Advanced Threat Protection Suite

CYBERHOUND

CORPORATE

Advanced Threat Protection Suite

Protecting Your Networks

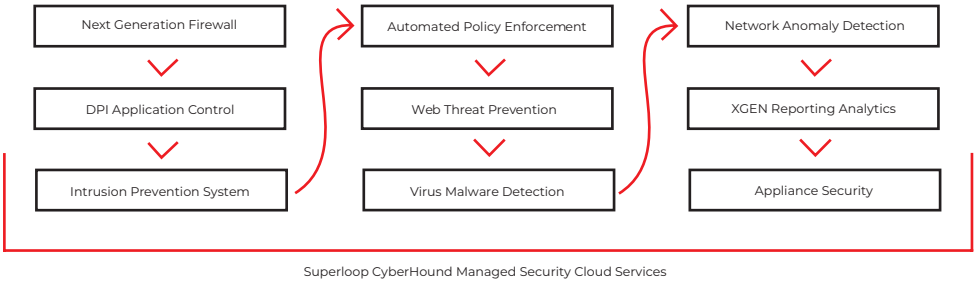
Superloop's CyberHound has invested millions of dollars in developing a unique security solution for businesses. Every aspect of our solution and service has been designed to meet the specific needs of the market.

CyberHound has developed one of the most advanced sets of multi-layered 'defence in depth' security platforms to deliver reliable cybersecurity.

This platform now sets the benchmark for security coupled with the extensive set of additional features within the Unified Threat Management or Secure Web Gateway solutions.

These are all supported and updated by CyberHound's Managed Security Cloud Services - all delivered securely from the most secure data centres in Australia.

9 Layers of Security



Firewall

Next Generation Firewall delivers application aware firewalling to the enterprise with inbuilt controls for the identification and control of evasive technologies such as anonymisers, VPNs, proxies and more.

This mature and evolving core capability of the CyberHound platform boasts flexible configuration for network, port, application, protocol, time of day, group and custom date range.

Optimised for high throughput networks up to 10 Gbps it now also includes new advanced Application Controls.

Category Web Filtering

Advanced category web filtering provides 500+ categories of content to ensure granular access to online digital content in real-time.

Categorization is informed by over 600 million users globally and 4 trillion queries a month, and uses a combination of machine learning and 24×7 human quality assurance to maintain access and acceptable use policies in real time.

This includes URL, IP and page level detection of emerging exploits e.g. malware, phishing, fraud, botnets and zero day threats.

Virus & Malware Protection

Next generation technology identifies new threats with highly accurate detection and prevention of malware pre-execution.

This provides protection from system and memory based attacks as well as scripting, spear phishing and malicious programs.

Traffic is scanned using the latest virus and malware signatures available that are updated daily, ensuring the best protection for the network.

Application Control

Superloop CyberHound's Unified Threat Management (UTM) Series Appliance delivers enhanced application control utilising scalable Deep Packet Inspection (DPI) technology resulting in prevention of malicious content, external threats and inappropriate activity.

1600+ application signatures with regular updates are seamlessly analysed through layers 3 to 7. Our IPS identifies applications in as few as 3 packets allowing early packet discard (e.g. in cases of malware) and enables granular application visibility, monitoring and control.

Intrusion Prevention System

High performance flow-based Intrusion Prevention System (IPS) delivers advanced threat protection by inspecting network traffic for exploits and vulnerabilities.

Our IPS includes hyperscale architecture with real-time threat detection prevention and detection including malware and zero day identification.

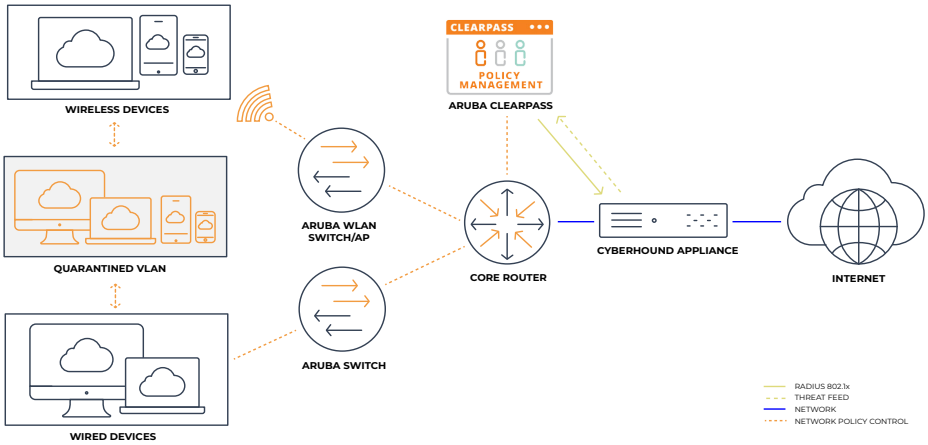
With 12,000+ rules, weekly updates and advanced GeoIP controls, live monitoring and historical reporting and analytics that can be integrated with third party SIEM providers, our IPS provides protection against the latest known and unknown threats.

Aruba ClearPass

Aruba ClearPass extends a network's security capabilities by utilising CyberHound's IPS threat intelligence feeds to manage infected devices and apply automated policy enforcement.

Our certified integration with Aruba ClearPass enables automated actions based on threat severity, category and your customised policies.

Block and remove users from the network as well as automatically move infected devices to a quarantined network with custom block messages. See diagram below for more information.



Network Anomaly Detection

Active scanning of network traffic for anomalous behaviour, brute force detection, prevention and alerting as well as Botnet alerting and known threat detection enhances network protection, including in BYOD environments.

Plus IP based connection rate limits are able to be set to further ensure network security.

XGEN Reporting

The XGEN Reporting platform contains a centralized repository incorporating live data collected from the various layers of network traffic for easy to use reporting, alerting and analysis of data.

Data includes 5 major sources across network monitoring, firewall activity, IPS data, virus and malware detection and GeoIP events and more.

XGEN Reporting also includes template best practice reports, admin access audit logging and integration to third party tools and SIEM providers.

> **"We are proud to partner with Superloop CyberHound to accelerate their innovative, vertically-focused solution built on HPE ProLiant DL360 Gen10 servers, the industry's most secure industry-standard server."**

Philip Spiessens, Senior Director, Global OEM, Aruba

Data Privacy Protection

Data protection and privacy is much more than just security, it requires control over services providers, data location, access and support.

Superloop CyberHound is owned by Superloop, an Australian Telecommunications provider subject to extensive legislation to protect customer data and networks and is fully compliant with the Australian Privacy Act.

All data used for cloud Managed Security services is hosted in tier 3 data centres in Australia with full data encryption.

Appliance Platform

CyberHound's HPE appliance platforms (Gen10) boasts the world's most secure industry standard server platform.

HPE's iLO Advanced Premium Security includes run-time firmware validation, unique silicon "root of trust" protection for BIOS and firmware updates, prevention against firmware and BIOS attacks and automated recovery capabilities.

HPE's iLO also provides other advanced monitoring capabilities. HPE's platforms offer best-in-class performance and value for schools.

Support

We provide the highest level of support from experienced technical experts, based in Australia, with deep expertise in our technology and school network requirements. We also provide proactive service reviews to ensure optimal use of the technology. All hardware appliances are provided through our OEM partnership with HPE and are custom built for performance and in-built hardware reslience. These are backed up by 24x7x4 on-site hardware support (subject to HPE terms).

Managed Security Services

Our Managed Security Services ensures real-time security updates are provided seamlessly to our customers with zero downtime or need for local administration.

These updates are managed from our secure cloud service infrastructure that also includes secure configuration backups in the event of a critical restore.

CyberHound's security updates cover all aspects of the Advanced Threat Protection Suite and utilise global and local threat intelligence feeds in combination with our security partnerships with leading cybersecurity service providers.

Deployment Options

Most customers deploy the CyberHound solution as a physical on-premise appliance using one of CyberHound's tested appliance range.

We also support VMware (5.0+) and Hyper-V (2012 R2+) for virtualised environments and can recommend appropriate resource requirements.

The Micro platform is supported directly by CyberHound with return to base warranty.

The CyberHound platform can be hosted in private or public clouds and we also offer hosting services and full managed service options.

MICRO	H-SERIES
Up to 100 Users	Up to 400 Users
Quad-core Embedded Platform	Intel Quad-core E3 Xeon CPU
8GB RAM	16GB Ram
120GB SSD Storage	2 x 200GB Hot Swap SSD Drives, Raid 1 Storage
6 x 1Gb Ethernet Ports	4 x 1GB Ethernet Ports (expandable to 6)
	Single Power Supply + 2 x Fans
HR-SERIES REDUNDANT	
400 to 1,000 Users	Intel Octa-core E5 Xeon CPU
32GB Ram	2 x 480GB Hot Swap SSD Drives, Raid 1 Storage
6 x Hot Swap Fans	Optional 2 x 10GB Cat6e Ethernet or SFP+ Ports (expandable to 6)
Redundant How Swap Power Supplies	HPE iLo Systems Management Suite

Additional Services

Added Benefits

Superloop is one of Australia's leading Internet and managed services providers.

Many CyberHound customers are already benefiting from a broad range of services available from the Superloop Group. Superloop is also one of nbn™'s largest partners in Australia and has built a backhaul network to every nbn Point of Interconnect (all 121) with additional services available at the edge.

As a large international service provider Superloop also offers low latency from its network to cloud services in and outside Australia.

Service Summary

- Fibre Internet services, including additional capacity
- Fixed Wireless Internet services for redundancy or cost-effective additional capacity
- Point to point links between buildings
- nbn™ connections at up to 1 Gbps (symmetrical) with excellent SLAs
- Phone and voice solutions
- WiFi solutions - including fully managed options
- International connectivity through our subsea and Asia-Pac fibre assets

Superloop has become a strategic and trusted partner to many organisations through the provision of critical services and the excellent support network it offers.