As Director of IT for the Parks School District, Travis works diligently to protect 24 schools, 15,000 students, and approximately 725 staff. Given their resource constraints, Travis and his small team do an impressive job protecting the district from cyberattacks.

Recently, Travis has grown concerned about a weakness in the district’s cybersecurity posture: the world’s most commonly attacked operating system—Windows—is literally in the hands of children. Travis and his team have limited (to no) control over this problem.

When Travis read about a cybercriminal organization initiating ransomware attacks by way of phishing emails, he knew he had to do something. The attack started by enticing unsuspecting users to download a seemingly legitimate application. The application contained hidden code and, when opened, executed malicious software that left an open door for the criminals behind the attack.

**An ounce of prevention avoids pounds (££) of cure**

The common advice was to educate users on identifying and deleting suspicious emails. While Travis scheduled training for district administrators, faculty and staff, he didn’t believe that educating children on this topic would help. How do you explain to grade-schoolers that a sense of urgency, a first-time sender, and a poor use of spelling and grammar all point to phishing?
Travis also knew that no single layer of security can catch all of today’s sophisticated and obfuscated malware. Layering security defenses is an essential best practice for preventing attacks.

To help address the risk of students accidently launching malware (and inadvertently allowing criminals to initiate an attack), Travis needed a solution that could:

- **Prevent malicious software from executing on Windows endpoints**, adding another layer of protection.
- **Deploy with ease** so that learning continued uninterrupted.
- **Add protection without increasing complexity**.

### Increasing security without increasing complexity

To find a solution that would meet these needs, Travis and his team researched nearly one dozen prospects, which they soon narrowed down to three. After comparing the solutions’ pros and cons, the team selected Malwarebytes Application Block.

As an add-on module for the cloud-based Malwarebytes Nebula platform, Application Block is purpose-built to extend the solution that Parks School District already trusts for endpoint protection: the award-winning Malwarebytes Endpoint Detection and Response (EDR). No other solution matched the convenience, ease of deployment and use, and single point of endpoint protection management that Malwarebytes Application Block offered the district.

### How Malwarebytes solved the problem and delivered benefits

Like all Nebula modules, Malwarebytes Application Block required only a few mouse clicks in the Nebula management console to activate. Once he activated the module, Travis was able immediately to begin blacklisting unsafe, outdated, and unused applications.
Malwarebytes Application Block added a much-needed layer of security to the district’s Windows endpoints, increasing security and saving time.

He took comfort knowing that if a student downloaded blacklisted software, Malwarebytes Application Block would stop that software from executing on any Windows laptop, desktop or server running the Malwarebytes EDR agent.

With Malwarebytes Application Block, Travis and his team added a layer of protection to their Windows endpoints and gained these immediate benefits:

- **Reduced complexity**
  - Activates within minutes
  - Requires no training
  - Consolidates endpoint protection management

- **Improved endpoint protection**
  - Stops applications identified as unsafe or untrusted from launching on Windows endpoints
  - Offers pre-populated application and vendor lists to simplify rule creation
  - Offers simple alternative to uninstalling outdated applications
  - In conjunction with Malwarebytes Vulnerability module, offers easy way to block vulnerable apps for which patches are unavailable or not yet applied

- **Enforce acceptable use policies**
  - Block applications that serve no business purpose
  - In conjunction with Malwarebytes DNS Filtering, block time-wasting or otherwise inappropriate Windows and web-based applications

- **Help with verification for data protection regulations and cyber insurance requirements**
  - Generate reports to show what has been blocked and on which endpoints

Malwarebytes believes that when people and organizations are free from threats, they are free to thrive. Much more than malware remediations, the company provides cyberprotection, privacy, and prevention to tens of thousands of consumers and organizations every day. For more information, visit https://www.malwarebytes.com.

Malwarebytes and the Malwarebytes logo are trademarks of Malwarebytes. Other marks and brands may be claimed as the property of others. All descriptions and specifications herein are subject to change without notice and are provided without warranty of any kind. 01/2023