SONICWALL®

SOLUTION BRIEF

CARES Act Funding: How To Get Your Share.

Is your school leaving money on the table?

In 2020, the Homework Gap turned into the Schooling Gap. With the arrival of school closures related to the COVID-19 pandemic, virtually overnight the problem went from the inability of K-12 students to do homework due to a lack of internet at home … to students not being able to attend school at all.

Unfortunately, this is not an isolated problem. While previous estimates had put the number of children potentially impacted by the at 14 million, this proved to be a gross underestimate. At the beginning of the pandemic, the federal government tasked state governments with getting an accurate count of the number of students that lacked adequate and reliable internet access at home.

These studies revealed that the number of students impacted during COVID-19 was actually 21 million … a full 50 percent higher than previously anticipated.

In other words, with schools, after-school programs and public libraries all shuttered, nearly 40% of K-12 students were effectively cut off from public education.

To help address this inequality, the federal government passed the Coronavirus Aid, Relief, and Economic Security Act, also known as the CARES Act — which included funding to help schools ensure every child has an equal opportunity to learn.

Roughly $3 billion of the nearly $31 billion allocated to the Education Stabilization Fund through the CARES Act was set aside for the Governor's Emergency Education Relief Fund (GEER).

GEER funds were given to governors to help provide connectivity to students as quickly as possible, and covered everything and anything you need to create a remote learning environment, including a secure, remote learning environment.

This funding was needed because, during the pandemic, it was extraordinarily hard to ensure that opportunity without one-on-one device learning. Some children were only able to access the internet access from a parent's cell phone, which — aside from bandwidth limitations — may be unavailable a large part of each day while the parent is at work. In addition, many of the applications needed for remote schooling aren't available on all cell phones, if they're available on phones at all.

But schools also have responsibilities to their students beyond just ensuring access. According to the Children's Internet Protection Act (CIPA), every school is responsible for the safety of children while they're on the internet. Regardless of where students are accessing connectivity, schools still have to remain compliant with CIPA — a much bigger concern when EVERY child is at home and using the internet away from school supervision.

Unfortunately, this security aspect was largely set aside in the rush to ensure connectivity. Schools frequently came back online, only to have to shut down soon after — not due to COVID, but due to threats making their way into online classrooms. These attacks, both at the hands of students and outsiders, were made possible by a lack of security in the networks.

In March 2020, another fund, amounting to 13.2 billion, was set aside from the Elementary and Secondary School Emergency Relief Fund (ESSER Fund). These grants are awarded by the state educational agencies (SEAs) to offer local educational agencies (LEAs) — including charter schools that are classified as LEAS — with emergency relief funds to help address the impact that the pandemic continues to have on elementary and secondary schools. This grant can be used to fortify and expand a school's network and is not limited by solution or service.

In response to the ongoing crisis, the Coronavirus Response and Relief Supplemental Appropriations Act (CRRSAA) was passed in December 2020. CRRSAA provided an additional $54 billion infusion into the ESSER Fund, called **ESSER II.** Similar to the original ESSER Fund, ESSER II granted funds for SEAs, which in turn awarded grants to LEAs to address the impact of COVID-19 on elementary and secondary schools across the nation. These funds can be used to cover eligible costs dating back to March 31, 2020, the date that COVID-19 was declared a national emergency.

Eligible expenditures under ESSER II are similar to those under ESSER I, but the additional funding offers expanded uses and an expanded window for eligibility. In addition to the expenses allowed under ESSER I, ESSER II can also be used to prepare schools for reopening, address student learning loss (particularly among disadvantaged students), and the testing, repairing and upgrading of school infrastructure to improve air quality and reduce the spread of the virus.

Can My School Still Access This Funding?

While some have claimed from the beginning that states are keeping, redistributing or otherwise making unavailable the funding made available through the CARES act, these are only rumors. The federal government has dictated that 90% of the funding must go to schools, and every single school entity has a right to their piece of the pie if they get Title 1 Funds.

The money is allocated based on the amount of Title 1 funds your school was awarded in the previous year. This doesn't mean you'll lose your Title One funds — it means that, on top of that, you'll *also* get the same amount again in CARES Act funding.

If you haven't taken advantage of this funding allocated to help make your school safer and more connected, it isn't too late. And luckily, the process is probably a lot easier than you think.

Most every state is managing their funding through their statewide grant website. And while there is an application process, it isn't as complicated as you might imagine. However, the sooner you fill it out, the better: The deadline is September 30, 2022.

Why You Should Consider Upgrading Your Security Infrastructure

Keeping students safe online was hard enough when they were in the same room. Now they may not even be in the same *town.* While older students can be taught the basics of security awareness, it's often difficult at that age to understand the implications — so it's easy for kids to overlook suspicious URLs or emails in their rush to get their homework done.

And younger students, who may be accessing computers for things like beginning reading lessons, have no way of understanding complex topics such as ransomware and phishing. Unlike teens, young students cannot be counted on to provide any assistance in keeping themselves safe — it's all up to you.

Meanwhile, you're also faced with meeting all the school connectivity and security needs in a way that doesn't blow the budget and keeps costs as low as possible.

In the beginning of the pandemic, many schools made the numbers work by skimping on security. But doing so has never been a riskier proposition. Once cybercriminals realized that K-12 schools were protected with makeshift security — or in some cases, no security at all — they came out in force. **In 2020,** the number of publicly disclosed cybersecurity incidents affecting K-12 school systems rose by 18% over the previous year, according to a report published by the K-12 Cybersecurity Resource Center, K12 Security Information Exchange and K12 Six, a new nonprofit group.

Ransomware has continued to become a bigger problem for three main reasons. First of all, in many cases the attacks cause a loss in valuable classroom time that cannot easily be reclaimed. Some of these attacks resulted in school systems canceling both in-person and online classes. Secondly, the ransom demands themselves are rising, in many cases topping $1 million.

Worst of all, however, is that ransomware operators have begun selling the personal information of teachers and students to other cybercriminals. Data theft is also increasingly lucrative, with cybercriminals netting an average of $265 apiece for student records on the black market.

Unfortunately, sometimes even those that schools are attempting to protect are working to circumvent cybersecurity protections. In 42% of schools, students and/or staff are circumventing existing cybersecurity measures intended to help them — underlining the need for stronger security to both protect against outside and inside threats.

SonicWall Solutions for Secure Schools

SonicWall has developed a robust, end-to-end platform to secure remote education — all at a lower total cost of ownership.

The cornerstone of SonicWall's threat detection capabilities is our patented, reassembly-free deep packet inspection (RTDMI). This technology scans every port, every time, using machine learning to become extremely efficient at recognizing and mitigating cyberattacks, even those never seen by anyone in the cybersecurity industry. With a quarter of all attacks in 2020 coming over nonstandard ports, this has never been a more important part of stopping advanced threats. And RTDMI is much better at stopping these threats than other technologies on the market — in the first half of 2020, RTDMI identified 62% more malware than a traditional sandbox.

SonicWall Secure Mobile Access (SMA Series)

The centerpiece of the secure access solution for the education market, SonicWall Secure Mobile Access (SMA Series) is a powerful enterprise-class VPN that provides work-from-anywhere and on-any-device solution.

SonicWall Capture Client

Capture Client delivers next-generation malware protection and application vulnerability intelligence. It leverages cloud sandbox file testing, comprehensive reporting, and enforcement for endpoint protection.

SonicWall Content Filtering Service

Content Filtering Service supports web filtering policies from over 50 categories, controlling access to objectionable, unproductive and unsecure web content, even for devices off the network.

SonicWall Cloud App Security

Cloud App Security offers students, teachers and staff next-gen security within cloud applications, including email, messaging, file sharing and file storage. For schools adopting SaaS applications, SonicWall Cloud App Security delivers best-in-class security and a seamless user experience.

SonicWall Network Security Manager (NSM)

Network Security Manager offers school IT admins the ability to orchestrate all firewall operations, see hidden risks, discover misconfigured policies, and make compliance easier with a full audit trail.

SonicWall has been helping schools secure their networks at a lower total cost of ownership for decades. Our team of cybersecurity experts works with you to ensure the network you're providing to home classrooms is secure from end to end, all at a price you an afford.

Contact us to get in touch with an authorized SonicWall SecureFirst partner or SonicWall security expert.

If you have further questions about the CARES Act funding, please call the SonicWall CARES Hotline at 1-800-465-5251.

About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era and a work reality where everyone is remote, mobile and unsecure. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

SONICWALL®

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners. The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON- INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.