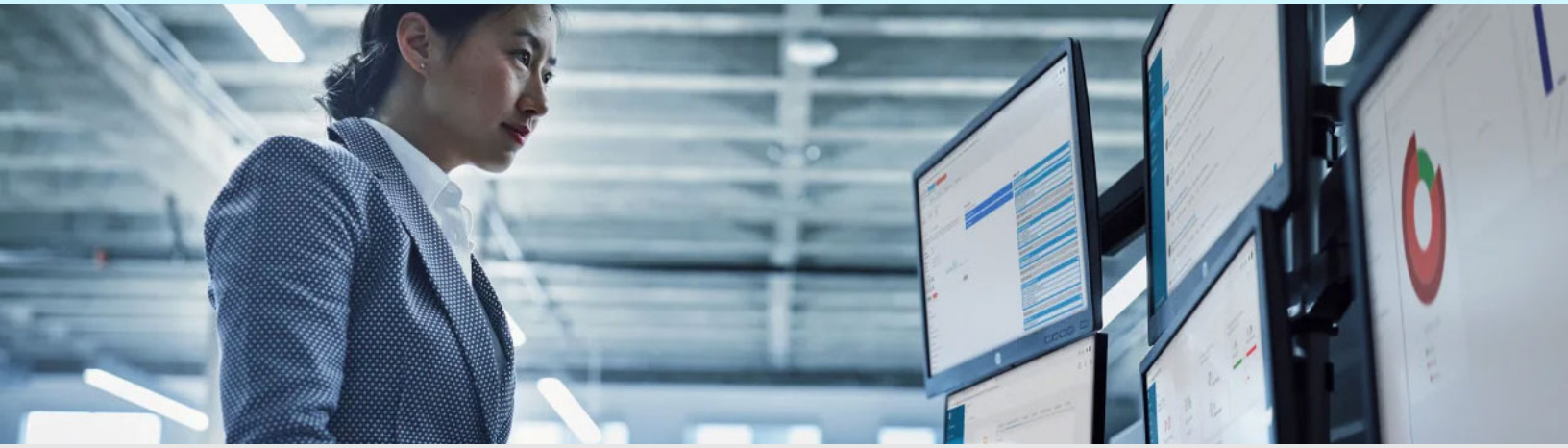
HP Sure Click Enterprise

Efficient Compensating Control for Patch Management



HIGHLIGHTS

- Patching is a critical security control, but endpoints are exposed between patch cycles
- Sure Click Enterprise (SCE)[1] isolates and contains malware so that it cannot exploit a vulnerability between patching cycles
- SCE can be used as a compensating control between patch cycles
- A compensation control activity based on SCE is both reliable and efficient, as well as effective

The Problem with Patching

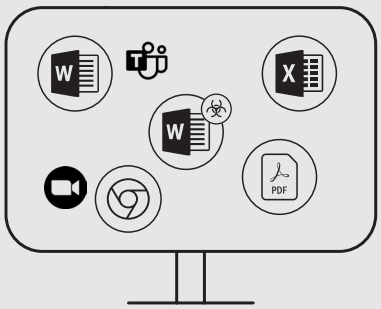
Timely patching is one of the most basic security controls, but it isn't easy to implement at scale. Patching is essential because it's the best way to eliminate vulnerabilities that could be exploited, and because it allows the target system to be improved on a regular basis. Therefore, virtually all compliance regimens, internal audit control requirements and security best practices mandate patching on in-scope systems.

However, systems are vulnerable between patching cycles - it's impossible to patch all systems all the time. A typical implementation is to scan every 30 days, and to remediate any findings within 30 to 90 days. Even if an organization wants to move faster, they often can't because of the need to validate and test all patches before deployment.

Unfortunately, threat actors develop exploits in a matter of hours or even minutes following a vulnerability disclosure. This creates significant risk that the vulnerability can be exploited in the gap before the next patch cycle. The risk is especially large for end-user PCs: they are plentiful, they are often not firewalled, and the compromise of any of them can lead to the compromise of the whole organization. Whereas previously just a small number of data center devices would have been "in-scope", with rise of remote working and hybrid cloud, all the user PCs are now too. So what's needed is a way to protect endpoint PCs between patching cycles without creating an unacceptable burden for the IT team or impacting user productivity.

Sure Click Enterprise – The Ideal Compensating Control for Patch Management

HP SURE CLICK ENTERPRISE



Sure Click Enterprise (SCE) is an effective compensating control to reduce the risk created by imperfect patching on endpoint PCs. Its core Threat Containment technology isolates and contains each user task that could result in a successful malware exploit.

SCE's "micro virtual-machines" (uVMs) are built dynamically for each task and are enforced by the PC's CPU hardware, so malware can't get around it. The idea is that between patch cycles SCE's uVM isolation is "inherently protective": preventing an attacker from leveraging a vulnerability that's been disclosed but not yet patched.

In practice, Sure Click Enterprise is deployed on each PC, and is complimentary to vulnerability and patch management solutions. As it doesn't require tuning to cope with particular vulnerabilities, it's a simple matter to operationalize SCE on endpoint PCs at scale.

SCE's primary role is to isolate and contain risky activity, but it also offers Introspection. This capability observes and records activity within the uVMs, providing superior visibility of the techniques, tactics and processes (TTPs) being used by threat actors. This data is centralized (either on-prem or in the cloud) and combined with other threat intelligence to provide TTP framework analysis, historical analytics, and recommendations for security policy improvements.

SCE as a Compensating Control Delivers Substantial Operational Benefits

SCE Threat Containment provides a unique combination of benefits when used as a compensating control for endpoint patch management:

EFFECTIVENESS

- Risk is significantly reduced, because vulnerabilities can't be exploited between patch cycles.

RELIABILITY

- The SCE compensation control is "self-contained". Its inherent protection operates independently of integrations with other systems, manual procedures, or updates.
- Easy to provide evidence of reliable control activity to an auditor.

OPERATIONAL EFFICIENCY

- SCE does not require significant monitoring, tuning, or response to provide the compensation control.
- Pressure on SOC teams is reduced, because there are fewer "high priority" tickets occurring because of real or suspected endpoint compromise.

Summary

Patching is a critical but flawed control because “continuous patching” is impossible. The “inherent protection” provided by Sure Click Enterprise isolation protects systems from vulnerability exploits between patch cycles. It is operationally efficient, simple to deploy, and highly reliable.

[1] Sure Click Enterprise supports Microsoft Windows 10 Professional and Windows 11 Professional operating systems.

4AA8-1543ENW, April 2022