Telos Ghost for K-12 and Higher Education

What Do Kindergarteners and PhD Candidates Have in Common?

Students, faculty, and staff in every level of academia are high-value targets for hackers, marketers, and nation-states. In open environments where security isn't always top-of-mind, how can educational institutions protect their people and data?

Educational CTOs are under a lot of pressure to stop the threat of the day. Today, it's ransomware. Tomorrow, it will be something else. We need to change our focus. Instead of thinking about stopping a particular type of threat, think about how to achieve the right outcomes. Is the real goal to prevent students from visiting a certain site, or is it to protect student identities? Is the real goal to stop researchers from accessing project data through the public Wi-Fi at the coffee shop, or is it to preserve the value of the research and enable the university to win future grants?

Administrators block certain sites because they have a bad reputation with parents and the media—which only makes them more attractive to young people, who are quite capable of googling "how to unblock TikTok."

Ransomware attacks are on the rise in education.

The severity of K-12 ransomware attacks increased in 2020 as assessed by the intrusiveness of the attacks, the amount of ransom demanded, and the number of resulting closures and cancellations.

("The State of K-12 Cybersecurity: 2020 Year in Review"; K-12 Cybersecurity Resource Center and K12 SIX)

Ransomware attacks against colleges and universities have more than doubled since the onset of the coronavirus pandemic.

("Cybersecurity in Higher Education"; BlueVoyant, February 2021)

So the decision to block a site ends up pushing students down a more perilous path. Students download and install free VPNs to get around the content filtering mechanisms, but there's a reason those services are free: they mine data and traffic for analytics, tracking, and advertising purposes, or they take control of users' browsers for various purposes. Data is sold to unknown third parties, ads can entice users to visit websites poisoned with malicious code, or users' browsers can be hijacked to a poisoned site without their permission.

$300 billion in Intellectual Property is stolen every year.

Ideas flow freely in the collaborative culture of academia, and so do people—research assistants and post-docs rotate in and out, staff turns over, and new business or academic partners are brought into the mix. Few of them are aware that their work, even in the earliest stages of research, is highly valuable to those outside the project. Is a research assistant likely to think a nation-state actor is behind the email they received about their library enrollment? And yet that's how an Iranian threat group called Silent Librarian targeted specific universities and made off with 31 terabytes of intellectual property worth $3.4 billion.

In 2020, the FBI conducted about 1,000 investigations into suspected Chinese theft of US technology involving every sector of the economy.

(VOA News)

Be anonymous. Be invisible.
Be secure with Telos Ghost.

The power of invisibility: Network Obfuscation.

Traditional cybersecurity focuses on protecting the network infrastructure and its endpoints, firewalls, apps, secure web gateways, and other technologies. Network obfuscation focuses on the internet itself. It hides servers, applications, and unified mobile communications from the internet so attackers can't find their targets even if they are expressly hunting them.

Now, these capabilities are delivered by **Telos Ghost** from Telos Corporation, a virtual obfuscation network-as-a-service that protects students, faculty, staff, and school systems from the ravages of ransomware, cyberbullying, phishing attempts, data exfiltration, and other attacks.

The Intelligence Community uses network obfuscation to protect its digital resources and its agents from exposure, no matter where on the globe they are operating. Now, Telos Ghost makes these same capabilities available to educational institutions to help them secure their students, faculty, researchers, and data without having to attempt the impossible goal of securing every endpoint in their dispersed dynamic environments.

K12 Alert: Telos Ghost is a managed network service covered by E-Rate

Telos Ghost provides safety and security for students, faculty, and researchers.

Telos Ghost is a robust, scalable, secure network-as-a-service that privatizes the public internet to hide network resources and mask the identity and location of users to ensure total protection as they interact with the school's network.

Telos Ghost dynamically routes IP traffic among cloud transit nodes. Advanced managed attribution makes users and their locations completely anonymous, which is a particularly compelling case for schools practicing remote learning, partnering with government or business entities, or operating research facilities.

Every device connected to Telos Ghost creates its own unique obfuscated network pathway. And since each device is the only device on that pathway, ransomware and DDoS attacks can't achieve scope or scale. The attack surface has been reduced by using the invisible, untraceable connections to the Telos Ghost network.

Telos Ghost can fully encrypt data in transit from endpoint to the network, anonymizing students and removing their digital footprints. Students, staff, and faculty are untrackable and untraceable, even when they go to legitimate websites. They can't be geo-located or targeted by advertisers. Large data sets used in university research are not a problem. They can be processed and stored inside the Telos Ghost network, unseen by anyone but the researcher working on them.

And, Telos Ghost can be embedded in other technologies as well, such as video surveillance systems, so attackers can't drop into classes or observe activities in a lab or university hospital. This same protection also ensures the integrity of emergency and mass notification platforms so that bad actors can't take those systems offline as part of a larger physical assault on educational facilities.

Your investment in Telos offerings for cybersecurity, risk management, and compliance may be eligible for coverage by ESSER or GEER funds through the U.S. Department of Education. Contact the grants and funding office for your state or ask your Telos representative for further information.

Discover how Telos Ghost can protect your students, staff, and schools.

Implementing Telos Ghost's next-generation cybersecurity technology will not only protect the privacy and security of students, faculty, and administration, but will ensure the learning organization's critical enterprise network resources are invisible on the public internet and inaccessible to those who mean to do harm. To learn more, please contact Telos.

Telos®

Solutions that **empower** and **protect** the enterprise.™