The mobilization of workforce has led to demand for anytime-anywhere access to network resources. This, along with increasing number of users like customers and partners connecting to an enterprise network from outside, and trends like rise in number of network users and devices, application explosion, virtualization, and more are leading to loss of security controls for enterprises over their networks. Cyberoam Next-Generation Firewalls (NGFW) with Layer 8 Identity-based technology offer actionable intelligence and controls to enterprises that allow complete security controls over L2-L8 for their future-ready security. Cyberoam’s Human Layer 8 acts like a standard abstract layer that binds with real Layers 2-7, enabling organizations to regain lost security controls.

Cyberoam CR750iNG-XP offers inline application inspection and control, website filtering, HTTPS inspection, Intrusion Prevention System, VPN (IPSec and SSL) and granular bandwidth controls. Additional security features like WAF, Gateway Anti-Virus, Anti-Spam are also available. The FleXi Ports (XP) available in CR750iNG-XP appliances offer flexible network connectivity with I/O slots that allow additional Copper/Fiber 1G/10G ports on the same security appliance.

Layer 8 Identity over IPv6
- Secure Authentication – AD, LDAP, Radius
- Clientless Users
- Authentication using Captive Portal

Logging/Monitoring
- Real-time and historical Monitoring
- Log Viewer - IPS, Web filter, WAF, Anti-Virus, Anti-Spam
- Authentication, System and Admin Events
- Forensic Analysis with quick identification of network attacks and other anomalies
- Syslog support
- 4-eye Authentication

On-Appliance Cyberoam-View Reporting
- Integrated Web-based Reporting tool
- 1,200+ drilldown reports
- Compliance reports - HIPAA, GLBA, SOX, PCI, FISMA
- Zone based application reports
- Historical and trend reports
- Default Dashboards: Traffic and Security
- Username, Host, Email ID specific Monitoring Dashboard
- Reports – Application, Internet & Web Usage, Mail Usage, Attacks, Spam, Virus, Search Engine, User Threat Quotient (UTQ) for high risk users and more
- Client Types Report including BYOD Client Types
- Multi-format reports - tabular, graphical
- Export reports in - PDF, Excel, HTML
- Email notification of reports
- Report customization – (Custom view and custom logo)
- Supports 3rd party PSA Solution – ConnectWise

Virtual Private Network
- IPSec, L2TP, PPTP
- Encryption - 3DES, DES, AES, Twofish, Blowfish, Serpent
- Hash Algorithms - MDS, SHA-1
- Authentication - Pre-shared key, Digital certificates
- IPSec NAT Traversal
- Dead peer detection and FD’s support
- Offline Helman Gateway 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
- Threat Free Tunnelling (TFT) Technology

SSL VPN
- TCP & UDP Tunnelling
- Application Authentication – AD, LDAP, RADIUS, Cyberoam (Local)
- 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 Tunnelling 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, VTELNET, SSH

Web Filtering
- On-Cloud Web Categorization
- Controls based on URL, Keyword and File type
- Web Categories: Default (99), External URL Database, Custom
- Protocols supported: HTTP, HTTPS
- Block Malware, Phishing, Phารning URLs
- Block Java Applets, Cookies, Google Cache pages
- CIPA Compliant
- Data leakage control - block HTTP and HTTPS upload
- Schedule access control
- Safe Search enforcement, YouTube for Schools

Bandwidth Management
- Application, Web Category and Identity based
- Bandwidth Management
- Guaranteed & Burstable bandwidth policy
- Application & User Identity based Traffic Discovery
- Data Transfer Report for multiple Gateways

Web Application Firewall
- Post-recon Detection model
- Unique "Intuitive Website Flow Detector" technology
- Protection against SSL Injections, Cross-site Scripting (XSS), SQL Injections, Cross-site Request Forgery (CSRF)
- Thin Client support
- 2-factor authentication: 3rd party support
- SMS (Text-Based) Authentication

Additional purchase required. FlexiPorts are not HQT swappable. Appliance needs to be turned off prior to changing the FlexiPorts Module. If enabled, will bypass traffic only in case of power failure. “Antivirus, IPS and Firewalls” perforf efficiency tested using scripts and electronic load. Additional purchase Required. For list of compatible platforms, refer to OS Compatibility Matrix on Cyberoam DOCS.