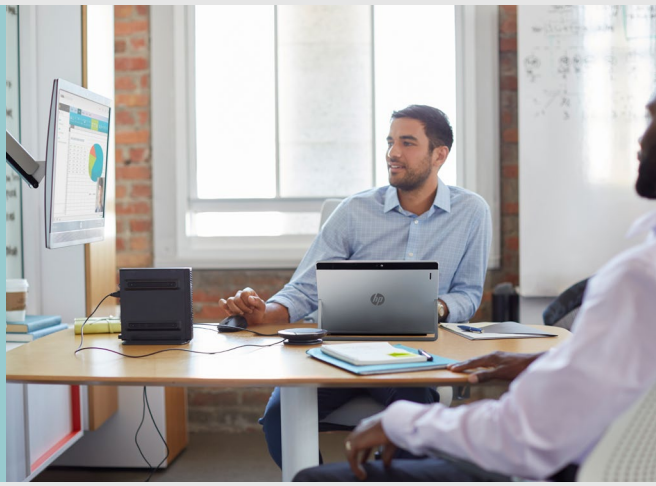
Threat Containment for State and Local Governments



State and Local Government Challenges

State and Local governments are increasingly facing more successful cyberattacks. The attacks hit a variety of areas from 911 or emergency services, public school systems, road safety to local elections. Many state and local government offices can't follow security industry best practices due to reduction in budget or changes to the political climate. They struggle to hire and retain qualified IT and Security staff to protect the technology infrastructure. As with any organization, the most vulnerable part of the infrastructure is the endpoint PC, where employees, data, and the Internet converge. Keeping employees safe from unknown threats and malware becomes paramount. State and local governments must balance the need for PC security to keep all employees safe with limited budget and security staff expertise while ensuring government services continue to protect residents' personal data and support the local community.

Threat Containment using Endpoint Isolation

Many employees inadvertently click on suspicious email attachments or open files that may contain Zero-Day, phishing, or ransomware attacks. HP's Threat Containment helps state and local governments meet those cybersecurity challenges. Based on our unique Endpoint Isolation technology, HP Threat Containment enables organizations to efficiently manage large amounts of PCs, filling security gaps that other solutions often miss while allowing employees to go about their normal daily tasks. 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 PC or moving laterally to other parts of the network. When the task is completed, the μVM is deleted taking the malware with it. This Threat Containment method is enforced by the CPU's hardware, so attacks can't get around it. And, it works on any PC with a modern Intel or AMD CPU.

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. Local government IT teams can use this data to tune their security polices and architectures.

Benefits for State and Local Municipalities

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 allowing employees 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 state and local government 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 local regional IT departments must deal with. It also decreases the number of costly and time consuming remediations.

4 End-user Experience

Employees can work with confidence. There is no need for extensive phishing training, since high-risk tasks are automatically contained. All employees in the local government area 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 Solution

HP Sure Click Enterprise (SCE)[1]	HP Wolf Pro Security (WPS)[2]
 HP Sure Click Enterprise (SCE) provides Threat Containment through Endpoint Isolation for government organizations.	 HP Wolf Pro Security delivers Threat Containment with a simplified management model for smaller organizations. It also comes with a Next Generation Antivirus (NGAV) that can be enabled or disabled depending on customer needs.

Summary

Existing endpoint security solutions have proven unable to reliably prevent cyberattacks on 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 employees can work with confidence knowing they are "inherently protected." It acts as a virtual safety net for Employees preventing unknown threats from slipping into the technology infrastructure. Therefore, Endpoint Isolation technology should be considered by state and local governments 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.

4AA8-2724ENW, May 2023