



CYBERHOUND

Unique Capabilities for Business





CyberHound

CyberHound is a leading provider of innovative internet compliance, management and security solutions. We provide organisations with unique, real-time social media governance and security controls with predictive outcomes and tangible business benefits.

Established in 1999, CyberHound is part of the Superloop Group, an independent provider of connectivity services across the Asia Pacific region.

All in One Solution

Reliable internet connectivity is the lifeline of business, however this connectivity also creates complex security issues. Business owners and leaders need to ensure they are able to protect themselves against Malware (particularly ransomware), internal threats, internet outages, while also avoiding breaches.

CyberHound can supply an 'all-in-one' solution to help address all of these concerns. More information can be found at cyberhound.com or by calling 07 3020 3330.



Cyber Security
& Internet Optimisation



BYOD Enablement



Advanced Web Filtering



Social Risk Management



Support & Professional Services



Models, Platforms & Sizing



Cyber Security & Internet Optimisation



The internet has become a critical conduit for people to create, communicate and collaborate. Organisations of all types rely on internet connectivity to enable the people in their organisations to interact with clients and stakeholders, to research, to publish, and to connect with people across the hallway or around the world.

Since 1999, CyberHound has been delivering internet management and web optimisation systems that enable organisations to leverage the benefits of the internet. These systems are designed to make the internet more reliable, cost-effective and easier to use. Our solutions including firewalls, secure web gateways and advanced web filtering through to social media governance and compliance platforms that reduce the risks associated with accessing the internet.

Security at the Edge

Your CyberHound system can work at the edge of your network providing the Next Generation Firewall and security capabilities required to protect your organisation's information. The CyberHound Appliance in this mode acts as a Unified Threat Management (UTM) system providing IT teams with a single easy-to-use web interface for all internet security functions. Critical connectivity systems including advanced firewall rules, network address translation, port forwarding, intrusion prevention, virtual private networking (VPNs) and email gateway services are easily implemented to securely connect your organisation to the internet.

Additionally, your CyberHound Appliance can be positioned behind existing routers and/or firewalls. In this mode the CyberHound Appliance acts as a Secure Web Gateway (SWG) providing your organisation with best-in-house internet authentication, URL filtering, quota management and proxy services. Whether the CyberHound Appliance is deployed as a UTM or SWG, CyberHound's unique pattern matching technology for internet searching, instant messaging and social media is available to protect your staff.

Internet Link Optimisation

CyberHound not only secures internet connectivity for organisations, we also optimise this connectivity. Our PipePlus system enables an organisation to use multiple internet links to provide additional bandwidth to that site while at the same time providing critical link redundancy that ensures high availability internet access. Some CyberHound customers have combined many low cost internet services to deliver a large aggregated connection. Others use PipePlus to back up their main fibre-based connection with a wireless or low cost copper-based service.

Internet Download Optimisation

Internet usage is continuing to grow particularly in light of cloud-based services, rich media and applications. CyberHound has created an innovative method to reduce large file downloads. For organisations with Apple iOS devices (iPads, iPhones, iPods) and Mac OS X computers, the Apple 'App Store' is now the default way for downloading and updating operation systems and applications. Likewise Adobe's Creative Suite is now also delivered as a cloud-based subscription model (Creative Cloud).

The internet acceleration transparently (and automatically) caches Apple, Adobe and Microsoft software downloads and updates. These downloads can range in size from just a few MBs through to several GBs. A recent operating system upgrade was in excess of 4GBs. The Large Object Cache greatly enhances the speed of these downloads and updates, and significantly reduces the load on the internet connection enabling other applications and services to be accessed without impact.

The CyberHound Content Acceleration Platform now also caches YouTube videos, preserving internet bandwidth for mission critical applications.

With major iOS updates now over 1GB in size, the benefits of preventing every user downloading these updates from the internet are obvious. For many customers this also saves money and provides enhanced confidence in network performance. Other services, such as VoIP and Digital Media services can be embraced without these internet risks.



BYOD Enablement



Most organisations today provide Wi-Fi access to managed networks for devices such as smart phones, tablets and laptops. These devices may be supplied and managed by the organisation or increasingly may be user-owned or 'Bring Your Own' (BYO) devices. Traditional corporate owned and managed device scenarios see IT teams spending extensive resources ensuring a robust and reliable standard operating environment (SOE) for PCs and devices.

In BYOD scenarios the main network and security architecture needs to be even more robust to cater for the multitude of device types. Additionally, since the IT teams have almost no control or management of the devices being connected to their networks, user authentication and management become paramount to ensure compliance with network and internet usage policies.

Rapid 'No-touch' BYOD On-boarding

CyberHound enables simple self-service authentication for BYO devices, including CyberHound's 'on-boarding' process, which ensures security certificates are seamlessly installed and enabled. This allows for powerful management and reporting options for unmanaged devices and facilitates https inspection filtering. The reporting options include internet usage and bandwidth quota management, web content filtering, and real-time moderation and management of social media applications, including IM and enterprise collaboration tools.

Seamless Authentication

CyberHound's solution provides seamless (user-based) authentication to deliver the ultimate user experience whilst providing powerful security and reporting. Seamless authentication refers to authenticating a user once, without prompting for their details again. CyberHound's patent pending 802.1X pass-through authentication module works in partnership with existing directory services to provide single-sign on functionality for users of secure managed wireless networks together with the ability to enforce internet usage policies across all internet and Web 2.0 traffic.

Extending Security Beyond the LAN for all Mobile Devices

Critical to both BYOD and traditional managed devices is the need to extend security controls to devices when they leave the managed network. CyberHound has a small software agent for MS Windows and Apple OS X devices that provides the ability to extend web filtering and social media management controls to devices wherever and however the device connects to the internet. The agent is tamper-resistant and also provides reporting and alerting data.

Advanced Web Filtering



With the rise in popularity of web sites that provide information on almost everything and anything, organisations of all types and sizes have enabled internet access for users across their network. It's hard to imagine not being able to just 'Google it' to source some information you may need.

Unfortunately, amongst the useful and productive sites are the useless, distasteful and productivity-sapping sites. Beyond productivity, the organisation must also consider their duty-of-care to the users on their network, ensuring that their network is used only to view or download appropriate content.

CyberHound's premium Category Web Filtering, which is included in the Corporate Bundle enables organisations to implement and enforce a flexible policy to ensure inappropriate or unproductive content is reliably blocked and the internet is used productively.

The Category Web Filtering system provides organisations with a simple way to implement web URL filtering. Selecting one or more of the many pre-defined categories enables organisations to decide which web sites may be accessed.

Policies can also be set at a very granular level. This can give organisations the ability to grant different access rights to different groups. For example a marketing team may require different access to content than what the administration department requires. These policies can also be set up by time of day. A full reporting and alerting solution is included for compliance reviews and audits.

The technology has more than 200 million users globally contributing to the categorisation of URLs, so organisations can be confident that most URLs are already categorised. The system also has more than 500 million websites categorised including 100% categorisation of the top one million websites. Each CyberHound Appliance is updated automatically from the 'cloud' in real-time ensuring users only gain access to appropriate content while not being blocked from legitimate content. Any CyberHound Appliance can be upgraded seamlessly to include Category Web Filtering within the existing service, and can be managed within the current user friendly web interface.

Unique Controls for Off-Network Devices

For organisations that supply devices to staff, CyberHound has the ultimate solution. Our agent is highly secure (i.e. it cannot be removed or bypassed) and it can be used to enforce group and time of day rules for web and social media use.



Social Risk Management



Social media use is almost ubiquitous within organisations today, both via official communication channels and unofficially via employees and other stakeholders. Facebook, Twitter & LinkedIn are quickly becoming common for both business and personal use. While organisations are looking for ways to harness the power of social media the associated risks are becoming more evident with examples proliferating the news each day.

Risks

Many organisations have already experienced the damage and costs associated with inappropriate or ill-considered social media posts. A few years ago a common strategy may have been to block social media, but today most organisations are instead choosing to leverage social media, both for official use and general use by employees, customers and other stakeholders.

The risks associated with social media for organisations include:-

- Brand and reputational damage from inappropriate or ill-considered posts
- Reduction in employee productivity
- Leakage and loss of private or confidential information
- Personal and organisational identity theft
- Workplace bullying, discrimination, defamation and harassment
- Vicarious liability.

CyberHound uniquely provides organisations with a suite of proven tools to effectively manage social media and reduce the growing number of associated risks. The platform is built on patented technology and is being used by organisations around the world to address the risks associated with social platforms and web applications.

ClearView®

ClearView® is CyberHound's unique Social Risk Management Platform that allows organisations to seamlessly and flexibly monitor, manage, filter and report on all common social media. This includes instant messaging, search engines and webmail application use through a suite of granular controls. Rather than blocking or limiting popular communication tools such as Facebook, LinkedIn and Twitter, CyberHound's unique platform enables real-time policy matching and compliance enforcement across the organisation.

Social Information Governance

CyberHound's unique platform enables organisations to include social information risk management in their governance programs. The platform provides granular control over employee social media access as well as content posted and read in social media conversations and discussions.

Organisations can now regain control over the use of social media. Granular policies can be set to prevent issues arising from inappropriate communications on social media.

Social Information Compliance

While organisations are increasingly recognising the benefits and risks associated with social media, they are also experiencing an increasing level of regulatory compliance and legislation associated with social media use. These requirements are impacting publicly listed companies, government agencies, not-for-profit organisations, schools and private companies.

The growing list of regulations include reporting and disclosure requirements, privacy law compliance and employee duty of care and safety obligations. In many jurisdictions directors and management are held directly responsible for cyberbullying via social media that directly impacts staff and other stakeholders.

The CyberHound Social Information Platform provides the ability to manage these risks in a positive way. This means that organisations can still enjoy the corporate networking and communication benefits from social media and staff can still be granted access to social media.

Secure Archive

The Platform includes a unique archive integration capability to ingest communications into supported Enterprise Information Archive platforms. This can be delivered by push technology (using SMTP) or by a fetch service (using XML) from the archive platform. Communications can be delivered with threading (for greater contextual value), de-duplication and all necessary metadata to ensure value from the data and digital sustainability.



Support & Professional Services



CyberHound prides itself on delivering outstanding service to our customers. Our extensive suite of services range from installation and technical consultancy through to business process re-engineering and systems design. All services are provided by qualified CyberHound team members and/or CyberHound Certified Partners.

Implementation Services

Implementing a CyberHound Appliance in your organisation starts with an initial scope of work. We make a point of understanding each customer's individual requirements and tailoring a solution to these needs. We also make a point of only promising what we can deliver – and our culture is one of aiming to delight our customers by going the extra distance at every opportunity.

Our Customer Service Managers work with you to formalise the implementation of your solution with a detailed plan that ensures the installation meets everyone's expectations. Our Post-Implementation Ambassador program means that the engineer who installed your solution will be available for any further help and assistance that you may require to ensure the implementation is a success.

System Health Checks

CyberHound recommends a professional Health Check service be performed periodically. This ensures the configuration is optimised and all of the latest capabilities are being utilised within the solution. The Health Check service provides valuable time-saving and productivity benefits with an integrated training component.



Our CyberHound solution has provided the benchmark for what we expect from all of our ICT solutions. It worked fabulously right from the get go and enabled us to address our major concerns immediately.

Terry Chenery, CEO, **Link Up NSW**



Ongoing Support

Whether you're a CyberHound customer or one of our trusted partners, you can be sure of ongoing quality support.

The help documentation in each CyberHound Appliance provided in context to our customers. CyberHound also actively provides regular news updates, webinars and web forums.

Managed Services Support Option

CyberHound is able to provide a fully Managed Service with the CyberHound Platform. This ensures the platform is optimally managed with any changes being implemented quickly and professionally by CyberHound removing administrative and technical burdens for our customers. The service can be used to supplement in-house expertise when team members are on vacation or involved with other projects.

It offers the highest level of support for a customer and provides services directly from the solution developer, ensuring the highest level of competency and knowledge. Changes are requested via an online change request form and can be scheduled in advance as required.

Models, Platforms & Sizing



Platform Flexibility

Each CyberHound Appliance is configured according to your needs and your existing network environment. CyberHound has four on-premise platform options:-

- CyberHound Mini small format appliance
- Rack mount server (H Series)
- High performance / redundant rack mount server (HR Series)
- Virtualised using VMware /HyperV (2012 R2)

In addition to these on-premise solutions, each CyberHound Appliance can be deployed in private or public cloud environments. CyberHound also offers fully managed cloud-based services for web and social media management (see CloudControl®).

Multi-site Organisations

The CyberHound Appliance is commonly deployed by organisations with many locations. CyberHound Appliance Branch servers automatically connect to a central server and all other Branch servers to create a mesh network. All CyberHound Appliances can also be set to have firewall rules and policies replicate to ensure uniformity of rules and policies across the organisation.

Model Flexibility

The CyberHound Appliance can be configured as a full edge device providing IP routing, firewall, web security, and network management functionality, or the system can be configured to perform a subset of specific functions like social media content filtering or web filtering alongside existing routers, firewalls and content management systems.

CyberHound has three CyberHound Appliance server options:-

- Unified Threat Management (UTM)
- Secure Web Gateway (SWG)
- Branch (BR).

Unified Threat Management (UTM)

CyberHound's UTM solution is a multifunction internet management and security server. This model includes all Secure Web Gateway functionality (below) along with an advanced stateful firewall and traffic shaping. The UTM model can be deployed at the edge of your network and can directly connect to wide area networks including internet access links.

Secure Web Gateway (SWG)

The Secure Web Gateway provides an extensive internet security and management functionality. This functionality includes virtual private network (VPN) support, transparent and direct proxy support, URL

filtering, email gateway, user authentication and quota management, malicious software filtering and application controls for common web applications. The system also includes advanced reporting capabilities that provide alerts along with scheduled and advanced 'drill-down' ad-hoc reporting.



CyberHound provides us with the ultimate confidence our network is protected. The team have been and continue to be very professional and all our support requirements are answered promptly.



Paul Barlow, ICT, Link Up NSW

Branch (BR)

CyberHound's Branch server is a cost-effective dedicated remote office gateway that is configured to work in partnership with a host CyberHound Appliance UTM or SWG server. The Branch server automatically creates a secure and optimised VPN connection to the host server and other Branch servers in its private network. The Branch server reduces network administration by enabling central configuration of network policies at the host server.

Users	Platform Options	Model Options
15, 30	Mini, Virtual	(NG UTM)
50, 100, 200, 500	H Series, Virtual	NG Unified Threat Management
500+	HR Series, Virtual	(SWG) Secure Web Gateway
N/A*	Mini, Virtual	(BR) Branch

*The Branch server user count is considered in the central CyberHound Appliance server.

Premium Features

CyberHound has several premium features that provide additional functionality for CyberHound Appliance deployments. Please contact CyberHound to see how ClearView®, Category Web Filtering, PipePlus, YouTube Cache, MS Exchange Plug-in, the RoamSafe Agent and others can complement your CyberHound Appliance.

Reverse Proxy

The CyberHound system includes a reverse proxy with support for HTTP and HTTPS, and mapping between either. This feature allows seamless sharing of several servers on a single port and exposing HTTP internal servers securely on the public internet via HTTPS.

The initial support from CyberHound to implement the system was tremendous, and this great level of service has continued for over 8 years now. The tech guys are always very helpful.

Chris Morahan, IT Manager, The Colleges' Information Technology Group

All of our expectations were exceeded. The CyberHound Appliance is very easy to manage and the results were very impressive. We had no hesitation in purchasing the CyberHound Appliance.

Hellen Ryan, Assistant & Human Resources Manager, Hervey Bay RSL

