Protecting IT infrastructures in schools, colleges, and universities.

Barracuda

Your journey, secured.

Network security is a lesson educational institutions can prepare for

When it comes to network security, organizations can — and must — learn from the experiences of others. The real challenge is in identifying which lessons are applicable and implementing those lessons to provide the most effective protection. Getting network security right is one of the toughest tasks for any security team, but there is a lot of knowledge that is transferable.

Network security is a term that refers to many different technologies and principles and it is not a question of just buying the right product. It includes advanced firewalls, but network security goes beyond securing the perimeter, it also includes regulating network traffic, managing bandwidth utilization, and the detection and quarantining of internet-borne threats. In today's fast paced IT environment driven by digitalization and cloud adoption, organizations require solutions that can maximize security while improving performance to users on a distributed network.

Remote working — whether at distributed sites or campuses, or from home — was on the rise and has been greatly accelerated by the COVID-19 pandemic. Organizations need to secure a much larger attack surface, often connecting devices and networks that are not under their direct control. Education is one sector where network security is particularly challenging.

The education challenge and how to meet it

It might be counter-intuitive but education is the sector most at risk of cyberattacks — Microsoft says it accounts for four-fifths (82.6%) of all malware encounters in the last 30 days but education has been at or near the top of the list for years. Our analysis of 3.5 million spear-phishing attacks over a four-month period found that more than 1,000 educational institutions were targeted. And, compared to the average, educational institutions were more than twice as likely to be hit by a business email compromise attack, which is when bad actors impersonate a staff member or faculty to try to trick others into sharing information or approving financial transactions. Distributed denial of service (DDoS) attacks — which flood networks with an overwhelming amount of traffic — targeting educational institutions have risen as well. These DDoS attacks can not only disrupt online learning, but they can also act as cover for attempts to penetrate network defences and inject malware into the system.

Educational institutions vary considerably — from small schools and colleges to large universities with multiple campuses. However, there are some common things that make these institutions attractive targets. Awareness of risks is key to mitigation. Those risks include:

- **A new batch of targets every year:** Educational institutions will take in a new cohort of students every year who might need training on how to handle their provided IT equipment, need support to get familiar with the mandatory authentication routines, and learn about best practices for accessing the resources required for their success in learning.

- **Increased e-learning:** E-learning and remote learning were already growing when the COVID-19 pandemic hit, resulting in an exponential increase of network traffic, which can make it easier for attackers to hide. The drastic increase of students learning from home also makes seamless availability of data and applications, and scalability of remote access mechanisms indispensable.

- **Multiple locations:** Whether it’s a large university with campuses across a city or region, a board of education, or a multi-academy trust, multiple locations mean an increased security challenge. Students, faculty, and staff may be legitimately accessing the network from many locations, making it harder to pick out attackers.

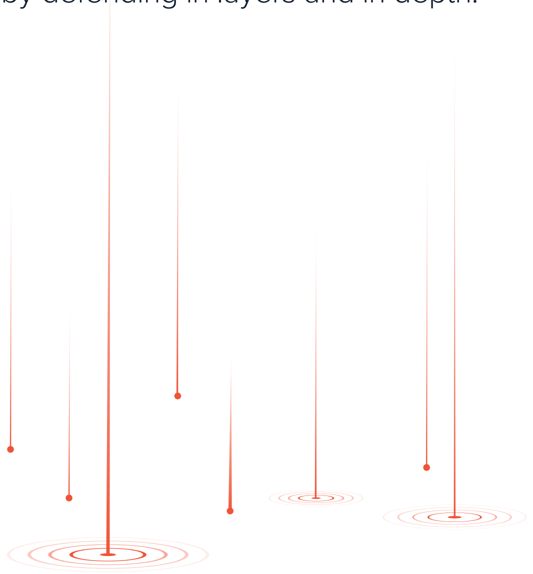
- **Valuable data:** While some attacks are simply malicious mischief, most cyber criminals are looking for financial or material gain. Educational institutions hold large amounts of valuable data, including personal identifiable information (PII) on students, parents, faculty, and staff; payment and account information; and, in many cases, valuable intellectual property in the form of research data. This can make them targets for extortion, cyber espionage, and even state-sponsored attacks.

- **Public or semi-public network access:** Many institutions might have public Wi-Fi access for parents and visitors and/or shared terminals in public spaces.

- **User training is needed:** Users are your first, and arguably best, line of defence against compromises. Provide users, and this means students as well as staff and faculty, with the training to recognize and report threats to network security.

- **Supplier/partner vulnerability:** Educational institutions have relationships with suppliers, contractors and research partners in both the public and private sectors. It’s vital to ensure those parties maintain good network hygiene. If not, those third-parties can be the foundation for an island-hopping attack where the attacker uses the supplier’s or partner’s network to gain entry into yours.

It's possible that an attacker may be purely malicious with no motive beyond causing disruption and destruction. However, it’s more likely that attackers are looking for some gain. It may be a ransomware gang looking to extort money to release data it has encrypted. It may be identity thieves who want to steal PII and sell it. Or it could be corporate or state-sponsored agents who want to remove exfiltrate intellectual property. The net result is that these goals mean educational institutions must improve network security by defending in layers and in depth.



Network security layers keep educational institutions secure yet agile

Network security isn't a product, a program, or a checklist. It is a holistic approach that builds layers of defence to keep organizations safe while still allowing them to be effective. For educational institutions, making security so tight, with so many checkpoints, passwords, and verifications that students cannot easily access their classes, use email, or access reference materials is a failure. Making it a single layer, no matter how tough, won't work either. If a criminal compromises a professor's email account and can then run freely through the network, that's also a failure.

Layers of security that encompass the entire network to provide different types of security across the entire organization is the way to go. Multi-layered security including full emulation sandboxing ensures effective protection against sophisticated advanced threats and mitigates the risk to fall victim of a ransomware attack. A shift into the cloud offers major advantages, with expertly managed security that is always up to date.

Network security comes from robust components working together. Strong firewalls and access control mechanisms should be used to keep out intruders, network segmentation should be used to limit lateral movement of any users or potential intrusions in case they should find their way past the access controls. Ideally access to all applications, regardless if inside the network, cloud-hosted or even SaaS should be combined with Zero-Trust principles, continuously checking user id, device health and other vital parameters before allowing encrypted access to the application. ZTNA also makes sure the right user has access to the needed applications only, avoiding privilege creep.

Software-defined wide area network (SD-WAN) solution can connect buildings, distributed sites or campuses, and trusted partners via multiple encrypted connections and is much cheaper over pseudo-secure MPLS or other leased lines.

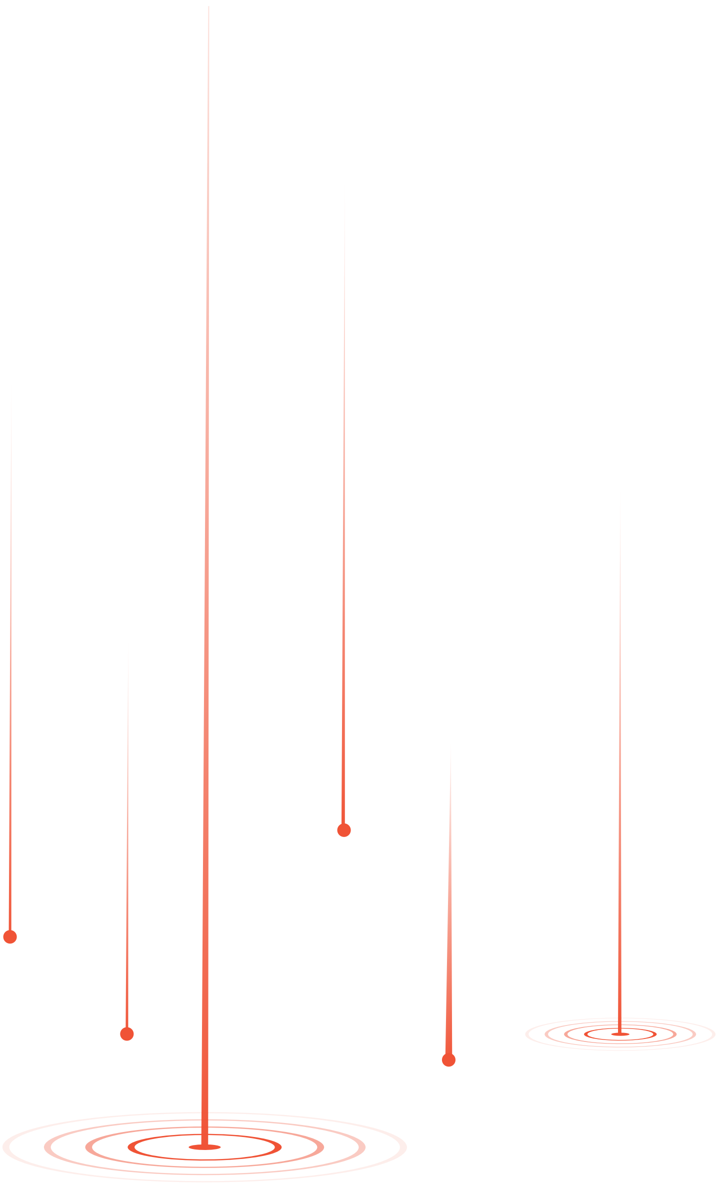
A safe learning environment requires safe computing. Ransomware and other malware can infect your network through social media or compromised websites. Microsoft Security Intelligence reports that most devices in the education sector have been infected by adware or backdoor trojans. Web security is a regulatory requirement for many schools and it provides several benefits when configured correctly. Content filtering blocks distracting sites and helps protect students from cyberbullying and online predators.

Conclusion

The education sector is facing a barrage of threats from cybercriminals attempting to breach their networks for profits. Malware, ransomware, and all other kinds of cyberattacks are wreaking havoc on educational institutions. One thing is for sure: the time to secure against these threats is now.

Network security looks like a big job because it is. But it is achievable. Best of all, this security can be cloud-based and provided via an as-a-service model, reducing the load on overworked IT staff and providing educational institutions with a cost-effective way to ensure security remains up to date.

Learn how to build an effective network security strategy with Barracuda's powerful security tools. We're ready to help.



About Barracuda Network Security

Barracuda's solutions include three core products: Barracuda CloudGen Firewall, Barracuda CloudGen WAN, and Barracuda CloudGen Access, covering all requirements for today's state-of-the-art network security.

Barracuda CloudGen Firewall combines best-in-class next-generation security with a full-featured set of secure SD-WAN capabilities. Barracuda CloudGen WAN is the industry's only cloud-native SASE platform offering a global secure SD-WAN service built natively on Azure. Barracuda CloudGen Access is an innovative Zero Trust Access solution providing secure access to applications and workloads from any device and location.

Barracuda CloudGen Access™

Barracuda CloudGen Firewall™

Barracuda CloudGen WAN™

About Barracuda

At Barracuda we strive to make the world a safer place. We believe every business deserves access to cloud-first, enterprise-grade security solutions that are easy to buy, deploy, and use. We protect email, networks, data, and applications with innovative solutions that grow and adapt with our customers' journey. More than 200,000 organizations worldwide trust Barracuda to protect them — in ways they may not even know they are at risk — so they can focus on taking their business to the next level. For more information, visit barracuda.com.

Barracuda
Your journey, secured.

Feel free to contact us with any questions about how to secure your applications.