untangle

K-12 NETWORK SECURITY CHECKLIST

K-12 schools have a unique challenge when it comes to network security. First, they must have an adequate network setup that includes proper infrastructure and solutions to proactively block and prevent hackers and threats from infiltrating the network. Second, they must ensure students and teachers have adequate bandwidth to optimize online learning tools and solutions. Thirdly, they must adapt to all the bring-your-own-devices (BYOD) brought onto the campus by students and guests, while still maintaining control over what those devices can access when they connect to the school's network. And finally, schools need to maintain CIPA compliance by blocking students from accessing inappropriate content on websites and applications. If you have a large IT team and unlimited resources, tackling these challenges is simple. However, most schools have small IT teams and very strict budgets to adhere to, so costly and complex solutions to solve these challenges are not acceptable.

Schools can take some simple steps to stay ahead of evolving threats and hackers, while also maintaining CIPA compliance and ensuring the network always stays up and running for critical online learning tools.

☐ **Update Software**
Maintaining software updates for all devices is crucial to ensure any vulnerabilities found are swiftly mitigated.

☐ **Lock Down Administrative Control**
By preventing students and teachers from downloading applications that could house malware, you can minimize the exposure and protect the network.

☐ **Separate Backups**
Always have backups of critical data in a separate location. In the event of a malware or ransomware attack, schools can quickly get their data and configurations restored without paying the ransom.

☐ **Separate Network for Guest/student Devices**
By separating the main school network from all the guest and student devices that you don't control, you can quickly mitigate any issues that may happen on the guest network without impacting the school network's performance.

☐ **Captive Portal to Gain Visibility to Guest/student Devices**
Use a Captive Portal page that requires users to log in before gaining access to the network. You can then create rules and policies for what those devices can access while connected.

☐ **Threat Intelligence**
Utilizing solutions that have built-in threat intelligence engines that proactively protect against unknown and emerging threats is critical for schools to stay protected against hackers and malware.

☐ **Next-generation Firewall**
Next-gen firewall solutions provide protection at the gateway in an all-in-one solution that encompasses web content and application filtering, bandwidth shaping, advanced threat protection, and VPN connectivity options.

☐ **Reporting**
Data-driven reporting is a key aspect for schools to showcase their CIPA compliance. Ensure reporting include detailed audit logs of every traffic event occurring on the network.

Untangle NG Firewall provides network security capabilities integrated with robust policy management tools that enable school IT administrators to monitor, protect and control their networks while also providing protection from evolving threats.

- Gain visibility into all the devices connecting to the network
- Stay secure with advanced threat protection from malware, spam, phishing and emerging threats
- Block students from accessing inappropriate content
- Ensure network bandwidth is optimized for learning
- Create detailed reports to prove CIPA compliance

Untangle offers special pricing for qualified private and public schools. Contact us today to learn more.

ABOUT US

Untangle is the most trusted name in solutions specifically designed to help small-to-medium businesses and distributed enterprises optimize their networks while safeguarding their data and devices. Untangle's Network Security Framework provides cloud-managed security and connectivity options that work together seamlessly to ensure protection, monitoring, and control across the entire digital attack surface from headquarters to the network edge. Untangle's award-winning products are trusted by over 40,000 customers and protect millions of people and their devices. Untangle is committed to bringing open, innovative and interoperable solutions to its customers through its rapidly growing ecosystem of technology, managed services, and distribution partners worldwide. Untangle is headquartered in San Jose, California.

Untangle, Inc.
25 Metro Drive, Ste. 210
San Jose, CA 95110
www.untangle.com

For sales information, please contact us by phone in the US at +1 (866) 233-2296 or via e-mail at sales@untangle.com.