ADVERTISING FEATURE

Cyber threat protection

Above: The Red Piranha team with CEO Adam Bennett, centre, holding the Consensus Innovation Award.

Global interest in innovative solution

The risks, complexity and costs of cyber-attacks are growing exponentially, as the cybersecurity industry struggles to keep up with digital criminals intent on perpetrating data theft, business disruption, fraud and ransom on a global scale.

Business is squeezed between tighter rules on individual privacy, on the one hand, and the rising cost of security solutions on the other.

Businesses rely on network to manage and share data and every network is prone to cyber threat. As we adopt advanced technologies such as Cloud and IoT, cyber threats are also becoming sophisticated.

To monitor and control such sophisticated threat we need to move from traditional security measures and apply advanced threat detection and monitoring techniques. A Unified threat management (UTM) solution uses intelligent defence, adaptive analytics and integrated controls to detect and demolish the attacks in real-time.

The industry needs innovation and Australia's only next-gen firewall company Red Piranha provides just that with its Crystal Eye product a Unified Threat Management (UTM) solution.

Recently awarded the Consensus Innovation Award, following in the footsteps of Atlassian and WiseTech Global, Crystal Eye is leading the way with its list of features, with judges saying Red Piranha's business model was comprehensive and well designed for their target market.

Not only the world's most powerful UTM, Crystal Eye also features the industry's first in-built gateway application whitelisting as well as email scanning, data loss prevention and several other innovative features, that collectively provide exceptional security orchestration, automation and response. All of this on one platform with only one set of policies and logs to adjust, a critical factor in reducing the response time to threats, responding to incidents, and creating consistent security policies that are easy to apply across the network.

Industry analyst Gartner predicts worldwide spending on information security products and services will hit $US124 million in 2019. The cost of so-called "mega breaches," can run as high as $US350 million with the average price of a data breach being $US3.6 million, according to a joint report from IBM and the Ponemon Institute.

The Office of the Australian Information Commissioner said 215 breaches of privacy were reported under the Notifiable Data Breaches Scheme in the March quarter 2019. Of these, 61 per cent were due to malicious or criminal attacks, 35 per cent to human error, and 4 per cent to system errors. In the year to March, breaches totalled just under 1000.

But cybersecurity expert Adam Bennett, CEO of Red Piranha, says anecdotal evidence suggests the actual number of breaches is probably far higher.

"We believe it only captures a fraction of what's happening," he says.

Small and medium enterprises are particularly at risk because few cybersecurity products have been developed to meet their needs at an affordable price, says Bennett.

"What these enterprises need is a cost-effective way of delivering multiple controls that address business risk, and real business issues around cyber-security as well as automating compliance and governance."

The consequences of having data compromised have grown enormously. Twenty years ago, if an enterprise was hacked, their home page might have been defaced. Now entire business systems are being affected, operations are having to shut down, and vital data is being lost.

"Clients are protected up to the minute against the evolving threats."
Adam Bennett

At the same time, computer networks are growing faster than we can keep up with, and this increases the available attack surface, Bennett says.

"The threat landscape increases along with it, and it's almost impossible for IT teams to defend against it."

Building a cybersecurity system is often compared to making a house secure, starting with doors, windows, locks and a fence and progressing to bars, alarms and CCTV.

"In information security, we call these things 'controls'," says Bennett.

"Often you can't see them or touch them – they're technical or policy responses, and it's the layering up of these controls which allows you to get overall security."

Security is no longer a matter of protection, but also one of detection and response. For example, if a company puts up a brand-new firewall and no one is watching it a hacker could breach the firewall, but no one would be the wiser.

"We address that 'defence in depth' problem by deployment in the infrastructure where we put what's called a Unified Threat Management platform, to cover these areas of protection as well as detection and response," Bennett says.

"The UTM approach gives you a single pane of glass and allows you to reduce management burden and integration points … [as opposed to] buying from multiple vendors, where the technology might not integrate well."

Bennett says the company aims to "bring top-level, defence-grade cybersecurity to everyone".

Red Piranha has established partnerships with Managed Service Providers so they can provide its products to SMEs and enterprises as part of the bundle of IT services.

The company with its global partners in the Open Information and Security Foundation, one of the most significant international threat-sharing consortiums, together process more than 14 million "indicators of compromise" a day.

"If one of our partners' clients gets hacked in France, within hours our clients are protected against it," he says.

"That threat data is processed and fed back in and used to update our platform up to four times a day, so our clients are protected up to the minute against the evolving threats."

It's not one thing that gives you security; it's all of them collectively that provide peace of mind.