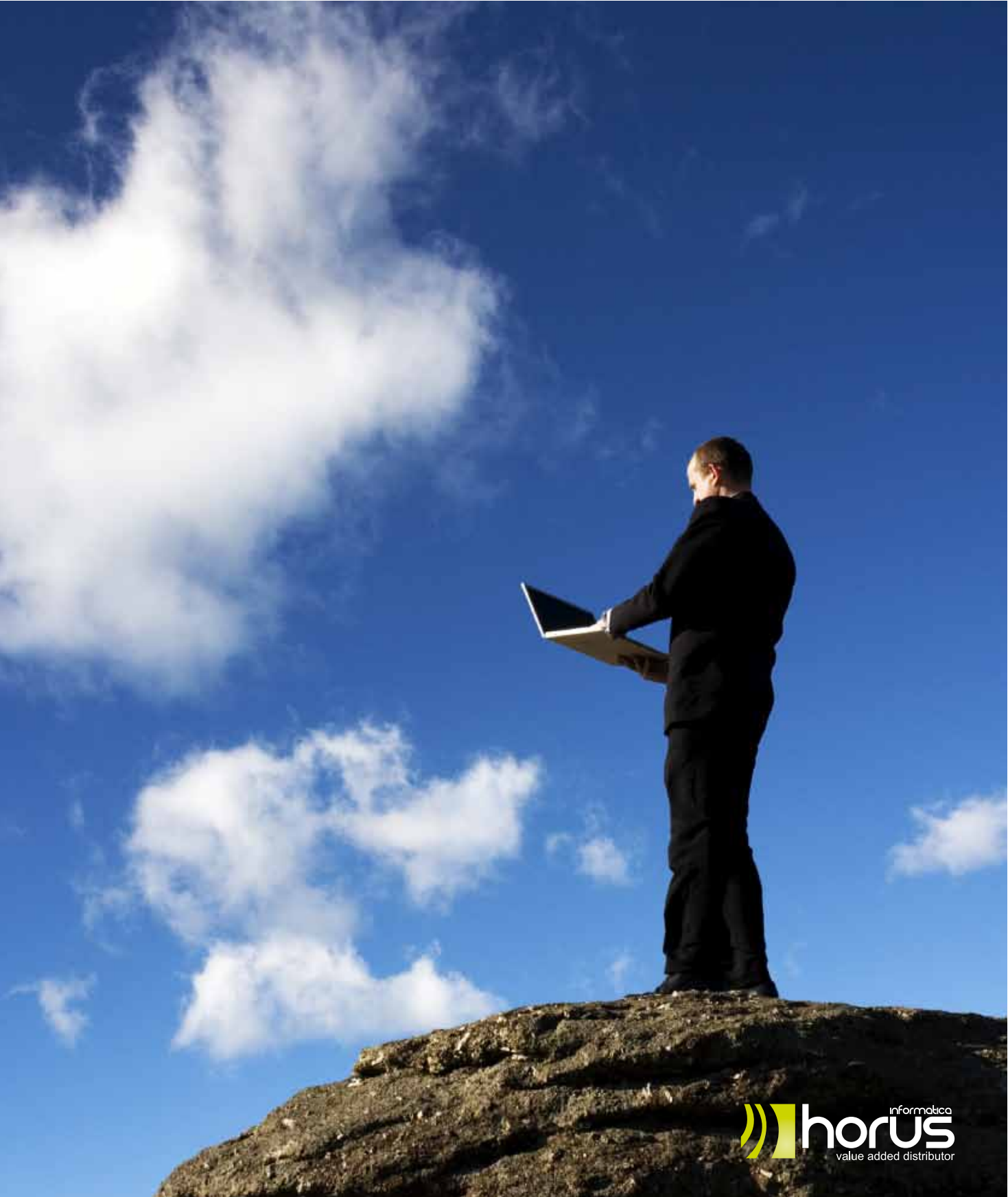


horus

 **horUS** informatica
value added distributor



DAL 1997 ABBIAMO ***LA TESTA TRA LE NUVOLE***

Innovazione è sempre stata la parola chiave alla base delle nostre scelte.

Abbiamo portato il cloud nelle aziende ben prima che divenisse un tema caldo del mercato e che operatori e vendor ne iniziassero a parlare.

E' dal 1997 che i nostri clienti possono godere di soluzioni tecnologicamente all'avanguardia che consentono a centinaia di utenti di gestire il proprio business in modo sicuro, efficace e professionale senza dover effettuare onerosi investimenti in risorse o competenze.

Le necessità del mercato

Indipendentemente dai contesti e dai settori industriali in cui si trovano a operare, oggi per le aziende la tecnologia informatica e Internet sono elementi abilitanti di importanza fondamentale per la buona gestione del business. Si tratta però di risorse da maneggiare con estrema cura perché al ruolo cruciale dell'hi-tech e del networking nelle attività di un'impresa moderna fa da contraltare la crescente complessità degli ambienti distribuiti.

Temi come quello della *mobility*, con la possibilità di accedere ai dati aziendali da postazioni remote e con strumenti portatili; e della *security*, ovvero la necessità di amministrare i flussi di dati in modo affidabile e protetto, assumono un peso sempre più rilevante.

Il successo nella scelta delle soluzioni da adottare, e di conseguenza la riuscita in un mercato quanto mai competitivo, è perciò spesso una questione di dettagli. Per curarli in maniera efficiente e, soprattutto, vincente, le aziende non hanno più bisogno di semplici fornitori di hardware e software, ma di partner in grado di seguirli passo dopo passo nella realizzazione di strategie in linea con le loro esigenze, con un'offerta composta sì di prodotti di qualità, ma soprattutto di consulenza a 360°.

L'Azienda

Sul mercato della distribuzione di *information technology dal 1997*, *Horus Informatica* si propone come il naturale alleato delle società italiane nella loro inarrestabile marcia verso l'innovazione.

Grazie a una rete di oltre 100 fra rivenditori, *system integrator e dealer* in grado di coprire l'intero territorio nazionale, Horus Informatica garantisce non soltanto la progettazione di applicazioni su misura scelte fra prodotti *best of breed*, ma segue anche i servizi di assistenza pre o post vendita e di formazione dei clienti, erogata sul posto da personale qualificato e certificato.

Il Supporto al cliente

Su tutte queste soluzioni Horus Informatica è in grado di intervenire presso i clienti direttamente o attraverso i suoi partner di canale assicurando un'accurata analisi delle infrastrutture prima della vendita e successivamente il design, la progettazione e l'implementazione dei prodotti.

A corredo di tutte queste operazioni, Horus Informatica si presenta in qualità di referente unico della clientela anche per quel che riguarda l'assistenza post-vendita e il training. E in virtù dello studio accurato delle reali necessità dei suoi interlocutori, può proporre architetture chiavi in mano personalizzate, che rispettano non soltanto le necessità tecnologiche delle aziende, ma anche i loro budget di spesa.



Horus Informatica scommette oggi principalmente su cinque brand di cui è distributore ufficiale a valore aggiunto per il mercato italiano.

Cyberoam, con le soluzioni:

Cyberoam Unified Threat Management, un pacchetto completo e flessibile per la gestione identity-based e la reportistica degli strumenti di sicurezza e anti-intrusione presenti sulle reti aziendali accessibili anche in mobilità;

Cyberoam End Point Data Protection, suite modulare che punta a massimizzare la sicurezza dei dati aziendali e i protocolli di gestione delle infrastrutture informatiche;

Cyberoam iView, soluzione open source per il logging e il reporting che aiuta le aziende a monitorare le reti attraverso dispositivi multipli in modo da garantire elevati livelli di sicurezza e riservatezza dei dati nella totale conformità alle normative vigenti.

PineApp, con le soluzioni:

PineApp Mail-Secure, una gamma di software per la protezione delle comunicazioni via e-mail le cui caratteristiche principali sono la scalabilità e l'affidabilità. Disponibile in tre differenti versioni in base alle diverse classi dimensionali delle aziende e distribuito sia grazie ad appliance hardware-software sia su classico Cd. Mail-SeCure è certificato per assicurare una ricognizione anti-spam superiore al 99%;

PineApp Archive-SeCure, compatibile anche con ambienti VMware, la serie delle appliance Archive-SeCure di PineApp rappresenta un tramite fra i server di storage locale, quelli di posta e i programmi client degli utenti. Nonostante sia largamente personalizzabile e scalabile è un esempio di soluzione all-in-one che non richiede il ricorso ad altri software o applicazioni provenienti da terzi;

PineApp Surf-Secure, le appliance della linea Surf-SeCure provvedono a un filtraggio in tempo reale del traffico Internet generato da protocolli http oppure dal transito sui server FTP in modo da garantire una protezione generalizzata dalle minacce in arrivo dal Web. E in più, garantiscono il rafforzamento delle difese e delle policy di sicurezza preesistenti. Disponibili nelle versioni 2000, 3000 o 5000.

Array Networks, con le soluzioni:

Array Networks Spx, una nuova famiglia di controller che garantiscono la sicurezza perimetrale delle informazioni sensibili per le aziende e la estendono via via a tutte le applicazioni client e ai singoli utenti;

Array Networks Apv, una gamma di controller tesi a migliorare l'efficienza, la sicurezza e la disponibilità delle applicazioni basate sul Web;

Array Networks Desktop Direct, applicazione enterprise di protezione dei dati critici che è oggi progettata per servire al meglio le esigenze degli utenti mobile ed è compatibile anche con dispositivi come iPad e iPhone di Apple.

NComputing, con le soluzioni:

vSpace, il cuore dell'offerta di NComputing è rappresentato dal software vSpace che permette alle imprese di ottimizzare le operazioni di abilitazione dei virtual desktop assicurando l'accesso simultaneo a un solo sistema operativo da parte di una molteplicità di utilizzatori;

Dispositivi di accesso, a basso costo e basso consumo, piccoli e duraturi, i dispositivi di accesso alla desktop virtualization della gamma NComputing si connettono da un lato alle periferiche degli utenti come il mouse, la tastiera o il monitor; dall'altra a un server centralizzato raggiungibile direttamente o via Ethernet che ospita ogni desktop virtuale e le applicazioni necessarie.

Disponibile nelle gamme L-Series, U-Series e X-Series.

24Online Billing & Bandwidth Management

Soluzione esaustiva per il controllo degli accessi, l'ottimizzazione e l'amministrazione della banda nelle infrastrutture di rete.

SKANDIA ridefinisce le policy di accesso e la sicurezza delle sue reti con Cyberoam e Horus Informatica

“Horus Informatica ha messo a disposizione uno staff molto preparato e professionale e il processo di integrazione e implementazione si è rivelato un’esperienza del tutto positiva... Credo si tratti di un partner superiore alla media del mercato per quel che concerne la sicurezza aziendale, l’hosting e l’housing delle infrastrutture web in azienda e le procedure di gestione tecnologica”.

Marino Cattabriga, System & Network Administrator, Skandia Vita

La CROCE ROSSA ITALIANA sceglie le soluzioni di Cyberoam per rendere più sicure le comunicazioni mobile dei suoi consulenti sul territorio

“Abbiamo scelto Cyberoam perché ha una gestione granulare dell’utenza ... Questo fa di Cyberoam una partner ideale per le nostre esigenze di connettività mobile basata su reti senza fili Wi-Fi. Il rapporto costi/benefici proposto dalle appliance di Cyberoam, confrontato con quello di altri vendor, è molto vantaggioso, ed elimina il rischio che i laptop dei consulenti diventino veicoli di diffusione di virus e malware eventualmente contratti sulle strutture di rete dei clienti con cui sono in contatto”

Giulio De Matteis, responsabile dei sistemi informativi, Comitato centrale della Croce Rossa Italiana

Horus Informatica mette al sicuro le attività di ESPRINET con le soluzioni di Array Networks

“Le soluzioni TMX e SPX o VPN di Array Networks implementate a quattro mani con Horus Informatica possiedono tutte le caratteristiche che Esprinet cercava e Horus Informatica ha garantito il massimo supporto nella realizzazione delle configurazioni più complesse... Anche il rapporto fra qualità e prezzo si è rivelato in linea con quanto avevamo sottoscritto prima di dare inizio all’intervento.”

Alessio Pellegatta, Network & Security team leader, Esprinet

LOQUENDO Spa garantisce accessi remoti sicuri al team commerciale grazie alle soluzioni di Array Networks distribuite da Horus Informatica

“Sicuramente l’installazione dei prodotti di Array Networks ci ha permesso di facilitare molto gli accessi da parte del gruppo commerciale alle nostre risorse intranet.

Ma credo che parte del merito vada anche a Horus Informatica, che si è rivelata un’organizzazione molto competente, propositiva e affidabile sia dal punto di vista tecnico sia per quel che riguarda il supporto, l’assistenza e la chiarezza della sua proposta commerciale”.

Antonio Cappellari, amministratore di rete, Loquendo

OCTO TELEMATICS semplifica la gestione delle sue Virtual Private Network grazie alle soluzioni di Cyberoam distribuite in Italia da Horus Informatica

“...il nostro personale ha ricevuto anche un’adeguata formazione, grazie alla preparazione di alto livello del team di Horus Informatica...il team tecnico di Horus si è dimostrato competente, preparato e adattabile alla nostra realtà aziendale”

Mario Pandolfi, Responsabile dei Sistemi informativi, Octo Telematics

IL MINISTERO DELLA GIUSTIZIA DEL MAROCCO rinnova le reti e consolida le difese anti-intrusione grazie a Mitre Networks e a Cyberoam, distribuito in Italia da Horus Informatica

Gli apparati UTM (Unified Threat Management) di Cyberoam distribuiti da Horus Informatica sono risultati vincenti perché riescono a coniugare un vasto ventaglio di funzionalità importanti con un costo di mercato decisamente competitivo rispetto alla concorrenza

Donato Ierardi, General Manager, Mitre Networks

Mondo (II), 29 ottobre 2010

La rete di Octo a prova di traffico

LA TECNOLOGIA CYBEROAM PER IL PROVIDER DI SERVIZI

Capital, 1 ottobre 2010

A chi serve il security manager

"...TRA I MARCHI MIGLIORI CI SONO CISCO (www.cisco.com) E CYBEROAM (www.cyberoam.com)..."

Pc Professionale, 1 ottobre 2010

Le appliance Cyberoam per l'Utm arrivano in Italia

Sole 24 Ore, 19 luglio 2010

Dall'ipad al pc fisso con Array Networks

Computerworld Italia, 1 luglio 2010

La scarsa sicurezza delle aziende italiane

Mondo (II), 16 aprile 2010

Rete sicura per i road warrior Esprinet

B2b24.ilsole24ore.com, 18 marzo 2010

Accesso remoto al desktop aziendale con iPhone

Mondo (II), 12 marzo 2010

E' più facile operare su desktop aziendale dall'iphone

Corriere Economia, 22 febbraio 2010

Croce Rossa Italiana sceglie Cyberoam

Mondo (II), 5 febbraio 2010

Croce Rossa Italiana sceglie Cyberoam

Pc World, 1 febbraio 2010

La protezione di desktop e portatili

Data Manager, 1 gennaio 2010

Cyberoam: tanti pericoli, un solo guardiano

Top Trade Informatica, 1 gennaio 2010

Horus-Cyberoam, il valore della sicurezza





HORUS E IL GREEN

Il rispetto dell'ambiente e per il risparmio energetico è sempre stato un elemento determinante nella scelta delle nostre soluzioni.

Attualmente adottare soluzioni green non è solo un impegno etico, ma una necessità per le aziende.

Tutte le soluzioni proposte da Horus Informatica permettono di ridurre notevolmente i consumi energetici e di ottimizzare le risorse aziendali ed i processi di lavoro con un risultato di maggiore efficienza e risparmio di costi.



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

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 Lic, 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, AI-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, antispam 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.

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

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*.

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 compatibilità con Windows 7

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.

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.

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.



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 si trovano ad affrontare le problematiche legate alla sicurezza delle loro infrastrutture lottando su 2 fronti. Da una parte le minacce esterne sono in continua evoluzione, dall'altra, e quasi in egual misura, è necessario adottare strumenti di protezione dai pericoli provenienti dall'interno della propria rete. Inoltre in un contesto in cui ogni azienda ha uffici dislocati in diverse sedi ed infrastrutture IT complesse composte da dispositivi di vario tipo sorge l'esigenza di una protezione globale che garantisca la visibilità completa di tutte le attività di rete sia delle sedi centrali che di quelle remote.

Cyberoam iView La soluzione per Logging & Reporting

LCyberoam iView è una soluzione per il logging e il reporting che aiuta le aziende a monitorare le loro reti attraverso dispositivi multipli in modo da 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 su tutti i dispositivi geograficamente dislocati. In questo modo le aziende sono in grado di applicare security policy o modificarle da una postazione centrale. L'interfaccia grafica di iView è molto semplice e fornisce diversi tipi di report in una singola pagina così da offrire costantemente la visuale su tutti i parametri della rete.

Cyberoam iView permette alle aziende di individuare l'anello debole del sistema grazie a report identity-based sui vari tipi di anomalie. Offre ad esempio la visuale degli attacchi principali, delle applicazioni maggiormente usate per gli attacchi, dei

principali destinatari di mail spam, dei virus più diffusi ed altro. In questo modo è possibile individuare velocemente i problemi e risolverli in conformità alle normative vigenti.

Informazioni legate all'identità come quelle sugli utenti che occupano maggiormente la banda per upload e download o sulle principali applicazioni usate aiutano le aziende a gestire le loro risorse ed a pianificare le necessità future oltre a migliorare i livelli di sicurezza.



Caratteristiche principali

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.

Log Management

Cyberoam iView raccoglie, filtra, normalizza, archivia e centralizza i log provenienti dall'infrastruttura in tutte le sue componenti su standard syslog rendendo disponibili funzionalità di ricerca e reporting evoluto riducendo in modo significativo il costo e la complessità delle attività di analisi.



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.



Security Management

Cyberoam iView offre una visuale completa dello stato di sicurezza dell'azienda attraverso una singola interfaccia. Le aziende possono individuare immediatamente attacchi di rete, la loro origine e la destinazione attraverso un rapido sguardo al pannello principale e possono subito intraprendere azioni sulla rete in qualsiasi luogo del mondo.

Compliance Reporting

Cyberoam iView fornisce report che rispondono alle normative vigenti. Grazie al facile accesso ai report ed alla verifica dei log si riducono notevolmente i costi per mantenere il sistema conforme alle normative. Gli amministratori sono subito informati di comportamenti che si scostano dalle pratiche di sicurezza con una conseguente riduzione dei tempi di risposta agli incidenti.

Analisi legali

Cyberoam iView, attraverso i suoi log ed i suoi report, aiuta le aziende a ricostruire la sequenza degli eventi che si sono verificati nel momento di una determinata violazione alla sicurezza. Consente alle aziende di estrarre lo storico degli eventi relativi alla rete, riducendo i costi necessari a indagare sull'accaduto e ridurre il downtime della rete.

Multiple Devices Support

Le appliance Cyberoam iView garantiscono logging e reporting intelligente su diversi dispositivi di rete compresi firewall UTM, Linux IP Tables/Net Filter firewall, Squid ed altri. Le aziende sono così dotate di report sui

log attraverso una singola GUI molto semplice da utilizzare.

Spazio Terabyte per lo Storage

Cyberoam iView offre Terabyte di spazio disponibile per le esigenze di archiviazione di tutta la reportistica.

Ridondanza dei dati

Le appliance Cyberoam iView utilizzano tecnologia RAID per garantire ridondanza ed elevati livelli di affidabilità di storage in modo da salvaguardare l'appliance anche in caso di guasto dell'hard disk.

SCHAEDE 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 area¹
- 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 area¹
- IP address Black list/White list
- Spam Notification through Digest²
- 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 VPN³
- 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^{*}
- 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 Discovery⁴
- 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 AVAILABILITY⁵

- 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 REPORTING⁶

- 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

¹1,2,3,4,5,6 Available in all the Models except CR15i

^{*}3G card and modem details are not included.

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

⁵ Not Available in Wireless Series"

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, 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	1000i	1500i
10/100 Ethernet Ports	-	-	-	-	-	-	-	-
10/100/1000 GBE Ports	6	6	6	6	10	14	10	10
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	-	-	-	-	-	-	2	2
USB Ports	2	2	2	2	2	2	2	2
Hardware Bypass Segments	1 [#]	1 [#]	1 [#]	1 [#]	2	2	2	2
Firewall Throughput (UDP) (Mbps)	1,000	1,250	2,200	2,600	5,000	6,000	6,500	7,500
Firewall Throughput (TCP) (Mbps)	750	1,000	1,500	1,800	3,000	4,500	3,500	6,000
New sessions/second	8,000	10,000	12,000	15,000	25,000	35,000	25,000	40,000
Concurrent sessions	220,000	400,000	450,000	500,000	700,000	900,000	750,000	1,000,000
3DES/AES throughput (Mbps)	60/90	80/100	150/180	180/200	325/400	500/750	400/500	600/750
Antivirus throughput (Mbps)	150	200	280	450	750	900	700	900
IPS throughput (Mbps)	200	300	750	850	1000	1,250	1,200	2500
UTM throughput (Mbps)	130	160	250	350	550	650	600	750
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	3.46 x 16.7 x 20.9	3.46 x 16.7 x 20.9
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	8.8 x 42.4 x 53.1	8.8 x 42.4 x 53.1
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	15.2 kg, 33.51 lbs	15.2 kg, 33.51 lbs
Input Voltage	100-240VAC	115-230VAC	115-230VAC	115-230VAC	100-240VAC	100-240VAC	90-264VAC	90-264VAC
Consumption	47.8W	90W	90W	62.7W	128W	185W	210W	210W
Total Heat Dissipation (BTU)	163	200	200	324	375	475	718	718
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

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

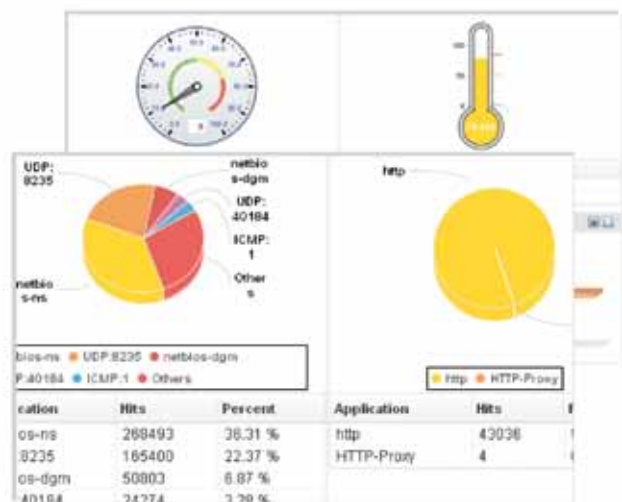
- Endpoint startup
- User logon & logoff
- Patch installation
- Dialup logs & IP Address/MAC Address information

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

SAMPLE SPECIFICATIONS



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 UTMs
- Proxy Firewalls
- Custom Applications
- Syslog-compatible devices



CYBEROAM IVIEW
Intelligent Logging & Reporting Solution

TECH SHEET

Hardware Specifications	CR-iVU25	CR-iVU100	CR-iVU200
Storage			
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
Performance			
Events per Second (EPS)	250	500	1000
Devices supported	25	100	200
Interfaces			
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
Dimensions			
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
Power			
Input Voltage	100-240 VAC	100-240 VAC	100-240 VAC
Consumption	65W	265W	265W
Total Heat Dissipation (BTU)	175	425	425
Environmental			
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%

HORUS INFORMATICA

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

www.horus.it

UFFICIO CONTABILITA' & AMMINISTRAZIONE

contabilita@horus.it
Fax: 02 33510838

UFFICIO COMMERCIALE

commerciale@horus.it
Tel : 02 33510135
Fax : 02 33510199

SUPPORTO TECNICO

Pre vendita
presales@horus.it
Post vendita
support@horus.it

UFFICIO MARKETING

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