HP WOLF SECURITY

HP Engage for Healthcare End-Point Security

Overview

Healthcare data has long been targeted by cybercriminals, because it yields a high payout due to the high cost per data breach. So it is not surprising that healthcare has received a large increase in the number of ransomware attacks.[1]

How is this happening?

- Email communication within healthcare organizations has become more prevalent and the increased use of telehealth services has added to the risks of possible interception by cybercriminals. In fact, the most common (94%) entry point for cybercriminals to attack an organization is through email.[2]
- Medical professionals often need to access medical data remotely, making them a prime target for phishing attacks. The breach might occur when an employee (with a health system email account) responds to a phishing attempt by typing in their log-in credentials, which in turn enables the cybercriminal access to the network.
- Other phishing attacks may occur within browsing environments, collaboration apps, or e-documents. These threats continue in part because the use of traditional anti-virus and detection-based security tools has not been strong enough. Healthcare institutions continue to fall victim and need solutions to stop these attacks at the outset.

HIGHLIGHTS

- Healthcare IT Operations teams need a plan for resilience and recovery.
- HP Engage Long Lifecycle systems have been designed, from the hardware up, to be resilient not just against the attacks of today, but also against the evolving attacks of tomorrow.
- Healthcare organizations utilizing HP's Wolf Security[3] stack can lower their IT costs with fewer support calls and interventions, resolving malware attacks.

HP's FULL-STACK APPROACH ON SECURITY

In order to be fully resilient at the system or endpoint level against attacks, healthcare organizations need to consider the different layers at risk and take a 'full-stack' approach to securing their environment. Each layer represents an area of potential risk and needs to be protected by security tools that:

- Detect threats
- Thwart them off and eliminate them
- Swiftly recover at every level of the system

HP's full-stack approach on endpoint security begins below the OS with foundational protection at the BIOS level, then continues in and above the OS, and finally extends to the physical level with built-in user security features.

PC Platform Security

HP Sure Start[4]	Remediation of a system with a firmware issue is expensive, complex, and can cause significant downtime for a healthcare operation. HP Engage long lifecycle systems featuring HP Sure Start are perpetually inspecting the system BIOS/firmware and automatically self-heal if the BIOS is damaged by malware, rootkits, or other forms of corruption. If any BIOS/firmware tampering is detected, HP Sure Start, in concert with the HP Endpoint Security Controller, replaces the affected BIOS/firmware with a clean version and boots up the system with a fully functional BIOS/firmware. HP's protection at the foundational level allows healthcare employees to remain productive without interruption.
HP Sure Admin[5]	Using weak passwords or a single one across multiple systems can open up areas of attack. Healthcare IT administrators can bypass the need for a password altogether by using HP Sure Admin. This modern BIOS management tool utilizes digital certificates and strong public-key cryptography, allowing healthcare IT administrators to securely and remotely manage system BIOS settings over a network without the need for a password.
HP Sure Run[6]	Healthcare IT environments run many processes that are critical to the well-being of their patients. Malware attacks that threaten these ongoing operations must be stopped in their tracks. HP Sure Run monitors key processes, alerts users and IT of any unwanted changes to security settings, and restarts key processes automatically if users or advanced malware try to shut them down.
HP Sure Recover[7]	When disaster strikes a system user, healthcare IT administrators need a recovery process in place to prevent downtime and lost productivity. HP Sure Recover leverages the power of the HP Endpoint Security Controller to quickly restore the operating system when the hard drive has been compromised or corrupted. Users can be supported remotely and have their image recovered even if their primary drive has been completely erased.

Application Layer Security

Even when a platform has security, the applications above it can still be vulnerable. HP's Wolf Security[3] stack also includes hardware-enforced isolation technology, anti-phishing credential protection, and next generation antivirus for unrivaled protection at the application layer.

HP Sure Sense, a Next Generation Antivirus[8]

Traditional antivirus protection can't always recognize new attacks. HP Sure Sense harnesses the power of deep-learning AI to identify and quarantine never-before-seen attacks, helping prevent infections before they happen. It is a lightweight agent that doesn't require constant updating to protect your system in real time. HP Sure Sense operates within the OS in concert with HP Sure Run to keep endpoints protected 24/7 whether the endpoint is online or offline.

HP Sure Click Enterprise using Endpoint Isolation Technology[8]

Comprehensive protection against browser-based, email, or social media attacks has never been more imperative. HP Sure Click is a hardware-enforced, secure browsing solution within the OS that isolates web content in a CPU-isolated virtual machine, where malware cannot affect other applications, documents, intranets, or the operating system. Malware is automatically erased when the browser tab is closed, thereby eliminating costly remediation and downtime. HP Sure Click also isolates threats for read-only mode viewing of PDF, Microsoft Word, and Microsoft Excel files.

Physical Security

Physical attacks are difficult to detect and remediate. HP Engage long lifecycle systems include built-in physical protections against intruders including biometric authentication, chassis locks, and port disablement options. Physical theft or loss, while more common in the mobile environment, can open up healthcare organizations to unnecessary risk. The HP Engage Go 10 tablet can be securely locked in the HP Engage Go 10 Convertible Dock[9] or in the HP Engage Go 10 Multi-charger[9]. When ready for use out on the floor the tablet can be mechanically unlocked. To assist with this transition, the HP Smart Dock app allows users to automatically unlock their tablet from the HP Engage Go 10 Convertible Dock by inputting a password, or PIN, through Windows Hello and facial recognition, or by fingerprint reader for additional factor authentication.[10]

HP Engage for Healthcare Environment Security

	OUTCOME	DESCRIPTION	CAPABILITIES
Incident & Disaster Recovery	Incident & Disaster Recovery	Re-establish employee productivity in case of endpoint corruption failure or disaster scenario	Recover clean OS image at scale on HP Engage long lifecycle systems to avoid interruption and continue operations; secure, remote re-imaging of customized Windows OS using HP Sure Recover
Operation Continuity	Operation Continuity	Reduce downtime, disruptions, and IT trouble tickets to drive operational efficiency	Rapid OS re-imaging, self-healing BIOS, and seamless firmware updates
PC Platform Integrity	PC Platform Integrity	HP Isolation technology and threat containment	Using hardware-enforced protection rooted in Zero Trust principles, malware is prevented from infecting the PC
Loss Prevention	Loss Prevention	Loss of sensitive data and/or device through unattended PC system	USB controls, Secure BIOS, HP Smart Dock
IT Cost Savings	IT Cost Savings	Lower TCO due to fewer support calls and interventions resolving malware attacks	
Compliance	Assists with HIPAA and GDR Regulatory Requirements	Data protection helps contribute to a successful compliance with regulatory requirements	

Summary

Stable and continuous operations are critical to healthcare organizations. Keeping processes going can mean everything for patient care. Many of today's traditional anti-virus solutions are not enough to protect critical data from the persistent threat of cyberattacks. Healthcare organizations need a new and comprehensive approach that provides protection at every level, starting with a firm foundation. HP full-stack solution starts with a hardware root of trust, the HP Endpoint Security Controller, which provides hardware-based protection and is the key driver behind the resilience of HP Sure Start, Sure Run, and Sure Recover. This combination security stack preserves platform integrity and dramatically reduces interruptions and the potential for a catastrophic breach and loss.

Sources:

1. Cost of a Data Breach Report 2021, IBM Security, July 2021. Cyberattacks on healthcare have continued to rise over the years and have seen a 29% increase in the average cost of a breach in 2021. Why? Because healthcare data provides the highest return for cybercriminals, putting healthcare institutions at the top of their list of victims. Example shown in articles: San Diego Health Faces Class Action Lawsuits Over Phishing Attack – CalHIPAA and UC San Diego Health announces data breach - The San Diego Union-Tribune (sandiegouniontribune.com)

2. https://www.teiss.co.uk/r3/cth_schedule/94-of-cyber-attacks-start-with-an-email-how-resilient-is-your-endpoint-protection-solution/

Disclaimers:

3. HP Wolf Security for Business requires Windows 10 or higher, includes various HP security features and is available on HP Engage products. See product details for included security features.

4. HP Sure Start Gen6 is available on select HP systems and requires Windows 10 or later.

5. HP Sure Admin requires Windows 10 or later, HP BIOS, HP Manageability Integration Kit from http://www.hp.com/go/clientmanagement and HP Sure Admin Local Access Authenticator smartphone app from the Android or Apple store.

6. HP Sure Run Gen4 is available on select HP systems and requires Windows 10 or later.

7. HP Sure Recover Gen4 is available on select HP systems and requires Windows 10 or later and an open network connection. You must back up important files, data, photos, videos, etc. before using HP Sure Recover to avoid loss of data. Network based recovery using Wi-Fi is only available on systems with Intel Wi-Fi Module.

8. HP Wolf Pro Security: 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.

9. Accessories sold separately.

10. Configure HP Smart Dock to establish a list of approved users.

4AA8-2479ENW, January 2023

HP WOLF SECURITY