Endpoint Isolation

A superior approach to endpoint protection and SOC efficiency

The Endpoint Protection Challenge

The PC endpoint is the key security battleground. Most successful attacks target the endpoint and use social engineering techniques to trick users into assisting the attack. This is despite the wide range of solutions organizations have in place to fend off such attacks. These facts mean that new approaches to endpoint security are required. However, endpoint security solutions must meet two criteria. First, they must be easy to operate at scale. Second, they cannot impact user experience.

Isolation Technology Defined

Endpoint Isolation is a technological approach that addresses the endpoint protection challenge. It consists of three components:

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

The most important component of Endpoint Isolation 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 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. Security teams can use this data for threat hunting and to tune their security polices and architectures.

Endpoint Isolation - Benefits

Endpoint Isolation 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.

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. And it's safer than EDR, because the malware is contained in a µVM.

3 Security Efficiency

By preventing malware from installing, Endpoint Isolation significantly decreases the number of "high priority" tickets that a Security Operations Center (SOC) or MSSP must deal with. It also decreases the number of costly and time-consuming remediations.

4 End-user Experience

Users can work with confidence. There is no need for extensive phishing training, since high-risk tasks are automatically contained. Users 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, Isolation is operationally efficient, and easily validated during an audit.

HP Security Solutions Based on Endpoint Isolation

HP offers Endpoint Isolation technology in the following solutions:

Sure Click Enterprise[1]	Wolf Pro Security[2]	Sure Access Enterprise[3]
Isolation-based Threat Containment for Windows PCs, with full support for complex policies, RBAC, and integrations.	Isolation-based Threat Containment with a simplified management model for smaller organizations or those that lack a security team. Includes optional NGAV.	Protects privileged user activity by isolating sensitive activity such as remote IT administration from potential threats.

Endpoint Isolation - Example Scenarios

Ransomware Attack on Accounts Payable

Scenario: A ransomware attack is encapsulated in a fake invoice PDF. The file is attached to an email that is sent to the Accounts Payable Department of the targeted company. An employee opens the email and the attached invoice. This unleashes a ransomware attack on the entire organization. This scenario is very simple, and very common.

Now let's assume that Sure Click Enterprise is installed in the organization. The fake invoice would have been opened within a hardware-enforced µVM. The ransomware would run, but would not be able to encrypt any files since it ran within the µVM, rendering it harmless. The attack would not have succeeded, and the Security Team or MSSP would be able to detect and understand the attempted attack through Introspection.

IT Administrator Spear Phishing

Scenario: An IT administrator at an electric utility company uses his PC for both company and personal activities. He was successfully spear phished via his Gmail account and malware is resident on his PC. He later works on critical IT and cloud systems remotely using RDP and web portals. The attacker is able to exfiltrate both sensitive data and privileged credentials by using the malware on the PC to monitor the user's activity.

However, if the PC had been running Sure Access Enterprise, the remote access sessions to the critical systems would have been isolated from the PC's operating system. This means that the malware would have no access to the privileged keyboard, display or memory activity and would have been unable to exfiltrate data or credentials.

Summary

Existing endpoint security solutions have proven unable to reliably prevent cyberattacks on endpoint systems and users. Endpoint Isolation is an innovative technology that changes the game. It delivers a broad set of benefits to security teams and end users: IT and security teams gain operational efficiencies, threat visibility, and simpler compliance controls, while end users can work with confidence knowing they are "inherently protected." Therefore, Endpoint Isolation should be considered by all types of organizations seeking to improve their defenses and reduce operational challenges.

[1] HP Sure Click Enterprise is sold separately and requires Windows 8 or 10 Pro and higher and Microsoft Internet Explorer, Google Chrome, Chromium or Firefox are supported. Supported attachments include Microsoft Office (Word, Excel, PowerPoint) and PDF files, when Microsoft Office or Adobe Acrobat are installed.

[2] HP Wolf Pro Security is available preloaded on select HP devices, is available as a subscription and in term licenses. See HP Wolf Security.

[3] HP Sure Access Enterprise is sold separately and requires Windows 10 Pro or Enterprise. HP services are governed by the applicable HP terms and conditions of service provided or indicated to Customer at the time of purchase. Customer may have additional statutory rights according to applicable local laws, and such rights are not in any way affected by the HP terms and conditions of service or the HP Limited Warranty provided with your HP Product. For full system requirements, please visit www.hpdaas.com/requirements.