CRYSTAL EYE SERIES 70

Red Piranha

Australia's first Extended Detection & Response (XDR) solution and the World's most powerful XDR platform

Our Series 70 XDR security appliance is high performance protection capable of supporting multiple internet connections of up to 40Gb/s each.

Crystal Eye 70 delivers powerful, flexible protection for large telecommunications or high performance data centre operations. Combined with our range of integrated services, these extreme performance devices are an easy to deploy, easy to manage, effective security solution.

Through Crystal Eye's powerful threat intelligence system, the platform processes over 19-million Indicators of Compromise (IoC) per day using real-time visibility & analytics to enable automated actionable intelligence.

Complete XDR Platform

- Integrated XDR capabilities
- Automated Actionable Intelligence
- Multi-layered security delivering defence in depth
- Built-In Compliance Feature Set
- Risk Assessment Reports
- Vulnerability Scanning

Full Network Control

- Network Security Monitoring
- Advanced deep-packet inspection and decryption
- Instant SOC & embedded SIEM solution
- On-demand PCAP forensic analysis and logging
- Gateway application whitelisting
- Extended log processing, retention & policy management controls

Firewall throughput:	40Gbps	The maximum capacity between two ports of the same bandwidth with no packet loss.
IDPS throughput:	9Gbps	The maximum volume of data that can be processed by the Intrusion Detection & Prevention modules with no packet loss.
True Security Throughput (TST):	4Gbps	The lab tested peak load with all security features turned on and processing a typical enterprise network profile: 76% http(s) web browsing, 12% real-time applications (VoIP, Video conferencing) and 12% other traffic types.

SPECIFICATIONS

Processing System
"Dual Intel XEON Gold 6526Y
16 cores, 32 threads, 37.5MB cache per processor.
Total 32 Cores, 64 Threads @ 2.8GHz/3.9GHz max."

Memory Capacity
128GB ECC DDR5

Networking capacity
• Onboard : Dual 10GbE UTP
Options (up to 6 of the following in any combination)
• Intel XL710QDA2 (Dual 40GbE QSFP)
• Intel XXV710 (Dual 25GbE SFP28)
• Intel X710-DA4 (Quad 10GbE SFP+)
• Intel X710-T4 (Quad 10GbE RJ45)
• Intel i350-T4 (Quad 1GbE RJ45)"

Interfaces
5 x USB 3.2 (Type A)

Stateful Inspection Firewall Features
• Multiple Security Zones
• Location-aware and Device-aware Identity-based Access
• Control Policy
• Security Policies – IPS, Web Filtering, Application Filtering,
   Anti-virus, Anti-spam and QoS
• Policy based Source and Destination NAT, Gateway
   Specific NAT Policy
• MAC & IP-MAC Filtering
• Spoof Prevention

Gateway Anti-Virus & Anti-Spyware Features
• SSL Mismatch Detection
• Cloaked URL Detection
• Virus, Worm, Trojan Detection and Removal
• Spyware, Malware, Phishing Protection
• Scans HTTP, HTTPS, FTP, SMTP/S, POP3, IMAP, IM, SMB, VPN Tunnels
• Customised Individual User Scanning
• Scan and deliver by file size
• Block by file types

Web Filtering Features
• More than 130 categories
• Auto category updates
• Exception list
• IP or hostname based
• Controls based on URL, Keyword and File type
• Protocols supported: HTTP, HTTPS
• Block malware, Phishing, Pharming URLs
• Block java Applets, Cookies, Active X, Google Cache pages
• Data leakage control by blocking HTTP and HTTPS upload
• Banned phrase list, YouTube for Schools
• Custom Denied Message per Web Category

SD WAN Support
• IPSEC VPN for site to site communications
• Authentication – Active Directory, LDAP, RADIUS,
• Multi-layered Client Authentication - Certificate, Username/Password
• Lightweight SSL VPN Tunnelling Client
• TCP based Application Access – HTTP, HTTPS, RDP, TELNET, SSH
   Wireguard SSL VPN

AI and Automated Actionable Intelligence
• AI rule matching to detect anomalies in network traffic
• Automatic defence rules from over 19 million IOC's processed daily
• Machine learning smart detection of network based SSH attacks

End Point Application Whitelisting (CEASR)
• Easy Device application mapping
• Ability to whitelist known good device Applications from the gateway
• Protect against Zero-day attacks
• Deal with encrypted malicious traffic with one click

Advanced Compliance Features
• Azure AD threat analysis
• Vulnerability Scanning
• DLP Alerting and Blocking

Intrusion Prevention System Features
• 5 managed rule sets, comprising of 30k+ rules updated daily from
   the latest threats
• HTTP/TLS/DNS Logging
• Actions – Drop, Block, Reject, Pass
• Auto IPS Updates from Red Piranha threat intelligence sharing platform
• Protocol Anomaly Protection
• SCADA Aware
• VoIP and SIP protocol reporting
• Easy tuning in dashboards to reduce false positives

Application Filtering Features
• Layer 7 (Application) & Layer 8 (User) Control and Visibility
• Inbuilt Application Category Database
• Visibility and Controls for HTTPS based micro-apps like
   Facebook chat, YouTube video upload

SD WAN Features
• TCP & UDP Tunnelling
• Authentication – Active Directory, LDAP, RADIUS, Local
• Multi-layered Client Authentication - Certificate, Username/Password
• Lightweight SSL VPN Tunnelling Client
• TCP based Application Access – HTTP, HTTPS, RDP, TELNET, SSH

Bandwidth Management Features
• QoS Policies
• Guaranteed & Burstable bandwidth policy
• Application & User Identity based Traffic Discovery
• Data Transfer Report for multiple Gateways

Networking Features
• Automated Fallover/Failback
• Interface types: Alias, Multisport Bridge, LAG (port trunking),
   VLAN, WWAN, TAP
• Multiple DHCP Servers support
• Supports HTTP proxy, Parent proxy with FQDN
• Dynamic Routing: RIP v1&v2, OSPF, BGP
• IPv6 Support: Dual Stack Architecture: Support for IPv4 and IPv6 Protocols
• IPv6 Route: Static and Source

Administration & System Management Features
• Web-based configuration wizard
• Role-based Access control
• Firmware Upgrades via Web UI
• Web 2.0 compliant UI (HTTPS)

User Authentication Features
• Internal Database
• Microsoft Active directory connector
• Internal active directory server

Storage System/Optional Extended Storage (max)
Dual 1TB System Drive
Up to 4 x 2.5 inch hot swap SSD (max 32TB)

Dimensions
19 Inch 2RU x 450mm deep

General Details
1 x VGA port, NVMe M.2 Main Storage GEN4
5TB/sec transfer, 6Gb/s SATA 3 extended storage subsystem
Voltage spike protection
802.3az (Energy Efficient Ethernet) support
Certifications: FCC, CE

Power
Input Voltage 110 VAC/220-240 VAC
800W 1+1 Redundant Power

AUTOMATED **PROTECTION** ▶ AUTOMATED **DETECTION** ▶ AUTOMATED **RESPONSE**

Red Piranha