Malwarebytes

INDUSTRY SOLUTION BRIEF

Malwarebytes for education

Preventing and removing threats for safer learning

THREATS SCHOOL FACE

Email phishing
- Staff and students redirected to malicious websites

Botnet attacks
- Student and campus computing resources infected and hijacked

Malvertising
- Malware and scams delivered via infected ads on popular sites (e.g., msn.com, nytimes.com, bbc.com)

Ransomware
- Campus storage arrays and student machines attacked and encrypted—data held for ransom

PUPs and PUMs
- Potentially unwanted programs and modifiers downloaded, slowing down computer performance

Threat proliferation
- Malware spreading across endpoints (e.g., infected homework emailed to professors, compromised files uploaded to class webpages or portals)

State of education

Today's 21st century connected classrooms embrace technology an integral part of the educational experience. Technology affords teachers and students with unprecedented opportunities for interactivity and collaboration, connecting students to a wealth of current information and engaging them using innovative educational tools. Technology is also a crucial component in readying college graduates for their future careers and in safeguarding sensitive student data. Unfortunately, when that technology doesn't function, it can interrupt lesson plans, disrupt learning, and put important information at risk of breach.

Challenges schools face

Budgets and infrastructure

Many educational institution budgets are tight, forcing schools to struggle with legacy systems, outdated equipment, and limited staff. Even schools with healthy budgets need to put technology investments on hold due to funding changes made at the local, state, or federal level. Schools don't have the dedicated IT budgets and resources that corporate enterprises enjoy, but they encounter many of the same challenges and threats every day.

Wide open campuses

Data is used and stored across multiple departments and colleges, and more than ever, confidential personal information is gathered and shared across different systems (e.g., academic records, financial aid, accounting, housing, health records, student counseling). In addition, colleges and universities face complications due to separate schools, such as law, engineering, or business, each having different IT departments and staff.

LAN and Wi-Fi networks across campuses provide multiple ingress and egress connection points for computers, including classrooms, labs, libraries, dormitories, outdoor spaces, and even stadiums. This facilitates an always-connected lifestyle that supports learning, but makes securing the shared data and roaming endpoints difficult.

Diverse endpoints

Google Chromebooks are the most prevalent devices used in classrooms, representing 53% of the market for K-12 devices purchased by schools

and districts in the United States. Although Chromebooks supply the lion's share of classroom devices, education IT staff are busy supporting a mix of student and employee devices from different manufacturers running different operating systems—each with their own software vulnerabilities and risks.

IT departments within colleges and universities have an equally difficult job as they face the challenges of consumerization that BYOD and open campus cultures introduce. They support a combination of school-provided and student-owned devices on college campuses where some are managed by the school, but most are managed directly by the user.

External threats

On top of these challenges, schools are prime targets for a variety of advanced cyberthreats that continue to evolve. For example, as students are conducting research on websites—regardless of the site's reputation—they're at risk of being compromised by malicious advertisements, or malvertising, hosted on those pages. Malvertising is an increasing attack vector for the delivery of ransomware, an especially dangerous form of malware for teachers and students.

Any of these threats can be easily spread or propagated from students to teachers to staff and back again, due to the open sharing policies that make the connected classroom concept work. Educational institutions require advanced threat protection that can also address the challenges their IT departments face.

How Malwarebytes can help

Campus systems

Malwarebytes Endpoint Security
Centrally protects campus endpoints against known and unknown attacks.

Malwarebytes Breach Remediation
Rapid, lightweight Windows and Mac remediation. Use it to sweep servers and storage arrays for malware. Also a perfect solution for large schools supporting student endpoints across campus.

Students and alumni

Malwarebytes 3.0 (Windows)
Malwarebytes Anti-Malware (Mac, Android)
Automatically and instantly stops malware threats on Windows computers and laptops. Removes malware and adware from Mac computers. Protects Android smartphones, tablets, and Google Chromebooks from malware, infected applications, and unauthorized surveillance.

What schools and universities say

> Malwarebytes works flawlessly and has been a big help. We haven't had to take any machines down since we deployed it. It's one of the best purchases we've made.
>
> —Mário Bernardo, Assistant Director, Florida Gulf Coast University

> Malwarebytes has saved us hundreds of hours otherwise spent remediating systems. This translates to significant cost savings and allows technicians to focus on more productive projects.
>
> —Dan Boltjes, Director of Technical Services, Colorado Springs School District 11

Educational institutions trust Malwarebytes

Purdue University · University of Michigan · Stanford University · Cal · The University of Texas at Austin · Columbia University · University of Notre Dame · Wellesley

malwarebytes.com/education | edusales@malwarebytes.com | 1.800.520.2796

Malwarebytes protects consumers and businesses against dangerous threats such as malware, ransomware, and exploits that escape detection by traditional antivirus solutions. Malwarebytes Anti-Malware, the company's flagship product, has a highly advanced heuristic detection engine that removed more than five billion malicious threats from computers worldwide. More than 10,000 SMBs and enterprise businesses worldwide trust Malwarebytes to protect their data. Founded in 2008, the company is headquartered in California with offices in Europe, and a global team of researchers and experts.