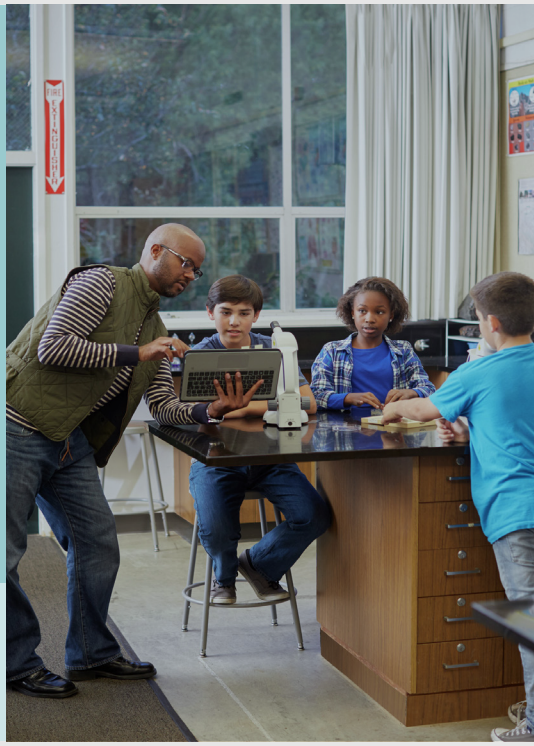
Protecting School Districts with Threat Containment



A superior approach to Endpoint Protection for K-12 Education

Kindergarten through 12th grade schools focus on giving students a strong education in a safe environment with the help of educators, faculty, and administrators. Part of providing a safe environment is the security of the schools' technology infrastructure. As with any organization, the most vulnerable part of the infrastructure is the endpoint PC, where students and faculty, data, and the Internet converge. Keeping students, administrators, and faculty safe from unknown threats and malware becomes paramount. School districts must balance the need for PC security to keep all users safe with limited security staff expertise and the need to support growth, creativity, and exploration.

Threat Containment using Endpoint Isolation

HP's Threat Containment helps K-12 meet those challenges. Based on our unique Endpoint Isolation technology, HP Threat Containment enables schools to efficiently manage large amounts of Windows PCs while allowing students and faculty to go about their daily task of teaching and learning. There are 3 components to Endpoint Isolation:

- Hardware-enforced micro-virtual machines (μVM)
- Introspection of each task within the μVM
- Cloud Analytics

The most important component of Threat Containment using Endpoint Isolation technology is the micro-virtual machine (μVM). Each potentially risky task, from surfing the web to opening attachments or inserting a USB drive is securely opened within its own μVM, preventing embedded malware from infecting the Windows PC or anything on the network. When the task is completed, the μVM is deleted, eliminating malware in the process. This threat containment method is enforced by hardware capabilities built into all modern business class CPU, so that malware cannot get around it.

Introspection is the next component of endpoint isolation. As each task is run within a μVM, all suspicious actions are observed and recorded, and the actions are compared to known suspicious behaviors. For example, Microsoft Word documents should never try to write to the firmware. All forensic data is gathered and observed. It is important to note that while this information is highly valuable, the "inherent protection" provided by the μVM will stop attacks independent of Introspection. It's "prevention without the need for detection."

The final component is Cloud Analytics. Information gathered during introspection is uploaded to the cloud and combined with other threat intelligence sources, where both manual and AI-driven analytics are applied. This surfaces insights into the techniques, tactics, and processes (TTP) of threat actors, and provides historical analysis. School district IT teams can use this data to tune their security polices and architectures.

Benefits for K-12 Education

Endpoint Isolation for Windows PCs is a particularly powerful approach because it delivers clear benefits in five key areas:

1 Inherent Protection

Isolation is a true Zero-Trust approach: all content from untrusted sources is contained in µVMs, with no need for threat detection allowing students, faculty, and administrators to continue to work without interruption.

2 Visibility

Isolation exposes and records in detail how malware attempts to execute its kill chain. It provides better forensics than sandboxing, because it allows malware to execute in the most realistic environment possible, even including user interactions while contained in a µVM. This visibility allows school district IT teams to review any attacks at a later time.

3 Security Efficiency

By preventing malware from installing, Endpoint Isolation significantly decreases the number of "high priority" tickets that school district IT departments must deal with. It also decreases the number of costly and time consuming remediations.

4 End-user Experience

Students, faculty and administrators can work with confidence. There is no need for extensive phishing training, since high-risk tasks are automatically contained. All users in the school district can "work without worry."

5 Compliance

Endpoint Isolation can be used as a primary or compensating control depending on the situation. For example, it can act as the foundation for endpoint Threat Prevention and Threat Detection control activities. It can also act as a compensating control for patch management, by protecting the PC between patch cycles. In both cases, Endpoint Isolation is operationally efficient, and easily validated during an audit.

HP Endpoint Isolation Solutions

HP Wolf Security offers two options to help K-12 schools to improve endpoint protection.

HP Sure Click Enterprise[1]

Threat Containment via Isolation Technology for Windows PCs with full support for complex policies, role-based access controls and integration. Sure Click Enterprise allows sophisticated schools with larger IT security teams the granular control to set policies based on a school district's IT requirements while enabling students, faculty, and administrators to continue learning and working with confidence.

HP Wolf Pro Security[2]

Isolation-based Threat Containment with simplified management for smaller school districts that lack a security team. Using Wolf Pro Security for Windows PCs, smaller K-12 school districts gain the same benefits as larger school districts, but with a simplified deployment and management model that reduces IT training and support requirements. Includes Credential Protection and optional NGAV.

Summary

Existing endpoint security solutions have proven unable to reliably prevent cyberattacks on Windows PC endpoints. Threat Containment through Endpoint Isolation is an innovative technology that changes the game. It delivers a broad set of benefits to IT security teams and end users: IT and security teams gain operational efficiencies, threat visibility, and simpler compliance controls, while students, faculty and educational administrators can work with confidence knowing they are "inherently protected." Therefore, Endpoint Isolation technology should be considered by K-12 schools seeking to improve their defenses and reduce operational challenges.

1. HP Sure Click Enterprise is sold separately. Supported attachments include Microsoft Office (Word, Excel, PowerPoint) and PDF files, when Microsoft Office or Adobe Acrobat are installed. For full system requirements, please visit System Requirements for HP Sure Click Enterprise for details.

2. HP Wolf Pro Security is available preloaded on select HP devices, is available as a subscription and in term licenses. Contact your HP sales representative for more details.

4AA8-2059ENW, September 2022