Securing Access for K-12 Digital Environments at School and Home

zscaler™

Even with many students returning to in-person learning, the security challenges of remote access remain -- providing protection from cyberthreats and inappropriate content. School Districts must develop and implement solutions for securing student internet access at home, both on district owned devices as well as BYOD.

Zscaler has identified six evolving challenges and considerations that impact how schools can deliver on an end-to-end solution providing every student and teacher secure, protected Internet Access.

1. Student Safety (CIPA)

With the Children's Internet Protection Act (CIPA), school districts are required to have visibility into what students are viewing online, which has made web content filtering a focus for years. However, there is much more to it than just need for the filtering and basic visibility into what students are accessing. It is also important to make sure appropriate alerts are activated to bring immediate awareness of what is going on to make real-time decisions on how to manage it. Whether it is inappropriate content on social media, cyberbullying, or malicious actors using student accounts to infiltrate the network, cloud-based threat monitoring is a must-have part of any cybersecurity stance.

2. Home Internet Access for Every Student

Access equity has been a growing concern over time, one that the pandemic response brought into sharper focus. Students, teachers, and staff in rural and underprivileged communities may or may not have sufficient access to the internet. For those that do have access, it may be in shared locations or on open networks. Administrators have no way of knowing what level of security exists for each user.

Access equity is not only about equal access to education and learning tools, it is about how to provide that access in a safe manner. Administrators need to understand the various circumstances within their systems and how to apply cybersecurity to these parameters going forward.

3. Multi-Device and BYOD Availability

The traditional mindset that a student uses a standard device provided by their school system and that there is only one device a student is using has changed. Students and teachers are accustomed to using multiple and varying devices to access learning – Windows, Apple, Chromebooks, Android devices or any smart device are now the expected norm.

Users want and need to be able to access the school system network from anywhere and any device, which is a key consideration in developing a security architecture. Each platform has different capabilities and different security stances that can go across devices. It's important to build a platform that is flexible enough to adapt as needs do.

4. Targeted Cyber Threats

The cyberthreat landscape continues to evolve, with the number of targeted instances growing. Zscaler monitors cyberthreats, and saw a six-fold increase in the last six months of 2020 alone. Instead of general, wider phishing, these hyper-targeted cyber threats are customized to either specific schools or even specific administrators. Even with the best cybersecurity training for school staff, there may be volunteers and other users on the network with access to systems that may not have the sophistication or training to prevent and avoid these attacks.

Ransomware continues to be a major threat, with an increase in malicious actors delivering these attacks via encrypted mechanisms, and creating a blind spot in many school systems. Having 100% visibility into encrypted traffic that flows in and out of the network removes the blind spot, and thus the root cause for cyber attacks inside the school system.

5. Seamless Identity-Based Access

With the reality of people working from locations outside of the school building itself, it is important to consider the ease of use of cybersecurity solutions being deployed and to focus on how to best roll out communication. If the plan requires a difficult configuration and is only locked down to specific devices, it could cause an inability to implement the solution, increasing risk to the data, for students, and to the entire school system.

At home and on the road, there are various levels of security to be considered. To make implementation as easy as possible, addressing the various levels of security upfront must be seamless. The solution needs to work with minimal interaction and minimal configuration, allowing users to be protected without having to know about it or do anything active in order to get the security level that they need.

How Zscaler can help secure the K-12 environment

Budgets are constantly shrinking while demand grows. The pandemic and related tax pressures are exacerbating these constraints. One way to get the most from limited resources is to prioritize spend to focus on creating procurements and requirements that have a broad set of abilities to address all of the challenges facing K-12 schools today and plan for tomorrow.

With these wide ranging security needs, securing the K-12 environment requires a holistic approach. Looking at discrete products that may help with one area of cybersecurity is an outdated approach. Through the Zscaler Zero Trust Exchange, we can provide a secure platform to address the evolving challenges, mentioned above, that school systems are facing today. Our approach starts from a web security perspective to protect the students and the faculty in the multi-mode, multi-device, multi-connectivity world that is today's reality and beyond.

Zscaler Services

Advance Threat Protection

Home internet access
for all students

Cloud Filtering

Children's internet
protection act (CIPA)

Cloud Firewall

Target
cyber threats

Web Security

NIST CSF
(Identity - Protect - Detect
Respond - Recover)

Private Access

Seamless identity
based access to secured
applications

Data Loss Prevention

Inappropriate
disclosure of personal
information

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com