CRYSTAL EYE SERIES 20

Red Piranha

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

Our Series 20 XDR security appliance is the ideal solution to defend your small business or branch-office from cyber threats supporting multiple internet connections of up to 250Mb/s each with the full range of features enabled and actively protecting your network.

Crystal Eye 20 delivers powerful, flexible protection for up to 50 users across multiple devices and network segments. Combined with our range of integrated services, our desktop 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:	2Gbps	The maximum capacity between two ports of the same bandwidth with no packet loss.
IDPS throughput:	800Mbps	The maximum volume of data that can be processed by the Intrusion Detection & Prevention modules with no packet loss.
True Security Throughput (TST):	250Mbps	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.

Processing System

- Intel Generation 11 i-3-10100
  (4 cores, 8 threads, 3.8GHz)
- Chipset Z690, Socket 1200

Memory Capacity

RAM: 32GB DDR4 2666MHz

Networking capacity

- 1 x Intel Gb WAN1 port
- 1 x RTL8125 2.5GB WAN2 port
- 4 x Intel Gb LAN port
- Wireless 802.11ax

Interfaces

6x USB 3.1
2x USB 2.0

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

Gateway Anti-Spam Features

- Inbound and Outbound Scanning
- Real-time Blacklist (RBL), MIME header check
- Filter based on message header, size, sender, recipient
- Subject line tagging
- IP address Black list/White list
- IP reputation-based Spam filtering

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

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

- 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

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)

1 x 240GB M.2 NVMe

Dimensions

W x D x H	280mm(w) 300mm(d) 80mm(h)
Weight	5Kg

General Details

1 x HDMI port, x2 USB 2.0, x5 USB 3.1 type A Gen 2 10Gbs
x1 USB 3.1 type C Gen 2 10Gbs
6Gb/s SATA 3 storage subsystem
Voltage spike protection
802.3az (Energy Efficient Ethernet) support
Certifications: FCC, CE

Other add-on options

Wireless Module for WIFI Application

Power

Input Voltage	110 VAC/220-240 VAC

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