CYBER SECURITY
FOR SCHOOLS

High performance networking and cyber safety

The AARNet Cyber Security for Schools service has been created for AARNet Direct Connect schools with the objective of integrating high performance networking and cyber safety.

We take a portfolio approach to service development, partnering with specialist security vendors to develop cost-effective interoperable solutions that meet the unique needs of K-12 Schools. AARNet is a telecommunications carrier, which means that schools also benefit from our ability to apply security controls, such as DDoS detection, at the perimeter of our global network.
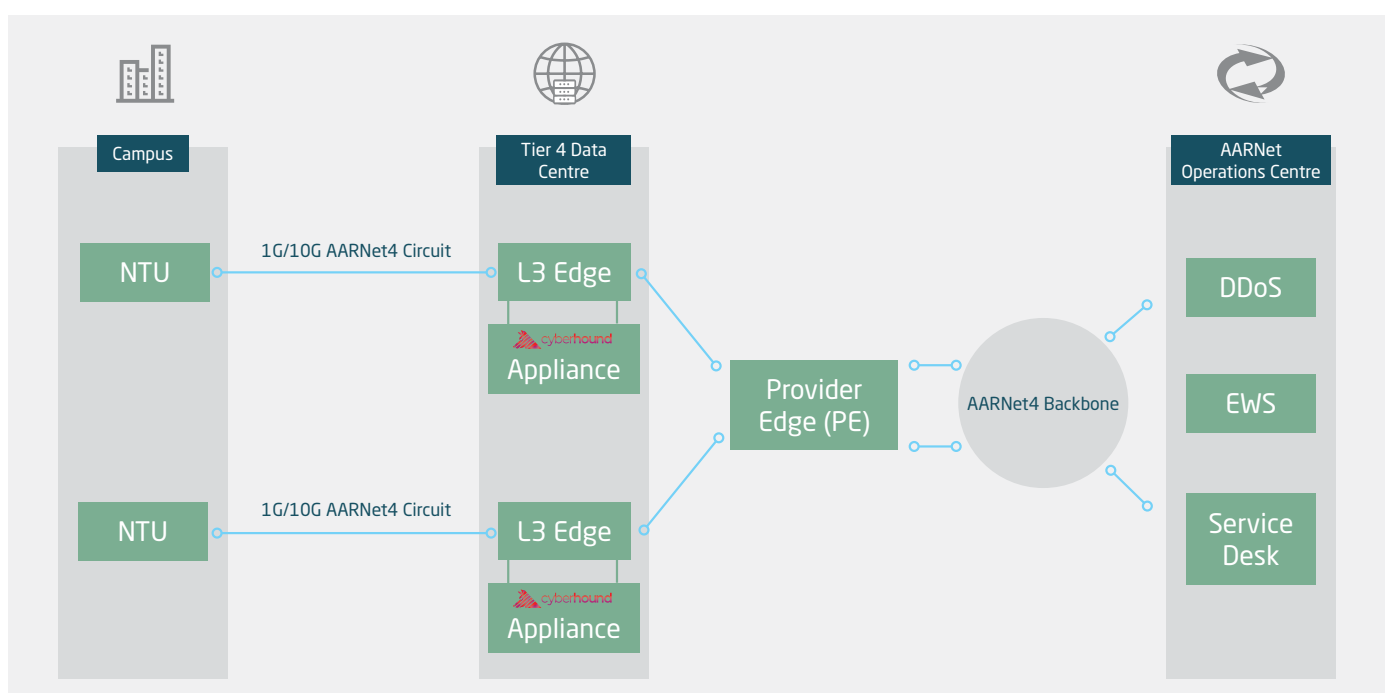
The Cyber Security for Schools service portfolio is offered as a shared responsibility model. AARNet provisions and operates the underlying infrastructure and service platforms and provides schools with the training and tools they need to manage their own policies, self-service reporting and other day-to-day security operations.

Fast and reliable connectivity

Schools typically start with a 1 Gigabit per second (Gbps) direct fibre connection to the AARNet backbone with a growing number of schools now opting for 10 Gbps and diverse connections as they adopt greater usage of cloud-based services for day-to-day operations and curriculum delivery. The network resilience that diverse connections provide is increasingly becoming a mainstream requirement.

Firewall, content filtering and behavioural analytics

The CyberHound Unified Threat Management solution (UTM) provides cyber security, cyber safety and a range of tools to enable reliable internet management, reporting and behavioural analytics, and in-class controls for teachers. CyberHound's UTM provides a highly effective level of security and protection for a school's community and assets.

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, optimised for high throughput networks up to 10 Gbps.

Intrusion Prevention System

High performance flow-based Intrusion Prevention System (IPS) delivers advanced threat protection by inspecting network traffic for exploits and vulnerabilities. With 12,000+ rules, weekly updates and advanced GeoIP controls, protection is provided against the latest known and unknown threats. Automated network protection and policy enforcement is via ClearPass integration.

Virus and malware protection

Traffic is scanned using the latest virus and malware signatures available ensuring the best protection for the network. Daily signature updates are provided as part of the service and automatically enabled.

Category web filtering

Advanced category web filtering provides 500+ categories of content to ensure granular access to online digital content. Categorization is informed by over 600 million users globally and 4 trillion queries a month and uses a combination of machine learning and 24x7 human quality assurance to maintain access and acceptable use policies in real time.

XGen reporting

The XGen reporting platform contains a centralized repository incorporating data collected from the various layers of network traffic. Data includes internet and application usage, malware and virus events, GeoIP events, network utilisation, content analytics and more.

LiveZone portal

LiveZone provides teachers and students a real-time dashboard view of data from their web-based activities. Data includes website and content breakdown as well as access to YouTube video usage by title, category and views.

Classroom control

Classroom Control allows teachers to maximise productivity, student focus and learning by providing in class tools to manage access to content for individual students. With individual Classroom Controls and variable time options, teachers can allow certain web pages and whole sites that may otherwise be restricted, or even turn off all internet access as required.

SpeakUp

SpeakUp is an easy-to-use self-service portal that provides a safe and secure way for students to inform school leadership of important welfare matters such as bullying, cyber-bullying, physical threats, self-harm and more.

ClearView

ClearView scans and analyses internet traffic usage logs to identify indicators of student behavioural or welfare risk, providing the requisite visibility of internet activity to support a school in enforcing nominated duty of care policies.

RoamSafe

RoamSafe prevents students from accessing inappropriate material on iOS devices away from school. Ideal for Primary and Middle School.

Layer 3 edge network integration

Offered as an optional integrated service, the AARNet engineering team will design, optimise and manage the network integration for the AARNet Cyber Security Services for Schools, including dynamic BGP failover, HA scenarios, performance tuning and monitoring.

Security infrastructure monitoring

The AARNet Operations Centre monitors environmental and performance metrics of related service infrastructure. This approach provides for a more efficient and pre-emptive service support function.

Support

The AARNet Operations Centre provides a single point of contact for all AARNet network and security services issues and support.

What our customers are saying

"The level of experience and knowledge really instilled confidence and allayed any apprehension for us transitioning to such a critical service. The service levels subsequent to the implementation have been second to none and of the highest levels we have experienced in any service arrangement".

Adam Ryan, Infrastructure and ICT Manager at Ballarat Clarendon College.

DDoS Protection

Using AARNet's extensive international and domestic network of border routers, real-time traffic analysis and automated application of DDoS mitigation can occur in seconds with our DDoS Protection service, significantly faster than most current commercial offerings. Legitimate traffic is unaffected, following its normal route, without limitation or disruption to your network's performance.

Early Warning System

The AARNet Early Warning System (EWS) compliments the DDoS Protection service by providing early notification of issues affecting the performance of the network. Schools nominate critical services, such as a public website or learning management system, for monitoring by our EWS system. Our Operations Centre is alerted when a nominated service at a customer site is not responding or meeting expected performance metrics, allowing AARNet and customer teams to respond more quickly to DDoS threats and other incidents impacting network availability.

Customer Success consultancy

AARNet's engineering consultancy service provides schools with cost-effective remote and on-site assistance and professional advice for security and network design and deployment requirements. The AARNet Customer Success team assists schools in achieving an optimal and timely ROI in onboarding AARNet security services.

Choose the option that suits you:

	Standard	Enhanced
Secure Web Gateway	✔	✔
Layer 7 firewall	✔	✔
Category Web Filtering	✔	✔
L3 Edge w/NAT/SNAT/PAT	✔	✔
Intrusion Prevention System	✔	✔
Aruba ClearPass Integration	✔	✔
Content Reputation Analysis	✔	✔
Certificate Authority	✔	✔
BYOD Certificate Onboarding Service	✔	✔
SSL Decryption & Inspection	✔	✔
Captive Portal	✔	✔
Active Directory Integration	✔	✔
RADIUS Authentication	✔	✔
XGen Reporting	✔	✔
YouTube Analytics	✔	✔
DDoS Early Warning System		✔
Volumetric DDoS Detection		✔
Behavioural Analytics		✔
Real-time Classroom Analytics		✔
Office 365 Email Scanning		✔
Social Media Policy Enforcement & Auditing		✔
Classroom Control for Teachers		✔
Fully Managed/Hybrid Deployment Options	✔	✔
Service Training & Orientation	✔	✔
AARNet4 Consolidated Billing	✔	✔

More information

Find out more about the AARNet Cyber Security for Schools service at aarnet.edu.au
or contact our Customer Relations team: CustomerRelations@aarnet.edu.au

aarnet
CONNECTING K-12