FORTINET

SOLUTION BRIEF

Meeting CIPA Compliance with Fortinet

Excutive Summary

Schools are expected to keep their students safe, even with rapidly increasing numbers and types of devices connecting to their networks. While numerous attack vectors make complying with the Children's Internet Protection Act (CIPA) more complicated, pervasive Internet use by tech-savvy students make it more important than ever. Much has changed since CIPA was enacted by Congress in 2000, but the rules enforced by the Federal Communications Commission remain in place. Essentially, CIPA requires K-12 schools and libraries to certify that they are enforcing Internet safety policies, in order to be eligible for E-rate discounts.

Fortinet Solutions

Fortinet offers products that can help you achieve CIPA compliance, with E-rate discounts for your school or library.

FortiGate: Our E-rate eligible, next-generation firewalls deliver top-rated network security, as well as the ability to monitor your network and filter Internet traffic for inappropriate content in real time. Granular controls let you decide whether to allow, block, or partially enable Internet-based applications, such as Facebook, Twitter, and Skype, on an individual or group basis. Antivirus, intrusion prevention (IPS), and data loss prevention (DLP) add additional protection against malicious content, unlawful activities, and unauthorized disclosure.

FortiMail: Email is the most frequently used delivery method for malware. Our secure email gateways feature high performance, top-rated security effectiveness, and DLP.

FortiClient: Our endpoint protection platform delivers easyto-manage, automated, customizable antivirus, web filtering, application control, IPS, and more, for endpoints on- or offnetwork, including Chromebooks.

FortiWeb: Our web application firewalls (WAFs) monitor, allow, or block application traffic by categories. It can prevent the use of unwanted applications including proxy apps and HTTPS messaging apps.

FortiSandbox: Proactive advanced threat protection (ATP) stops the latest and most sophisticated threats

FortiGuard Services: Around-the`eat research and analysis provides regular updates to block new cyber threats and unsavory websites.

CIPA Requirements

Schools and libraries subject to CIPA are required to adopt a policy that addresses all of the following:

- Access by minors to inappropriate matter on the Internet and World Wide Web

- The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications

- Unauthorized access, including "hacking" and other unlawful activities by minors online

- Unauthorized disclosure, use, and dissemination of personal information regarding minors

- Access to materials harmful to minors. (Security measures must be able to block or filter pictures that are obscene or contain child pornography.)

How Fortinet Products Address Specific CIPA Requirements

CIPA Requirement	Addressed With
Prevent minors from accessing inappropriate matter on the Internet and World Wide Web	**Fortinet:** ■ Web filtering to block sites under inappropriate categories such as adult/mature content. ■ Manual website blacklisting to block webpages by keywords or URLs. ■ Safe search enforcement to rewrite search queries with Safe Search option to deliver child-appropriate results. **FortiWeb:** ■ Prevents the use of unwanted applications including proxy apps and HTTPS messaging apps.
Address the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications	**Fortinet:** ■ Antivirus to detect malicious attachments or file transfers over electronic communications. ■ Anti-spam, DLP to stop malicious or inappropriate content. ■ Web filtering to restrict social media and online communication sites **FortiSandbox:** ■ Sandboxing to stop advanced threats that evade traditional security measures. **FortiMail:** ■ Secure email gateway to protect from email-borne threats.
Prevent unauthorized access, including "hacking" and other unlawful activities by minors online	**Fortinet:** ■ Firewall to enforce access to other networks and Internet. User authentication can also be implemented. ■ Application control to prevent use of malicious or inappropriate applications. ■ IPS to detect and block unlawful activities.
Prevent unauthorized disclosure, use, and dissemination of ersonal identification information regarding minors	**Fortinet:** ■ Firewall to prevent unauthorized access to internal hosts. ■ Antivirus to mitigate malicious code infections that allow external control. ■ DLP to protect against servers and terminals from disclosing personal information. **FortiMail:** ■ Integrated, robust data protection to prevent disclosure of confidential information.
Address measures designed to restrict minors' access to materials that are harmful to minors	**Fortinet:** ■ Web filtering to blocks sites under inappropriate categories such as violent content. ■ Manual website blacklisting to block web pages by keywords or URLs. ■ Safe search enforcement to rewrite search queries with Safe Search option to deliver childappropriate results. **FortiClient:** ■ Device-level security and web filtering, IP reputation, and application control to keep students from accessing inappropriate sites, even when off the network. **FortiWeb:** ■ Prevents the use of unwanted applications including proxy apps and HTTPS messaging apps.

Visit Fortinet at http://www.fortinet.com/education or email us at education@fortinet.com for more information.

F⦂RTINET.