Why You Need A Security Led Approach To Employee Device Management

It's Time To Start Taking Device Security Seriously - Here's How…

Protect, Secure and Manage - The New Way To Manage Devices

Cybercrime Is On The Rise - How To Protect Company Devices

Secure Your Devices with DaaS - An Overview Of The Solution Security Features

Unfortunately, during these tough times of economic uncertainty and operational changes caused by the COVID-19 pandemic, the coronavirus isn't the only virus to sweep the world, with organisations seeing an increase in data breaches and specifically, ransomware attacks.

> *By 20 May, over 150 organisations globally have had their data published on leak sites; the majority of these (60%) have occurred after 11 March, when the WHO first declared the COVID-19 outbreak to be a pandemic. Of these, the overwhelming majority (80%) were leaked after 23 March, when the lockdown commenced in the UK.* (Why has there been an increase in cyber security incidents during COVID-19?, pwc)

Although we can't be certain that all of the attacks are due to cyber-criminals taking advantage of the crisis situation, there is a lot of speculation that 'bad actors' are making the most of less-secure home networks to access and hold business data to ransom. Cyfirma even report that their threat visibility and intelligence research showed a 600% increase in cyber threat indicators from February to March in relation to the pandemic.

Further to this, some of the more sophisticated attacks and phishing emails are using news related information and the names and logos of official organisations, such as the World Health Organisation (WHO) to trick people into opening links disguised as information about the pandemic.

With so many employees still working remotely, security is of the utmost importance and while employees are using devices away from the office, you need to consider how to approach security issues and make sure everyone is protected regardless of the network they're connected to.

It's also important to realise that every company is vulnerable to these attacks - for example, Honda recently suffered a large breach, meaning they had to stop global production and give some employees time off as they couldn't access their work laptops.

> *The attack on Honda is the latest in a string around the world, as cyber security experts have warned of the risk of an increase because the pandemic has left hundreds of thousands of staff using computer laptops on unsecured home WiFi.* (Carmaker Honda targeted in cyber attack, FT)

With cybercrime currently on the rise, it's a good time to realise that the laptops you dug out of a back cupboard in the IT department when lockdown began might not be up to the job when it comes to keeping employees safe on their home networks.

The best form of security is prevention - essentially, don't let it happen in the first place. But second to this, is the opportunity to catch the security breach early, keep it contained and overcome it before it becomes a problem.

Prevent, Secure, Manage

HP recently set out a 7-point program that they recommend for IT decision makers, security ops, IT admins and end users: (Endpoint Security Best Practices in the New Norm, HP)

1) Protect your endpoints
2) Advocate and Enable Digital Hygiene
3) Secure Sensitive Data
4) Ensure Safe Network Access
5) Take Special Care of Credentials
6) Manage Conferencing Security and Privacy
7) Productivity

These 7 points are a great approach to security, and with HP-Xenith Device-as-a-Service (DaaS), you can ensure that all of these points are covered.

The devices provided with DaaS are secure laptops with multi-layered, enterprise-class security providing: malware protection, real-time policy violation and firewall, and antivirus disruption alerts, plus find, lock, and erase functionality.

They are the only laptops capable of protecting against both Malware and Ransomware attacks effectively, without the need for IT intervention.

Here's a breakdown of the prevention, security and management features included with our HP DaaS solution: (The World's Most Secure PCs - A complete guide to HP security, HP)

HP Sure Sense
Sure Sense uses deep learning AI to detect and prevent threats in real-time, meaning any malicious or unusual activities are picked up on before they can become an issue.

HP Sure Click
Sure Click is a hardware-enforced secure browser solution that isolates web content in a CPU isolated virtual machine. What this means is that any malware cannot affect other open browser tabs, applications or crucially the operating system - it's essentially a secure lockbox for individual web content a user opens.

HP Sure View

Sure View is a built-in privacy screen that can be enabled at a touch of a button, allowing only the user sitting directly in front of the screen to see what's on it.

HP Privacy Camera
The privacy camera on the HP secure devices includes a physical shutter to protect from malicious surveillance of the user.

HP Secure Erase
Secure Erase takes deleting files to the next level, using a BIOS-level feature that permanently destroys sensitive data from hard drives and solid-state drives meaning it can never be recovered or compromised.

Certified Self-Encrypting Drives
Self-encrypting hard drives and solid-state drives employ hardware-based encryption to protect the content on the drive, even if the drive is removed from the device.

HP Sure Start
Sure Start continuously inspects the BIOS and automatically heals the BIOS if it's been damaged by malware, rootkits or corruption. *It is the world's ONLY self-healing BIOS.*

HP Sure Run
Sure Run is all about keeping critical processes running with the help of hardware enforced protection by monitoring all key processes and alerting users and IT of any changes *and* restarting processes automatically if they are stopped.

HP Sure Recover
Sure Recover is built into the device hardware and firmware and enables end-users to restore their machines quickly and securely to the latest image using a network connection. IT can even schedule reimaging for an entire fleet of devices.

HP Endpoint Security Controller
Endpoint Security Controller is the hardware foundation for the security architecture in HP devices. It's physically isolated and cryptographically protected hardware creates the root of trust that enables hardware-enforced, self-healing, manageable security solutions like HP Sure Start, HP Sure Run and HP Sure Recover.

HP Client Security Manager
Client Security Manager enables IT professionals to control a variety of the security features built into the HP devices - including Sure Run and SpareKey.

HP SpareKey
SpareKey allows you to reset passwords and restore access to locked PCs (for when someone forgets their password!) without the need of IT intervention, using a set of predetermined security questions.

HP Multi-Factor Authenticate

Multi-Factor Authenticate helps keep your network and VPN safe from unauthorised access by requiring up to three factors of authentication for login.

HP Image Assistant

Image Assistant is all about developing and maintaining a robust software image and ensuring that it remains up to date with the latest patches and upgrades and is implemented consistently across the fleet of devices.

HP Manageability Integration Kit

The HP Manageability Integration Kit (MIK) is designed to integrate with Microsoft System Center Configuration Manager (SCCM) to help IT administrators update and maintain software and security settings across your fleet of PCs.

While IT teams are not able to mitigate attacks that occur at unsecured locations, such as people's homes or internet hotspots, HP Xenith DaaS is the only option that can ensure your information is secured and kept safe. It is the true way to take a security led approach to device management.

As we previously stated, the best defence is prevention. That means deploying protection before it's too late. We want to help by offering you a free trial of Tech Pulse Proactive Management. 'link to Xenith techpulse signup'