CRYSTAL EYE SERIES 30





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

Our Series 30 XDR security appliance is the ideal solution to defend your small business or branch-office from cyber threats supporting multiple internet connections up to 1Gb/s each with the full range of features enabled and actively protecting your network.

Crystal Eye 30 delivers powerful, flexible protection and combined with our range of integrated services, our rackmount 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.

Full Network Control

Complete XDR Platform

8	Integrated XDR capabilities	4	Network Security Monitoring
C	Automated Actionable Intelligence		Advanced deep-packet inspection and decryption
	Multi-layered security delivering defence in depth		Instant SOC & embedded SIEM solution
17 ⁴	Built-In Compliance Feature Set		On-demand PCAP forensic analysis and logging
1	Risk Assessment Reports		Gateway application whitelisting
	Vulnerability Scanning	ęęą	Extended log processing, retention & policy management controls

Firewall throughput:	4Gbps	The maximum capacity between two ports of the same bandwidth with no packet loss.
IDPS throughput:	1.4Gbps	The maximum volume of data that can be processed by the Intrusion Detection & Prevention modules with no packet loss.
True Security Throughput (TST):	880Mbps	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	Intrusion Prevention System Features			
- Intel Generation 10 i-5-10400 (6 cores, 12 threads, 2.9GHz) - Chipset Z490, Socket 1200	 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 			
Memory Capacity RAM: 32GB DDR4 2666MHz	Actions – Drop, Block, Reject, Pass Auto IPS Updates from Red Piranha threat intelligence sharing platfor Protocol Anomaly Protection SCADA Aware VoIP and SIP protocol reporting			
Networking capacity	Easy tuning in dashboards to reduce false positives			
• 2 x Intel Gb WAN port • 4 x Intel Gb LAN port	Application Filtering Features			
Interfaces 6x USB 3.1	 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 			
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	SD WAN Features • TCP & UDP Tunnelling • Authentication – Active Directory, LDAP, RADIUS, Local • Multi-layered Client Authentication – Certificate, Username/Passwor • Lightweight SSL VPN Tunnelling Client • TCP based Application Access – HTTP, HTTPS, RDP, TELNET, SSH			
 Policy based Source and Destination NAT. Gateway Specific NAT Policy MAC & IP-MAC Filtering Spoof Prevention 	Bandwidth Management Features • QoS Policies • Guaranteed & Burstable bandwidth policy • Application & User Identity based Traffic Discovery			
Gateway Anti-Virus & Anti-Spyware Features	• Data Transfer Report for multiple Gateways			
 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 	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 Protocol			
Gateway Anti-Spam Features	· IPv6 Route: Static and Source			
 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 	Administration & System Management Features • Web-based configuration wizard • Role-based Access control • Firmware Upgrades via Web UI • Web 2.0 compliant UI (HTTPS)			
Web Filtering Features	User Authentication Features			
• More than 130 categories • Auto category updates • Exception list • IP or hostname based	 Internal Database Microsoft Active directory connector Internal active directory server 			
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	Storage System/Optional Extended Storage (max) 500GB NVMe/4TB SSD			
 Data leakage control by blocking HTTP and HTTPS upload Banned phrase list, YouTube for Schools Custom Denied Message per Web Category 	DimensionsW x Dx H485mm(w) 505mm(d) 44 mm(h)WeightTBA			
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	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 NVMe M.2 SSD 6Gb/s SATA 3 extended storage subsystem Voltage spike protection 802.3az (Energy Efficient Ethernet) support			
Al and Automated Actionable Intelligence	Certifications: FCC, CE			
 Al 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 	Power Input Voltage 110 VAC/220-240 VAC			
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 	AUTOMATED AUTOMATED AUTOMATE RESPONS			
LIGHT WITH OPERATING MELICIOUS TRATTIC WITH OPA Click				

