Barracuda

PARTNER LOGO

Four Tips to Counter Network Security Threats on Remote Schooling

A coin has two sides – while online classes bridge learning gaps during the pandemic, the distinctive rise of “virtual schools” are posing severe cybersecurity risks at the same time. Especially when remote access is poorly configured, it offers hackers a prime opportunity to exploit network vulnerabilities.

Open ports like Remote Desktop Protocol (RDP) are particularly vulnerable entry points for threat actors. When IT teams enable RDP to offer remote desktop support over the Internet, it also allows invaders to force their way into the school network easily. Bot attacks, for example, are used by cybercriminals to find vulnerabilities on websites and firewalls for launching DDoS attacks.

Here are four steps to secure your access, network and applications, from A to D.

1. **Achieving** secure access for authorized users
2. **Blocking** ransomware and other advanced threats
3. **Combating DDoS**, credential stuffing, and other automated attacks
4. **Detecting and stopping** network intrusions

Barracuda Vulnerability Manager offers a comprehensive solution that automatically identifies, assesses, and mitigates web application security risks during remote schooling. Contact us now for more information or to schedule a demonstration.

Contact Us Now

Forward this to a colleague