

CYBER RISK IS EVERYONE'S BUSINESS



Red Piranha
unified threat management

 info@redpiranha.net

 +618 6365 0450

 www.redpiranha.net

 RedPiranhaSec

 RedPiranhaSec

 RedPiranha



Solving the cybersecurity business issue

“Does management understand the importance and have confidence that they have the best protection in place to defend their digital infrastructure?”

Cyberattacks make headlines every day. It's no longer a question of whether your business will be breached, or even when; it's likely to have happened already.

Threats are evolving continually, targeting organisations of all sizes across all industries, while becoming more prevalent and high-profile.

For the last 20 years, our dependence on technology has increased, and with these advancements and increased demands, with it, the attack surface has grown exponentially. Traditionally the solution to this was to increase security staff and therefore, costs.

Red Piranha develops technology that allows us to scale with the problem, addressing fundamental flaws in our approach to dealing with corporate cybersecurity issues.

“Cybercrime is the second-most reported economic crime, second only to asset misappropriation, affecting more than 63% of organisations in Australia, costing the economy an estimated \$13 billion annually.”

At the heart of what Red Piranha does is the belief that securing people, property and information ensures business longevity and reputation.

Our depth of experience in information assurance and security also gives us an unrivalled understanding of the range of threats that organisations face.

Unlike other companies in the cyber marketplace, Red Piranha designs, engineers, manufactures and delivers end-to-end unified threat management solutions aligned to customers' business and technology needs.

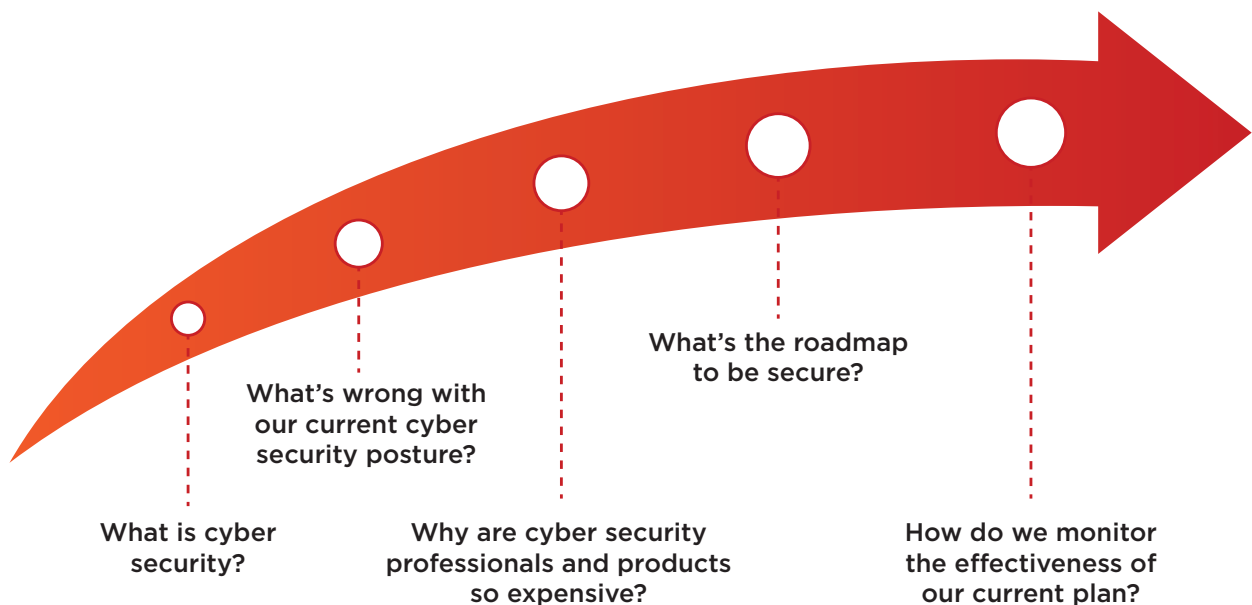


Journey to Security Maturity

Our team work alongside Management and the board to implement a tailored cybersecurity strategy, giving you the confidence and capability to deal with cyber risks and provide solutions to security questions through:

- Independent and thorough review of your organisation's cybersecurity readiness, and ability to address relevant threats.
- A secure Crystal Eye dashboard, providing detailed insight into your organisation's maturity also delivering 24/7 protection, detection and response KPI's for Cybersecurity standards.
- Concise security reporting for stakeholders compliance to meet regulatory requirements.
- Red Piranha's comprehensive cybersecurity service to measure return on investment which could also see a reduction in overall security expenditure.

Common board questions about security and risk management





Our Approach

“Can your organisation explain how ongoing cyber risk assessment and mitigation is handled?”

No, but we can.

We implement a full security plan ensuring your business is protected around the clock.

Our range of cybersecurity solutions:

- Analyse and manage cybersecurity risks across your organisation
- Deliver training and support to staff, reducing your exposure to potential threats
- Assist with industry compliance requirements
- Improve the operational resilience of your systems to increase cybersecurity effectiveness
- Provide comprehensive support and exceptional response times during security incidents

Our approach is to bring you the best options to secure your organisation and its data, leveraging leading global cybersecurity, products, methodologies, and an in-depth understanding of critical infrastructures.



More than meets the Eye

Not only do we manufacture and sell Crystal Eye, the worlds most powerful UTM, we can also implement a full security program through our range of additional services.

These services include:

- Comprehensive security audits, policy & procedure review
- Vulnerability scanning, assessment and confirmation
- Penetration testing (internal, external, web application)
- Security awareness courses and staff education
- Information security management system (ISMS) consulting
- Incident response services
- Digital forensic services
- Chief Information Security Officers Services - Virtual and Contracted

Penetration & Vulnerability Testing services

Vulnerability scanning determines the services and software running on your system, checking these against known security issues to identify potential weaknesses in your network. Doing so establishes a top-level understanding of baseline security levels within your network. Penetration testing offers positive assurance by testing those vulnerabilities in the way a malicious attacker would, exploiting any weaknesses to identify any false positives, and determine what a hacker might have access to.

Red Piranha analyses security measures like firewalls, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS) appliances, password complexity policies, application software, physical security and policy best practices.

We identify vulnerabilities and, by using cutting-edge techniques, we try to exploit them. This presents a clear image of the flaws in your systems and offers an opportunity to solve issues that may pose a serious threat. The testing process is followed by a comprehensive report prioritising vulnerabilities and outlining actionable remediation strategies.

Security Incident Response

The integrity of your business operations relies on your security. After a breach, you must contain, determine the extent, contain affected systems to reduce the chance of further damage, review the efficacy of procedures and their execution, and manage business reputation. Red Piranha utilises methodologies that are proven and focus on business continuity management.

After a breach, recovery time is critical. The cost of not having a plan in place is exponentially larger than the cost of developing one ahead of time and utilising its guidance to get your operations safeguarded, minimise damages to reputation and return to daily business operations.

Public reporting of cyber breach, and increased compliance requirements

With the Australian government enacting the “Notification of Data Breaches” legislation imposing mandatory serious data breach notification obligations on entities governed by the Privacy Act. Business owners and Board Directors need to take reasonable steps to protect both their organisations and personal risk, to provide confidence knowing they have the right technology and systems in place.



Virtual and Contracted CISO – more skills and knowledge, less cost

A Virtual CISO (VCISO) gives your business a key contact with an entire team of experts behind them providing the skills and experience, without the liability and expense of additional on-site staff.

A team's worth of knowledge, access to our current threat intelligence knowledge and lower costs meaning you pay for only what you need when you need it.

Virtual CISO packages include:

- Remote support
- Integration with Crystal Eye reporting and complete GRC reporting platform
- Information Security Policy Framework ISO 27001:2013
- Annual Remote Board Meeting and Reporting
- Remote ISMS Consulting
- Quarterly Vulnerability Scanning
- Annual Packet Capture Analysis (PCAP) audit

Contracted CISO

Chief Information Security Officers (CISO's) are becoming increasingly sought after, and with that demand comes growing costs, often unattainable for many businesses.

Our contracted CISO packages offer:

- Thorough initial consultation with an onsite resource to act as CISO for the organisation
- Fixed hourly rate
- Option to use our Crystal Eye and Governance Risk Management Compliance (GRC) system
- Attendance at Annual Board Meeting
- On-Site ISMS Consulting and AGM ISMS reporting
- Complete Governance, risk and compliance (GRC) Policy Reporting
- Onsite incident response & escalation
- Onsite file Packet Capture Analysis (PCAP) service
- Security policy and staff awareness training

Protection 24/7



Red Piranha is Australia's only dedicated next-generation firewall manufacturer and our flagship product, Crystal Eye is the world's most powerful Unified Threat Management (UTM) platform.

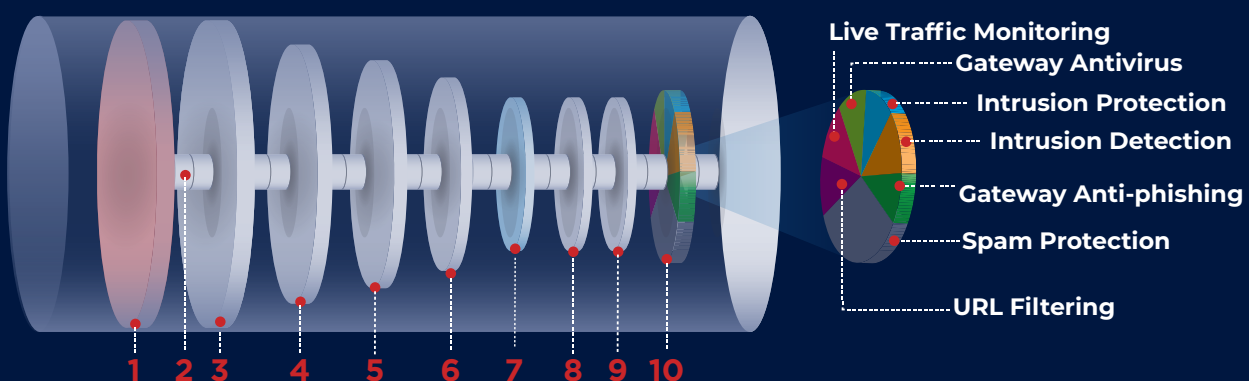
The concept is simple: an all-inclusive threat protection solution, that works.

The result is a complex ecosystem of threat management tools that ensure total protection – from prevention and detection to advanced threat intelligence.

Crystal Eye is an all-encompassing, complete solution managed from a single easy to use platform.

Instead of managing multiple devices from different vendors, Crystal Eye allows you to consolidate and manage everything on one platform, with one set of policies and logs to adjust.

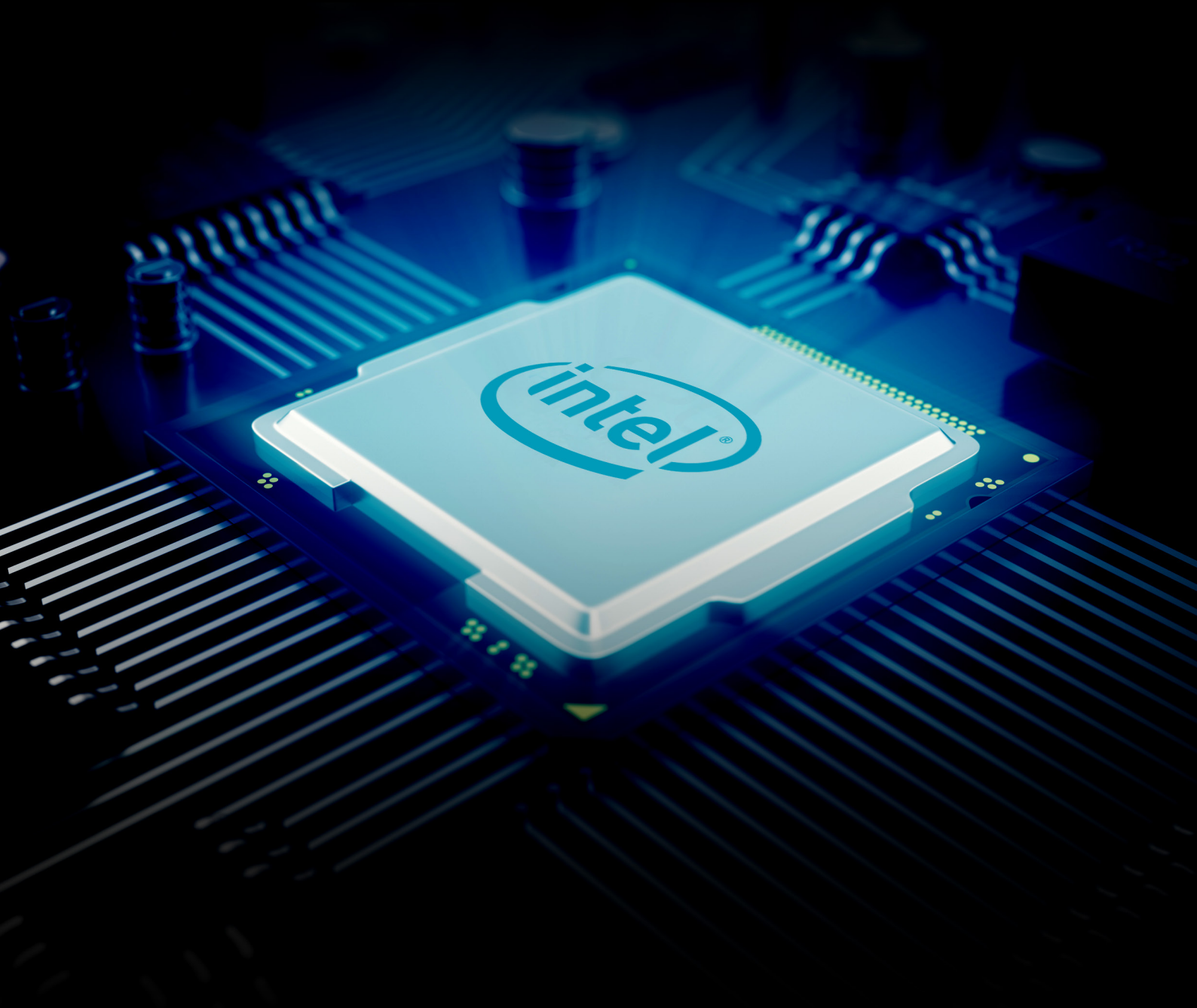
Crystal Eye identifies the flaws in your system testing to find the unknowns, and fixes them, offering an assurance against risk within your network.



- | | |
|---|--|
| <ul style="list-style-type: none">1. Zero Day Protection / AI Unauthorised SSH
TLS Detection / Gateway Application Whitelisting2. Automated Actionable Intelligence
Processing 14 million incidents of compromise (IOCS) daily3. Compliance Features / SIEM
Vulnerability Scanning4. Data Integrity / Data Loss Protection5. VPN | <ul style="list-style-type: none">6. Stateful Firewall7. MSP Client Security / Service Delivery Network (SDN)8. Deep Packet Inspection9. Alert and Alarm Analysis10. Content Security |
|---|--|

Crystal Eye

Now built with
Intel® Generation 9 Processors



Red Piranha
unified threat management