

Centralized Security Management for MSSPs & Distributed Enterprises



Centralized Security Management

Zero-hour threats spread to millions of computers within hours whereas blended attacks like viruses, worms, Trojans, phishing and pharming compromise networks at the weakest entry points in the network, which are remote and branch offices of Enterprises that are less equipped to handle complex threats. Besides, rise in sophistication of threats is increasing the need of organizations to outsource their network security management to MSSPs. Both enterprises and MSSPs today struggle to implement, monitor and control a uniform security policy across branch offices and clients resulting in security, productivity and legal issues. A Centralized Management system that ensures adherence of security policies and regular security updates at multiple sites is essential for them for easy and cost-effective security.

Cyberoam Central Console

Cyberoam Central Console (CCC) is a centralized, integrated management and monitoring solution that allows enterprises and MSSPs to manage multiple, dispersed Cyberoam UTM installations across remote or branch offices and clients respectively, offering the flexibility of hardware CCC appliances and virtual CCC appliances.

Dedicated CCC Appliances

CCC hardware appliances meet the centralized management and monitoring needs for 15-1000 Cyberoam UTM appliances. Their range includes CCC15, CCC50, CCC100, CCC200, CCC500 and CCC1000.

Virtual CCC Appliances

VMware-based CCC Virtual appliances are available for Server-based Virtual environment and workstation-based Virtual environment. Virtual CCC offers full set of features as CCC hardware appliances. By allowing organizations to use the virtual VMware environment, CCC Virtual appliances eliminate the need for dedicated hardware, reduce cost of ownership and simplify future upgrades. Their range includes CCC VMS 15, CCC VMS 50, CCC VMS 100, CCC VMS 200, CCC VMW 15, CCC VMW 50, CCC VMW 100 and CCC VMW 200.

The CCC virtual appliances allow customers to manage up to 5 Cyberoam UTM appliances without any license fee, beyond which Appliance Licenses can be purchased.

Cyberoam Central Console (CCC) Features:

Centralized Management

CCC lowers the operating cost of upgrading and maintaining security of Cyberoam UTMs across dispersed office locations, offering complete control over distributed networks from the central office of enterprises or the Security Operations Center (SOC) of MSSPs.

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. This allows real-time protection against zero-hour threats in enterprises and reduces response time against newly identified threats across multiple customer networks of MSSPs.

Add UTM appliances

Grouping of UTM appliances

Configure UTM appliance from CCC

Update configuration of UTM appliances

Ease and Flexibility of Management

CCC offers quick management of distributed Cyberoam UTM appliances by allowing grouping of these appliances based on their geography, Cyberoam UTM models, firmware version, organizations (especially for MSSPs) and service subscriptions. Enhanced with Web 2.0 benefits, the Dynamic Views in CCC provide at-a-glance information on the dashboard that helps in managing, searching and sorting appliances by firmware versions, appliance models and all appliances. This helps in quick monitoring and action. CCC offers flexibility in sorting appliance views on the dashboard by allowing customizable selection criteria for sorting.

Grouping of UTM appliances

Based on Geography

Based on Appliance Models

Based on Client

Flexible Policies to Support Business Requirements

Enterprises and MSSPs have the flexibility to customize policies for various offices and clients. CCC enables template-based configuration where MSSPs can define custom policies (e.g. for education vertical) to create vertical-focused policies for their clients in minimum time. Updating of rules and policies can be centrally scheduled for individual UTM appliances or a group of UTM appliances.

Security against Misuse of Administrator Privileges

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

CCC access

Configuration	<input type="radio"/> None	<input type="radio"/> Read-Only	<input checked="" type="radio"/> Read-Write
Dashboard	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Objects	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Network	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Firewall	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Console access from GUI	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Web Filter	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Application Filter	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
IM	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
QoS	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
+ System	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
+ Identity	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
+ VPN	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
+ IPS	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
+ Anti Virus	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
+ Anti Spam	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
+ Logs & Reports	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
+ CCC Management	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
+ Appliance Management	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
+ Appliance Monitoring	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
+ CCC Logs	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

Access to group of UTM appliances

Audit Logs & Alerts - Instant Organization-wide Security Visibility

CCC's Log Viewer offers logs and views of administrator actions on CCC as well as dispersed UTM appliances which helps in investigative analysis, supports regulatory compliance as well as keeps track of historical activities across distributed networks.

Email alerts can be set for individual or group of Cyberoam UTM appliances across branch offices and client offices based on expiry of subscription modules, excess disk usage, IPS and virus threat counts, unhealthy surfing hits and other parameters. CCC's alert configuration facility helps enterprises and MSSPs reduce false alarms. Administrators can set an alert when the CPU usage reaches above 90% for a specific time period (say 20 minutes) instead of setting an alert when it momentarily peaks to 90% -- which can trigger a false alarm.

CCC Logs

View Log For : Policy Configuration
 Start Date : Management Console
 End Date : System Events

Search

Records per page: 20 (1 of 10)

Time	Event	User Name	IP Address	Entity	Sub Entity	Action	Status	Appliances	Message
2011-04-04 16:39:44	1300539026050	admin	10.103.6.142	User	Clientless User	Insert	Error	Elitecore_US	Entity blocked. CCC is not able to connect to the appliance as Remote management through CCC is not enabled from appliance.
2011-04-04 16:39:40	1300459968004	admin	10.130.1.47	Alerts	Alert profile	Insert	error	Elitecore_APAC	Push operation blocked as appliance is not synchronized.
2011-04-04 16:38:56	1300539026050	admin	10.103.6.42	Users	Clientless User	Insert	Error	Elitecore_ME	Entity blocked. CCC is not able to connect to the appliance as Remote management through CCC is not enabled from appliance.

Cyberoam UTM appliance logs

Appliance Logs

Start Date: 2011-04-04 00:00:00
 End Date: 2011-04-04 23:59:59

Appliance: Elitecore_US
 File Type: Elitecore_US, Elitecore_APAC, Elitecore_ME, Elitecore_WE

Go

From: 2011-04-04 00:00:00
 To: 2011-04-04 23:59:59

Archived Files

Show 5 days per page Page 1 of 3 Go to page :

Date	File Details	Total Size	Action
2011/03/21	<input checked="" type="checkbox"/> 00_23hrs.log (92.71 KB)	92.71 KB	View Data Unload
2011/03/20	<input type="checkbox"/> 00_23hrs.log (1.54 KB)	1.54 KB	View Data

Alert configuration

Update Alert Profile

Profile Name * Alert.From.10_103_7_1

Send email(s) alert to ben@elitecore.com

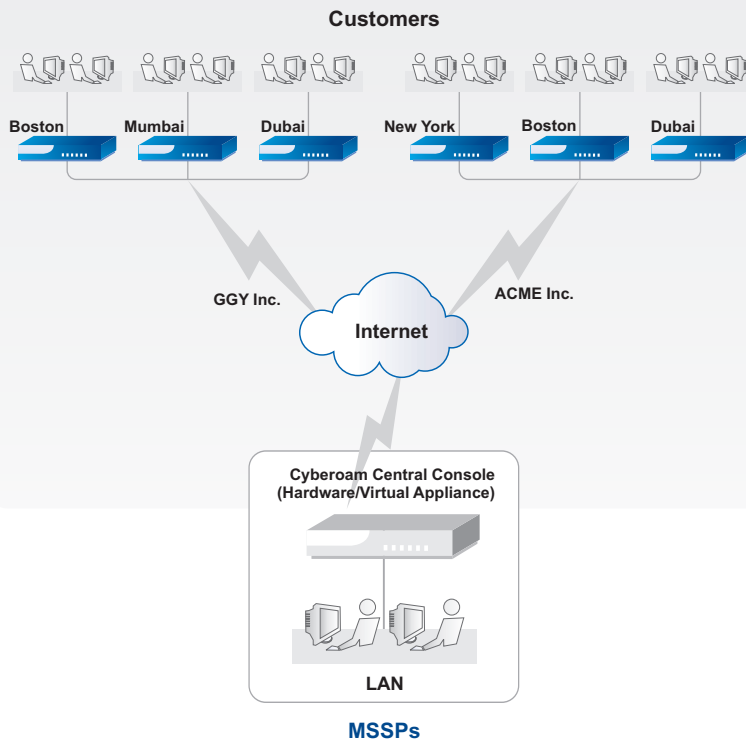
Appliance(s) All Appliance

Alerts criteria

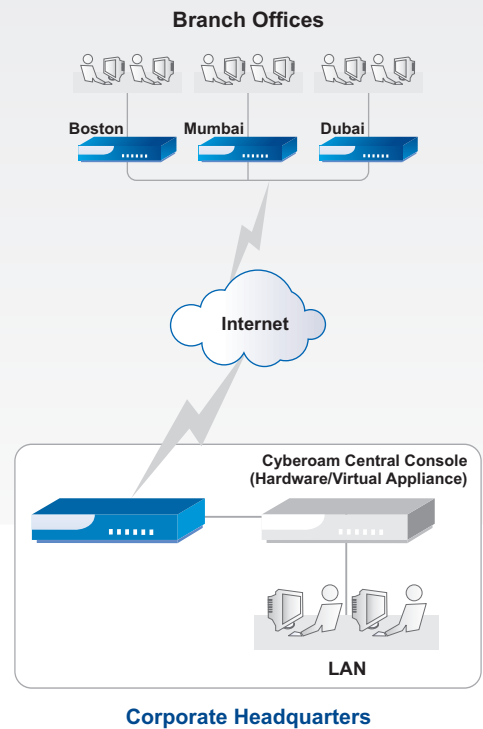
- Any subscription module expires within 7 day(s)
- CPU usage exceeds 50 % since last 20 Minutes
- Memory usage exceeds 50 % since last 20 Minutes
- Disk usage exceeds 90 %
- IPS Threats count exceeds 1000 since last 30 Minutes
- Web virus count exceeds 50 since last 30 Minutes
- Mail Virus count exceeds 50 since last 30 Minutes
- Total virus count exceeds 50 since last 30 Minutes
- Spam Mail count exceeds 50 since last 30 Minutes
- Unhealthy Surfing hits 1000 since last 30 Minutes
- Appliance Connection Status

Cyberoam Central Console Deployment

Cyberoam Central Console Deployment- MSSP



Cyberoam Central Console Deployment- Large Enterprise









CCC Features & Benefits

Features	Benefits
Centralized controls	<ul style="list-style-type: none"> • Real-time protection against newly identified threats • Lower operational cost, complexity and time to maintain dispersed networks • Organization-wide security implementation • Complete control over distributed networks from central location
Web 2.0 enabled GUI offers <ul style="list-style-type: none"> - Dynamic views - Customizable, multiple dashboards 	<ul style="list-style-type: none"> • Dynamic views help in managing, searching and sorting Cyberoam UTM appliances • View of multiple Cyberoam UTMs deployed across offices at a glance • Quick policy setting and security management
Role-based administration controls	<ul style="list-style-type: none"> • Security against misuse of administrator privileges
Group-based Cyberoam UTM management	<ul style="list-style-type: none"> • Allows centralized security management based on clients (for MSSPs), geography, UTM model and more • Enables MSSPs to have different personnel for managing distributed Cyberoam UTM appliances for quick, error-free security management
Centralized visibility <ul style="list-style-type: none"> - Alerts & Audit Logs 	<ul style="list-style-type: none"> • Real-time visibility of threat summary and trends for instant action • Helps in investigative analysis; supports regulatory compliance

CCC Appliance Range

CCC Hardware Appliance Range

CCC 15	CCC 50	CCC 100	CCC 200	CCC 500	CCC 1000
					

Virtual CCC Appliance Range

CCC for Server-based Virtual Environment

CCC VMS 15	CCC VMS 50	CCC VMS 100	CCC VMS 200
------------	------------	-------------	-------------

CCC for Workstation-based Virtual Environment

CCC VMW 15	CCC VMW 50	CCC VMW 100	CCC VMW 200
------------	------------	-------------	-------------

Cyberoam Product Portfolio

Unified Threat Management(UTM)



Cyberoam Central Console



Cyberoam iVIEW Intelligent Logging & Reporting



Cyberoam Endpoint Data Protection



Toll Free Numbers

USA : +1-800-686-2360 | India : 1-800-301-00013

APAC/MEA : +1-877-777-0368 | Europe : +44-808-120-3958

Copyright©1999-2011ElitecoreTechnologiesPvt.Ltd. AllRightsReserved.
Cyberoam and Cyberoam logo are registered trademark of Elitecore Technologies Pvt. Ltd. Although Elitecore has attempted to provide accurate information, Elitecore assumes no responsibility for accuracy or completeness of information neither is this a legally binding representation. Elitecore has the right to change, modify, transfer or otherwise revise the publication without notice. 1.0-20110203

