Independent Technology Report

Red Piranha's Crystal Eye Next Generation Firewall Operating System

Peter Hannay & Clinton Carpene
peter@hannay.id.au, clinton@carpene.id.au

6th August 2017

Executive Summary

Red Piranha Limited is a public, unlisted company registered in Australia. Red Piranha Limited ("Red Piranha", the "Company") is currently based out of Perth and Sydney, developing information security technologies and products. Red Piranha is a fully integrated supplier of cyber security services for small to medium enterprises in Australia with export capabilities for global markets.

Red Piranha's advanced intrusion and detection systems, backed by the Company's threat intelligence, updates systems multiple times a day giving greater protection against zero day attacks and advanced persistent threats. The Company is currently working with its business associates and partners to produce a bundled insurance product. The product provides a complete cyber security service through a combination of technology and insurance packages to provide remediation should some damage or loss eventuate.

In 2015, Red Piranha purchased the DNS.Insure platform and began development on the Crystal Eye Unified Threat Management systems (UTMs; the "Technology"). Under the conditions of the acquisition, all related intellectual property and concepts are now entirely under the express control of Red Piranha.

Red Piranha and its range of managed information security solutions, provides a cost-effective framework and a platform for individuals, families, small to medium enterprise, as well as custom solutions for larger enterprise environments, giving the client real-time protection. Red Piranha provides a range of flexible, managed, cost effective services and products for deployment offering the client options to cover the growing attack surfaces.

In early 2016, Red Piranha entered into an agreement to purchase 40% of E-Way Technology, a technology assembly factory in Taiwan. This arrangement provides Red Piranha with the capability to manufacture its own hardware for the Crystal Eye product range. This arrangement gives Red Piranha security over the supply chain and making Red Piranha a total end-to-end security solutions provider. This acquisition places Red Piranha in the position to build, distribute and install its cutting-edge technology to all of its clients, placing Red Piranha at a substantial advantage to the rest of the cyber security marketplace.

Preamble

The Directors
Red Piranha

7th August, 2017

Level 11
216 St George's Terrace
Perth, WA 6000

To whom it may concern,

The size of the cyber security problem is significant. According to a report from CSO cybercrime damages will climb to an annual $6 trillion global economic impact by 2021 [1]. Common types of cybercrime include hacking, scams, fraud, identity theft, attacks on computer systems, and illegal or prohibited online content. Not only is financial loss a major result of cybercrime, many victims may feel that their privacy has been violated and that they are powerless. As reliance on technology grows the cost and incidence of cybercrime is expected to increase.

In 2016, the amount spent on cybersecurity was estimated to be more than $80 billion and the cybersecurity market is expected to exceed $1 trillion from 2017 to 2021 [2]. In fact, according to a new Telstra study it was found that the rate of cybercrime in Australia has doubled in the past 12 months with more and more companies detecting security incidents within their organisations. The cyber security report found that almost 60 percent of local organisations surveyed detected a security incident on at least a monthly basis in 2016.

Data breaches can leave directors and officers of victim organisations vulnerable to civil suits (including possible class actions) for breaches of privacy legislation, corporate regulation, negligence, or claims of misleading or deceptive conduct (for not adhering to the company's own privacy policy, especially in respect of IT security). Directors and officers liability (D&O) insurance does not typically cover cyber incidents and the liability of directors personally.

Red Piranha aims to provide an all-encompassing security solution for individuals and small to medium enterprises as well as offering bespoke solutions for larger enterprise environments. Through the Company's range of managed information security services the Company is able to provide a cost-effective framework in order to provide its clients with real time protection which aims to provide cover across a growing number of attack surfaces which are vulnerable in the current information technology security market.

With the recent reporting of a major cyber-attacks across the globe, effecting nearly 100 countries, it is now more important than ever to invest in cyber security [3]. In fact this fact is proven in cyber security based stocks increased performance in the market place. For example the ASX listed ETF Betashares Global Cyber Security (ASX:HAC) increased from a price of 5.33 to 5.93 within a time frame of less than five months during 2017.

Information Security is a major issue for all businesses and virtuous activity is being generated at the top end of town, however there is a glaring omission with the lack of engagement with, and empowerment of, Australia's small and medium businesses. Red Piranha Limited is tackling this Australian business issue [4].

Red Piranha is Australia's first next generation firewall developer they have recently announced their acceptance into the Open Information Security Foundation Consortium. Again, an Australian first. The partnership will see the Red Piranha Team work alongside some of the world's best minds with the Open Information Security Foundation (OISF) being led by world-class security experts, programmers, and others dedicated to open source security [?].

Red Piranha, recently announced its acceptance as a Red Hat Connect Technology Partner. The partnership will see the Red Piranha Team have access to new Red Hat technology, gain certifications for it's hardware, Crystal Eye software and its managed security cloud based services. The partnership will give Red Piranha technology adoption resources and options for event visibility. The partnership

between Red Piranha and Red Hat will establish brand differentiation and help Red Piranha gain competitive and flexible pricing models.

As Red Piranha moves towards the launch of its Crystal Eye operating system in late 2017, the partnership can also help with marketing, sales training, and progressive relationship benefits. The partnership also opens up opportunities for system integrators, cloud and service providers, reseller ISV's and more.

Red Piranha has been working and developing its core product around the Red Hat kernel, which has been shown to be mature, robust and well supported. Red Hat has a long history of assisting its customers navigate technology and business disruption through open innovation. Partnership with the Red Hat allows Red Piranha to be at the cutting edge of developing robust and relevant information security technologies.

The Red Piranha Next-Generation Enterprise Crystal Eye Unified Threat Management (UTM) product family protects the network internally as well as the perimeter, optimizing connectivity and simplifying the administration of network operations. The Crystal Eye product range will be the first product of its kind designed and owned in Australia and is planned to be released late in 2017. Red Piranha manufactures and supplies End-to-end security solutions to safeguard your information across the entire network and its borders helping you maintain Confidentiality and Integrity. The easily deployed Crystal Eye multi-layered security next generation firewall range increases security awareness reducing risk exposure from advanced cybercrime, malicious software and insider threats.

Regards,
Peter Hannay & Clinton Carpene

Peter Hannay:  7th August, 2017

Clinton Carpene:  7th August, 2017

Contents

1 Introduction

Red Piranha limited is a public unlisted company registered in Australia and currently based out of Perth and Sydney developing information security technologies. Red Piranha Limited ("Red Piranha", the "Company") is the sole owner of the Crystal Eye operating system and supplier of cyber security services for small to medium enterprises in Australia and for export into global markets.

The global information security market saw a global spend of over $81 billion for the year of 2017, which has grown by 7.9% since 2015 [5]. It has been projected that the global information security will exceed an annual spend of $101 billion annually by 2020 [6]. The security market has shown consistent growth and this growth is expected to continue at a rate of approximately 8% per annum for the foreseeable future. A Gartner report shows that the Network Access Control (NAC) market has grown by 26% from 2015-2016, a rate significantly higher than the information security industry as a whole [7]. UTM uptake in the SMB market is currently sitting at approximately 2% with a projected update of 25% by 2022.

The Australian cyber security spend was 3.4 billion in 2016 and is currently expected to experience annual growth in excess of 10% for the period of 2016-2026 [8]. This growth in combination with the disproportionately large growth demonstrated in the NAC space provides excellent potential for the Crystal Eye product to be positioned within the local market.

Fortinet are the current recognised leader within the UTM space. Globally Fortinet are recognised as having wide geographic spread, competitive pricing and excellent understanding of the market [9]. However outside of the North American market their prices are significantly higher and they may not prove competitive on the pricing front. Additionally the Fortinet product has been found to be quite weak in the areas of HTTPS interception and malware prevention [10].

Cyberroam (acquired by Sophos) provides a UTM solution aimed at the SME market segment. The product development and support is primarily based in India [10]. Sophos is in the process of merging the Cyberroam product lines with its own, however it is expected that migrating to the new Sophos branded platforms will be quite costly and cause significant disruption to the user experience [10].

There is significant potential for a next generation UTM product of Australian origin. The geopolitical landscape has resulted in tensions which have created a public interest in data provenance. As a result there is mass market appeal for a device of Australian origin with known and controlled supply chain from manufacture, software development, data storage, and deployment. The total potential market for this product is significant, with a current 3.2 million small businesses in Australia [11] and a projected 25% of these adopting a UTM solution by 2022 [10].

2 About the Auditors

Peter Hannay is a security researcher currently working within the School of Science at Edith Cowan university and is also involved in network vulnerability, malware and OT research projects under the banner of the Security Research Institute. His research focus is network security and digital forensics, specifically relating to small and embedded devices. Peter has been working within this role for near to ten years. In addition to teaching and research work, Peter has undertaken consulting work within the private and public sector, performing vulnerability assessments, source code review, for critical infrastructure providers and other high security environments.

Peter is currently enrolled as a post-graduate at Edith Cowan University. Peter's Doctoral thesis topic is focused on determining effective methods for reliably extracting locational information from generic embedded devices. Additionally, Peter holds Bachelors and Honours degrees in Computer Science, where his thesis focused on the extraction of locational history from small and embedded devices. As a result of his extensive experience and knowledge of locational forensics, Peter has engaged with law enforcement on several occasions to provide investigative assistance.

In addition to his professional work, Peter is an active member of the international cyber security community. Peter is a regular speaker at industry events including those run by IEEE, Interpol, ACSC, and ISACA. Peter is an organiser of Perth's largest annual security conference and has spoken at numerous security conferences including Defcon, BlackHat, Kiwicon, Unrestcon and BSides Canberra.

Clinton Carpene is a senior security consultant and security researcher. As a security consultant, Clinton has participated in numerous security testing engagements ranging from vulnerability assessments and penetration tests, to application source code review. Clinton focuses his research on the security issues surrounding IPv6 and the Internet of Things.

Prior to his work as a penetration tester he worked for five years at Edith Cowan University under the Security Research Institute. During this time Clinton undertook postgraduate research, with his position funded by Cisco. During this period, Clinton published numerous papers on the topics of IoT and IPv6 security.

Clinton holds a PhD in Computer Science. Clinton's doctoral thesis topic of IPv6 host enumeration search methods assessed the efficacy of various search algorithms for enumerating unknown devices in IPv6 networks. Clinton also holds the industry-recognised OSCP certification, that demonstrates practical security competency. In addition Clinton holds an Honours degree in computer science, for which he audited endpoint smartgrid devices from a network security perspective.

Clinton is an active member of the security community. Clinton is an organiser of Perth's largest annual security conference, organises monthly cyber security talks and is a member of national security organisations. Clinton has spoken at numerous national and international conferences.

Peter and Clinton are both respected members of the information security community and recognised experts within their fields. They have demonstrated their skills academically, professionally and are actively involved in the local community, working to build new talent and foster the future of cyber security within Western Australia.

3 Scope of technology Review

A functional examination of the CrystalEye UTM product was performed by the auditors against a virtual appliance provided by Red Piranha. All performance metrics were evaluated through a testbed and hardware appliance provided and configured in place by Red Piranha.

This report evaluates the CrystalEye product in terms of functionality against a set of claims made by Red Piranha. According to [7], network access control (NAC) refers to systems that enable organisations to control access to the network for devices and users. Unified threat management (UTM) refers to a system that combines multiple security functions, such as IDS/IPS, network firewalling and NAC, antimalware, dataloss prevention, and security information event management (SIEM). This report assessed the CrystalEye product under these definitions. Anything outside this set of claims was deemed out of scope. Additionally the Red Pirhana Service Delivery Network (SDN) was excluded from the scope of this review as it is external to the Crystal Eye platform itself. Finally, features supporting general function of the device or network, not related to network security functionality, were considered out of scope for this review. The capability and applicability of these features for the SME market were considered and appropriate commentary provided. Where functionality is not yet implemented it is discussed based on the merits of the proposed implementation.

The statements made and opinions expressed in this report are believed to be correct by the authors, however the authors assume no responsibility or liability for any errors or omissions in the content of this report. The information contained in this report is provided on an "as is" basis with no guarantees of completeness, accuracy, usefulness, or timeliness.

Any discussion of projections or future performance are subject to interpretation and it must be noted that past performance is not a reliable indicator of future results, as such no responsibility can be accepted for decisions made based on this report.

The audit process was undertaken over between February and August, 2017. The audit was conducted in two phases, the first a security audit and the second an evaluation of the functionality of the platform. Fees for the audit and preparation of this report are being charged at normal commercial rates. Payments of fees is in no way contingent upon the completion of these documents, nor on the outcome of any future capital raising by the company.

4 Unified Threat Management and the Crystal Eye Platform

Unified threat management (UTM) describes cyber security products that offer a full defense against a variety of cyber attacks. This differs from conventional approaches where companies are required to buy different capabilities, such as firewalls or anti-virus software, from different vendors and manually integrate them into an overall defense system. The overhead from managing multiple disparate systems from competing vendors has the potential to overwhelm users. UTM products aim to reduce the overhead of managing cyber threats by consolidating threat alerts. Red Piranha, via the Crystal Eye OS, provides a sophisticated simple to use UTM device built and supplied on its own secure and affordable hardware.

Red Piranha offers a UTM product designed for the small to medium enterprise. The Crystal Eye product allows users to monitor and manage cyber threats to their systems through a single console. The platform introduces sophisticated controls aimed at meeting basic information security compliance needs. The Crystal Eye operating system and Red Piranha's service delivery network (SDN) is in a position to offer a range information security controls. Customers are only required to deal with a single vendor and a single product in order to achieve a complete defense-in-depth security strategy.

The Crystal Eye operating system prioritises usability and functionality in addition to its comprehensive security and compliance feature list.

4.1 Feature Integration

4.1.1 System and Network Configuration

Configuration and management of the device is performed through the Web GUI. Table 1 contains a list of system and network configuration features that are provided by the platform.

Table 1: System and network configuration functionality, broken down by category

Category	Configuration level 1	Configuration level 2
Account Manager	Accounts	
		Directory Server
	Account Roles	Administrators
		Groups
		Users
	General Settings	
	Date and Time	
	Software Updates	
	Process Viewer	
	Mail Settings	
	Backup	Bare Metal System Backup
		Configuration Backup / Restore
	Infrastructure	
		IP Settings
		DNS Server
		SSH Server
		DHCP Server

4.1.2 Administration and System Control

Consolidated security administration is a key value proposition for UTM. The Crystal Eye platform offers role-based administration to ensure that administrators can be allocated the minimum privileges required for them to perform their duties. As an example, users can segregate roles between a desktop department to handle anti-virus configuration and a network group to manage the firewall setup.

Additionally, in order to facilitate multiple, concurrent administrators, a read-only mode is set to be available for the Dashboard. The read-only mode will allow administrators to view, but not change, the system's configuration. Table 2 contains a list of features that the platform provides.

Table 2: Administration and system control functionality, broken down by category

Category	Configuration level 1	Configuration level 2
Network Control	Web Proxy Server	
	Device Management	Network Map
	Email Scanning Gateway	
	Web Access Control	
	VPN	
	Quality of Service (QoS)	
	Certificate Manager	
	NAT and Routing	Port Fowarding
		Multi WAN

4.1.3 Authentication and Policies

Configuring and tuning security policies is a core aspect of security appliance maintenance. Ideally, you would an appliance should be accessible to novice and amateur users, but provide flexibility and advanced configuration facilities for power users. Additionally, it is important that adequate feedback is provided to ensure user configurations follow secure best practices.

Policies in the Crystal Eye product are module-specific. Policies that apply to particular users or network interfaces are desirable if your UTM appliance has multiple concurrent network connections. The Crystal Eye product allows users to deploy different policies by segment or by user group (for example, one with servers on it, or one with engineering users). An administrator may set one policy that restricts access to all of the individual security modules, with specifics for anti-virus, IDS and so forth.

Protection policies will give users a good starting point and examples that will make it easy adapt policies to their specific requirements. All of the Crystal Eye's protection rules are organised in a single section, and can be easily applied to appropriate interfaces.

4.1.4 Daily Operations

It is of critical importance for a UTM product to be able to quickly identify network breaches or if protective mechanisms must be adjusted. As the product provides access to firewall, IDS, and VPN functionality within the same device, it is possible for the platform to alert if incompatible configuration options are set between different modules. For instance if a VPN endpoint is configured, but a firewall rule prevents it from operating, it is possible for the product to detect and provide an alert to the administrator. This capability represents a significant reduction in the complexity of troubleshooting exercises, as debug logs from multiple platforms do not need to be examined and cross referenced in order to identify the issue.

4.1.5 Live Monitoring

The platform's live monitoring dashboard provides access to real-time information including CPU and memory load, current alerts, anti-virus related messages, and system health messages that require immediate attention. Access to this dashboard may prove helpful to see if the UTM is mismatched with the particular network traffic and inspection loads, allowing for reallocation of resources or up-sell opportunity.

The live dashboard provides helpful summary information in one convenient place. Such information includes details that can be used to determine details of the current threat environment or identify

ongoing issues such as those impacting email or network performance. A number of dashboards can be defined, the current iteration of the product includes a system dashboard, showing a summary view of the system status and a security dashboard, showing a summary view of the network security status and a real time view of detected security events.

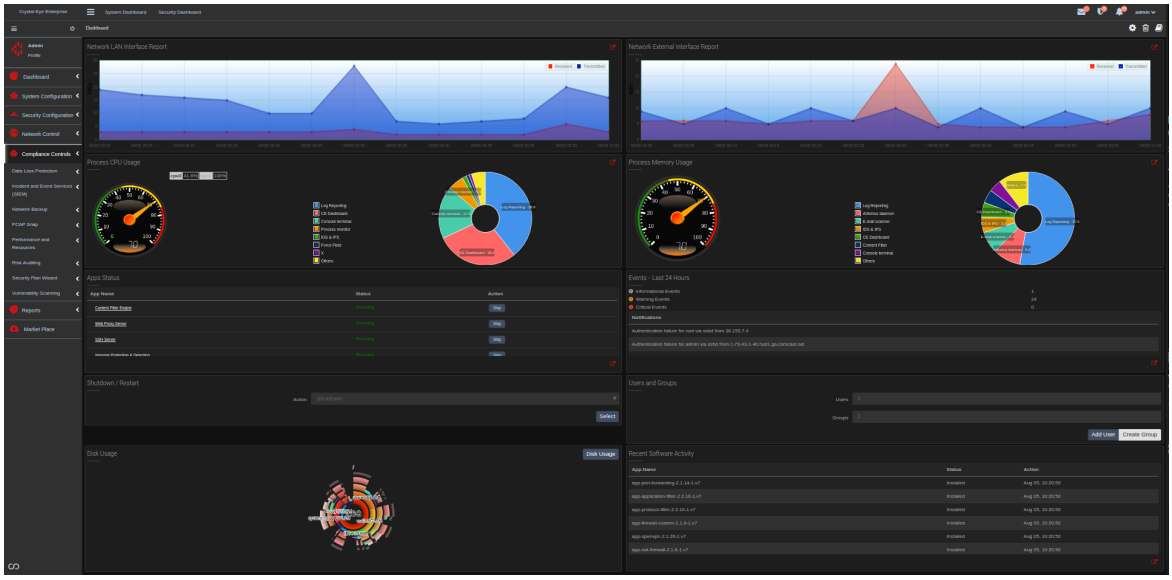

Figure 1: The System Dashboard gives users an "at-a-glance" overview of the CrystalEye system's resource usage.

4.1.6 Security Configuration

DNS filters DNS filtering will allow for specific DNS queries passing through the gateway to be blocked based on a administrator curated rule set. In addition to this, the Red Piranha service delivery network will provide updated lists of domain names to be blacklisted. These domain names are curated and sourced from Red Piranha's DNS.Insure technology.

Firewall functionality allows for packets to be processed based on a set of rules, performing a variety of actions depending on the rule provided. CrystalEye makes use of iptables as its' firewall engine, as such rules are incredibly flexible and can be used to implement both simple and advanced firewall actions. At its simplest the device can allow and deny transit based on the port, host, protocol, or state of the connection/packet. Through the implementation of more advanced rulesets, the platform supports port forwarding, load balancing, and packet mangling, of course this list is not exhaustive.

Application Filters allow for traffic to be allowed or denied based on the application protocol detected by the platform, The system will be able to identify and classify over 160 network protocols spanning broad range of applications protocol detection and filtering, as an example the production platform will be able to detect the following:

- File sharing applications (e.g. BitTorrent)
- Online gaming (e.g. Battlefield, Quake, WoW)
- Instant messaging (e.g. Jabber, IRC, Twitter)
- Media (e.g. Spotify, SHOUTcast, PPStream)
- Remote desktop (e.g. Teamviewer, Citrix Online, RDP)
- And many, many more

Gateway Antivirus enables the platform examine and evaluate files as they transit in real time. CrystalEye makes use of a combination of signature and heuristic analysis to classify files. The malware definitions are updated automatically in order to maintain currency without user intervention. Detected malware is automatically blocked in order to prevent infection from occurring. Placing anti-virus capability within the network gateway provides complimentary protection to traditional endpoint security models.

Interception and Decryption features of the Crystal Eye platform allow for full inspection of encrypted traffic in a transparent manner, enabled by installation of appropriate certificates on endpoint devices. The platform is able to intercept and decrypt transmissions that make use of SSL/TLS based encryption mechanisms. Once decrypted, the data can be fed to other modules of the Crystal Eye platform, enabling other features to analyse traffic that would otherwise be opaque to inspection. Decryption features of the Crystal Eye platform allow for full inspection of encrypted traffic in a transparent manner, enabled by installation of appropriate certificates on endpoint devices.

Gateway Antiphishing automatically inspects email as it passes through the gateway, to detect phishing attacks. The platform makes use of signature based and heuristic mechanisms from automatically updated rules. In addition to this the platform intelligently scans URLs and links within emails. The scanning engine ensure that cryptographic certificates are valid and match the host as claimed as well as detecting links that are cloaked in order to deceive end users. This functionality is critical to an organisations security stance, as modern phishing techniques cannot be fully mitigated through user education alone, technical countermeasures must be employed prior to email reaching the end user.

Forcefield provides security for the CrystalEye platform itself, detecting multiple failed login attempts against the services provided by the platform. For instance, if an attacker enters five incorrect passwords while attempting to log into a mail account, the attackers IP address will automatically be blocked for a period of time. This security feature provides excellent protection against both malicious "Internet background noise" and motivated attackers aiming to leverage weak, common, or harvested passwords.

Content Filter and Proxies provide functionality to filter web content based on a number of criteria, including (but not limited to): file extensions, file types, phrases, websites, and URL presentation. The content filtering engine provides SSL man in the middle capability with dynamic creation of certificates automatically being signed by a provided certificate. The interception and examination is transparent for endpoints that trust the signing certificate in use. This functionality is of critical importance due to the wide availability of free and automatically issued certificates. These freely available certificates have resulted in a large amount of malware using valid SSL/TLS connections when phoning home, infecting endpoints or exfiltrating data.

Integrated Firewall-IPS/IDS. Part of the usefulness of a UTM appliance is how its firewall and IDS work together, and flexibility in terms of where it can be used across different configurations of an enterprise network. In other words, the platform is able to position the IPS module outside of the firewall to repel attacks and reject this traffic before it is processed any further, or to work with an existing firewall infrastructure at a headquarters network.

The CrystalEye examines incoming encrypted packet streams and act on this analysis before passing these streams through other modules, thereby saving on processing power. In conjunction with the decryption engine the IPS/IDS scan for both attack signatures and attack behaviors in both encrypted and plain text communications. The functionality of the platform supports all functionality on both inbound and outbound traffic. As such, the platform is able to detect and block outbound attacks via firewall rules, deep packet inspection or recognition of attack signatures.

Table 3: Security configuration, broken down by category

Category	Configuration level 1	Configuration level 2
Security Configuration	AntiMalware/Gateway Security	Anti-Phishing Anti-Virus
	Intrusion Protection & Detection	
	Forcefield	
	Content Filter and Proxy	Content Filter Engine Content Filter IP Based
	Application Filter	
	Protocol Filter	
	DNS.Insure	
	Firewall	
	Log Processing and Reporting	

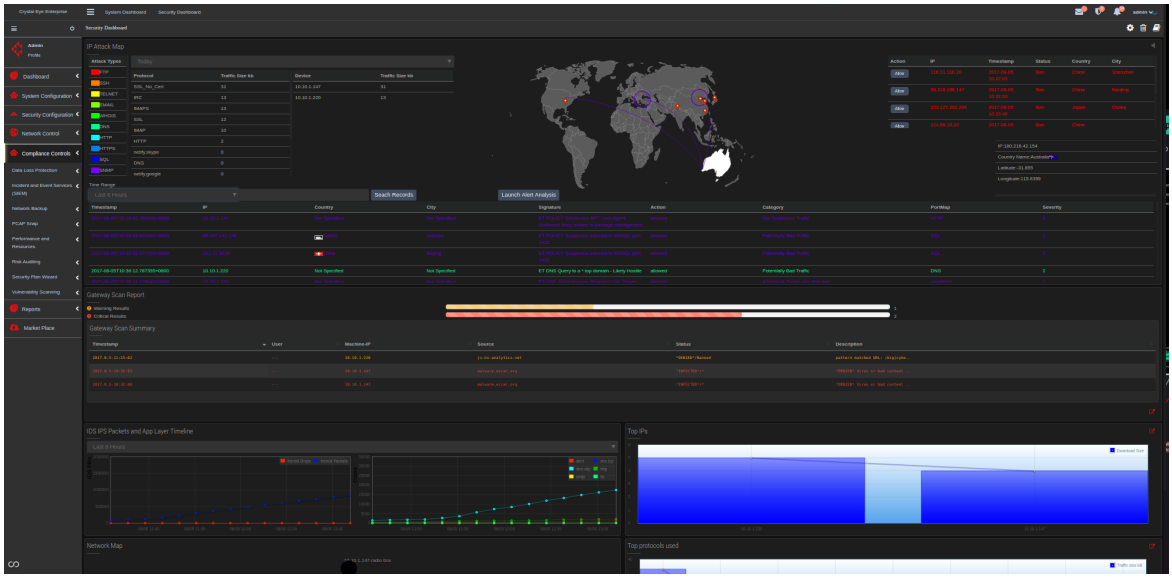

Figure 2: The Security Dashboard allows users to see current threats detected by the CrystalEye product.

4.2 Marketplace

The CrystalEye product allows for additional functionality to be deployed via an application marketplace. Application download, installation, and updating is backed by the Red Piranha Service Delivery Network (SDN). Each product has intricate licensing and signature file update capabilities, this is required primarily as the software and hardware will be deployed in varying configurations, with varying feature sets enabled. The marketplace consolidates all application updates, such as those for anti-virus, IDS and firmware in a single screen. The CrystalEye system will provide the capacity to check for updates on a specified schedule.

The primary purpose of the marketplace (as a component of the SDN) is to simplify the administrative burden of managing a UTM system and should allow for multiple deployment platforms to be easily managed by allowing easy access to the software needed to meet the requirements of various implementation types. At the time of review, the platform included many modules by default, however it is planned that the release version of the product will move more of the existing functionality into the market place. This shift should allow for minimised resource usage, as users can enable individual modules based on their needs, eliminating unnecessary overhead.

Red Piranha will maintain control of billing and licensing for add-on software and managed services via an integration of the market place and their in house CRM system. Through this interface changes

to service levels, hardware changes, device registration, etc.

Further to this the SDN enables risk, event, and incident management as a service. In many cases UTMs are set up and not monitored locally, often due to lack of adequate resources to do so. The SDN connection addresses this issue by allowing essential monitoring, maintenance and response to be undertaken remotely. The SDN is comprised of a number of servers that manage security updates, software updates, risk management, incident management, and event management service offerings.

4.3 IDS and IPS Security Features

Next Generation Intrusion Detection and Prevention Engine rule-based IDS/IPS engine that utilises externally developed rule sets to monitor network traffic and provide alerts to the system administrator when suspicious events occur. Designed to be compatible with existing network security components.

The System implements a complete signature language to match on known threats, policy violations, and malicious behavior. The IDS/IPS system will also detect many anomalies in the traffic it inspects. The Signatures are updated multiple times a day via the Red Piranha service delivery network that is fed via the Red Piranha threat intelligence center.

The IDS/IPS system automatically detects protocols such as HTTP on any port and apply the proper detection and logging logic. This greatly helps with finding malware, and command and control channels. The system can log HTTP requests, log and store TLS certificates, extract files from flows, and store these to disk. The full packet capture (PCAP) support allows easy analysis. All this makes Crystal Eye a powerful engine for your Network Security Monitoring (NSM) ecosystem. The system also allows you to match against most aspects of an SSL/TLS exchange within the ruleset language thanks to Suricata's TLS Parser, you can also log all key exchanges for analysis. Great way to make sure your network is not the victim of a less than reputable certificate authority.

The IDS/IPS engine features unified output functionality and pluggable library options to accept calls from other applications. The platform supports inline and passive traffic monitoring configuration capable of handling multiple gigabit traffic levels As a multi-threaded engine, the Crystal Eye IDS IPS system offers increased speed and efficiency in network traffic analysis. In addition to hardware acceleration (with hardware and network card limitations), the engine is build to utilise the increased processing power offered by modern multi-core CPU chip sets.

The IDS/IPS will be tunable via the security dashboard and the alert analysis report feature. This functionality enables fine tuning of the module with visibility of the implications of any changes. As such administrative load and guesswork typically associated with IDS/IPS tuning will be drastically reduced.

The protocols and capabilities employed by the IDS/IPS are shown in Table 4.

4.3.1 MultiThreading

The CrystalEye system supports a range of configurations options to enhance the performance of the security features it provides. The MultiThreading configuration option allows users to increase the number of threads that are allocated to IDS/IPS tasks. CrystalEye's MultiThreading feature can be configured to use a single thread, up to dozens of threads for IDS and IPS processing. This flexibility allows future product releases to take advantage of new hardware configurations. The MultiThreading feature enables the CrystalEye system to scale both vertically and horizontally as the resources of the system are used optimally.

In addition to the configurable number of threads that can be used for IDS/IPS tasks, the CrystalEye supports the Suricata CPU affinity feature. CPU affinity allows the user to specify specific CPU cores

Table 4: Engines and capabilities employed by the IDS/IPS

TCP/IP Engine	**Detection Engine**	**HTTP Engine**
Scalable flow engine	Protocol keywords	Stateful parser
Full IPv6 Support	Multi-tennancy	Request logger
Tunnel decoding	Xbits - flowbits extension	File extraction
Teredo	PCRE support	File identification
IP-IP	Rule profiling	File logging
IP6-IP4	File matching	Per server settings
IP4-IP6	*File magic*	Keyword mach on
GRE	*File size*	*URI/URL*
TCP streams	*File name*	*Headers*
Tracking sessions	*File extension*	*Raw headers*
Stream re-assembly	*File md5/checksum*	*Cookie*
IP defragmentation	*Pattern matching*	*User-agent*
	Live rule reloads	*Request body*
	Delayed rule initialisation	*Response body*
		Method
		Status
		Host

Protocol Parsers		**Packet Acquisition**
IPv4	HTTP	High Performance
IPv6	SSL	*AF_PACKET*
TCP	TLS	*PF_RING*
UDP	SMB	*NETMAP*
SCTP	SMB2	Standard Capture
ICMPv4	DCERPC	*PCAP*
ICMPv6	SMTP	*NFLOG*
GRE	FTP	*IPS mode*
Ethernet	SSH	*NFQueue (Linux)*
PPP	DNS	*ipfw (BSD)*
PPPoE	Modbus	*AF_PACKET (Linux)*
Raw	ENIP/CIP	*NETMAP*
SLL	DNP3	
VLAN		
QINQ		
MPLS		
ERSPAN		

that the IDS/IPS processing will occur on, and how the work load should be distributed between them. Doing so ensures that the IDS/IPS engine does not overload the available resources on the CrystalEye system. Additionally, the feature ensures that excessive CPU cores do not go underutilised.

In order to reduce the technical burden on users, the CrystalEye product will come with a number of run modes that can be used to configure the performance features, including MultiThreading and CPU affinity. These pre-baked modes, will provide a good set of defaults that are sufficient for most users, but also serve as a baseline configuration template for power users to tune to their needs. More advanced users can make use of completely customised configurations, to optimise performance for their specific needs.

4.3.2 IP Reputation

The IP reputation engine enables for rules to be created based on the reputation of the sender or receiver of individual packets. Databases of scores relating to the reputation of IP addresses are kept to track malicious actors on the Internet. These reputation scores can be leveraged by IDS/IPS systems to classify whether communicating devices are malicious or otherwise.

When a connection is made with the system the reputation score of the source and destination addresses are checked. If the reputation score check fails, then the connection can be terminated before any malicious activity takes place. The reputation engine classifies hosts both individually and based on the CIDR ranges to which they belong.

The platform receives IP reputation data from a central database hosted by the Red Piranha SDN. These updates occur automatically at a specified interval. New reputation information is committed to the device in-situ without requiring a reload. As a result, the device can act on new reputation information immediately without interruption to the device.

Through the use of this system it is possible to preemptively block hosts with poor reputation from interacting with sensitive services, enabling a proactive approach to traffic filtering.

4.3.3 Protocol Analysis and Content Filtering

Deep packet inspection is utilised to enable inspection of web traffic, including encrypted traffic. The platform can be configured to have multiple filter configurations to provide varying degrees of web filtering to different groups of users. The content of web traffic is examined to target phrases, request and response headers, URLs, etc. This method is in contrast to other engines which simply rely on a centralised repository of URLs and corresponding classifications. In addition to this the platform employs antimalware functionality, with the capability to scan and block content classified as malicious in real-time.

The protocol analysis and content filtering mechanisms support the following features:

- SSL Inspection
- NTLM and persistent connection support.
- Digest authentication support
- Basic authentication support
- IP authentication support
- DNS authentication support
- Header analysis and manipulation - you can also manipulate cookies -
- Large file (2GB+) download & scanning support
- Whitelist domains and URLs
- Blacklist domains and URLs

- Greylist domains and URLs
- Deny regular Expressions on URLs, body content, and headers (also in greylist mode)
- URL regular expression replacement so you can for example force safe search in search engines
- Deep URL scanning to spot URLs in URLs to for example block images in Google images
- Advanced advert blocking
- Many performance improvements
- Updates to handle all current web technology trends
- Blanket SSL blocking so you can block SSL anonymous proxies (without using SSL Bump)
- Limit POST size (upload)
- Temporary bypass provides a "click to acknowledge" capability
- Referrer Exceptions Exceptions based on URL in referring URL
- Time Based Blocking

4.4 Network Control

The Network Control menu allows administrators to configure various components of the CrystalEye appliance. A list of network control features that are provided by the Crystal Eye platform are described below:

- **Certificate Manager** - Allows users to manage the CrystalEye appliance's SSL/TLS certificates and private keys, including those used for the certificate authority.
- **Device Management** - network map shows in the security dashboard but also here allowing a visual on nodes in the network and mapping of devices to end users etc
- **Email Scanning Gateway** - Allows for appliance to be set up as complete email scanning gateway to help prevent malicious emails from reaching users.
- **Infrastructure** - The Infrastructure menu allows users to configure various network infrastructure components of the CrystalEye platform, such as the DHCP server, DNS Server, IP address information, and SSH Server.
- **VPN** - The VPN menu allows for setting up of virtual private networks (VPNs). The VPN configuration supports site-to-site and remote access VPN technologies.
- **Web Proxy** - Allows users to configure the Crystal Eye appliance as a web proxy. Web proxies can be used to intercept website requests from users, filter content that does not comply with the organisation's acceptable use policy, and save bandwidth using content caching technologies.

4.5 Compliance Controls

The CrystalEye platform is designed around security compliance. A list of compliance controls provided by the Crystal Eye platform are provided below:

- **Security Plan Wizzard** - The Security Plan Wizzard aims to guide novice users through secure configuration of the CystalEye device to meet specific requirements. The Security Plan Wizzard will be used in conjunction with risk audit functionality.
- **Vulnerability Scanning** - Vulnerability scanning allows users to manage vulnerabilities in their networked devices by periodically scanning for known software vulnerabilities. Vulnerabilities scan results are cataloged and can be included in reports for compliance auditing and risk management.

- **Network Backup** - The network backup feature allows CrystalEye systems to backup and restore the configuration. Backups can be stored on the device, on removable media connected to the device, or off-site devices. A backup schedule can be created to ensure frequent backups are maintained. Multiple backup features are provided by the CrystalEye:

  - *BackupPC* - Allows single nodes to use the CrystalEye appliance for a local backup solution.

  - *Forensic logging* - Allows logs to be backed up to offsite locations such as cloud services or data storage blockchain systems.

  - *Database backup* - the Database backup application allows for direct backups of the databases. Support to backup offsite to remote storage locations (such as cloud services).

  - *Network Fileshare Backup* - The network fileshare backup feature allows other devices to backup to the CrystalEye platform.

- **PCAP Snap** - Allows scheduled transfer of captured network traffic to be transmitted to Red Piranha servers for automatic analysis and manual examination where warranted.
- **Incident and Event Services (SEIM)** - Enables transmission of incident and event data to the Red Piranha SIEM server. This functionality allows for remote monitoring services via a managed service to be offered by Red Piranha.
- **Data Loss Prevention** - Allows a user to create document audit trails and tag confidential documents that are to be blocked from being transmitted. An alternate use for this toolset would be alerting on transfer of canary documents, thus allowing for the detection of data exfiltration attempts.
- **Risk Auditing** - The risk management system is tied into the cloud dashboard and aims to provide basic ISMS support and aid in generation of more formal risk scores. This functionality aims to support a future cyber insurance product to be offered by Red Piranha.

4.6 Reports

The CrystalEye platform provides a number of reports to assist with diagnostic, monitoring, and network maintenance tasks. A list of reporting features provided by the Crystal Eye platform are described below:

- **App Status** - The App Status page displays all of the applications and modules that are installed on the CrystalEye platform and their associated statuses. Where applicable modules can be started or stopped using this feature.
- **Disk Usage** - Provides a visual representation of proportional disk usage on the platform. This feature allows administrators to easily identify problems in the case of high disk utilisation.
- **Events and Notifications** - provides a way for other apps to listen for events that occur on the system, such as invalid logins against platform services. Events can be acknowledged by an administrator in order to clear them. This section allows for easy tracking of which events have and have not been reveiwed. This feature will enable bulk reporting and email notification tasks to be undertaken.
- **Gateway Scan Report** - The Gateway scan report app provides a tabular display about content filter and virus scan results. This section allows administrators to gain a rapid understanding of the current threat environment.
- **Log Viewer** - Provides a tabular display of all system log files. Administrators are able to view and search log files. The examination of log files is an essential first step when investigating platform or network issues.

- **Network Detail Report** - Provides a summary of network information including the most active users, external hosts, internal hosts, and device types. This information can prove useful when identifying and addressing high volume usage or capacity issues.
- **Network Report** - Provides real time monitoring of network throughput on each network interface. It is important to monitor network throughput to identify throughput issues or undertake network capacity planning tasks.
- **Risk Report** - The risk reporting module will track risks, allows management oversite of identified risks, and allows for examination of risk trends. This section will provide comprehensive support to risk analysis and planning activities.
- **Protocol Detail Report** - Will provide reports summarising the network usage, these reports are broken down by protocols, devices, and traffic classification.

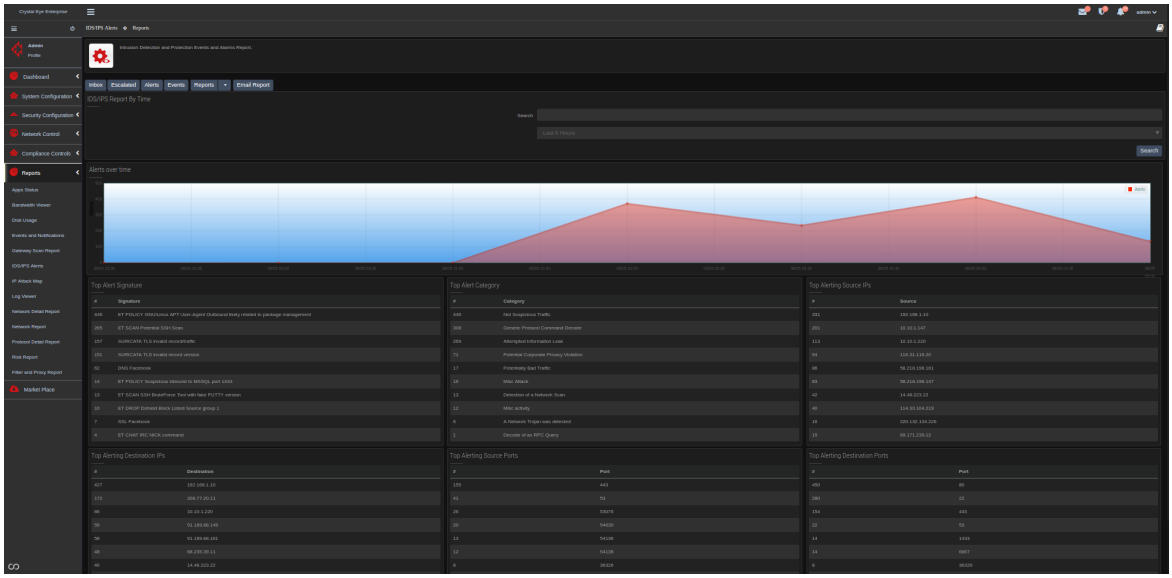

Figure 3: The Alert Dashboard allows users to view alerts and generate reports in the CrystalEye product.

4.7 Deployment Options

Red Piranha will deploy the Crystal Eye software product on a range of platforms to suit different network and application needs. The proposed hardware appliance models provide excellent value, with hardware specifications at least double those of the current market leaders, at a similar price point. Managed platforms and cloud deployments through mechanisms such as Azure and AWS appliances allow for the platform to be implemented effectively on cloud or hybrid cloud networks.

Virtual and hybrid networks are becoming increasingly commonplace as additional network infrastructure is outsourced to cloud platforms. In these implementations it can be difficult or inefficient to implement existing UTM solutions, as these assume they are placed on the physical network boundary. In the situation where network boundaries exist across both physical and virtual infrastructure there is a need for flexible deployment of security devices. The CrystalEye platform can be deployed on existing hardware, virtual infrastructure, or as a dedicated appliance. As such SMEs will be able to logically position the CrystalEye solution on all network boundaries, regardless of the infrastructure model in use.

5 Product Security

The auditors undertook an initial technical security review of the Crystal Eye platform in Q1 2017. The security review was a grey-box vulnerability assessment of the Crystal Eye product. The auditors assessed the security of the product from an unauthenticated and authenticated perspective in an effort to identify security flaws in the product.

During the course of this review there were no pre-authentication vulnerabilities identified. The auditors provided a number of recommendations to improve the security, functionality, and user experience of the Crystal Eye platform. These changes are being implemented in accordance with a continuous integration and improvement program. The continuous integration and improvement program is a best-practice approach that is key to the integrity and security of the Crystal Eye product. It is the opinion of the auditors that the product deployed meets or exceeds the the security standards of the UTM SME market.

Naturally, it is not possible to predict technological changes which may undermine the security of all products of this category or those including any particular technology product. However, based on the auditors observations of Red Piranha, the auditors are confident that security issues discovered with the Crystal Eye product will be addressed in a timely fashion as they emerge.

6 Conclusion

Peter Hannay and Clinton Carpene conducted a security audit of Red Piranha's Crystal Eye appliance. The audit was performed with the intention of verifying and validating the features and performance and security of the Crystal Eye platform. The biggest strength of the CrystalEye product pertains to its feature integration. The Crystal Eye product offers consumers a comprehensive range of security functions that typically would require multiple discrete appliances in a single platform. These features include; SIEM, firewall, IDS/IPS, backup, DLP, and more. In our opinions, the platform introduces sophisticated controls aimed at meeting basic information security compliance needs.

The CrystalEye platform incorporates a next-generation IDS and IPS system based upon the open-source Suricata IDS. The IDS/IPS configuration in the CrystalEye platform is simplified to reduce the administrative burden of managing a complex IDS/IPS installation. As a multi-threaded engine, the Crystal Eye IDS IPS system offers increased speed and efficiency in network traffic analysis, this MultiThreading feature enables the CrystalEye system to scale both vertically and horizontally, allowing for potential use in higher end corporate deployments. The platform will also provide reporting and tuning options that will drastically reduce administrative load when compared to other IDS/IPS implementations.

In addition to the IDS and IPS controls, the platform provides advanced packet inspection capabilities. Traditional firewalls typically filter network traffic by inspecting the source and destination addresses. The CrystalEye platform introduces a sophisticated application layer firewall that can filter traffic based upon information available within data at the application layer.

The importance of compliance controls is often understated within the SME market, with more focus on traditional perimeter security. This oversight represents a huge risk to the operation of core businesses within such organisations. Compliance and auditing tasks may be not implemented adequately due to cost constraints or lack of appropriate resources to deal with complex implementations. Red Piranha provides support for these tasks through the use of a collection of services and controls implemented in the UTM product. These technologies are enabled through increased hardware capacity and architecture decisions when compared with competing products. Technologies such as SIEM, DLP and backups, which are enabled via the platform are an important factor when dealing with business disrupting events such as ransom-ware attacks.

The platform provides various mechanisms to reduce the administrative burden placed on IT staff, the most significant of these are the two dashboards which provide at a glance details of the state of the device and the network threat landscape. In addition the dashboards will provide the ability to perform common tasks such tuning network security controls and enabling/disabling various feature

sets. These features provide both technical detail and 'eye candy' which should prove attractive to potential customers.

The Crystal Eye operating system and Red Piranha's service delivery network (SDN) is in a position to offer a range information security controls often not accessible to the SME market due to cost constraints and the complex nature of management of these controls. Additionally, in conjunction with the built-in application marketplace, the CrystalEye platform promises to be extensible and capable of providing future extendability.

The auditors determined that the Crystal Eye platform meets or exceeds the industry standard for unified threat management (UTM) products in the categories of features offered, system performance, and device security. The Crystal Eye product allows users to monitor and manage cyber threats to their systems through a single console. It is the opinion of the auditors that the Crystal Eye product would be a significant asset to a small or medium sized enterprise. Furthermore the framework of the CrystalEye operating system leaves potential for Red Piranha to develop its products further and expand into future markets for home users and larger corporate environments.

7 Glossary of Terms and Abbreviations

- **Authentication**: The processing of credentials to establish the legitimacy of an identity claim.
- **AWS**: Amazon Web Services, a cloud services platform provided by Amazon.com Inc.
- **Azure**: A cloud services platform provided by Microsoft.
- **Blacklist**: A list of items to which access will be denied.
- **Certificate**: A token, usually consisting of a public or public/private key-pair, used to establish the authenticity of one or more parties involved in a communication.
- **DHCP**: Dynamic Host Configuration Protocol is a protocol that allows a server to provide some basic configuration to networked devices (including IP address, DNS servers, etc.).
- **DLP**: Data-loss prevention is a system that prevents unauthorised disclosure of data.
- **DNS**: Domain Name System, the system which translates addresses such as example.com to IP addresses such as 93.184.216.34.
- **Endpoint**: Individual client systems within a network, examples include desktops, laptops, and mobile phones.
- **Exfiltration/Exfiltrating**: The transmission of sensitive data from a compromised network to a location under attacker control.
- **Firewall**: A technology which filters network connections based on criteria such as origin IP address, destination IP address, origin port, and destination port. A firewall will typically provide options for connections that match criteria, including drop, pass, deny, log, and alert.
- **Greylist**: Greylisting provides a means to initially deny connections, allowing them after a period of time. Greylisting is normally employed with the idea that malicious actors will not retry a connection if it fails initially. As such this concept provides a filter of sorts to reduce the number of malicious connections, while still allowing legitimate connections.
- **IDS/IPS**: Intrusion detection system/Intrusion prevention system. Systems used to detect or prevent cyber attacks by analysing network traffic.
- **MITM**: Man in The Middle refers to any technology which places itself between the client and server in order to intercept traffic.
- **PCAP**: Packet Capture, the term refers to a full record of all network communication, saved in a specific format to enable analysis.
- **Phishing**: The act of sending fraudulent emails that utilise deception in order to obtain information such as usernames, passwords, or financial data.
- **SIEM**: Security information and event management. A system that is used to gather and correlate security event data.
- **SME**: Small-to-medium enterprise.
- **SSH**: Secure Shell refers to a protocol used to remotely make use of computer systems via a TCP/IP connection. SSH was created as a secure replacement for the Telnet protocol.
- **SSL**: Secure Sockets Layer, a technology used to provide encryption to various communication protocols. SSL is often used as a generic term to refer to both SSL and TLS.
- **TCP/IP**: Transmission Control Protocol / Internet Protocol, the core suite of protocols on which the Internet is built.
- **TLS**: Transport Layer Security is a technology that provides encryption to various communication protocols. TLS is intended as a replacement for SSL.
- **UTM**: Unified threat management. A system that aggregates a number of security functions such as firewall, IDS/IPS, VPN, etc.

- **VPN**: Virtual Private Network, a class of technologies which provide an logical equivalent to local network access via a remote connection.
- **Whitelist**: A list of items to which access will be allowed, these often override anything present in a blacklist.

References

[1] CSO Online. Cybercrime damages expected to cost the world 6 trillion by 2021. [Online]. Available: http://www.csoonline.com/article/3110467/security/cybercrime-damages-expected-to-cost-the-world-6-trillion-by-2021.html

[2] ——. Cybersecurity spending outlook: 1 trillion from 2017 to 2021. [Online]. Available: http://www.csoonline.com/article/3083798/security/cybersecurity-spending-outlook-1-trillion-from-2017-to-2021.html

[3] ABC. Biggest ransomware outbreak in history hits nearly 100 countries with data held for ransom. [Online]. Available: http://www.abc.net.au/news/2017-05-13/biggest-ransomware-outbreak-in-history-hits-nearly-100-nations/8523102

[4] J. Turner. Small business risks being left behind in australia's virtuous cyber security plans. [Online]. Available: https://amp-afr-com.cdn.ampproject.org/c/s/amp.afr.com/technology/web/security/small-business-risks-being-left-behind-in-australias-virtuous-cyber-security-plans-20170515-gw4w6b

[5] Gartner. Gartner says worldwide information security spending will grow 7.9 percent to reach 81.6 billion in 2016. [Online]. Available: http://www.gartner.com/newsroom/id/3404817

[6] J. Vijayan. Information security spending will top 101 billion by 2020. [Online]. Available: http://www.darkreading.com/operations/information-security-spending-will-top-\protect\T1\textdollar101-billion-by-2020/d/d-id/1327178

[7] Gartner. Market guide for network access control. [Online]. Available: https://www.gartner.com/document/3708117

[8] ACSGN. Cyber security sector competitiveness plan. [Online]. Available: https://www.acsgn.com/wp-content/uploads/2017/04/Cyber-Security-SCP-April2017.pdf

[9] K. Omotosho. Fortinet: The road to market dominance begins. [Online]. Available: https://seekingalpha.com/article/4065612-fortinet-road-market-dominance-begins

[10] Gartner. Magic quadrant for unified threat management (smb multifunction firewalls). [Online]. Available: https://www.gartner.com/document/3746429

[11] Australian small business key statistics and analysis. [Online]. Available: https://www.treasury.gov.au/~/media/Treasury/Publications%20and%20Media/Publications/2012/Australian%20Small%20Business%20-%20Key%20Statistics%20and%20Analysis/downloads/PDF/AustralianSmallBusinessKeyStatisticsAndAnalysis.ashx