

## Cyberoam

Le appliance UTM Identity-based di Cyberoam offrono una protezione completa contro le esistenti ed emergenti minacce Internet, inclusi virus, worm, trojan, spyware, phishing, pharming e altri ancora.

Cyberoam UTM offre in una sola piattaforma la gamma completa di funzionalità security come Stateful Inspection Firewall, VPN, gateway antivirus, gateway anti-malware, gateway anti-spam, intrusion prevention system, content filtering oltre a bandwidth management e multiple link management.

Il portafoglio di soluzioni Cyberoam comprende Cyberoam iView, una soluzione open-source di logging e reporting, e la suite End Point Data Protection di Cyberoam per proteggere i dati e gestire gli asset agli end point delle aziende. Cyberoam ha la certificazione CheckMark UTM Level 5, ICSA Labs, ed è un membro del Virtual Private Network Consortium.

Cyberoam è stata classificata come "Visionary" all'interno del Magic Quadrant per SMB Multi-function Firewalls di Gartner. Cyberoam è continuamente valutato con 5 stelle da SC Magazine. Cyberoam ha uffici a Woburn, MA e in India.

Per ulteriori informazioni visitare il sito [www.cyberoam.com](http://www.cyberoam.com)

## Alcune delle aziende che hanno scelto Cyberoam

### Banche ed assicurazioni:

Skandia Vita, Fortis, Axis Bank, Bank Sepah, Indian Overseas Bank, Imperial Bank, Indian Bank, LIC MF, CAL Insurance & Associates Inc., SGVietFinance

### Edilizia:

Jaypee Group, ASGC, Al Jaber, Sama Dubai, Force 10, ECC, Al Fardan, Wade Adams, Al Basti & Muktha Llc, Admac, Al Safeer, Commodore Contracting, Aube immobilier

### Education:

Università della Calabria, Ashbury College, University of Mumbai, Australian International Skyline University College

## Premi e certificazioni



### Energia:

ONGC, HOEC, Tabriz Petrochemical Company, Sabarmati Gas, Petromaint

### Enti governativi:

Ministero della Giustizia del Marocco, HAL, BHEL, NHPC, GACL, DGS&D

### Farmaceutico:

Cadila healthcare, Paras, Jamjoom Pharma, Intas, Troikka

### FMCG:

Marico, Yakult, Cdo, Adani Wilmar Limited

### Grandi aziende:

LG, Videocon, Hitachi, Tata Chemicals Limited, Carlo Gavazzi, Al-Futtaim, Adani Group, Tata Solar, Ernst & Young, Garware Industria manifatturiera: Form, Binani, Electrotherm, Gulf Heavy Industries, Hindalco, Sintex, Godfrey Phillips, Sanghi Cement

### Pubblicità e Media:

Times Now.Tv, Mccann Erickson, Mudra, Art, The Times Group, Saatchi & Saatchi, Ary Digital, Percept

### Sanità:

Croce Rossa Italiana, Max Healthcare, Saudi German Hospitals Group, Yuzyil Hastanesi, Cheng Gun Medical Hospital, Sincere Medical Imaging Center

### Tecnologia e Service Provider:

TVGH Digital Medical Library, Space2Host, makemytrip.com, TATA Interactive System, BSNL, axiom telecom

### Trasporti:

Octo Telematics, Hero Honda, Honda, Timco, Lucas-Tvs, Bajaj Auto, Eicher, Emirates Airline, Yeongnam Air, Hal, Samaco, Arabasco

### Viaggi e turismo:

Esperia, Millenium, Ramada, Concorde, Trident, Mayfair, Shangri-la

## UNIFIED THREAT MANAGEMENT DI CYBEROAM

Con le sue soluzioni di Unified Threat Management (UTM) Cyberoam centralizza le strategie per la sicurezza informatica senza incidere sui budget aziendali

### Le necessità del mercato

Il mercato delle soluzioni per la gestione degli imprevisti sulle reti info-telematiche e per la sicurezza dei dati sensibili è in crescita del 25% annuo e ha un valore complessivo di 1,3 miliardi di dollari americani.

E questo perché le aziende continuano a investire in strumenti di *reporting e logging* dati da una molteplicità di apparati e applicazioni: dai *firewall e proxy server* ai prodotti antivirus, antispy e di prevenzione degli accessi indesiderati.

La crisi e la necessità di contenere le spese spingono le organizzazioni verso la scelta di piattaforme unificate, di facile gestione e in grado di assicurare prestazioni ottimali rispettando le esigenze del *budget*.

Le soluzioni UTM (cioè *Unified threat management*, gestione unificata degli attacchi) di Cyberoam della famiglia CR rispondono facilmente a tutti questi requisiti. La loro flessibilità e la loro vasta gamma le rende inoltre adatte sia alle strategie delle piccole e medie aziende sia a quelle dei grandi *business* e delle organizzazioni di maggiori dimensioni.

### Una linea di appliance da record per sicurezza e convenienza

Commercializzata ufficialmente in Italia dal distributore a valore aggiunto Horus Informatica, con sede ad Arluno (Milano) e dalla sua rete di *partner, reseller e system integrator* attivi su tutto il territorio nazionale, la serie Cyberoam CR include diversi modelli di appliance in grado di soddisfare le esigenze delle aziende di tutte le dimensioni.



Il loro denominatore comune è un approccio *identity based*, cioè basato sull'identificazione e sul controllo dei singoli utenti, alla sicurezza informatica. Sempre più spesso, infatti, minacce esterne come *spyware, phishing e pharming* si concentrano proprio sull'utenza individuale: tentano di carpirne informazioni personali o trasformarne i dispositivi in botnet per sferrare attacchi generalizzati alle reti aziendali.

“Con queste soluzioni”, dice *Massimo Grillo*, general manager di Horus Informatica, “Cyberoam è in grado di rispondere alle necessità delle aziende da un triplice punto di vista: costi, sicurezza e prestazioni elevate.

Sono state studiate infatti proprio per fare fronte alle crescenti esigenze di sicurezza ad alte prestazioni da parte delle aziende italiane, ma con un occhio di riguardo per i loro *budget*, sui quali incidono in modo molto contenuto”.

### Tante funzionalità e una sola console di controllo

Disegnate per svolgere anche funzioni di gestione della banda (*bandwidth management*), di filtro dei contenuti (*content filtering*), e di *firewall*, le *appliance* UTM della serie CR possono essere amministrare centralmente attraverso il cruscotto unificato Central Console di Cyberoam.

Ma le loro prerogative di difesa dei dati sensibili in transito sui

network aziendali comprendono anche funzionalità VPN SSL e IPSec, *gateway* anti-virus, anti-spam e anti-spyware e di *Multiple link management*.

Grazie a questa ricca gamma di risorse sono in grado di



fronteggiare con successo la continua diffusione di virus, *malware* e intrusioni indesiderate in ambienti di rete sempre più complessi.

E si adattano senza problemi all'evoluzione di tecnologie e applicazioni caratterizzate da un ampio consumo di banda come SaaS e *Web 2.0*.

## UNIFIED THREAT MANAGEMENT DI CYBEROAM

Con le sue soluzioni di Unified Threat Management (UTM) Cyberoam centralizza le strategie per la sicurezza informatica senza incidere sui budget aziendali

### L'opinione di Horus Informatica

La nuova generazione di sistemi *firewall* e UTM *identity based* di Cyberoam è in grado di soddisfare le esigenze delle aziende in materia di gestione e controllo sicuro degli accessi alle risorse in base all'identità degli utenti.

Semplice da gestire e implementare, integra funzionalità di *reporting* evoluto, di gestione *multilink*, supporto 3G su USB, controllo e gestione applicazioni di *instant messaging* e *bandwidth management*.

Si tratta di una soluzione flessibile e, dal punto di vista economico, estremamente vantaggiosa con un rapporto di efficacia, qualità, prestazioni e costo imbattibili e un supporto tecnico sempre puntuale ed attento.

È possibile testare la soluzione nel vostro ambiente richiedendo un nostro *pilot* con affiancamento dedicato dei nostri specialisti.

Estensione della salvaguardia dei dati dal gateway  
al desktop

### Le necessità del mercato

Secondo gli esperti del Ponemon Institute, un'organizzazione indipendente di ricerca e sensibilizzazione sulla sicurezza informatica, il costo medio totale di una violazione dei dati aziendali può raggiungere valori pari a 6,3 milioni di dollari. E nel 65% dei casi le violazioni si traducono in vere e proprie perdite in termini di *business*. Per gli ambienti di rete e per le imprese le minacce non vengono più soltanto dall'esterno: i rischi più temibili si annidano infatti dietro a strumenti di uso comune e generalizzato come le chiavette Usb rimovibili, le applicazioni di *chat* e *instant messaging* e, ultimi ma non meno importanti, i programmi per la condivisione di file online.

### Dal perimetro al cuore dell'azienda

La crescente raffinatezza delle metodologie di attacco e il moltiplicarsi dei potenziali punti deboli di architetture di rete sempre più complesse, necessitano risposte articolate e mirate. Proprio per questo motivo Cyberoam, multinazionale statunitense della security distribuita ufficialmente in Italia da Horus Informatica, con la nuova *suite* End Point Data Protection ha modificato il suo approccio alla difesa dei dati aziendali estendendo la protezione dai *gateway* ai *desktop*. In questo modo, riesce a erigere una barriera contro gli attacchi e la perdita di dati sensibili non soltanto al livello perimetrale esterno dei *network*, ma anche al cuore delle operazioni di tutti i giorni.

### Controllo completo sui *device* removibili

Scalabile e adatta a imprese di qualunque settore industriale e di qualsiasi dimensione, la *suite* End Point Data Protection è composta da quattro diversi moduli: Data Protection & Encryption, Device Management, Application Control e Asset Management. Grazie alle sue prerogative di protezione dei dati e di gestione degli *asset* che offrono un controllo delle *policy*

di accesso basato sia sulle identità dei singoli utenti sia sulla profilazione dei gruppi, la soluzione di Cyberoam può garantire monitoraggi esaustivi e visibilità su una varietà di tecnologie per il trasferimento dei dati: dall'uso di *device* rimovibili ai software di *chat*, dai sistemi di *network sharing* alle stampanti.

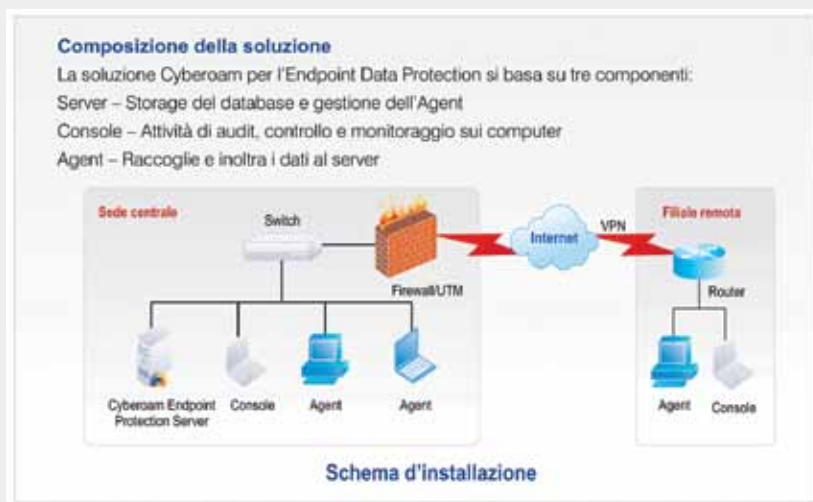
“Gli attacchi misti non distinguono fra un *gateway* e un *end point* per ottenere l'accesso” commenta infatti Hemal Patel, Ceo di Cyberoam “e con la *suite* End Point Data Protection

Cyberoam offre una soluzione di sicurezza unica e completa capace di difendere le aziende dal *gateway* al *desktop*”.

### Una soluzione attenta al valore dell'*hi-tech*

Il pacchetto di Cyberoam garantisce la personalizzazione delle *white* e *blacklist* e un controllo granulare sul trasferimento dei dati, fondato sul profilo degli utenti, dei gruppi e degli orari di accesso; sulla tipologia e la dimensione dei documenti trattati; sulla creazione di copie fantasma. Le operazioni di crittazione e de-crittazione su file e dispositivi Usb sono in grado di evitare la perdita delle informazioni critiche sia in caso di smarrimento dei *device* sia in caso di azioni malevole.





## L'opinione di Horus Informatica

La *suite* Cyberoam End Point Data Protection soddisfa le esigenze di *endpoint security* e *data loss prevention* della maggioranza delle aziende.

È semplicissima e immediata da implementare e gestire attraverso un'unica *console* di gestione per tutte le funzionalità e questo si risolve in un impatto prossimo allo zero sull'organizzazione e sull'operatività aziendale.

La grande novità della soluzione, che è già pienamente compatibile con il sistema operativo Microsoft Windows 7, è tuttavia rappresentata dalle funzionalità di Asset Management. Permette di tenere un costante inventario automatico del patrimonio hardware e software aziendale e offre la gestione automatizzata delle *patch* e del *bug fixing*. "L'implementazione di funzioni per l'*Asset Management* ci è stata esplicitamente richiesta dal 60% dei nostri *partner* di canale" ha detto Heman Patel "per i quali rappresenta una notevole opportunità di *business*".

In qualità di distributore a valore aggiunto ufficiale per il nostro Paese, Horus Informatica è già in grado di fornire consulenza, servizi e *training* alla sua rete di rivenditori e *system integrator* e ai clienti finali su tutto il territorio nazionale. E offre una versione di prova della nuova suite alla Url [http://www.horus.it/Cyberoam\\_EDP.htm](http://www.horus.it/Cyberoam_EDP.htm).

È possibile testare la soluzione grazie al *libero* download della versione *evaluation* della validità di trenta giorni o richiedendo un nostro *pilot* con affiancamento dedicato dei nostri specialisti.

Cyberoam End Point Data Protection è un prodotto molto flessibile ed estremamente vantaggioso dal punto di vista economico con un rapporto di efficacia, qualità, prestazioni e costo imbattibili e un supporto tecnico sempre puntuale ed attento. Si tratta dell'unica soluzione di questo genere con licenza di *acquisto* onetime: costi di gestione e operativi bassissimi che permettono alle imprese di introdurre una soluzione esaustiva di *endpoint security* e *data loss prevention* a fronte di *budget* limitati.



## CYBEROAM IVIEW

Cyberoam iView è una soluzione per la gestione di elevati volumi di log, in grado di facilitare le analisi e la produzione di report, semplificare le attività di audit, le analisi di sicurezza, le attività di conformità.

### Le necessità del mercato

Le aziende moderne lottano per difendere le loro infrastrutture sia dalle minacce esterne in continua evoluzione, che dai pericoli provenienti dall'interno della rete. Inoltre in realtà complesse con uffici distribuiti in più sedi e dispositivi multipli da gestire è fondamentale avere la visuale completa dell'intera infrastruttura di rete.

Cyberoam iView è la soluzione per logging e reporting che consente di monitorare centralmente le reti aziendali e garantire elevati livelli di sicurezza e riservatezza dei dati nella totale conformità alle normative vigenti. Una singola interfaccia centrale restituisce il quadro globale della sicurezza aziendale. Le aziende gestiscono centralmente le policy di sicurezza attraverso un'interfaccia grafica intuitiva con report che offrono costantemente la visuale di tutti i parametri della rete e consentono di individuare l'anello debole del sistema. Offre ad esempio la visuale degli attacchi principali, delle applicazioni maggiormente usate per gli attacchi, dei principali destinatari di mail spam e dei virus più diffusi.

Informazioni legate all'identità degli utenti (es. chi occupa maggiormente la banda per upload / download; quali sono le applicazioni più usate) aiutano a gestire le risorse aziendali oltre a garantire un maggiore livello di sicurezza.

### Caratteristiche principali

Cyberoam iView consente di personalizzare *white* e *blacklist* e offre un controllo granulare sul trasferimento dei dati, basato sul profilo degli utenti, dei gruppi e degli orari di accesso, sulla tipologia e la dimensione dei file usati e sulla creazione di copie fantasma.

Le operazioni di criptazione e de-criptazione su file e dispositivi USB evitano la perdita delle informazioni critiche sia in caso di

smarrimento dei *device*, che in caso di azioni malevole.

**Log Management:** raccoglie, filtra e archivia i log provenienti dal sistema su standard syslog con funzionalità di ricerca e reporting evoluto riducendo in modo significativo il costo e la complessità delle attività di analisi.

**Security Management:** offre una visuale completa dello stato di sicurezza dell'azienda. Le aziende possono individuare immediatamente attacchi di rete, la loro origine e la destinazione con un rapido sguardo al pannello principale e intraprendere azioni sulla rete in qualsiasi luogo del mondo.



**Compliance Reporting:** il facile accesso ai report ed alla verifica dei log riduce i costi necessari a garantire la conformità alle normative vigenti. Gli amministratori sono informati tempestivamente dei comportamenti anomali con una conseguente riduzione dei tempi di risposta agli incidenti.

**Analisi legali:** le aziende possono ricostruire rapidamente la sequenza degli eventi che si sono verificati nel momento di una violazione riducendo i costi necessari a indagare sull'accaduto e a ridurre il downtime della rete.

**Supporto multiple device:** supporto di diversi dispositivi di rete tra cui firewall UTM, Linux IP Tables/Net Filter firewall, Squid.

**Spazio Terabyte per lo Storage:** Terabyte di spazio disponibile per l'archiviazione di tutta la reportistica.

**Ridondanza dei dati:** la tecnologia RAID garantisce ridondanza ed elevati livelli di affidabilità di storage in modo da salvaguardare l'appliance anche in caso di guasto dell'hard disk.

## Le necessità del mercato

Sono sempre più diffusi fenomeni come gli attacchi zero-hour che in poche ore si espandono su milioni di computer o gli attacchi misti come virus, worm, Trojan, phishing e pharming che compromettono le reti aziendali nei loro punti di accesso più deboli quali sedi remote o filiali delle aziende meno attrezzate per gestire minacce complesse. Inoltre l'aumento della sofisticazione delle minacce spinge le aziende ad affidare la gestione delle loro infrastrutture IT ai MSSP.

Attualmente implementare, monitorare e controllare policy di sicurezza estese all'intera infrastruttura di rete comporta diverse problematiche da gestire a livello di sicurezza, produttività e legalità.

In questo scenario sorge la necessità di un sistema di gestione centralizzato che garantisca l'applicazione delle policy e l'aggiornamento periodico del sistema di sicurezza su tutte le filiali con enormi vantaggi in termini di semplicità di gestione e di risparmio economico.

## Caratteristiche principali

Cyberoam Central Console (CCC) è l'appliance per la gestione centralizzata ed il monitoring che consente di gestire molteplici installazioni di Cyberoam UTM distribuite su più uffici remoti e filiali con risparmi economici, di tempo e di training tecnico.

**Security Management:** semplifica la gestione e migliora il livello della sicurezza grazie alla possibilità di creare policy centrali e a implementare, registrare ed effettuare aggiornamenti su tutte le appliance Cyberoam UTM distribuite per quanto riguarda tutte le UTM (Firewall, Intrusion Prevention System, Anti-Virus scanning). CCC garantisce alle infrastrutture di rete distribuite una difesa coordinata contro le minacce miste e zero-hour.

Le aziende ed i MSSP possono personalizzare con flessibilità le policy di tutte le sedi. I MSSP possono inoltre configurare, tramite template, policy verticali specifiche (es. per settore education).

Gli aggiornamenti di rule e policy possono essere schedulati centralmente per ogni singola appliance o per gruppi di appliance.

**Semplicità e flessibilità di gestione:** veloce gestione delle appliance Cyberoam UTM distribuite grazie alla possibilità di raggruppare le appliance per area geografica, modello



di Cyberoam UTM, versione firmware, tipo azienda o tipo di licenza. E' possibile creare con flessibilità viste per gruppi di appliance che aiutano a monitorare ed intraprendere azioni tempestivamente.

**Prevenzione dall'abuso dei privilegi amministrativi:** possibilità di impostare diversi livelli di amministrazione in base al ruolo sia per la gestione delle appliance CCC che per gruppi o singole appliance di Cyberoam UTM.

**Log ed Alert:** tramite la funzionalità Log Viewer sono disponibili log e viste sia delle operazioni effettuate sulle appliance CCC che su tutte le appliance Cyberoam UTM in modo da poter effettuare analisi investigative, garantire la conformità alle normative vigenti e mantenere lo storico di tutte le attività.

Gli amministratori possono impostare alert email da inviare in occasione di scadenza di una licenza, eccessivo utilizzo di un disco, per fornire elenchi IPS e di virus, report su navigazione inappropriata ecc. E' possibile impostare alert da attivare quando l'utilizzo della CPU supera il 90% per un determinato periodo di tempo (es. 20 minuti) evitando così falsi allarmi.

# SCHNEDE TECHNISCHE



## UNIFIED THREAT MANAGEMENT DI CYBEROAM

Con le sue soluzioni di Unified Threat Management (UTM) Cyberoam centralizza le strategie per la sicurezza informatica senza incidere sui budget aziendali

### FEATURE SPECIFICATIONS

#### STATEFUL INSPECTION FIREWALL

- Layer 8 (User - Identity) Firewall
- Multiple Security Zones
- Access Control Criteria (ACC) - User - Identity, Source & Destination Zone, MAC and IP address, Service
- UTM policies - IPS, Web Filtering, Application Filtering, Antivirus, Anti-spam and Bandwidth Management
- Layer 7 (Application) Control & Visibility
- Access Scheduling
- Policy based Source & Destination NAT
- H.323 NAT Traversal
- 802.1q VLAN Support
- DoS & DDoS attack prevention
- MAC & IP-MAC filtering and Spoof prevention

#### GATEWAY ANTI-VIRUS & ANTI-SPYWARE

- Virus, Worm, Trojan Detection & Removal
- Spyware, Malware, Phishing protection
- Automatic virus signature database update
- Scans HTTP, FTP, SMTP, POP3, IMAP, IM, VPN tunnels
- Customize individual user scanning
- Self Service Quarantine area<sup>1</sup>
- Scan and deliver by file size
- Block by file types
- Add disclaimer/signature

#### GATEWAY ANTI-SPAM

- Real-time Blacklist (RBL), MIME header check
- Filter based on message header, size, sender, recipient
- Subject line tagging
- Redirect spam mails to dedicated email address
- Image-spam filtering using RPD Technology
- Zero hour Virus Outbreak Protection
- Self Service Quarantine area<sup>1</sup>
- IP address Black list/White list
- Spam Notification through Digest<sup>2</sup>
- IP Reputation-based Spam filtering

#### INTRUSION PREVENTION SYSTEM

- Signatures: Default (3000+), Custom
- IPS Policies: Multiple, Custom
- User-based policy creation
- Automatic real-time updates from CRProtect networks
- Protocol Anomaly Detection
- DDoS attack prevention

#### WEB FILTERING

- Inbuilt Web Category Database
- URL, keyword, File type block
- Web Categories: Default(82+), Custom
- Protocols supported: HTTP, HTTPS
- Block Malware, Phishing, Pharming URLs
- Category-based Bandwidth allocation and prioritization
- Block Java Applets, Cookies, Active X
- CIPA Compliant
- Data leakage control via HTTP, HTTPS upload
- Schedule-based access control
- Custom block messages per category

#### APPLICATION FILTERING

- Inbuilt Application Category Database
- Application Categories: 11+ e.g. Gaming, IM, P2P, Proxy
- Schedule-based access control
- Block:
  - P2P applications e.g. Skype
  - Anonymous proxies e.g. Ultra surf
  - "Phone home" activities
- Keylogger
- Layer 7 (Applications) & Layer 8 (User - Identity)

#### Visibility

#### VIRTUAL PRIVATE NETWORK

- IPsec, L2TP, PPTP
- Encryption - 3DES, DES, AES, Twofish, Blowfish, Serpent
- Hash Algorithms - MD5, SHA-1
- Authentication: Preshared key, Digital certificates
- IPsec NAT Traversal
- Dead peer detection and PFS support
- Diffie Hellman Groups - 1,2,5,14,15,16
- External Certificate Authority support
- Export Road Warrior connection configuration
- Domain name support for tunnel end points
- VPN connection redundancy
- Overlapping Network support
- Hub & Spoke VPN support

#### SSL VPN<sup>3</sup>

- TCP & UDP Tunneling
- Authentication - Active Directory, LDAP, RADIUS, Cyberoam
- Multi-layered Client Authentication - Certificate, Username/Password
- User & Group policy enforcement
- Network access - Split and Full tunneling
- Browser-based (Portal) Access - Clientless access
- Lightweight SSL VPN Tunneling Client
- Granular access control to all the Enterprise Network resources
- Administrative controls - Session timeout, Dead Peer Detection, Portal customization
- TCP-based Application Access - HTTP, HTTPS, RDP, TELNET, SSH

#### INSTANT MESSAGING (IM) MANAGEMENT

- Yahoo and Windows Live Messenger
- Virus Scanning for IM traffic
- Allow/Block Login
- Allow/Block File Transfer
- Allow/Block Webcam
- Allow/Block one-to-one/group Chat
- Content-based blocking
- IM activities Log
- Archive files transferred
- Custom Alerts

#### WIRELESS WAN

- USB port 3G and Wimax Support<sup>\*</sup>
- Primary WAN link
- WAN Backup link

#### BANDWIDTH MANAGEMENT

- Application and User Identity based Bandwidth Management
- Category-based Bandwidth restriction
- Guaranteed & Burstable bandwidth policy
- Application & User Identity based Traffic Discovery<sup>4</sup>
- Multi WAN bandwidth reporting

#### USER IDENTITY & GROUP BASED CONTROLS

- Access time restriction
- Time and Data Quota restriction
- Schedule based Committed and Burstable Bandwidth
- Schedule based P2P and IM Controls

#### NETWORKING

- Failover
- Automated Failover/Failback, Multi-WAN failover, 3GModem failover
- WRR based Load balancing
- Policy routing based on Application and User
- IP Address Assignment - Static, PPPoE, L2TP, PPTP & DDNS Client, Proxy ARP, DHCP server, DHCP relay
- Support for HTTP Proxy

- Dynamic Routing: RIP v1& v2, OSPF, BGP, Multicast Forwarding
- Parent Proxy support with FQDN
- IPv6 Ready Gold Logo

#### HIGH AVAILABILITY<sup>5</sup>

- Active-Active
- Active-Passive with state synchronization
- Stateful Failover
- Alerts on Appliance Status change

#### ADMINISTRATION & SYSTEM MANAGEMENT

- Web-based configuration wizard
- Role-based Access control
- Firmware Upgrades via Web UI
- Web 2.0 compliant UI (HTTPS)
- UI Color Styler
- Command line interface (Serial, SSH, Telnet)
- SNMP (v1, v2c, v3)
- Multi-lingual support: Chinese, Hindi, French, Korean
- Cyberoam Central Console (Optional)
- NTP Support

#### USER AUTHENTICATION

- Internal database
- Active Directory Integration
- Automatic Windows Single Sign On
- External LDAP/RADIUS database Integration
- Thin Client support - Microsoft Windows Server 2003 Terminal Services and Citrix XenApp
- RSA SecurID support
- External Authentication - Users and Administrators
- User/MAC Binding
- Multiple Authentication servers

#### LOGGING / MONITORING

- Graphical real-time and historical Monitoring
- Email notification of reports, viruses and attacks
- Syslog support
- Log Viewer - IPS, Web filter, Anti Virus, Anti Spam, Authentication, System and Admin Events

#### ON-APPLIANCE CYBEROAM I-VIEW REPORTING<sup>6</sup>

- Integrated Web-based Reporting tool - Cyberoam-iView
- 1000+ drilldown reports
- 45+ Compliance reports
- Historical and Real-time reports
- Multiple Dashboards
- Username, Host, Email ID specific Monitoring Dashboard
- Reports - Security, Spam, Virus, Spam, Traffic, Policy violations, VPN, Search Engine keywords
- Multi-format reports - tabular, graphical
- Exportable formats - PDF, Excel
- Automated Report Scheduling

#### IPSEC VPN CLIENT

- Inter-operability with major IPsec VPN Gateways
- Supported platforms: Windows 2000, WinXP 32/64-bit, Windows 2003 32-bit, Windows 2008 32/64-bit, Windows Vista 32/64-bit, Windows 7 RC1 32/64-bit
- Import Connection configuration

#### COMPLIANCE

- CE
- FCC

#### CERTIFICATION

- ICSA Firewall - Corporate
- Checkmark UTM Level 5 Certification
- VPNC - Basic and AES interoperability
- IPv6 Ready Gold Logo

<sup>1</sup>1,2,3,4,5,6 Available in all the Models except CR15i

<sup>\*</sup>3G card and modem details are not included.

See <http://www.cyberoam.com> for supported USB devices.

<sup>5</sup> Not Available in Wireless Series<sup>7</sup>

Specifications	15wi	25wi	35wi	15i	25ia	35ia
10/100 Ethernet Ports	3	-	-	3	-	-
10/100/1000 GBE Ports	-	4	4	-	4	4
Configurable Internal/DMZ/WAN Ports	Yes	Yes	Yes	Yes	Yes	Yes
Console Ports (RJ45/DB9)	1	1	1	1	1	1
SFP (Mini GBIC) Ports	-	-	-	-	-	-
USB Ports	1	1	1	1	1	1
Hardware Bypass Segments	-	-	-	-	-	-
Firewall Throughput (UDP) (Mbps)	150	450	750	150	450	750
Firewall Throughput (TCP) (Mbps)	90	225	500	90	225	500
New sessions/second	2,000	3,500	5,500	2,000	3,500	5,500
Concurrent sessions	30,000	130,000	175,000	30,000	130,000	175,000
3DES/AES throughput (Mbps)	15/25	30/75	50/80	15/25	30/75	50/80
Antivirus throughput (Mbps)	20	65	125	20	65	125
IPS throughput (Mbps)	40	70	150	40	70	150
UTM throughput (Mbps)	15	50	90	15	50	90
Authenticated Users/Nodes	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
H x W x D (inches)	1.7 x 6 x 9.1	1.7 x 6 x 9.1	1.7 x 6 x 9.1	1.7 x 6 x 9.1	1.7 x 9.1 x 6	1.7 x 9.1 x 6
H x W x D (cms)	4.4 x 15.3 x 23.2	4.4 x 15.3 x 23.2	4.4 x 15.3 x 23.2	4.4 x 15.3 x 23.2	4.4 x 23.2 x 15.3	4.4 x 23.2 x 15.3
Appliance Weight	1.5 kg, 3.307 lbs	2.3 kg, 5.07 lbs	2.3 kg, 5.07 lbs	1.5 kg, 3.307 lbs	2.3 kg, 5.1 lbs	2.3 kg, 5.1 lbs
Wireless Standards	IEEE 802.11 n/b/g (WEP, WPA, WPA2, 802.11i, TKIP, AES, PSK, 802.1x EAP)					
Antenna	Detachable 2x3 MIMO					
Access Points	Up to 8 bssid					
Transmit Power (EIRP)	11n HT40 : +17dBm, 11b CCK: +19dBm, 11g OFDM: +17dBm					
Receiver Sensitivity	65dBm at 300Mbps, -70dBm at 54Mbps, -86dBm at 11Mbps					
Frequency Range	USA (FCC): 2.412GHz ~ 2.462GHz, Europe (ETSI): 2.412GHz ~ 2.472 GHz, Japan (TELECOM): 2.412GHz ~ 2.483GHz					
Number of Selectable Channels	USA (FCC) - 11 channels, EU (ETSI) / Japan (TELECOM) - 13 channels					
Data Rate	802.11n: up to 300Mbps, 802.11b: 1, 2, 5.5, 11Mbps, 802.11g: 6, 9, 12, 18, 24, 36, 48, 54Mbps					
Input Voltage	100-240VAC	100-240VAC	100-240VAC	100-240VAC	100-240VAC	100-240VAC
Consumption	13.2W	33.5W	47.8W	13.2W	33.5W	47.8W
Total Heat Dissipation (BTU)	45	114	163	45	114	163
Redundant Power Supply	-	-	-	-	-	-
Environmental	Operating Temperature - 5 to 40 °C, Storage Temperature - 0 to 70 °C, Relative Humidity (Non condensing) - 10 to 90%					

\*If Enabled, will bypass traffic only in case of Power failure. \* Antivirus, IPS and UTM performance is measured based on HTTP traffic as per RFC 3511 guidelines. Actual performance may vary depending on the real network traffic environments.

Specifications	50ia	100ia	200i	300i	500ia	750ia	1000ia	1500ia
10/100 Ethernet Ports	-	-	-	-	-	-	-	-
10/100/1000 GBE Ports	6	6	6	6	10	14	12	22
Configurable Internal/DMZ/WAN Ports	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Console Ports (RJ45/DB9)	1	1	1	1	1	1	1	1
SFP (Mini GBIC) Ports	-	-	-	-	-	-	4	4
USB Ports	2	2	2	2	2	2	2	2
Hardware Bypass Segments	1 <sup>#</sup>	1 <sup>#</sup>	1 <sup>#</sup>	1 <sup>#</sup>	2	2	2	2
Firewall Throughput (UDP) (Mbps)	1,000	1,250	2,200	2,600	5,000	6,000	7,500	10,000
Firewall Throughput (TCP) (Mbps)	750	1,000	1,500	1,800	3,000	4,500	5,500	7,500
New sessions/second	8,000	10,000	12,000	15,000	25,000	35,000	50,000	75,000
Concurrent sessions	220,000	400,000	450,000	500,000	700,000	900,000	1,200,000	1,500,000
3DES/AES throughput (Mbps)	60/90	80/100	150/180	180/200	325/400	500/750	900/1200	1200/1500
Antivirus throughput (Mbps)	150	200	280	450	750	900	1,250	1,550
IPS throughput (Mbps)	200	300	750	850	1000	1,250	2,000	3,000
UTM throughput (Mbps)	130	160	250	350	550	650	800	1,200
Authenticated Users/Nodes	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
H x W x D (inches)	1.7 x 16.8 x 10.3	1.7 x 16.8 x 10.3	1.7 x 17.3 x 14.6	1.7 x 17.3 x 14.6	1.72 x 17.25 x 11.50	1.72 x 17.44 x 15.98	1.77x17.25x18.30	3.54x17.5x23.23
H x W x D (cms)	4.3 x 42.7 x 26.2	4.3 x 42.7 x 26.2	4.3 x 43.9 x 37.1	4.3 x 43.9 x 37.1	4.4 x 43.8 x 29.21	4.4 x 44.3 x 40.6	4.5 x 43.8 x 46.5	9 x 44.5 x 59
Appliance Weight	5.3 kg, 11.68 lbs	5.3 kg, 11.68 lbs	6.5 kg, 14.33 lbs	6.5 kg, 14.33 lbs	5.54 kg, 12.118 lbs	6.04 kg, 13.198 lbs	13.5 kg, 29.76 lbs	18.5 kg, 40.78 lbs
Input Voltage	100-240VAC	115-230VAC	115-230VAC	115-230VAC	100-240VAC	100-240VAC	90-260VAC	90-260VAC
Consumption	47.8W	90W	90W	62.7W	128W	185W	129W	258W
Total Heat Dissipation (BTU)	163	200	200	324	375	475	626	881
Redundant Power Supply	-	-	-	-	-	-	Yes	Yes
Environmental	Operating Temperature - 5 to 40 °C, Storage Temperature - 0 to 70 °C, Relative Humidity (Non condensing) - 10 to 90%							

\*If Enabled, will bypass traffic only in case of Power failure. \* Antivirus, IPS and UTM performance is measured based on HTTP traffic as per RFC 3511 guidelines. Actual performance may vary depending on the real network traffic environments.

## FEATURE SPECIFICATIONS

### DATA PROTECTION & ENCRYPTION

#### Document Control

Policy creation based on

- Disk types - Fixed, Floppy, CD-ROM/DVD, Removable, Sharing
- File name and extension
- Application type

Logging and search: Local and Shared files based on

- Access, modify, delete, copy, create, restore, rename
- Source, destination path
- File name, extension, size
- Application, disk type

#### Encryption over Removable Devices

Support USB-based storage devices

- Pen drives
- Hard drives (indicative list only)

Add, classify storage devices by

- Black List & White List
- Hierarchy / Group-based
- Encryption

Policy-based control for

- Read & Write
- Encryption on Write; Decryption on Read

Encryption based on files, devices

Removable storage logs by

- Device description
- Plugin / plugout record with time stamp

#### Email Control

Policy creation based on

- Sender, recipient
- Subject
- Attachment: File name, extension, size

Email logs

- Email content, attachment
- Protocols: SMTP / POP3
- Applications - Exchange®, Lotus Notes®
- Webmail - Hotmail, Yahoo Mail®
- Search email by
  - Application, sender / recipient
  - Subject
  - Attachment - File name, extension, size

#### Instant Messaging (IM) Control

Applications supported - MSN, Yahoo, Skype, ICQ, QQ, Google Talk, UC, Popo, RTX, LSC, ALI, Fetion, TM

Policy creation based on

- File name, extension, size

IM Logs

- Chat conversation logs
- File upload, download
- Search on
  - Content of chat conversation
  - UserId / nickname

#### Printer Control

Printer access: Local, network, shared and virtual printers

Printer name

Application-based printing

Print logs by

- Printer type, name, time
- Number of pages
- File / Task, application name

#### Shadow Copy

Backup of files transferred over:

Removable, fixed and shared devices based on

- Modify, cut / copy to, delete activity
- File name, extension and size range

Instant Messaging (Files transferred / blocked)

- File name, extension and size range

Email based on

- Sender / recipient
- Email size range

Printer based on

- Print records / logs
- Record printed file / task image

### DEVICE MANAGEMENT

Access policy for

Storage Device

- Floppy, CDROM, Burning Device, Tape, Movable Device

Communication Device

- COM, LPT
- USB, SCSI, 1394 Controller
- Infrared, PCMCIA
- Bluetooth, Modem, Direct Lines

Dial-up Connection

USB Device

- USB Keyboard, Mouse, Modem, Image

Device

- USB CDROM
- USB Storage and Hard disk
- USB LAN Adapter and other USB Devices

Network Device

- Wireless LAN Adapter
- PnP Adapter (USB, PCMCIA)
- Virtual LAN Adapter

Other devices - Audio & Virtual CDROM

### FEATURE SPECIFICATIONS

#### APPLICATION CONTROL

Application access policy for: Games, IM, P2P (indicative list only)  
Add, classify applications based on hierarchy and role  
Create white list / black list of classified applications  
Granular, policy-based application access controls  
Application usage logs

- By application
- Start / stop, timestamp, path

#### ASSET MANAGEMENT

Automatic collection of endpoint information

- Hardware configuration
- List of installed applications

Inventory tracking of hardware assets

- CPU, memory, network adapter, disks, motherboard, integrated peripherals

Inventory tracking of software assets

- Anti-virus information
- Application name, version, manufacturer, installed path
- OS information - Name and version, license number
- Install date, service pack
- Microsoft® patch information
- Security update
- Hotfix
- Microsoft® application updates

Historical information

- Track addition and deletion of hardware and software

Add custom tags to software and hardware assets  
Add custom assets such as printers, routers, switches, and more

#### Patch Management

Microsoft® patch management by listing of patches  
Microsoft® patch management by nodes  
Auto download of patch at nodes  
Centralized installation of patches

#### Alert Policy

Monitors hardware and software changes

#### Remote Deployment

Creation and installation of packages  
Deployment of packages based on node or group

#### Administration

Role-based granular administration  
Role-based access to computer, user groups  
Multiple administrators, user levels  
Multiple console support  
Robust, tamper-proof agents  
Centralized deployment of agents  
Auto agent installation on multiple endpoints  
Automatic installation of agent in domain controller environment

#### Alerts & Warning Messages

- Policy violation alerts to administrator
- Alert level - Low, Important & Critical
- Customized warning message to end user
- Warning - Pop-up dialog box

#### General Policy Control

- Control Panel, Computer Management
- System (Task Manager, Registry Editing, Command Prompt)
- Network, IP/MAC Binding and ActiveX controls
- Printscreen key stroke
- Lock computer on policy violation
- Policy enforcement for offline endpoints
- Temporary policy creation: Set expiry, date, time

#### Logging & Reporting

Logging and search based on date, time, endpoint range  
Graphical, real-time and historical monitoring  
Basic endpoint logging

- Endpoint startup
- User logon & logoff
- Patch installation
- Dialup logs & IP Address/MAC Address information

#### Requisiti di sistema

Modulo	Sistema operativo	Database	Hardware raccomandato
Server	Win2000 SP4/XP SP2/2003 SP1/Vista	SQL Server 2000 SP4 or above / SQL Server 2005 SP1 or above MSDE SP4 / SQL Server 2005 Express	Pentium IV 2GHZ/512MB Memory/50GB HDD space
Console	Win2000 SP4/XP/2003/2008/Vista	NA	Pentium III 1GHZ/256MB Memory/4 GB HDD space
Agent*	Win 2000/XP/2003/2008/Vista(32 bit only)/Win 7**	NA	Pentium III 500 MHZ/128MB Memory/1 GB HDD space

\*Licensing is based on number of Agents. \*\*In Roadmap



## FEATURE SPECIFICATIONS

### Logs

- Real-time log
- Archive log
- Audit Log
- Archived Log search
- Log storage (Backup/ restore)
- Exportable format - MS Excel
- Compliance support

### Reports

- 1000+ drilldown reports
- Historical reports
- Search Reports
- Customized Report Views
- Reports Include: Security, Spam, Virus, Traffic, Blocked
- Attempts, Blocked Web Attempts
- Multi-format reports - tabular, graphical
- Exportable formats - PDF, Excel
- Email Alerts/automated Report Scheduling
- Real-time reports

### Administration

- Role-based administration
- Multiple Dashboard - Report, Resource, Custom
- Automatic Device Detection
- Device Grouping
- geographical location
- device type
- device models
- administrators
- Reports accessible from any location using standard Web browser

### Operating Environment

- Hardened Linux OS

### Supported Web Browsers

- Microsoft Internet Explorer 6.0+
- Mozilla Firefox 2.0+ (Best view)
- Google Chrome

### Supported Network and Security Devices

- Custom/Proprietary devices including UTM's
- Proxy Firewalls
- Custom Applications
- Syslog-compatible devices

Hardware Specifications	CR-iVU25	CR-iVU100	CR-iVU200
<b>Storage</b>			
Total Available Storage	Total Available Storage	3.5TB	7TB
Number of Hard Drives	Number of Hard Drives	8 (500GB each)	8 (1TB each)
RAID storage Management	RAID storage Management	RAID 5	RAID 5
<b>Performance</b>			
Events per Second (EPS)	250	500	1000
Devices supported	25	100	200
<b>Interfaces</b>			
Ethernet Ports	4GbE	4GbE	4GbE
Memory	2GB	4GB	4GB
Console Ports	1 (RJ45)	1 (DB9)	1 (DB9)
USB Ports	1	Dual	Dual
DVD-RW	No	Yes	Yes
VGA	No	Yes	Yes
<b>Dimensions</b>			
H x W x D (inches)	1.72 x 10.83 x 17.32	3.46 x 16.7 x 20.9	3.46 x 16.7 x 20.9
H x W x D (cms)	4.4 x 27.5 x 44	8.8 x 42.4 x 53.1	8.8 x 42.4 x 53.1
Weight	3.78kg, 8.35lbs	16 kg, 36lbs	16 kg, 36lbs
<b>Power</b>			
Input Voltage	100-240 VAC	100-240 VAC	100-240 VAC
Consumption	65W	265W	265W
Total Heat Dissipation (BTU)	175	425	425
<b>Environmental</b>			
Operating Temperature	5 to 40 °C	5 to 40 °C	5 to 40 °C
Storage Temperature	20 to 70 °C	20 to 70 °C	20 to 70 °C
Relative Humidity (Non condensing)	20 to 70%	20 to 70%	20 to 70%

**TECHNICAL SPECIFICATIONS**

Specifications	CCC15	CCC50	CCC100	CCC200	CCC500	CCC1000
<b>Interfaces</b>						
10/100/1000 GBE Ports	6	6	6	6	6	8
Console Ports (RJ45)	1	1	1	1	1	1
SFP (Mini GBIC) Ports	-	-	-	-	-	-
USB Ports	2	2	2	2	2	2
<b>Dimensions</b>						
H x W x D (inches)	1.72 x 17.25 x 11.50	1.72 x 17.25 x 11.50	1.72 x 17.25 x 11.50	1.72 x 17.44 x 15.98	1.72 x 17.44 x 15.98	1.77 x 17.25 x 18.30
H x W x D (cms)	4.4 x 43.8 x 29.21	4.4 x 43.8 x 29.21	4.4 x 43.8 x 29.21	4.4 x 44.3 x 40.6	4.4 x 44.3 x 40.6	4.5 x 43.8 x 46.5
Weight (kg, lbs)	5.54, 12.188	5.54, 12.188	5.54, 12.188	6.04, 13.31	6.04, 13.31	13.5, 29.76
<b>Power</b>						
Input Voltage	100-240VAC	100-240VAC	100-240VAC	100-240VAC	100-240VAC	90-260VAC
Consumption	128W	128W	128W	185W	185W	129W
Total Heat Dissipation (BTU)	375	375	375	475	475	626
<b>Environmental</b>						
Operating Temperature	5 to 40 C	5 to 40 C	5 to 40 C	5 to 40 C	5 to 40 C	0 to 40 C
Storage Temperature	0 to 70 C	0 to 70 C	0 to 70 C	0 to 70 C	0 to 70 C	-20 to 80 C
Relative Humidity (Non condensing)	10 to 90%	10 to 90%	10 to 90%	10 to 90%	10 to 90%	10 to 90%
Cooling System (40mm Fan)	3	3	3	3	3	3
No. of CR Devices Supported	15	50	100	200	500	10000

**FEATURE SPECIFICATIONS**
**CENTRALIZED REMOTE MANAGEMENT**
**Configure and Manage:**

- Individual Devices
- Appliance Groups

**Global Enforcement:**

- Firewall rules and its parameters (Host, Host Group, Service, Service Group,)
- NAT policy
- DoS and Spoof Prevention Settings Schedule
- Network configuration – Static Route, DNS
- Web Filtering – Settings, Policy and Category
- Application Filtering – Category and Policy
- QoS Policy
- IPS Policy and Custom Signatures
- Anti Virus and Anti Spam – Configuration, Address Groups, Scanning rules
- pam Digest settings
- Custom Categories – File Type
- IM – Contacts and Filtering rules
- Syslog configuration
- VPN – Policy, IPsec connection
- L2TP, PPTP – Configuration, Connection
- NTP Server
- Certificates, Certificate Authority
- User and User Groups
- Authentication configuration
- Policies - Access Time, Surfing Quota, Data Transfer
- Administrator Profiles
- Appliance Port Settings and Access
- Captive Portal settings
- Parent Proxy configuration
- SNMP

**APPLIANCE MONITORING & ALERTS**

- Dashboard for Appliance Group, Individual Appliance, Custom
- Views for all Appliances, Firmwarespecific, Model-specific, Custom

**Email Alerts for:**

- Subscription expired
- Change in Device connectivity status
- Device Virus threats
- Unhealthy traffic
- Surfing Pattern
- IPS attack
- Spam attack
- CPU usage
- Memory usage
- Disk usage

**CENTRALIZED LOGGING**

- Audit log
- System log

**CONFIGURATION MANAGEMENT**

- USB port 3G and Wimax Support\*
- Primary WAN link
- WAN Backup link

**CONFIGURATION SYNCHRONIZATION**

- Centralized upgrade for:
  - AV and IPS Signatures
  - Web filtering categories
- Automated and Manual Backup for Appliances
- Backup Repository of Appliances
- Restore Backup from CCC

**OFFLINE CONFIGURATION SYNCHRONIZATION**
**UPGRADE DISTRIBUTION**

- CR Firmware
- AntiVirus and IPS Signature
- Web Filtering Categories

**ADMINISTRATION**

- Role-based Administration
- Granular Administrative controls
- Predefined and Custom Administrator profiles
- Local Administrator Accounts
- Appliance and Appliance Group
- Administrator Accounts

**COMMUNICATION**

- SSL RC4 128bit Encryption
- Mutual Authentication
- HTTP, HTTPS

**SYSTEM MANAGEMENT**

- Web Based User Interface
- Command Line Interface Web2.0 Compliant UI

**COMPLIANCE**

- CE
- FCC

## **HORUS INFORMATICA**

Via Enzo Ferrari, 21/B  
20010 Arluno - Milano - Italy

**[www.horus.it](http://www.horus.it)**

## **UFFICIO CONTABILITA' & AMMINISTRAZIONE**

[contabilita@horus.it](mailto:contabilita@horus.it)  
Fax: 02 33510838

## **UFFICIO COMMERCIALE**

[commerciale@horus.it](mailto:commerciale@horus.it)  
Tel : 02 33510135  
Fax : 02 33510199

## **SUPPORTO TECNICO**

Pre vendita  
[presales@horus.it](mailto:presales@horus.it)  
Post vendita  
[support@horus.it](mailto:support@horus.it)

## **UFFICIO MARKETING**

[marcom@horus.it](mailto:marcom@horus.it)  
Fax: 02 33510838

## **HOTWIRE UFFICIO STAMPA**

Via Conservatorio 22, Milano

Alessia Bulani  
D: +39 02 7729 968  
M: +39 348 018 98 46  
[alessia.bulani@hotwirepr.com](mailto:alessia.bulani@hotwirepr.com)