ARISTA
Edge Threat Management

Data Sheet

Securing Networks and Protecting Students for K-12 Schools

edge.arista.com

Keeping Students & Staff Safe Online

Online assessments, web-based learning tools, and mobile devices are driving the future of K-12 education. Network administrators have tried costly network upgrades to increase bandwidth and expand the efficacy of their Wi-Fi networks, but have found these efforts insufficient.

Unfortunately, most schools still use legacy web filters that are ineffective and inflexible when it comes to allocating what network resources users, apps and devices have access to. Customers choose Arista for next generation web filtering which includes application control, SSL inspection and bandwidth management, along with the ability to block, flag and alert on search terms, enforce safe search, and log YouTube searches, readying classrooms for the demands of the 21st century.

Special Pricing on Arista Software

Public Sector pricing is available to qualifying state and local government institutions, public schools and libraries. This package contains the same software as NG Firewall Complete and Micro Edge, but at a greatly reduced rate.

Nonprofit pricing is available to qualifying not-for-profit institutions, NGOs, private schools and religious organizations. This package contains the same software as NG Firewall Complete and Micro Edge, but at a greatly reduced rate.

K-12 Network Security Checklist

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.

□ 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 includes detailed audit logs of every traffic event occurring on the network.

K-12 Case Study

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.

Brown County Schools

Location: Nashville, Indiana
Industry: K-12 Schools
Size: 2,000+ students and teachers
Challenges:

- Current solution too expensive
- Constantly exceeded device limit of appliance
- CIPA compliance
- Needed solution to manage diverse network of six campuses in various locations

Results:

- Maintain and prove CIPA compliance
- Solution provides enough bandwidth and control for large network
- Separate student and teacher networks
- Used existing servers to save money

> *"The new user interface is a nice improvement. The Dashboard provides me with a quick view of my network."*
>
> **– David Phelps | Technology Director**

CIPA Compliance

CIPA Compliance relates to the Children's Internet Protection Act (CIPA), a federal law enacted by Congress to address concerns about access to offensive content over the Internet on school and library computers. CIPA imposes certain types of requirements on any school or library that receives funding for Internet access or internal connections from the E-Rate program – a program that makes certain communications technology more affordable for eligible schools and libraries.

What CIPA Compliance Requires

- Schools and libraries must also certify that, as part of their Internet safety policy, they are educating minors about appropriate online behavior, including cyberbullying awareness and response and interacting with other individuals on social networking sites and in chat rooms.
- Schools subject to CIPA are required to adopt and enforce a policy to monitor online activities of minors.
- Schools and libraries subject to CIPA are required to adopt and implement a policy addressing: (a) access by minors to inappropriate matter on the Internet; (b) the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications; (c) unauthorized access, including so-called "hacking," and other unlawful activities by minors online; (d) unauthorized disclosure, use, and dissemination of personal information regarding minors; and (e) restricting minors' access to materials harmful to them.

What is E-Rate

E-Rate is the schools and libraries program run by USAC to help these institutions provide telecommunications and Internet access to the communities they serve. Most K-12 public and private (not-for-profit) schools and public and private libraries are eligible to participate.

NG Firewall Helps You Make the Most of Your Broadband Investment

- Keep your network CIPA (Childrens Internet Protection Act) compliant with web content filtering and application control, as well as security measures for data privacy.
- Ensure quality of service (QoS) with bandwidth optimization and web caching, as well as the ability to block, prioritize or optimize traffic of all types.
- Get granular control over every challenging traffic type with layer 7 deep packet inspection (DPI), which gives you the ability to tackle challenging applications like BitTorrent and UltraSurf that may be inroads for malware and illegal downloads.

SPIN #: 143032755

Santa Clara—Corporate Headquarters
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-866-233-2296
Email: edge.sales@arista.com

Copyright © 2022 Arista Networks, Inc. All rights reserved. CloudVision, and EOS are registered trademarks and Arista Networks is a trademark of Arista Networks, Inc. All other company names are trademarks of their respective holders. Information in this document is subject to change without notice. Certain features may not yet be available. Arista Networks, Inc. assumes no responsibility for any errors that may appear in this document. October 19, 2022