SSL Inspection: **Keeping K-12 Students and Schools Safe**

Learn how to reduce risk as teachers and students leverage online resources.

zscaler™

In 2019, **ransomware attacks cost the U.S. $7.5 billion**[1].

Among the victims were 1,233 individual schools. In at least one instance, the attack prevented the school from accessing data about students' medications and allergies—a potentially life-threatening situation for the students.

That's only ransomware. Those numbers do not include any other types of malware, such as spyware or phishing attacks.

Further compounding the K-12 school security challenge is that simply fixing any immediate security incident doesn't guarantee the system is secure.

A fundamental problem is that if the security professionals don't know how these threats have evolved, there is no way for them to know if the malware contains some sort of time bomb that will re-engage later on, or how much of this malicious code is embedded.

With student safety at risk, how can K-12 school systems manage the malware challenge?

The answer:
Secure Sockets Layer (SSL) inspection, which is the ability to inspect encrypted traffic.

What Does SSL Have to do With Security?

In any school system, the paramount concern is keeping students safe whether the students are in the school facility or a remote classroom. From a technology standpoint, that means identifying threats. The only way to do that is be able to see inside the traffic. That is what SSL inspection does.

SSL encryption — the act of converting data into a cipher or code to prevent unauthorized access — has become the standard security protocol because SSL certificates, which used to be difficult to obtain, are now readily available at no charge[2]. More than 90 percent of internet traffic today is encrypted, and cybercriminals are using it too. It is an effective way for them to conceal and launch attacks.

> "Phishing, spyware, viruses, ransomware. These are facts of life in the security world, and addrevssing them is something every vendor does. But these attacks continue. Why? Because these things are transmitted over encrypted means. If you don't unwrap the encryption, you don't solve the security threat."
>
> zscaler™
>
> Public Sector Solution Architect

1. Emsisoft Malware Lab, "The State of Ransomware in the US: Report and Statistics 2019." December 19. 2019. https://blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/
2. Source: Zscaler "2019 Cloud Security Insights Threat Report – An Analysis of SSL/TLS-based threats."

If the malware is encrypted, it is difficult for traditional security tools and platforms to inspect it. They must be able to unwrap that encryption and see it in the clear to identify embedded threats.

While all schools are required to filter web traffic to be compliant with the Children's Internet Protection Act (CIPA), very few of them have successfully implemented SSL inspection across all web traffic. This leaves them vulnerable to threats and puts more pressure on other security tools further down the stack, such as endpoint protection, next-generation firewalls, and web filters.

Yet, without inspecting all SSL-encrypted traffic, these tools become reliant on URL reputation alone. This has created an enormous blind spot in school districts' cybersecurity.

During the first half of 2020, the Zscaler Security Cloud blocked more than 80 million threats aimed at the Education sector over encrypted channels. Among all industries monitored, the Education sector saw the following amount of threats:

- Phishing: **8.4 %**
- Advanced threats: **2.8 %**
- Malware: **1.4 %**
- Browser exploits: **3.8 %**
- Malicious threats: **11.9 %**

Imagine a school system where 200,000 students are learning remotely on both school supplied devices and their personal devices. It would not be hard for ransomware to proliferate once it's on a trusted device in the network. If that malware shut down the entire school system, they would have to rebuild everything from the ground up.

In school districts that hardly have the resources to manage their daily IT needs, that would be an enormous financial and technological problem.

Implementing SSL inspection can help school districts proactively identify and block cyberthreats from ever getting into the network.

Challenges for the Schools

The challenges for schools will only get more complicated with time, especially as remote, distance learning becomes the norm.

With 1-to-1 device initiatives (where the school provides a dedicated device for each student and teacher to use), virtual classrooms, bring-your-own-device (BYOD) policies expanding, and technology we can't even envision yet, the trend will shift toward treating every device as if it's not trusted. Yet students have to work as if they're in a classroom environment, and do it securely and effectively. Schools will need a way to quickly and securely scale, providing access to applications their students' need.

> "Schools in our state rely on technology and digital resources for instruction, testing and school administration, and protecting these resources is critically important to achieve their academic missions"
>
> **Chief Information Security Officer**
> Research and Education Network customer

Again, SSL inspection plays a key role in providing schools and school systems the confidence to give students and teachers access from any device and from any location.

SSL inspection also helps with student physical safety. Online predators, online bullying, talk of self-harm on forums — those communications are often in encrypted format. If you can't see what is in a message, you can't act on it. SSL inspection gives teachers and school officials insight into these messages so they can quickly act on any potential threats.

Most traditional systems run DLP engines, which can be programmed to look for certain signatures, words, and triggers that might help identify a student in danger. But those words or phrases could be misinterpreted as they don't provide the context of an entire conversation or message. SSL inspection gives schools the ability to see the entire message, helping them more accurately identify problematic situations.

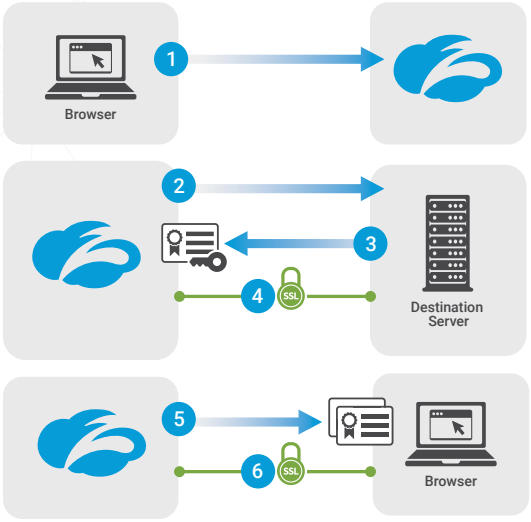
How SSL inspection works

SSL is a protocol for establishing authenticated and encrypted links between networked computers. It works by binding the identities of entities, such as websites and companies, to cryptographic key pairs via digital documents known as X.509 certificates. Each key pair consists of a private key and a public key. The private key is kept secure, and the public key can be widely distributed via a certificate.

The special mathematical relationship between the private and public keys in a pair means that it is possible to use the public key to encrypt a message that can only be decrypted with the private key. Furthermore, the holder of the private key can use it to sign other digital documents (such as webpages), and anyone with the public key can verify this signature.

If a publicly trusted certificate authority, such as SSL.com, signs the SSL certificate, client software, such as web browsers and operating systems, will implicitly trust the certificate.

Via the SSL handshake, the private and public keys can be used with a publicly trusted certificate to negotiate an encrypted and authenticated communication session over the internet, even between two parties that have never met. This simple fact is the foundation of secure web browsing and electronic commerce as it is known today.



Once the handshake is completed, the Zscaler policy engine evaluates SSL/TLS policy rules, applies global blocks/bypasses, checks certificates from untrusted issuers, and displays notifications (if needed).

1. A user opens a browser and sends an HTTPS request.
2. The Zscaler service intercepts the HTTPS request. Through a separate SSL tunnel, the service sends it's own HTTPS request to the destination server and consucts SSL negotiations.
3. The destination server sends the Zscaler service its certification with its public key.
4. The Zscaler service and destination server complete the SSL handshake. The application data and subsequent messages are sent through the SSL tunnel.
5. The Zscaler service conducts SSL negotiations with the user's browser. It sends the browser the Zscaler intermediate certificate or your organization's custom intermediate root as well as a server certificate signed by the Zscaler intermediate CA. The broswer validates the certificate chain in the browser's certificate store.
6. The Zscaler service and the browser complete the SSL handshake. The application data and subsequent messages are sent through SSL tunnel.

Unfortunately, cybercriminals also use SSL encryption to:

- Hide dangerous content, such as ransomware, viruses, spyware, and other malware.
- Build their own websites.
- Inject malicious content into well-known and trusted SSL-enabled sites.

SSL inspection is used to filter out malicious content. When the connection is made over HTTPS, the inspector intercepts all traffic, decrypts it, and scans it.

Why aren't school systems implementing SSL inspection?

When a school system has thousands (sometimes of hundreds of thousands) of devices to secure, if feels like a painful process to get SSL deployed because SSL inspection requires a certificate for every workstation and device—a monumental effort in school systems that need thousands (or even hundreds of thousands) of certificates. That's why organizations often skip SSL inspection when using on-premises network security appliances because SSL inspection uses resources on the appliance that degrades its performance. Therefore, users suffer from poor performance and organizations often have to purchase more hardware to throw capacity at the problem.

On top of the standard on-boarding process, each device that accesses the network needs a certificate. Historically that has created an administrative overhead problem, so people just don't do it unless they're reacting to a situation.

For network appliances to effectively deploy SSL inspection, the amount of network resources needed would almost immediately begin to diminish the user experience. Additionally, each computer/client needs an intermediate certificate that, in some cases, must be installed multiple times to accommodate different browser certificate stores.

The critical success factor for implementing a feature, solution, or technology is that the user experience is equal to or otherwise better than before the implementation. Yet, with SSL inspection, this is typically not the case. The optimal approach for schools is to deploy a one-step configuration/agent and have elastic or infinite resources to ensure that the user experience is greater and more secure than it was previously.

Having a multitenant cloud service that can infinitely scale and deliver SSL inspection without any performance hit or added cost to cover all of the school district's internet traffic, whether on or off the network, will close the security gaps that appliance performance limitations leave behind.

For example, one Zscaler public sector customer was trying to implement SSL inspection on its current on-premises next-generation firewalls, and it was seeing a 90-percent reduction in performance on the box when it was turned on. Implementing the Zscaler cloud service eliminated that performance issue without adding costs for the customer.

Delivering a security stack with full SSL visibility will help you find more threats and mitigate risks more effectively. And having unlimited capacity to inspect all your encrypted traffic, even as your bandwidth demands grow, guarantees that your security requirements are future proof.

How schools can leverage the power of cloud-based security to implement SSL inspection

To get started with pain-free SSL inspection, the school district needs to create a solid SSL policy.

The good news for schools is that getting a solid policy around SSL inspection is a best practice activity of determining what the tool will bypass or inspect.

For example, policies with respect to SSL inspection are inherently intrusive, such as in health care. If the user is going to a health care site, the policy can be set to bypass that conversation. Health care and banking are the two industries where these policies are most commonly implemented.

Several guidelines for creating SSL inspection policies are already in existence, so school districts do not need to start from scratch and can quickly move forward with SSL inspection.

Conclusion

As students, teachers, and administrators drive demand to support mobility, school districts are increasingly leveraging online resources. At the same time, the risks and challenges for securing these resources have grown exponentially. With this massive shift to the cloud and remote/mobile computing, your school's traditional hub-and-spoke model no longer makes sense as your network is being extended outside of your walls and off your campus.

How do you provide protection from cyberthreats and inappropriate content, as well as gain the appropriate visibility and controls necessary to meet CIPA, Family Educational Rights and Privacy Act (FERPA) and Children's Online Privacy Protection Act (COPPA) compliance standards if you can't build a firewall in the cloud? How can you provide a consistent user experience for your students, teachers, and administrators who work on campus, from a remote location, or at home while still keeping them and their data safe?

By giving your IT teams the ability to inspect traffic on your networks and proactively manage threats with SSL inspection, that's how.

About Zscaler

Zscaler was founded in 2008 on a simple but powerful concept: as applications move to the cloud, security needs to move there as well. Today, we are helping thousands of global organizations transform into cloud-enabled operations.

The Zscaler Cloud Security Platform enables complete SSL inspection at scale, without latency and capacity limitations. By pairing SSL inspection with the Zscaler complete security stack as a cloud service, you get improved protection without the inspection limitation of appliances.

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