CRYSTAL EYE SERIES 50

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

Our Generation 15 Series 50 XDR security appliance is the ideal solution to defend against cyber threats supporting multiple internet connections of up to 10Gb/s each.

Crystal Eye 50 delivers powerful, flexible protection for enterprise environments across multiple devices. Combined with our range of integrated services, our high performance rack mount 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:	34Gbps	The maximum capacity between two ports of the same bandwidth with no packet loss.
IDPS/TDIR throughput:	4.8Gbps	The maximum volume of data that can be processed by the Intrusion Detection & Prevention modules with no packet loss.
True Security Throughput (TST/ SWG):	2.5Gbps	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

Intel Core Ultra 265K, 20 Cores, 5.5GHZ W880 Chipset, Socket LGA1851

Memory Capacity

64GB DDR5 UDIMM - 4800 MT/S

Networking capacity

1 x Realtek GE RJ45 (management port)
2 x Intel 2.5 GE RJ45
4 x Intel GE RJ45
4 x Intel 10 GE RJ45

Interfaces

4 x USB 2.0 (Type A)
2 x USB 3.2 (Type A)
2 x USB 3.2 (Type C)

Secure Web Gateway

- Web traffic inspection and control
- URL filtering enforcement
- SSL/TLS inspection capabilities
- Content inspection and filtering
- DNS-based enforcement via Protective DNS integration
- Application-aware web traffic control

Stateful Inspection Firewall Features

- Stateful packet inspection on layer 3 and 7
- Multi-zone segmentation and policy enforcement
- Hybrid / borderless firewalling for on premise and cloud deployments
- Bridge interface support for an inline deployment without network redesign
- NAT / PAT support
- DNS-layer policy enforcement
- DDoS detection and protection using behavioural traffic analysis
- Enhanced flexible deployment modes
- SNMP Manager integration for network visibility

Gateway Anti-Virus & Anti-Spyware Features

- Signature-based malware detection - Detect all known CNC and malware families
- Behaviour-based detection
- Anti-spyware protection integrates with IDPS detection engines
- Cross-layer detection support via network and endpoint telemetry

Web Filtering Features

- Category-based filtering
- Policy-driven content control
- User-level filtering enforcement
- Enhanced reporting and visibility
- Application-layer protection using a Web Application Firewall (WAF) to mitigate web threats

SD WAN Support

- Post-Quantum Resistant VPN encryption
- WireGuard VPN support
- SSL VPN
- IPSec VPN including site to site encryption
- Authentication: Active Directory, LDAP, RADIUS
- Multi-layered authentication: Certificate, Username/Password, MFA
- Lightweight SSL VPN client
- TCP-based application access (HTTP, HTTPS, RDP, SSH, Telnet)

AI and Automated Actionable Intelligence

- AI-driven anomaly detection across network traffic
- Machine learning-based threat detection models
- Automated defence rule generation using large IOC datasets
- Correlation of telemetry across network, endpoint and DNS layers
- Detection of non-signature-based threats and hidden attack patterns
- Network Detection and Response combined with human machine teaming
- Enhanced multi-tenant AI detection architecture

EndPoint Application Whitelisting (CEASR)

- Endpoint application visibility and mapping
- Application whitelisting and execution control
- Protection against zero-day attacks
- Hash-based blocking
- Publisher-based application control

Advanced Compliance Features

- Policy enforcement and compliance monitoring including
- M365 policy enforcement
- Audit logging and reporting
- Entra ID threat analysis
- Integrated vulnerability scanning including container host scanning
- Scheduled Packet capture
- Risk Auditing application for fast, accurate and compliant asset-type based risk assessment
- Data Loss Prevention (DLP) - Microsoft Entra ID and Network based with alerting and blocking
- Configuration Management Database Integration with Orchestrate - Asset management and vulnerabilities found linked to assets at hand
- Risk Register Integration with Orchestrate - Consolidated list of Risks identified, affected infrastructure assets, risk scores, likelihood and impact, Mitigation strategies.

Intrusion Prevention System Features

- Proprietary Intrusion Detection & Prevention System
- Multi-tenant IDPS architecture
- Signature-based detection with over 76,000+ rules, regularly updated
- Protocol inspection across 3,000+ protocols including OT/ICS protocols and support for custom detection rules
- All known Malware and CNC detection
- Lateral movement detection
- Pivoting attack detection
- Advanced Persistent Threat (APT) detection
- Suricata-based engine (proprietary enhanced implementation)
- HTTP/TLS/DNS Logging
- TLS decryption and Inspection and logging
- PECA Inspection

Application Filtering Features

- Layer 7 (application) and user-level visibility and control
- Application identification and categorisation
- Policy-based application control
- Micro-application visibility
- Web Application Firewall to protect your websites, APIs and web applications from attacks

SD WAN Features

- Passive Encryption Control Application (PECA) - data encryption at the network gateway using cryptographic algorithms, decryption occurs only by secure user authentication methods.
- Application-aware routing
- Dynamic path selection
- Load balancing across WAN links
- TCP & UDP tunnelling
- Encrypted traffic optimisation
- Secure remote connectivity across distributed environments

Bandwidth Management Features

- Guaranteed & Burstable bandwidth policy
- Application & User Identity based Traffic Discovery
- Data Transfer Report for multiple Gateways

Networking Features

- VLAN support
- Multi tenant independent IDPS enforcement
- Zone based authorised network segmentation
- Routing protocols
- NAT / PAT
- SNMP monitoring support to monitor network devices across your infrastructure - CPU Polling, threshold cross alerts, auto-config settings changes across devices
- Protective DNS Server
- Bridge Interface deployment support

Administration & System Management Features

- Web-based configuration interface
- Out of band management access management
- Role-based access control (RBAC)
- Firmware upgrades via web UI
- Secure HTTPS management interface
- System monitoring and logging
- SNMP Manager integration
- Enhanced DNS reporting and analytics
- CMDB (Configuration Management Database) capabilities available in Orchestrate:
  - Network interface data ingestion
  - Device-to-customer mapping
  - Improved asset naming and matching
- Risk Register in Orchestrate:
  - Risk creation from categories
  - Unified risk visibility
  - Flexible risk tracking fields
  - Defined mitigation ownership
- Platform training system for user enablement in Orchestrate

User Authentication Features

- Enhanced Microsoft 365 identity visibility
- Declarative Authorisation Service - enforce security policies across APIs, microservices, AI workloads and multi-cloud environments
- Forcefield user authentication protection with actionable intelligence
- Internal user database
- Microsoft Active Directory integration
- Internal directory services
- LDAP and RADIUS authentication support
- Identity-based access enforcement

Storage System/Optional Extended Storage (max)

System : 1 x 1TB M.2 NVMe
Extended : up to 16TB combined SSD

Dimensions

2U Rack Form Factor 485mm(w) 593.2mm(d) 88.6mm(h)

General Details

Enterprise-class security appliance featuring multi-gigabit networking, expandable storage, dedicated management capabilities, and advanced threat inspection for high-throughput environments.

Power

Input Voltage 110 VAC/220-240 VAC

AUTOMATED PROTECTION ▶ AUTOMATED DETECTION ▶ AUTOMATED RESPONSE