SECURITY COMPLIANCE

GOVERNANCE, RISK & COMPLIANCE (GRC)

AUTOMATED PROTECTION | AUTOMATED DETECTION | AUTOMATED RESPONSE

84% OF ORGANISATIONS SUFFERED A BREACH THAT COST OVER $1M*

Can you afford the financial and reputational damage or a security breach?

It's time to get compliant and reduce risk.

STAY AHEAD OF THE THREATS AND YOUR COMPETITORS

Achieving certification is no longer just an obligation – it's a competitive advantage!

It's time to get the upper hand in your market .

CYBERSECURITY IS A BUSINESS ISSUE, NOT JUST AN IT ISSUE

Are your policies and procedures up to date and regularly reviewed?

It's time for the experts to get you compliant.

Increasing Pressure

Organisations are under increasing pressure to meet a range of information security compliance requirements such as ISO 27001, ISM, NIST, Essential Eight, GDPR, PCI and HIPAA in order to continue doing business in today's climate. Chief Information Security Officers (CISOs) who typically look after these compliance requirements are becoming highly sought after, and with that demand comes increasing cost – making them unattainable for many businesses. How are you going to find someone with all the skills and knowledge, without the liability and expense of additional head count? Achieving certification gives your sales and marketing teams something to shout about and gives you a competitive edge in the market.

The Compliance Journey

Achieving compliance against various standards is a long and demanding process. There is no quick fix - it takes time and requires ongoing support from senior management. It's important you find a trusted partner to help you along this journey because you'll need the right people around you to get to the destination. We're here to help.

How we're different

Red Piranha's global team consists of highly qualified and certified security and compliance experts deliver our extensive range of security services. Coupled with our ISO 27001 certified security operations for the Crystal Eye Platform, you can obtain a solid foundation to meet your compliance requirements and automatically protect, detect and respond to evolving threats.

Crystal Eye's machine learning capabilities provide automation of routine tasks such as traffic monitoring and network analysis which allows time to focus on priority tasks that require human intervention such as meeting compliance requirements. Red Piranha is one of only a few security organisations with a fully ISO 27001 certified process to ensure delivery of the highest quality of service, giving you the confidence and peace of mind you're partnering with the right team.

We have one of the fastest growing security teams in Australia and Asia-Pacific to ensure we continue developing our world-class technology platform and continue delivering our best-in-class security consulting services. In addition to our global presence, the majority of our security team reside in Australia to be able to provide hands-on capabilities to our Australian customers as well as customers in other regions.

* Cisco 2019 Asia Pacific CISO Benchmark Study

BENEFITS

Ensure Compliance

—

Ensure Awareness

—

Avoid Financial Penalties

Red Piranha's GRC services provide you with expert knowledge across relevant standards and frameworks, supported by our range of products to ensure you achieve compliance and raise your assurance levels.

Red Piranha
unified threat management

We're helping protect the world from cybersecurity threats by providing automated security solutions for every business; large and small.

Information Security Management System ISO 27001 Certified

Certificate No. 781489

Crystal Eye Security Operations

SECURITY COMPLIANCE

Security Maturity Model

Maturity Modelling is a pragmatic method of evaluating the current state of your cybersecurity posture as measured across the various security aspects that your business needs to address. It allows you to clearly communicate your current status to various stakeholders and allows you to prioritise high risk areas as well as mapping out the next steps in your organisation's security journey.

Basic

Security Aspect	Initial	Developing	Defined	Managed	Optimised
Patch Management and Anti-Virus	Inconsistent Automatic updates. No Reporting	Some automation and reporting	Documented & consistently applied	Measured and Reported. Enforced by end-point management tools	Continuous improvement and innovation
Firewall & Network Segmentation	Simple firewall at internet boundery. ad hoc use of desktop firewalls	Dedicated firewall appliance and/or DMZ	Multiple firewalls and network segmentation	Centralised firewall configuration management	Continuous improvement and innovation
Identity & Access Management	Ad hoc with no process	Domain users & computers, some access restrictions/ structure	Documented repeatable change control processes and JML processes	Analysis, visualisation and reporting tools	Continuous improvement and innovation
Asset and Configuration Management	None	Register of assets and deployment documentation	Asset discovery and reporting	Configuration Change Management and License Management tools deployed	Continuous improvement and innovation
Information Classification and Protection	None	Ad hoc file / disk encryption, inconsistent visual labelling	Structured & unstructured data classification, defined meta-data / templates	Discovery, Data Loss Prevention / Rights Management	Continuous improvement and innovation
Monitor, Alert and Incident Response	None	Some logging, inconsistent monitoring	Basic SIEM deployed Embryonic continuity plans	SIEM tools integrated with most areas. Regular reviews, response and recovery tests	Continuous improvement and innovation
Risk Management and Governance	None	Ad hoc risk assessments, developing security policies	Regular risk assessments and migitation planning, ad hoc awareness traning	Regular policy reviews. Training and compliance tracking	Continuous improvement and innovation

Advanced

1. Scoping

The compliance journey begins by defining the business objectives and setting roles and responsibilities for the business functions that need to be included in the compliance process.

2. Determine regulatory requirements

It's not easy to know which standards and frameworks are relevant to your organisation. Equifax were fined £500,000 for a GDPR breach after being hacked in 2017, even though the incident occurred with the US parent on US infrastructure. The Information Commissioner's Office (ICO) in Europe held the UK subsidiary accountable for not protecting their European customers' data. It's vital to know which regulations apply to avoid significant penalties and loss of business.

3. Security assessments / Gap analysis

Relevant security assessments need to be undertaken by an external party to gain a solid understanding of you current security posture. A Gap analysis will then benchmark you against your required level of security and identify the areas that need to be addressed. You can't fix what you can't see.

4. Implementation

A range of security measures across people, process and technology will then need to be implemented to ensure you fill the gaps identified in the previous step and ensure you stack up against the standards. Having a detailed understanding of your key risk areas before spending money on security controls allows you to focus your budget and resources on the priority areas to avoid a 'spray and pray' approach.

5. Auditing & measurement

It's one thing to meet the requirements of a given standard and another thing to be able to prove your compliance against that standard. This is where an independent 3rd party comes in to audit and verify that you meet the requirements. Auditing typically relates to mandatory standards, while frameworks can sometimes by self-assessed because they're not mandated by government regulation. Becoming compliant gives you visibility of your risk profile while getting certified avoids missing out on market opportunities and reduces supply chain risk.

SECURITY COMPLIANCE

Supply Chain Risk

The biggest threat to most organisations by not being compliant is the risk of losing valuable supply agreements with partners who require you to have certain certifications in place. This 3rd party risk can come as a surprise with little notice for you to achieve compliance before being dropped from the supply chain. Would you trust your suppliers if they weren't certified? Why would your partners trust you if you're not, especially if your competitors are?

Looming Audits

If you are already focused on compliance, then you will likely know when your next audit is coming up. However, if you're just getting started, you may be uncertain about how it all works and when audits may be required.

Preparing for an audit often takes far longer than expected and costs more than budgeted - easily costing in the tens of thousands of dollars and typically needing to be done every year. Instead of being overwhelmed, treat compliance audits like a year-long product launch. In other words, allocate resources (people, budget and tools) to your compliance project, just like you would an income-generating product (because compliance can actually help you generate additional income).

Income Generating Opportunities

Becoming compliant can help your company generate new business. Ultimately, it's a simple cost-benefit analysis. First, calculate the cost of becoming compliant. This cost may include hiring a compliance expert on a full-time or contract basis such as Red Piranha's vCISO service. It may also include securing a third-party firm to conduct the audit and buying software and products that are requirements to meet compliance standards or that enable you to do so. On the other side of the equation, try to calculate how much business you could pursue (and win) if you achieve certification with various standards. This benefit will have a significant impact on what type of projects your sales team can go after. For many organisations, while the upfront cost of compliance can be high, it is well worth the opportunities it opens for your sales teams.

Standards & Frameworks

The security compliance landscape can be a bit of minefield and it's hard to know which standards and frameworks apply to your organisation. It's important to map out a compliance journey that's relevant to you, and ensures you don't double up on effort or have to undo anything later on. As with any significant commercial undertaking, thinking long-term is key to ensure you futureproof your compliance strategy and make the most of your investment.

ISO 27001 is often a good framework for many organisations to start with to lay the foundations for a long-term compliance journey and other standards and frameworks can then apply to specific industries from there.

Achieving compliance opens new business opportunities for your company such as launching into new regions and expanding into new verticals. Organisations that plan to operate in Europe almost certainly need to be GDPR compliant to enable this business growth. Similarly, organisations planning to launch a new product in the fast-growing fintech and healthtech spaces will most likely need to be PCI or HIPAA compliant. Importantly, even those companies who may not currently have mandated certification requirements should be starting their compliance journey by applying proper security practices to not only reduce their risk, but also ensure they are prepared for their future compliance needs. It's a very costly and resource-hungry problem to have to rush a compliance process if the foundations aren't already in place.

Not implementing a suitable security framework can have devastating effects for any business, even where mandatory regulations don't apply. LandMark White was a publicly-listed property valuation company which experienced two major data breaches in 2019 due to a lack of security process. This led to the company being temporary suspended from the ASX and forcing them to change their name to Acumentis to minimise reputational damage. The direct costs relating to the breach were estimated at over $7M plus all the indirect costs associated with the fallout.

Given the significant impact to the bottom line, shareholders are holding Directors accountable if proper security controls aren't being put in place that could avoid a data breach or security incident. This has led to a trend where shareholder class actions are one of the fastest growing sectors within the legal profession to handle such cases.

Although industries such as critical infrastructure, fintech, manufacturing, technology and managed services are high on the radar for compliance obligations, it is becoming increasingly important for all business to follow a robust information security framework.

SECURITY COMPLIANCE

We can help you navigate a path through a wide range of standards and frameworks, including but not limited to, the following:

Standard	Region	Industry	Type
ISO 27001	Global	General	Standard
ISM	Australia	Government	Standard
Essential Eight	Australia	General	Guidelines
GDPR	Europe	General	Regulation
NIST	USA	Critical Infrastructure	Framework
HIPAA	USA	Healthcare	Regulation
PCI	Global	Payment processing	Standard
COBIT	Global	General	Framework
IRAP	Australia	General	Standard

ISO 27001

ISO/IEC 27001:2013 is an international standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) to define information security management systems. It is part of the ISO/IEC 27000 family of standards and is often considered the bible of information security standards. ISO certification is becoming more of a requirement to do business with companies who choose to set standards for their partners and suppliers. Certification against ISO 27001 is a demanding process and requires an authorised external auditor. The standard includes the following key steps:

- Organizational context and stakeholders
- Information security leadership and high-level support for policy
- Planning an information security management system; risk assessment; risk treatment
- Supporting an information security management system
- Making an information security management system operational
- Reviewing the system's performance
- Corrective action

Red Piranha is one of the few IT security organisations to achieve ISO 27001 certification and our exposure to the process enables us to take you through the process with an intimate understanding of what's required. Would you trust your ISO certification with someone who isn't ISO certified themselves?

ISM

The Australian Government Information Security Manual (ISM) is published by The Australian Cyber Security Centre, which is part of the Australian Signals Directorate. This standard outlines a cyber security framework for Australian Government departments and can also be applied to private enterprises looking for a risk management framework. It includes a comprehensive set of 22 guidelines covering topics such as security incidents, physical security, personnel security, enterprise mobility and system hardening to name a few.

Essential Eight

The Essential Eight is a prioritised list of 8 strategies put together by the Australian Cyber Security Centre to mitigate cyber security incidents to assist organisations in protecting their systems against a range of cyber threats. The strategies can be tailored based on an organisation's risk profile and the types of threats of greatest concern.

1. Application control
2. Patch applications
3. Configure Microsoft Office macro settings
4. User application hardening
5. Restrict administrative privileges
6. Patch operating systems
7. Multi-factor authentication
8. Daily backups

SECURITY COMPLIANCE

IRAP

The Information Security Registered Assessors Program (IRAP) is an Australian Signals Directorate (ASD) initiative to provide high-quality information and communications technology (ICT) security assessment services to government. ASD endorses suitably-qualified ICT professionals to provide relevant security services which aim to secure broader industry and Australian Government information (and associated) systems. IRAP Assessors assist in securing your ICT networks by assessing your security compliance and highlighting the information security risks facing your organisation.

Red Piranha is an IRAP-aligned organisation and we're undertaking the process for our products to go through the certification process. We also have a strategic partnership with the Australian CyberSecurity Centre based on our share ideals and we share threat intelligence data.

NIST

The NIST Cybersecurity Framework provides information security guidance for private sector organisations in the US to prevent, detect, and respond to cyberattacks. It was developed by the National Institute of Standards and Technology, which is an agency of the United States Department of Commerce. It includes a Framework Core, Framework Implementation Tiers and a Framework Profile. The Framework Core defines 5 key functions of information security:

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

GDPR

General Data Protection Regulation (EU) 2016/679 (GDPR) is a mandatory regulation enforced under EU law for data protection and privacy in the European Union (EU) and the European Economic Area (EEA). It also covers the transfer of personal data in and out of the EU and EEA areas which can impact companies outside of Europe who have customers or partners inside Europe. GDPR was put in place to give indivduals (defined as data subjects) control of their personal data and has led to sweeping changes for orgnaisations (data controllers and data processors) across the industry. It covers the following topics:

I. General provisions
II. Principles
III. Rights of the data subject
    1. Transparency and modalities
    2. Information and Access
    3. Rectification and erasure
    4. Right to object and automated decisions
IV. Controller and processor
    1. Pseudonymisation
    2. Records of processing activities
    3. Security of personal data
    4. Data protection officer
VIII. Remedies, liability and penalties

HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was enacted in 1996 to regulate the flow of healthcare information in the US and define how Personally Identifiable Information (PII) maintained by the healthcare and healthcare insurance industries should be protected from fraud and theft. Although it mostly applies to organisations in the US, it can also apply companies dealing with healthcare data with customers and partners in the US. The Act is broken into 5 Titles:

I. Health Care Access, Portability, and Renewability
II. Preventing Health Care Fraud and Abuse; Administrative Simplification; Medical Liability Reform
    1. Privacy Rule
    2. Transactions and Code Sets Rule
    3. Security Rule
    4. Unique Identifiers Rule (National Provider Identifier)
    5. Enforcement Rule
III. Tax-related health provisions governing medical savings accounts
IV. Application and enforcement of group health insurance requirements
V. Revenue offset governing tax deductions for employers

SECURITY COMPLIANCE

PCI

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major card schemes.

The PCI Standard is mandated by the card brands but administered by the Payment Card Industry Security Standards Council. The standard was created to increase controls around cardholder data to reduce credit card fraud.

Validation of compliance is performed annually or quarterly, by a method suited to the volume of transactions being handled. PCI typically doesn't apply to companies accepting credit card payments through a 3rd party payment gateway, but would usually apply if you are handling the credit card details yourself.

COBIT

Control Objectives for Information and Related Technologies (COBIT) is a framework created by Information Systems Audit and Control Association (ISACA) in the US for IT management and IT governance. It defines a set of generic processes for the management of IT and is broken into 5 key components as follows:

1. Framework
2. Process descriptions
3. Control objectives
4. Management guidelines
5. Maturity models

Key Areas of Compliance

Compliance mapping to our products and services

Compliance Area	Products	Services
Security Policy Management	CE UTM, CE End-point	Security Framework, Security Assessment, eCISO, vCISO
Awareness & Education		Security Training, Security Assessment, eCISO, vCISO
Identity & Access Management	CE UTM	Security Assessment, eCISO
Vulnerability Management	CE UTM, CE GRC, CE End-point	Security Testing, Security Assessment
Security Monitoring	CE UTM, CE SOC, CE End-point, CE Dashboard	Security Management, Security Assessment
Incident Response	CE UTM, CE SOC, CE End-point, DFIR App	Security Investigation, Security Assessment
BCM / DR	CE UTM, CE SOC, CE Dashboard	Security Investigation, Security Assessment

Technologies

Compliance isn't about creating policies that sit on a shelf to collect dust. A major part of the process is implementing hard and fast security controls and implementing relevant security procedures to prevent incidents occurring. The compliance process drives a process of continuous improvement and measurement to ensure your organisation is getting more secure over time.

Achieving compliance requires the implementation of a number of relevant security controls which can include technologies such as a firewall, anti-virus, IDS/IPS, identity & access management and vulnerability management among others. More advanced approaches such as Secure Access Service Edge (SASE) and managed Security Orchestration & Automated Response (SOAR) can help you integrate your security controls into your Governance, Risk & Compliance (GRC) framework to give you an improved security posture in meeting your compliance needs.

SECURITY COMPLIANCE

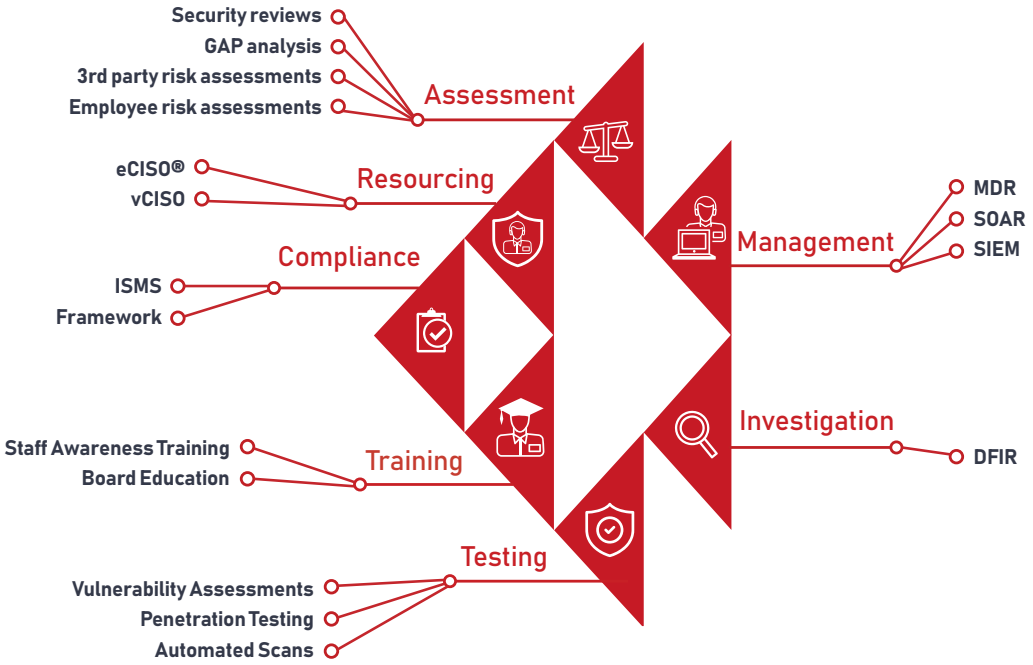
Compliance Mapping

It's important to understand how various security services map against the requirements of various standards. Our eCISO® service delivers the following compliance outputs, as they relate to the corresponding standards shown below. Our tailored security services can also deliver compliance requirements you may have beyond this.

Process and/or Security Service	ISO/ICE 27001	NIST CSF	COBIT 5
Security Policy Management	A.5.1.1	ID.GV-1	APO02*
Awareness and Education	A.7.2.2	PR.AT	APO07
Identity and Access Management	A9.1.1	PR.AC	DSS05, DSS06*
Vulnerability Management	A.12.6.1	PR.IP-12	BAI10, DSS03
Security Monitoring	A.12.4.1	DE.CM	DSS01.03, DSS05.07
Incident Response	A.16	RS	DSS02
BCM and DR (Note 3)	A.17	PR.IP-9*, PR.IP-10*	DSS04*
Normal font indicates an explicit reference to the process.Red font with an asterisk indicates a tangential reference. See discussion below.			

RED PIRANHA SERVICES

We can help you achieve compliance through our extensive range of services:



Security Compliance

You need to start your compliance journey with an overarching framework from which to build a solid foundation to establish your security posture. We can help you get started on the right foot along this journey.

Security Resourcing

Red Piranha's cost-effective CISO services give you the benefits of having access to a pool of industry-leading security specialists to help you achieve compliance, without the expensive overhead of a full-time CISO. Our eCISO® service provides automated compliance features to get the job done as efficiently as possible.

Security Training

Staff awareness of security issues and threats is one of the greatest risks to an organisation. We offer standard and tailored online cybersecurity training programs to help your staff and your Board understand risks as well as your policies and procedures to better protect your organisation.

Security Assessments

Security risk assessments and audits help you understand your organisation's security maturity model, identify potential gaps in your security controls and recommend changes to meet your compliance requirements.

SECURITY COMPLIANCE

Security Testing

Security testing is a hands-on technical engagement which gives you a view of the known and unknown vulnerabilities that exist in your IT environment, as well as providing a plan to mitigate and manage those risks.

Security Management

Our Managed Detection & Response service applies machine learning to automatically detect and block security threats using the Crystal Eye UTM platform. We also offer managed SOAR and managed SIEM capabilities to provide an even greater level of assurance.

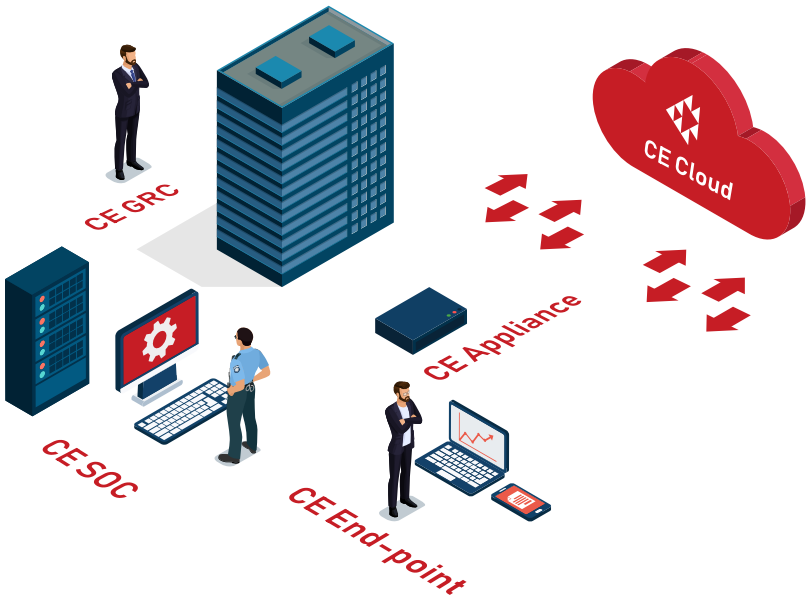
Security Investigation

Digital Forensic services can help you get to the bottom of what happened in relation to a security breach in your network, coupled with a comprehensive Incident Response plan to help you recover from the breach and get back to business as quickly as possible with minimal impact.

RED PIRANHA PRODUCTS – THE CRYSTAL EYE UTM PLATFORM

Our Crystal Eye (CE) Unified Threat Management (UTM) Platform is an automated security platform that protects your organisation from the cloud to the end-point. This Next-Gen UTM includes an extensive range of security technologies such as Next-Gen Firewall, Secure Access Service Edge (SASE), managed Security Orchestration & Automated Response (SOAR) and Governance, Risk & Compliance (GRC), all integrated into a single platform. These capabilities cover the following 5 key areas to help you meet compliance obligations across your organisation:

CE UTM Platform



CE UTM On-Premise

Crystal Eye UTM Cloud

Crystal Eye UTM Dashboard

Crystal Eye End-point

Crystal Eye SOC

Crystal Eye GRC

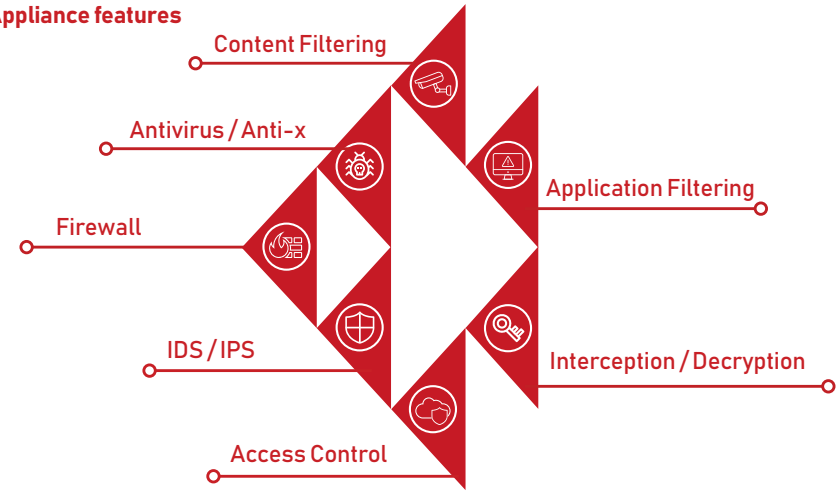
Our modular approach can be catered to meet the needs of each individual company, so you don't need to implement the whole platform.

CE UTM On-Premise

The Crystal Eye UTM Appliance is our hardware product that forms a key foundation of the Crystal Eye Platform. It features a next-generation firewall with a suite of integrated security controls to protect your organisation against the latest threats as well as a number of unique features such as agentless endpoint Application Whitelisting. It also includes a range of automated defence features to get you compliant with minimal overhead.

SECURITY COMPLIANCE

CE UTM Appliance features



Crystal Eye UTM Cloud

Crystal Eye UTM Cloud extends the same level of UTM protection across your entire cloud footprint including your remote users and cloud services to provide a Secure Access Service Edge (SASE) solution. 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.

Crystal Eye SOC

We've developed a deployable Security Operations Centre (SOC) platform that delivers the extensive capabilities of a full SOC, all with the convenience of an appliance or cloud deployment. This brings together a suite of automated detection and response capabilities not possible until now without significant manual effort by a team of security analysts. Our CE SOC solution can complement your existing SOC team to expand their capabilities as well as extend the operating hours of your security monitoring and management.

Crystal Eye End-point

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 and also provides ongoing device monitoring to keep track of your compliance baseline in real-time.

DFIR App

Our Digital Forensics & Incident Response (DFIR) App collects and reports on malicious activity across devices on your network 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.

SIEM App

Our Security Incident & Event Management (SIEM) App captures events and sends the relevant data back to the centralised SIEM data processor to correlate and report on relevant security activity and incidents across your network.

VPN App

Our Virtual Private Network (VPN) App provides your remote users with a secure connection from their devices back to the corporate network. This provides end-point protection for remote users and is a key foundation of the Secure Access Service Edge (SASE) model as part of the Crystal Eye platform.

Crystal Eye GRC

The Crystal Eye Governance, Risk & Compliance 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 visibility on the status of your compliance at a point in time. The compliance journey can be a pain-staking process that requires a log of investment in time and resources. Our GRC 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.

PRICING

Compliance consultancy services are priced based on your specific requirements.

NEXT STEPS

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

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

AUTOMATED PROTECTION ▸ AUTOMATED DETECTION ▸ AUTOMATED RESPONSE