

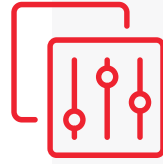
# Application Control

---

CYBERHOUND

# All New Application Control Engine

## Enhances Next Gen Firewall



Superloop's CyberHound UTM Series Appliances will now deliver an enhanced Next Generation Firewall with an all new Deep Packet Inspection (DPI) and Application Control Engine for high throughput networks.

The service supports thousands of users and is suitable for even the largest school networks. This ensures controlling access to Cloud hosted and SaaS based applications. Furthermore, applications can be controlled by user group, source, time of day, data and more.

### At A Glance

- Highly scalable application classification fast flow at speeds up to 10Gbps.
- Multi-instance engine with live application update support and hardware acceleration technologies.
- Application Flow replication for high availability deployments.
- Early packet discard mechanism.
- Enhanced metadata such as codec and bit rates to be used to enhance customer experience and network security.
- 1600 + applications with bi-weekly application signature updates.
- Identifies applications at Layers 3 through 7.
- Service ID for visibility of audio, video, file transfers and more.
- Classification of networking protocols and applications based on flow, pattern matching, bi-directional flow correlation, heuristics and statistical analysis.
- Single packet ID for many network based applications.

CyberHound's latest enhancements to its Next Generation Firewall offer new features and benefits. These continue to provide Superloop customers with the best K12 security, filtering and Internet management services in the industry.

---



## Early Packet Discard System

---

Customisable early packet discard mechanism provides handling for burst application loads during periods of high network load.



## Application Updates

---

Applications and their protocols change constantly and without notice. Superloop provides a secure path to reliable, always up-to-date DPI technology utilising constant telemetry and data analysis. Updated application signatures are deployable on-the-fly, without service interruption, on the scalable CyberHound appliances.



## MetaData Extraction

---

Superloop's new metadata extraction technology provides powerful insights into network traffic for enhanced visibility across the enterprise. Information such as application name, categorisation, protocol type, user, source IP and more are easily visible via the XGen reporting platform.



## Application Signatures

---

With over 1600 applications signatures, we can accurately identify traffic and match against extensive signature libraries that are updated and expanded regularly.

These contain applications such as VPN's, anonymisers, proxies, domain fronting services, social media, messaging platforms and content servers as well as platforms including G Suite and Microsoft Office 365.



## Performance

---

Architected from the ground up for scalability, allowing for data processing at speeds up to 10 Gbps per core (on Intel architecture) with multi-thread support of up to 96 cores and hardware acceleration components.



## Deployment Flexibility

---

CyberHound Micro, H Series, HR Series, HR2 / HR3 Series and Virtual Appliances are all supported.

# Solution Architecture

## Advanced Features

---

Superloop's CyberHound platform's new architecture provides advanced packet processing, accelerating and offloading configuration options for optimal integration with packet flow manager.

Switchable IP defragmentation and TCP flow reassembly allows for packet reordering to deliver enhanced application speed and performance.

Optional packet pre-filtering. Depending on application requirements, all packets or only a subset of packets are parsed by the engine ensuring optimal application efficiency.

## Flow Diagram

---

