

## MANAGING ISLAND HOPPING CYBER VULNERABILITIES FOR SCHOOLS

Schools today face ever growing threats from sophisticated cybercriminals. These bad actors are exploiting any network vulnerabilities including any devices connected or being added to the network. A good example is the risk posed from Internet of Things devices that often have limited or very basic security controls.

In addition to these known threats a growing threat is posed for schools through a technique known as “island hopping”.

In this scenario cyber criminals look to access a school's otherwise secure network through a less secure supplier or partner. This is often a service provider who legitimately retains access to the school's services but does not maintain the high security standards of a school and becomes a soft target for cyber criminals to “hop” through to your environment.

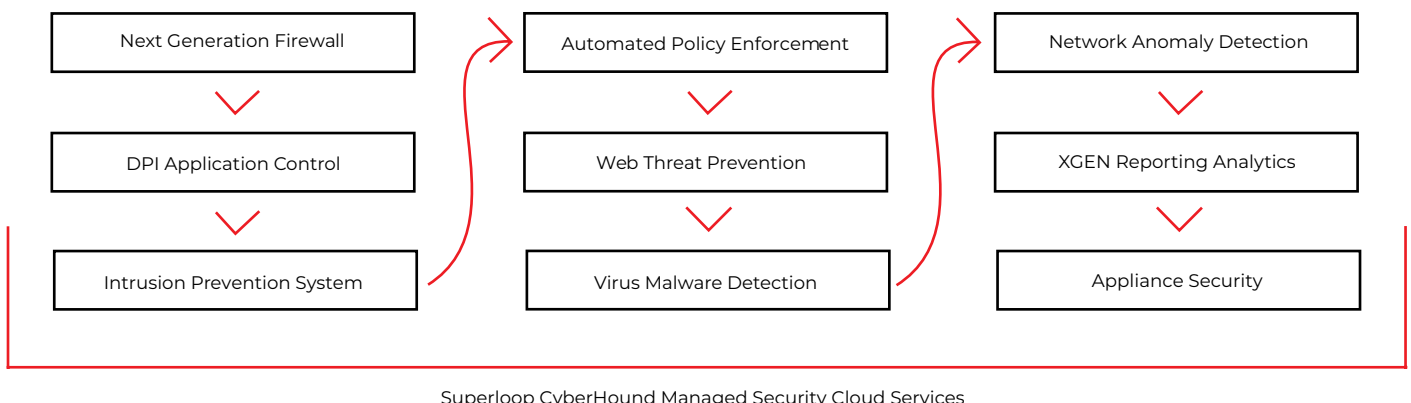
Schools must now look beyond the firewall and advanced security technology it deploys at the network level to manage the growing threat from these other forms of cyber attack.


This is where the CyberHound solution stands out - not only in providing its Advanced Threat Protection Suite - a multi-layered set of 9 independent layers of network protection tools, but also in providing the ultimate protection of its own services.

“Recent hacks of managed service providers (MSPs) are an example of this, where cyber criminals have been exploiting weak account credentials to access systems installed by MSPs to launch ransomware attacks.”

VMware Carbon Black

### CyberHound's 9 Layers of Security





“50% of cyber attacks now use  
island hopping.”


VMWare Carbon Black

## The Superloop Trusted Network Advantage

CyberHound is a wholly owned subsidiary of Superloop; an ASX listed Telecommunications company and a significant infrastructure provider. As such we are bound by stringent Australian legislative and compliance requirements including the Telecommunications Sector Security Reforms (TSSR) which is led by the Australian Government's Critical Infrastructure Team. This imposes strict obligations on us to protect our network and facilities and to maintain appropriate supervision and control over all of our infrastructure.

The risks have never been greater. Once a cybercriminal gains access to a school's network the risks are high. They gain lateral movement and can cause substantial financial and service threats including:

- > Ransomware
- > Data Theft
- > Financial Crime
- > Extortion
- > Network Denial Of Service
- > Reputational Damage



“These (island hopping) compromises  
are extremely difficult and sometimes  
impossible to detect.”

Joint report - National Cyber Security Centre & National Crime Agency, UK

# Industry Leading Protection

## Protecting School Networks



Superloop is a leader in protecting schools from island-hopping attacks by delivering a highly secure environment for our network, web-facing services and all the infrastructure we use to deliver managed security services for schools. This, coupled with CyberHound's Advanced Threat Protection Suite on the school's network, provides the ultimate level of protection in preventing cybercrime. These layers of protection, on and outside the school's network, form essential protection that ensures the integrity of the weakest element in a school's network - i.e. from a weakness in a supply chain partner.

### Key recommendations:



#### Protection of all web facing services and infrastructure

All services are delivered through Superloop's Australian based private cloud, hosted in dedicated Superloop racks within Tier 3 datacentres in Australia and are subject to the Australian Government's high standards of protection and supervision.



#### Real-time Threat Intelligence Feeds

We have direct access to the Australian Government's Cyber Emergency Response Team's services and real-time updates designed to support Telecommunications companies delivering Nationally significant infrastructure.



#### Active monitoring across our entire network and facilities using the latest services and technologies, including AI

We run Network Intelligence Platforms across our core network that identify malicious activity in real-time. Vulnerabilities are immediately scrubbed from our network using industry leading and automated DDoS protection platforms. This ensures zero hour protection for all Australian services.



#### Deployment of self-learning AI-based Intrusion Detection System technology

Running on our secure management infrastructure, this AI technology alerts us automatically to suspicious activity and behavioral changes, providing real-time intelligence and insights for our internal security team.



#### Regular independent security reviews

We conduct regular penetration tests of our infrastructure, including the CyberHound technology and its service delivery platforms. External security audits are also conducted by independent firms and we run independent real-time analysis and benchmarking of all our web-facing services.



#### Dedicated Chief Information Officer

With a specialised security team to provide ongoing assessment and management of our security obligations. This is supported by a Chief Risk Officer and formal risk management review process by the Board.



#### Resource Public Key Infrastructure (RPKI) network security

We are one of the first in Australia to secure our network using RPKI for secure BGP routing. This helps prevent BGP route leaks and hijacks using advanced cryptographic methods.



#### ISO 27001 certified

Demonstrating Superloop's commitment to the highest security standards.



#### Incident Management Response Team

This team has been established to respond to any threats or incidents.



# Principles of Supply Chain Security

## Ensuring and Maintaining Control of your Supply Chain

Key recommendations:

- **Establish control** - Communicate your view of security needs to your suppliers. Set and communicate minimum security requirements for your suppliers. Build security considerations into your contracting processes and require your suppliers do the same. Meet your own security responsibilities. Raise awareness of security within your supply chain. Provide support for security incidents.
- **Continuous improvement** - Encourage the continuous improvement of security within your supply chain. Build trust with suppliers.
- **Understand the risk** - Understand what needs to be protected and why. Know who your suppliers are and build an understanding of what their security looks like. Understand the security risk posed by your supply chain.
- **Check your arrangements** - Build assurance activities into your approach to managing your supply chain.

It is anticipated that the Australian Government will introduce new cybersecurity standards and minimum levels of protection following the recent National State attacks. Superloop is continually evolving its defence in depth posture for customers and will be in the best position to support CyberHound's school customers to ensure ongoing protection and peace of mind.

"Attack frequency has reached unprecedented levels; 94% of security professionals said the volume of attacks they faced has increased. Attackers are employing a more diverse range of tactics and techniques than ever before as they bid to extort, disrupt and infiltrate organizations. Island hopping was the fourth most common cause of breaches."

**VMware Carbon Black Australian Threat Report**

"Time and again, CrowdStrike observed successful intrusions in environments where security controls were in place that could have successfully blocked attacks, but were not configured by the organization to do so or were not fully deployed across the environment. Smart organizations will spend the time needed to maximize the protection they gain from existing security controls."

**CrowdStrike 2020 Global Threat Report**

"By maintaining the best cyber security hygiene across our own network and critical infrastructure we provide assurance to our customers that a Superloop solution can assist to lower their own cyber risk. We continue to invest significantly beyond the levels required to ensure we protect our customers from supply chain risks."

**Andrew Lawrence, CIO, Superloop**

"We have picked up several threats that could have been devastating if it weren't for the power of the CyberHound technology. I hate to think what could have happened as a result of a ransomware attack or having malicious actors operating within our network, given the sensitivity of data we hold."

**Adam Ryan, Infrastructure & ICT Manager, Ballarat Clarendon College**