Red Piranha
unified threat management

CRYSTAL EYE

TOTAL SECURITY PLATFORM

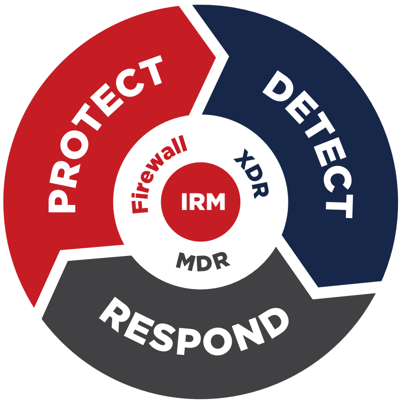
Red Piranha

CRYSTAL EYE

TOTAL SECURITY PLATFORM

The threat landscape is continually evolving with increased complexity, so security defences must continually innovate to protect your organisation effectively.

Crystal Eye is a comprehensive Extended Detection & Response (XDR) platform with fully integrated Managed Detection & Response (MDR), Firewall and Integrated Risk Management (IRM) to secure your organisation from the cloud to the end-point.



Comprehensive Security

Crystal Eye delivers a complete security solution in a single platform, eliminating the need for separate products from multiple vendors.

Simple Deployment and Management

With all your security technologies on the one platform, deployment is streamlined, and our simplified managed services let you get on with business.

High Performance

Running the latest 10th Gen Intel processors and latest hardware makes us the highest-performing Next-Generation Firewall appliances available on the market.*

Cost-Effective Solution

A unified platform that delivers a complete cybersecurity program with a lower total cost of ownership to suit your budget.

Predictive Protection

Our predictive and automated approach to security with Automated Threat Intelligence provides increased threat prevention.

* See our True Security Throughput (TST) scores

Crystal Eye is a unified cybersecurity platform that delivers a full range of comprehensive security capabilities.

Red Piranha
unified threat management

Red Piranha is helping protect the world from cybersecurity threats by making enterprise-grade security available for every business, large and small.

Information Security Management System
ISO 27001
Certified

Certificate No. 781489
Crystal Eye Security Operations

AustCyber
Australian Cyber Security Growth Network

AUSTRALIAN MADE AND OWNED

CRYSTAL EYE TOTAL SECURITY PLATFORM

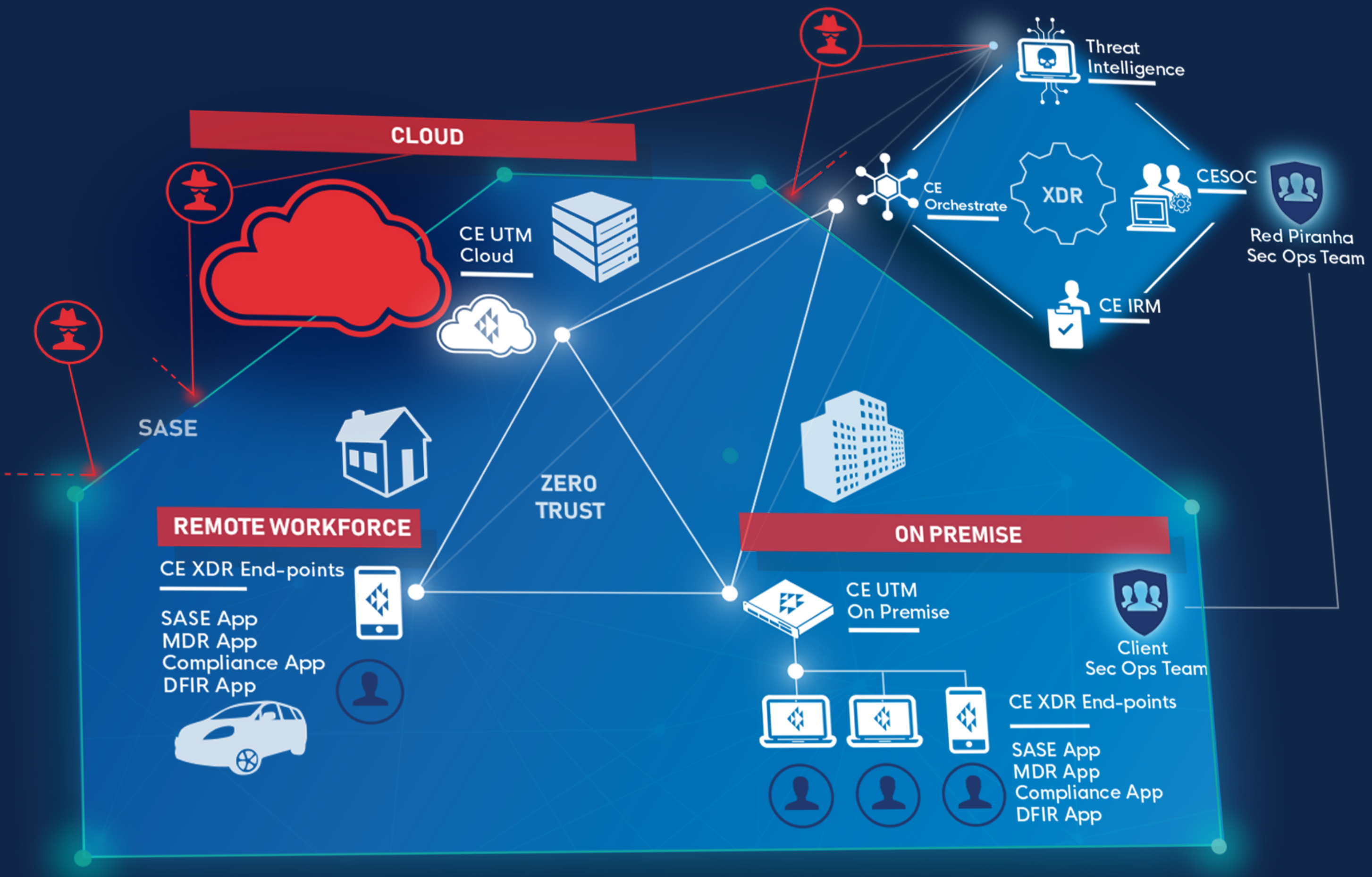
Problem

Security incidents are becoming more complex and more commonplace. Most organisations struggle to implement an effective security program and often don't know where to start. Running a complete program currently requires a mix from multiple products with significant integration effort. This leaves most organisations needing to compromise on their security or being left with poorly-configured systems that aren't providing effective protection.

Solution

A more progressive approach to security is required to overcome these issues with a simple, unified platform that can effectively protect, detect and respond to threats across your whole organisation. This requires a single platform from a trusted vendor who can deliver a suite of security products that can be used across the entire business including firewalls, vulnerability management, incident response and integrated risk management.

CRYSTAL EYE ARCHITECTURE



CRYSTAL EYE TOTAL SECURITY PLATFORM

XDR – Extended Detection & Response

XDR is an integrated security protection, incident detection and response platform. It involves the collection and correlation of event data from multiple security technologies that automatically trigger a coordinated response to secure the network. This all-in-one platform is pre-configured to be ready to go out-of-the-box, so it delivers a consistent level of security across your whole environment without the complexity of integrating products from multiple vendors. The key areas of an XDR solution are:

1. Automated security protection
2. Centralised data collection and correlation
3. Coordinated and automated incident response

Crystal Eye XDR pulls together end-point, network and cloud data from across the entire Crystal Eye platform to identify real threats in your environment and enable rapid response to minimise the impact to your business. Our network- and cloud-based sensors (via the Crystal Eye Firewall) and host-based sensors (via our XDR End-points) feed data back to our Crystal Eye Orchestrate centralised management console. Orchestrate acts as a data lake to collect all the data for correlation and response coordination. This is a significantly simpler process due to the standard data format used across the Crystal Eye suite of products, which avoids the laborious task of normalising and correlating data from different sources. More than just Security Information & Event Management (SIEM), XDR avoids complex integration and has the added benefit of pro-active and automatic rapid response to stop threats in their tracks before real damage occurs. XDR also goes a step further to provide advanced threat detection with research analysis labs to support the defensive efforts.

Our integrated XDR solution also implements the Security Orchestration, Automation & Response (SOAR) framework which allows you to automate responses to low-risk threats so high-risk threats can be prioritised and actioned. These capabilities are typically not accessible or affordable for small to medium businesses, but our integrated SOAR approach provides a comprehensive, cost effective response solution available to businesses of every size. Our automated incident response process is being executed immediately when a breach occurs and is significantly cheaper than alternatives.

MDR – Managed Detection & Response

We offer a fully integrated Managed Detection & Response service to complement the XDR capabilities of the Crystal Eye platform, so our certified security analysts in our 24/7 SOC are available to investigate and resolve security incidents in real-time across your network and help coordinate rapid response activities.

CESOC - Crystal Eye Security Operations Centre

CESOC is a combination of technologies and services that deliver the benefits of a full Security Operations Centre (SOC) with a suite of operational capabilities such as escalation and response, vulnerability management and Automated Actionable Intelligence all in one integrated platform, without you needing to build a SOC yourself. Building a SOC is a major undertaking for any organisation and is out-of-reach for most businesses. By implementing CESOC, a more comprehensive solution can be achieved at a fraction of the cost of building an internal team of security analysts with 24/7 coverage.

Unlike other managed security services, CESOC is flexible and can be delivered across the spectrum from a fully-managed to an internally-managed scenario, based on the capabilities of your own security team and your required level of assurance. Most companies have some level of IT security capability, but often don't have the required level of maturity (across people, process and technology) to operate their own SOC. That's why a tailored solution across all security areas can deliver the right fit for your organisation.

CRYSTAL EYE TOTAL SECURITY PLATFORM

CESOC leverages our XDR and MDR capabilities by bringing together a suite of automated detection and response capabilities not possible until now without significant manual effort by a team of security analysts. Our CESOC solution can complement your existing SOC team to expand their capabilities as well as extend the operating hours of your security monitoring and management. To operate effectively, a traditional SOC needs to integrate the available security controls, such as a firewall, into a separate vulnerability management system and a separate Integrated Risk Management (IRM) system. This has typically been a manual process for security analysts, but is now all automated through the integrated CESOC platform. There are so many disciplines with cybersecurity which require multiple roles within a SOC team that it's hard for business to provide that level of depth. Partnering with Red Piranha's managed services can give you the missing skills. Coupled with the rest of the CE platform, you get a full-featured holistic security program with a full-featured SOC.

IRM – Integrated Risk Management

The Crystal Eye Integrated Risk Management solution provides an automated and integrated approach to meeting your compliance obligations. It pulls together relevant compliance information and controls from multiple points across your network into a central dashboard that allows you to manage and report on that information to ensure you're compliant to a range of standards and provides a snapshot of your compliance posture at a point in time. The key compliance areas it addresses include:

- Security Policy Management
- Awareness & Education
- Identity & Access Management
- Vulnerability Management
- Security Monitoring
- Incident Response
- BCM / DR

The compliance journey can be a pain-staking process that requires a log of investment in time and resources. Our IRM module automates the majority of the work required to achieve and maintain compliance, thereby significantly reducing the cost for your business to gain a competitive edge in the market.

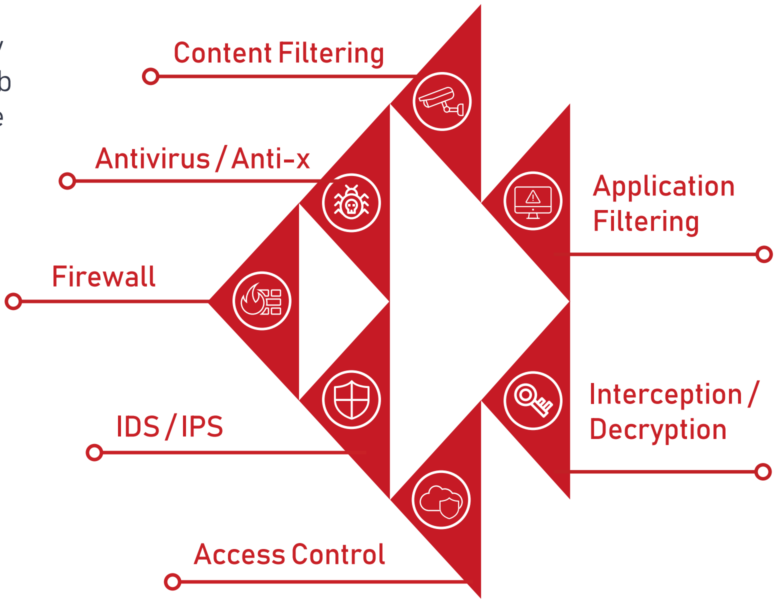
Crystal Eye IRM can also be integrated into our eCISO (electronic Chief Information Security Officer) product and vCISO (virtual Chief Information Security Officer) service to deliver a comprehensive approach to Integrated Risk Management for your organisation.

Crystal Eye Firewall

Crystal Eye FW offers a range of integrated security controls such as Firewall, IPS, antivirus, secure web gateway and access control in the following flexible deployments:

- Cloud platforms – IaaS (AWS, Azure, TPG)
- Cloud-native – FWaaS
- Cloud-managed
- On-premise appliances

No matter which deployment or appliance you choose, all customers get access to the same full-featured Crystal Eye platform.



Crystal Eye SASE Firewall

We live in a world where systems, applications and data all reside natively in the cloud. Crystal Eye SASE Firewall takes a cloud-first approach by providing comprehensive protection across your entire cloud footprint. Our advanced threat protection capabilities offer full coverage across your cloud attack surface with multiple points of presence and allow you to build private networks over the public Internet with a zero-trust policy to give you the assurance you need to do business in the cloud. SASE Firewall is available in the following deployments:

- Cloud platforms – IaaS (AWS, Azure, TPG)
- Cloud-native – FWaaS
- Cloud-managed

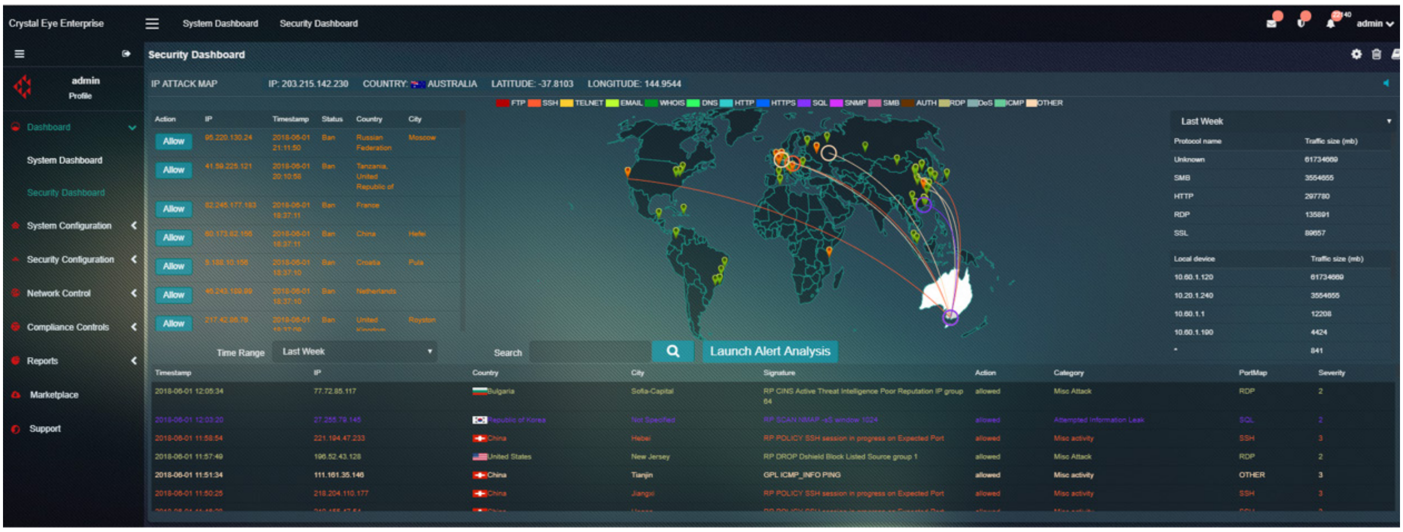
Crystal Eye On-Premise Firewall

Crystal Eye On-Premise FW is our hardware appliance that is deployed on-site and forms an essential foundation of our Total Security Platform with the same capabilities as Crystal Eye SASE Firewall for your corporate network and branch locations. It features a next-generation firewall with a suite of integrated security controls to protect you against the latest threats.

Advanced Protection

Crystal Eye provides integrated IPS, secure web gateway, anti-phishing, heuristic rules and Machine Learning capabilities, while our Automated Actionable Intelligence feeds into our professionally managed rulesets to help deliver advanced threat protection capabilities.

Our IPS engine has more than 43,000 rules which are managed and curated by our advanced SOC team to deliver some of the highest visibility in the industry. Combined with our superior hardware performance and backed by our extensive Automated Actionable Intelligence network, we can deliver increased visibility and better protection.



IP ATTACK MAP IP: 203.215.142.230 COUNTRY: AUSTRALIA LATITUDE: -37.8103 LONGITUDE: 144.9544

Action	IP	Timestamp	Status	Country	City
Allow	95.220.130.24	2018-06-01 21:11:50	Ban	Russian Federation	Moscow
Allow	41.59.225.121	2018-06-01 20:10:58	Ban	Tanzania, United Republic of	
Allow	82.246.177.183	2018-06-01 18:37:11	Ban	France	
Allow	60.173.82.156	2018-06-01 18:37:11	Ban	China	Hefei
Allow	5.188.10.156	2018-06-01 18:37:10	Ban	Croatia	Pula
Allow	46.243.189.99	2018-06-01 18:37:10	Ban	Netherlands	
Allow	217.42.86.78	2018-06-01 18:37:09	Ban	United Kingdom	Royston

Last Week

Protocol name	Traffic size (mb)
Unknown	61734669
SMB	3554655
HTTP	297780
RDP	135891
SSL	89657

Local device	Traffic size (mb)
10.60.1.120	61734669
10.20.1.240	3554655
10.60.1.1	12208
10.60.1.190	4424
*	841

Time Range: Last Week
Search

Timestamp	IP	Country	City	Signature	Action	Category	PortMap	Severity
2018-06-01 12:05:34	77.72.85.117	Bulgaria	Sofia-Capital	RP CINS Active Threat Intelligence Poor Reputation IP group 64	allowed	Misc Attack	RDP	2
2018-06-01 12:03:20	27.255.79.145	Republic of Korea	Not Specified	RP SCAN NMAP -sS window 1024	allowed	Attempted Information Leak	SQL	2
2018-06-01 11:58:54	221.194.47.233	China	Hebei	RP POLICY SSH session in progress on Expected Port	allowed	Misc activity	SSH	3
2018-06-01 11:57:49	196.52.43.128	United States	New Jersey	RP DROP Dshield Block Listed Source group 1	allowed	Misc Attack	RDP	2
2018-06-01 11:51:34	111.161.35.146	China	Tianjin	GPL ICMP_INFO PING	allowed	Misc activity	OTHER	3
2018-06-01 11:50:25	218.204.110.177	China	Jiangxi	RP POLICY SSH session in progress on Expected Port	allowed	Misc activity	SSH	3

High Performance

The Crystal Eye On-Premise Firewall appliance is the World's fastest security appliance, successfully achieving 60Gbps IDPS throughput in the lab on a single 2U device and verified by IEEE test results. Our ability to process Gigabit traffic puts us ahead of the pack and importantly enables us to process encrypted traffic more effectively.

Our appliances are multi-core 10th Gen Intel systems that enable multi-threaded applications to use the underlying hardware for high security performance, even with all features enabled.

Our appliance hardware is made-to-order, which ensures that all customers get the latest hardware specifications instead of using yesterday's technology with standardised OEM hardware.

Out-of-the-box Protection

Even large organisations with a range of security products and a large security team often get it wrong because the products aren't configured properly and the staff don't know how to manage them effectively. Red Piranha's security capabilities are all integrated into a single platform and work straight out of the box to ensure you get the right protection from day one.

Integrated Vulnerability Management

Crystal Eye offers vulnerability tuning within the IPS engine to provide virtual patching against known vulnerabilities identified in your environment, which is further supported by multi-function deployment options such as the Web Application Firewall.

The minute you install Crystal Eye, it shows you the number of vulnerabilities that have been detected in your specific environment, then it shows you how many have exploits which was leaving you at risk and how many are now being protected by Crystal Eye.

The Vulnerability Management process:

1. New vulnerability announced
2. Identified on x hosts
3. Virtual patch applied at IPS (via eCISO solution)
4. Blocked x malware threats

The objective here is to focus on the small number of vulnerabilities, not just the large number of malware that exploit those vulnerabilities.

Security Controls

- **Encrypted traffic metadata detection** running on our multi-threaded, high-throughput engine delivers unrivalled network protection against both clear and encrypted threats.
- **Integrated functions** work together intelligently, such as the IPS dynamically creating a firewall rule when it detects multiple attacks from the same IP address, to automatically block that address to shut down the attack source and reduce the load on the IPS engine.
- **Zero Trust Network Access (ZTNA)** reduces the risk of a data breach via a comprehensive approach which includes identity verification, user access control and network segmentation.
- **Cloud Access Security Broker (CASB)** delivers network-based and cloud-based security policy enforcement between users and cloud services via hybrid network segmentation.

- **Identity & Access Management (IAM)** provides greater control of users on your network and forms a critical part of ZTNA and CASB protection. Crystal Eye offers a standalone Active Directory (AD) instance or can be integrated with an existing AD using LDAP or OAuth.
- **Agentless Application Whitelisting (AWL)** blocks unwanted apps at the gateway to prevent them running on devices within the network.
- **DNS.Insure** provides DNS sink-holing and managed DNS to deliver advanced DNS protection across the network and bringing DNS back under enterprise control, increasing network visibility and control.
- **ForceField** identifies authentication failures across the network and blocks the source IP addresses of the failed login attempts to prevent brute force attacks and unauthorised access to systems.
- **Zero-day Protection**is delivered via our IPS engine which supports both vulnerability-facing signatures and threat-facing signatures to provide a more comprehensive level of protection.
- **BYOD & IoT** devices are protected with application filtering and protocol filtering at the gateway and network segments. On-premise protection is critical to cater for the expansion of IoT & BYOD across the enterprise. Our extensive security configuration capabilities deliver contextualised data across multiple security features dealing with encrypted traffic, including application-layer controls to manage IoT and BYOD to provide total visibility of the threats on your network.
- **VoIP monitoring** allows you to take control of voice traffic and Machine Learning will generate alerts when anomalies are detected. As the popularity of VoIP systems increases, they are being subjected to different kinds of intrusions, some of which are specific to such systems and some of which follow a general pattern of attacks against IP infrastructure. This app will monitor all VoIP traffic on your system.
- **Deception** capabilities allow you to create traps within your infrastructure by tagging decoys to trick attackers within your network for detection and notifications from internal attack vectors.
- **Machine Learning (ML)** delivers a range of automated defence features using defined playbooks to get you secure and compliant with little or no human intervention.
- **User & Entity Behaviour Analytics (UEBA)** uses ML to define behaviour profiles across network authentication (Kerberos), server connections (SSH) and file management (SMB) then alert when anomalies are detected to prevent attack pivoting.
- **Threat Analysis & Threat Hunting** is achieved by integrating various detection methods across the Crystal Eye platform to allow your security team, or ours, to pro-actively search security breaches, as well as being able to automate the threat hunting process via the platform.
- **PCAP** provides full packet capture (PCAP) support which allows for greater control and easy analysis.
- **Security Plan Wizard** guides novice users through the configuration of the Crystal Eye platform to simplify the setup and configuration process and can be used in conjunction with the risk audit functionality.
- **Backup PC** allows single nodes to use the Crystal Eye appliance for a local backup solution to simplify the backup and restore process.

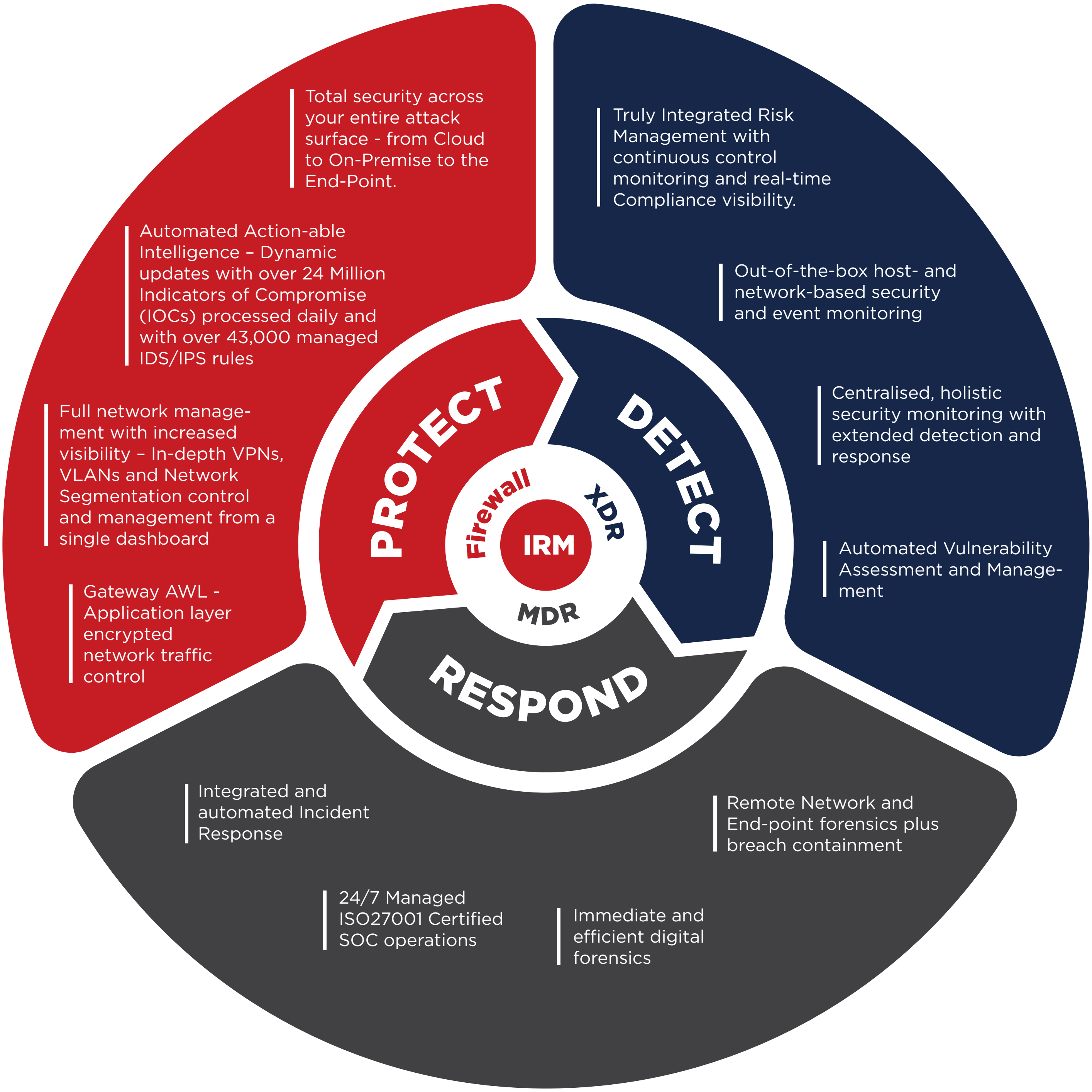
Compliance Controls

- **Integrated Risk Management** gives you better control of your risk profile in real-time, by providing visibility of your entire organisation from on-premise staff to your remote workforce.
- **Data Loss Prevention (DLP)** allows you to tag documents within your environment and track if they are being copied or removed from your network as well as VOIP monitoring to minimise the likelihood of data being exfiltrated out of your organisation.
- **Vulnerability Management** covers vulnerability scanning and reporting as well as pro-active protection measures such as virtual patching to provide zero-day protection and reduce the operational burden on IT staff.
- **Incident Response** services seamlessly integrate alerts into Red Piranha's managed services and professional services to provide rapid response to security incidents that occur across your network in real-time

CRYSTAL EYE TOTAL SECURITY PLATFORM

THE CRYSTAL EYE DIFFERENCE

Crystal Eye delivers a range of unique benefits across our entire platform. Traditional firewalls focus on security protection, while Crystal Eye's range of solutions offer automated protection, automated detection and automated response to security threats across your organisation:



Total security across your entire attack surface - from Cloud to On-Premise to the End-Point.

Automated Action-able Intelligence – Dynamic updates with over 24 Million Indicators of Compromise (IOCs) processed daily and with over 43,000 managed IDS/IPS rules

Full network management with increased visibility – In-depth VPNs, VLANs and Network Segmentation control and management from a single dashboard

Gateway AWL - Application layer encrypted network traffic control

Truly Integrated Risk Management with continuous control monitoring and real-time Compliance visibility.

Out-of-the-box host- and network-based security and event monitoring

Centralised, holistic security monitoring with extended detection and response

Automated Vulnerability Assessment and Management

Integrated and automated Incident Response

Remote Network and End-point forensics plus breach containment

24/7 Managed ISO27001 Certified SOC operations

Immediate and efficient digital forensics

CRYSTAL EYE INTEGRATED CAPABILITIES

The Crystal Eye firewall integrates into a range of other products to form the Crystal Eye Total Security Platform, including the following:

Crystal Eye Orchestrate

CE Orchestrate is the central management console that allows for monitoring and tuning of the Crystal Eye platform from a single interface for single and multi-tenanted scenarios at scale. Much more than just a dashboard – it's the central component in delivering Security Orchestration, Automation & Response (SOAR) across your environment which enables you to protect the confidentiality, integrity and availability of your data.

XDR

MDR

IRM

SOAR

SASE

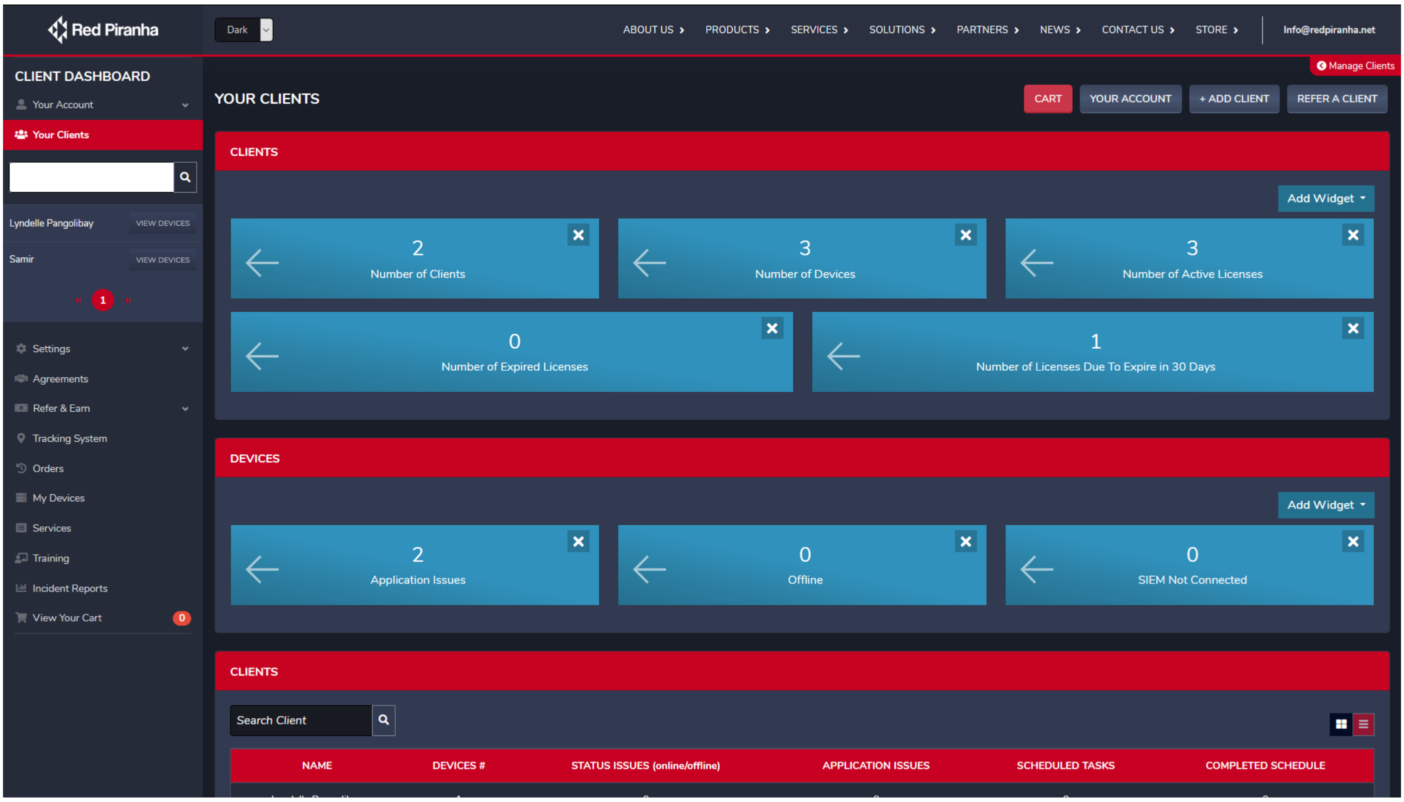
ZTNA

Vulnerability Management

Threat Intelligence

End-point Protection

The multi-tenanted capability also allows Managed Security Service Providers (MSSPs) to manage multiple clients from a single view to browse, filter and view clients by various metrics and track scheduled tasks. The dashboard also integrates into the IRM module to manage critical security and compliance reporting.



YOUR CLIENTS

CLIENTS

2 Number of Clients

3 Number of Devices

3 Number of Active Licenses

0 Number of Expired Licenses

1 Number of Licenses Due To Expire in 30 Days

DEVICES

2 Application Issues

0 Offline

0 SIEM Not Connected

CLIENTS

NAME	DEVICES #	STATUS ISSUES (online/offline)	APPLICATION ISSUES	SCHEDULED TASKS	COMPLETED SCHEDULE

CE Orchestrate provides a single view of all of your Crystal Eye devices and end-points with a holistic view of all your security events and alerts. You can drill into any alert or alarm to see more detailed alert analysis, alert escalation and reports for further investigation. You can also edit the rule action directly from the alert allowing for more granular tuning of the system.

SASE – Secure Access Service Edge

With more applications and data in the cloud and more staff working remotely, there is an increased need for simple and secure access for users in any location to access services in any environment. SASE is an architecture which aims to solve this problem by extending the bounds of the traditional security perimeter by deploying networking and security functionality at the business operational edge. It integrates multiple network security technologies such as SD-WAN, application-level access control and security policy enforcement. Crystal Eye integrates our network protection with our end-point apps to provide strong protection both on-premise and out to remote devices.

SASE is the convergence of network and security as a service into a single stack that allows organizations to secure users and devices accessing any service in any location. Bi-directional, single pass security inspection of traffic allows organisations to decrypt once and apply security controls such as advanced threat protection, DLP and application control to the connection.

Crystal Eye SASE can be deployed in localised regions to create local points of presence (POPs) to establish a SASE environment. Crystal Eye offers multiple options in Australia and globally to achieve this. Crystal Eye is cloud agnostic, supporting AWS, Azure and other cloud environments to give you flexibility.

Crystal Eye XDR End-points

SASE App

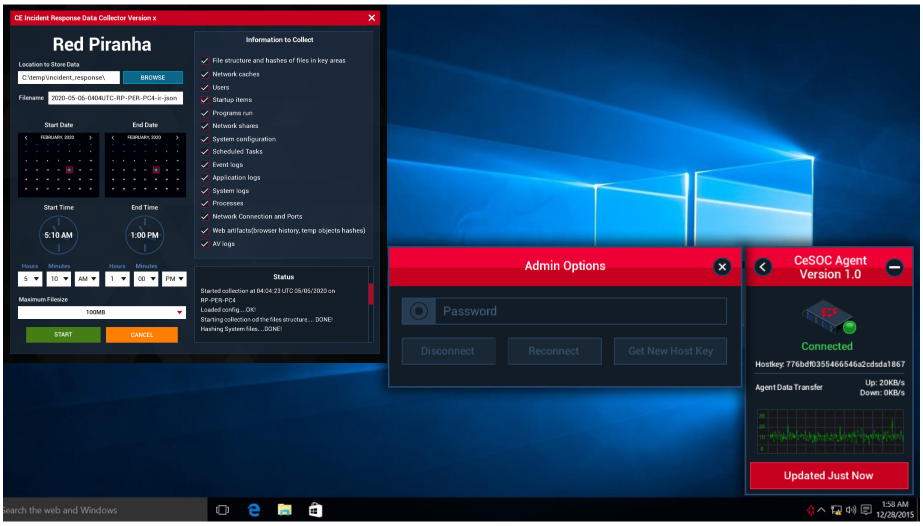
Our Secure Access Service Edge (SASE) App provides your remote users with a secure connection from their devices to the internet, back to the corporate network and to cloud-based apps, data and internet access. It provides comprehensive end-point protection for remote users and is a key foundation of the Secure Access Service Edge (SASE) model. ZTNA allows you to securely extend your private networks for client-to-site and site-to-site communication over the public Internet and protect your cloud environments.

MDR App

Our Extended Detection & Response (XDR) App captures events and sends the relevant data back to the centralised XDR data processor to correlate and report on relevant security activity and incidents across your network. This integrates with the CESOC to assist in delivering an enterprise-wide view of your overall security posture. This also adds host-based XDR capability to the network-based XDR features to support the overall security orchestration approach.

Compliance App

Our Compliance App ensures devices on your network conform to security policies based on the Australian Signals Directorate's Information Security Manual (ISM) and the Essential Eight guidelines. Not only does it allow you to apply operating system policies across a range of devices, it also provides ongoing device monitoring to keep track of your compliance baseline in real-time. Ensuring compliance across devices on your network has traditionally been an onerous task requiring trained resources to implement and manage. The Compliance App can handle the majority of the device audit process through a series of automated features, so you don't have to. It also integrates into the Crystal Eye On-Premise Firewall and the CE IRM backend to close the loop on your end-point compliance requirements.



Location to Store Data: C:\temp\incident_response\

Filename: 2020-05-06-0404UTC-RP-PER-PC4-ir-json

Start Time: 5:10 AM — 5 ▾ 10 ▾ AM ▾

End Time: 1:00 PM — 1 ▾ 00 ▾ PM ▾

Maximum Filesize: 100MB

Information to Collect

- ✓ File structure and hashes of files in key areas
- ✓ Network caches
- ✓ Users
- ✓ Startup items
- ✓ Programs run
- ✓ Network shares
- ✓ System configuration
- ✓ Scheduled Tasks
- ✓ Event logs
- ✓ Application logs
- ✓ System logs
- ✓ Processes
- ✓ Network Connection and Ports
- ✓ Web artifacts(browser history, temp objects hashes)
- ✓ AV logs

```
Started collection at 04:04:23 UTC 05/06/2020 on
RP-PER-PC4
Loaded config....OK!
Starting collection od the files structure.... DONE!
Hashing System files....DONE!
```

Hostkey: 776bdf0355466546a2cdsda1867

Agent Data Transfer — Up: 20KB/s Down: 0KB/s

PRICING

Crystal Eye products are available in a range of options to suit every budget.

—

NEXT STEPS

1. Get in touch
2. Get a quote
3. Get started

—

+61 8 6365 0450
redpiranha.net
sales@redpiranha.net

DFIR App

Our Digital Forensics & Incident Response (DFIR) App offers host-based forensics by collecting and reporting on malicious activity across devices on your network and is complemented by our post-breach consulting to support a rapid response during an outbreak and to assist in the efforts of understanding what has occurred during a breach, such as identifying the source and perpetrator of the attack.

This extends the coverage of the incident response team and the network-based DFIR capability provided by Crystal Eye On-Premise Firewall by also providing host-based data collection. This allows the Red Piranha team to work with your internal IT teams to rapidly respond to any incident with a comprehensive set of data. This delivers a very cost-effective solution for responding to an outbreak – achieving an Incident Response for a fraction of the typical cost for this type of service.

An Integrated Approach

The Crystal Eye Total Security Platform delivers a comprehensive solution across a range of security areas, with the whole platform working together to protect, detect and respond to threats in your environment. Together, this all works to provide a new level of threat protection, all integrated into a single defence-in-depth platform.

Our modular approach can be catered to meet the needs of each company, so you can pick and choose what matters most to you without implementing the whole solution. At the end of the day, it's not just about the technology – it's about managing risks specific to your needs. No matter what your budget or your capacity is, we have a solution to address your needs from SMBs to enterprises.

This is a conversation about managing security risks, not just deploying technical for technology's sake. We recommend starting with defining your required level of assurance, then looking at the most relevant technology to achieve that.

AUTOMATED PROTECTION ▸ AUTOMATED DETECTION ▸ AUTOMATED RESPONSE