and multicore architectures. | Cyberoam supports 64 bit hardware platforms based on business purpose.<br>Cyberoam provides flash-based UTM appliances series with HDD based appliances.<br>Cyberoam SOHO appliances come with VPN accelerator to provide higher performance.<br>Cyberoam higher end appliances are based on multicore threat scalable architecture.<br>The key feature of the Cyberoam architecture is its ability to adapt to new threats while maintaining a predictable level of performance and high level of security. |
| **Business Friendly Anti Virus / Anti Spam Scans:**<br>For most users, missing a legitimate email is an order of magnitude worse than receiving spam or virus.<br>To avoid such an unpleasant situation you need to control the parameters used to classify a mail as spam or virus infected and the necessary action.<br>User-based customized scans can ensure that not a single mailed business opportunity is lost to security. | SonicWALL UTM does not provide any such control over its AV and AS scans. | Cyberoam UTM has an OEM license from Kaspersky’s Gateway AV. Similarly, Commtouch RPD Anti-spam technology (OEM) is used in Cyberoam.<br>No separate AMCs are levied.<br>Using Cyberoam UTM you can define custom scan rules based on sender or recipient, IP address, mime header and message size.<br>You have the flexibility to configure a scan as per your needs, rather than adjusting yourself to the way a security solution operates. |

| Points to Ponder | SonicWALL UTM | Cyberoam UTM |
|---|---|---|
| **Self-service Anti Virus / Anti Spam Quarantine Area:**<br>Quarantine area is a safe holding area for all suspicious/ infected files. This allows organizations to remove infected files from general circulation without deleting them.<br>A gateway quarantine area should be self-service as there are a large number of users involved. So the users ought to get notified that a mail has been quarantined and he can access and deal with it without depending on the administrator. | SonicWALL UTM does not have this feature. | The Self-service quarantine area from Cyberoam UTM enables individual mail recipients to view and manage their infected / Spam messages.<br>The self-service feature removes user's dependency on administrator to manage quarantine mails. |
| **Superior Spam Filtering:**<br>In 2007, the spam proliferation has increased by 35% per year and 99% of all emails was spam. Image and Instant Messaging-based spam (spim) can prove to be a major drain on mail storage and employee productivity. Spim blockage requires specialized anti-spam filters. | SonicWALL UTM has per mail box based anti spam engine using almost obsolete technologies as Adversarial Bayesian, image inference analysis etc | Cyberoam has an OEM with Commtouch Software Ltd. Recurrent Patterns Detection (RPD) technology, based on the identification and classification of message patterns delivers the industry's best and highest spam and threat detection capabilities providing protection from all types of email-borne threats.<br>Cyberoam watches over SMTP, POP3 and IMAP protocols for Spam. This provides comprehensive anti-spam cover. |

| Points to Ponder | SonicWALL UTM | Cyberoam UTM |
|---|---|---|
| **Protection Against Phishing and Pharming:**<br>Phishing and Pharming are the next generation threats instigating the end users to breech the network security from within. Phishing is a passive baiting through mail and Pharming is an active process of host file corruption which leads the user unknowingly to a malicious site. | SonicWALL does not have Pharming protection. | Cyberoam UTM protects against Phishing and Pharming, both. Its Anti Spam technology and WEBCat database effectively mitigate Phishing threats.<br>In case of a host file corruption due to a Pharming attack, the DNS configured in Cyberoam UTM makes sure that the user is not directed to a malicious site. |
| **Security Readiness:**<br>Security is not a solution for yesterday's problems. It is all about present and future. So a UTM should have frequent proactive updates to secure the network from smart attacks. It should utilize both – push and pull technologies to keep it updated. | SonicWALL does not provide timely security updates.<br>Dependent on external AV | Cyberoam UTM empowers the user by providing regular updates of various security solutions:<br>• Virus and Spyware updates: Every 30 minutes.<br>• Spam updates: Every minute.<br>• IPS updates: Every 7 days<br>• Instant Outbreak updates |
| **Define Multiple IPS Policies and Custom IPS Signatures:**<br>Blanket policies, over time force the administrator to open security loop holes.<br>Customized policies provide you the comfort to deploy customized IPS policies as per your needs.<br>Custom IPS signatures reach deeper than a firewall and antivirus to protect the network from blended threats. | SonicWALL UTM does not have Custom IPS Policies. | Cyberoam UTM provides the administrator with the ability to attach an individual IPS policy to a combination of source, destination, application, identity and schedule.<br>This ensures customized IPS policy as per your needs.<br>Cyberoam UTM also provides you the facility to use custom IPS signatures.<br>These features ensure that your network security is geared up meet any exceptions as well as general threat conditions. |

| Points to Ponder | SonicWALL UTM | Cyberoam UTM |
|---|---|---|
| **Identity-based IPS Policies and Reporting Ensures Transparency:**<br>To deploy security policies the administrator has to know his target. IP addresses are not target enough.<br>The most harmful intrusion attempts are attempted from inside a network. In IP address based IPS policies and reporting the identity gets lost.<br>To ensure complete transparency in a network, the IPS policies and reporting should also take the user's identity into its ambit. | SonicWALL UTM does not have identity based IPS reporting. | Cyberoam UTM provides IP address and User-based reports. Providing complete visibility, it thwarts anonymity in DHCP, Wireless and Computer sharing environments.<br>In case of threat detection; it reduces the administrator's reaction time. The administrator can personally contact the erring user.<br>Identity based policies also lends unprecedented granularity to the IPS policies.<br>Cyberoam's IPS module also provides mail alerts. |
| **Clean VPN**<br>To ensure complete security of the network, it is necessary to scan traffic traveled through VPN tunnels for virus, spyware and other malware | Supports VPN traffic scanning | Ensures security of company's network by scanning traffic through and from VPN tunnels. |
| **Practical Approach to Bandwidth Management:**<br>Percentile based bandwidth management is not practical as, if a VoIP application needs 128Kbps; you cannot assign 10% of the bandwidth.<br>Moreover back calculating bandwidth on percentage basis is cumbersome. | SonicWALL UTM's bandwidth management policy is not very effective in the practical implementation because it allocates bandwidth on percentile basis.<br>It lacks user specific bandwidth allocation and does not have the Priority feature. | Using Cyberoam you can provide QoS to a combination of source, destination and service/service group by committing bandwidth to users, applications, Web categories and servers based on time schedules.<br>You can manage interactive applications like VoIP, Video Conferencing, SSH, telnet etc. better by assigning higher priority to get better and instant results |

| Points to Ponder | SonicWALL UTM | Cyberoam UTM |
|---|---|---|
| **Secure Vital Information by Rule based Application and IM Controls:**<br>Unmonitored content leaving an organization through an IM application introduces security, legal and competitive risk. It is difficult for the IT department to discover potential breaches of policy or to hold individuals accountable. | SonicWALL UTM does not support granular control over IM.<br>They are either fully allow or are deny an application, there is no granular control over it. | Cyberoam UTM's application filtering solutions is powerful enough to control file transfer over any IM application. Identity can be used as a control parameter in these control policies. |
| **Automated Single Sign On Ensures hassle free Transparent Authentication :**<br>Authentication often gives administrators nightmares as they involve a lot of hassles and changes in the existing setup.<br>SSO ensures that the user's authentication is seamless and transparent. It also ensures that the user has his well-defined secure microcosm. | SonicWALL UTM does not have automated SSO. | Cyberoam SSO ensures that the UTM remains transparent and it seamlessly blends into the network. The user is never explicitly aware of its existence. Only in case of treading on forbidden paths, he is reminded of the UTM's presence.<br>The SSO promotes a one stop, transparent entry into the network, reducing administrative maintenance. |
| **Data Transfer Accounting and Control:**<br>Data transfer accounting and control helps you to see the actual internet consumption by an individual user or an application.<br>This feature also helps when you want to find the exact costing of Internet usage in case if an ISP is charging for the amount of data transferred. | SonicWALL does not have this feature. | Cyberoam provides a comprehensive, application and user based data transfer accounting and control.<br>This feature comes in handy in educational institutions where Internet consumption per individual is important. |

| Points to Ponder | SonicWALL UTM | Cyberoam UTM |
|---|---|---|
| **Centralized Management:**<br>To reduce hassles of maintaining multiple appliances and ensure consistency, a UTM should support centralized management. | SonicWALL supports hard disk drive based Global Management System. | Cyberoam's CCC appliance handles multiple Cyberoam appliances from a single point. |
| **Network Diagnosis:**<br>A UTM should have some diagnosis tools to analyze the problem for providing network transparency. This, in result proves as a great aid to troubleshooting. | SonicWALL provides rudimentary diagnostic tool. | Cyberoam provides multiple ways to analyze the problem. Cyberoam HTTP diagnostic provides enormous deep packet level information to trouble shoot the problem. |
| **User Identity Based Comprehensive Reporting:**<br>Reports are an integral part of any security solution as they are the tools to provide visibility.<br>Clear and precise reports are the most valuable tools that makes sure that organization's resources are focused on maximum productivity | SonicWALL UTM comes with limited reporting facilities. However, if the organization needs extensive reporting, it has to buy and install a separate proprietary application SonicWALL Viewpoint.<br>After paying an extra cost also, the user is forced to bear unacceptable gap between the event and actual report.<br>The applications also needs separate hardware platform. | Cyberoam has an integrated plug-and-play reporting module which provides IP address and user identity based in-depth reports.<br>All reports are HTTP/HTTPS based, and so are platform, location and client independent.<br>As a value added feature Cyberoam reports are complimentary to CIPA, HIPAA, GLBA, SOX, PCI, FISMA compliances.<br>Cyberoam also provides external reporting with the help of Indigenously Designed **Open Source** Logging and Reporting Solution: Cyberoam-iView, Provides In-depth logging and reporting for **multiple devices** apart from Cyberoam |

Cyberoam

Unified Threat Management

Product Comparison

## Overview of Cyberoam’s Security Approach:

- Whom do you give access to: An IP Address or a User?
- Whom do you wish to assign security policies: User Name or IP Addresses?
- In case of an insider attempted breach, whom do you wish to see: User Name or IP Address?
- How do you create network address based policies in a DHCP and a Wi-Fi network?
- How do you create network address based policies for shared desktops?

Cyberoam UTM approaches the Security paradigm from the *identity* perspective. The blended threats circumvent the perimeter defense and launch an attack from within. The network’s own resources are used to subvert it. The main target is thus the end user who knowingly or unknowingly breaches the perimeter defense.

While providing a robust perimeter defense, Cyberoam UTM’s Identity-based access control technology ensures that every user is encapsulated in a tight, yet granular security policy that spans across Cyberoam UTM’s Firewall/VPN, Gateway Anti Virus, Anti-Spam, Web Filtering, Intrusion Prevention System (IPS) and Bandwidth Management solutions.

## Cyberoam Product Portfolio

Disclaimer:

1. This document is strictly confidential and intended for private circulation only.
2. The features of any of the products are likely to change without prior notice.
3. The comparison is based on publicly available information only.

Document Version: 5.4 – 96078 – 08/03/2010