Solution Brief

HP Security & Thin Clients

Enterprise computing is undergoing a significant transition. Workforces and workstyles are changing as the workplace modernizes. "Working from home" now encompasses coffee shops and airport lounges. Today, only 55% of an employee's time in the office is spent at a permanent desk[1]. Growth of mobile workers increases the chance of losing data and intellectual property. This can lead to a loss of revenue and opportunity, which can result in embarrassment and regulatory fines. Cyber-attacks are growing in frequency and in sophistication; 81% of healthcare companies had a security breach in the past 12 months, costing $3.6M on average[2]. Maintaining business continuity, complying with regulatory requirements, and responding to security incidents are the main security challenges facing organizations today.

HP is an industry leader with security innovations.

HP is a trusted partner and recognizes our responsibility to protect our customers' data and intellectual property. The HP product development framework is based on a set of principles intended to foster security innovations across all development teams and the programs they deliver to the market. Dedicated security core teams, made up of subject matter experts, consult with every HP business unit to drive the latest security principles and best practices into every product.

Cloud enhances security with app and desktop virtualization.

A modern and centralized cloud computing model moves processing and storage of data from the local client to the cloud. This ensures data is hosted and secured away from traditional threats that plague local clients. Thin clients support cloud computing with a naturally secure endpoint that easily interfaces with the internet, VDI, and cloud services, while keeping the local client's participation in processing and data storage to a minimum.

HP Thin Clients are secure by design.

Just like protection from a cold, effective security is all about layers. Adversaries can be thwarted one layer at a time from reaching their target. The security community refers to this as *defense in depth*. As part of an effective cloud computing strategy, HP Thin Clients build layer upon layer of hardware and software barriers that protect the device, data, and user's identity.

Device security for resiliency, recoverability, and tamper prevention.

HP Thin Clients are designed to be a total security machine, with hardware and software features built in right in:

- Security begins with a secure and manageable UEFI (BIOS). All models start up with UEFI Secure Boot, and our firmware is compliant with NIST SP800-147 and SP800-155 guidelines.
- HP Mobile Thin Clients include HP Sure Start[3], an industry leading technology layer that implements NIST SP800-193 guidelines, which detect and prevent malicious attacks on the UEFI.
- A certified Trusted Platform Module (TPM) integrated across our portfolio[10] provides a layer of hardware protection for identities, credentials, and encryption keys.
- The HP t640 and HP t740 Thin Clients are equipped with AMD Memory Guard[9], an innovative technology that neutralizes the threat of a cold boot attack. It does this by physically removing the volatile SDRAM modules to gain access to the data held before a reboot can wipe them clean.
- Sometimes you just need to protect against the old-school threat of someone stealing your physical assets. HP Thin Clients support industry-standard cable locks and integrated mounting solutions[11] to physically secure your device.

Data security for protecting transient data and preventing data leakage or theft.

Modern cloud computing is a balance between data security and user access. Users can be willingly, or unknowingly, a point of security weakness. HP Thin Clients include layers of protection to help IT administrators, and the users they support, defend the necessary user access tools such as passwords, security tokens, and USB access ports.

- The HP ThinPro operating system features a read-only locked file system and encrypted registry to keep user data safe. HP ThinPro OS also contains an integrated Intrusion Prevention System in the form of a configurable firewall to control and monitor inbound and outbound communications from the device.
- HP Thin Clients running Windows 10 IoT operating system use HP Write Manager to control access to the non-volatile flash storage. Data activities take place in SDRAM which is flushed with every reboot. Any issue experienced in a user-session is cleared and cannot be carried over to further sessions.
- USB ports, and the devices connected to them, are protected by HP USB Port Manager[5]. IT administrators can create custom policies as necessary layers of data security at this critical access point.
- Visual hacking is a real threat so select HP Mobile Thin Clients come with HP Sure View[6] technology. HP Sure View limits the field of view to the display to a narrow range only usable by the intended viewer. HP Sure View is integrated into the product, so the feature is available at the press of a button.

Identity security for ensuring the right access to the right person.

An integral component of any secure endpoint ecosystem is identity protection. Understanding who has access to what resources through authentication and authorization is a key component to maintaining proper controls over your devices, users, and applications.

- HP Thin Clients integrate seamlessly within an 802.1x authenticated network and also support machine level identity within Active Directory to provide identity, discoverability, and endpoint management functions.
- IT administrators can control user privileges and access to system resources, configuration options, and sensitive data using layers of authentication and identity confirmation. This includes fingerprint, face, contact, and contactless smart cards, USB security tokens, one-time-password tokens, and NFC.[7]
- HP Thin Clients also come preinstalled with support for industry standard SSO solutions.[7]

Management tools for centralized and simplified device management.

HP Device Manager (HPDM) is a highly scalable and centralized device management tool. With HPDM, changes can be applied swiftly and uniformly across the infrastructure whether the endpoint is available or offline[8], ensuring your endpoints always have the latest security patches and updates.

HP Thin Clients provide solutions for every security challenge that enterprises face.

Security is key to maintaining business continuity, complying with regulatory requirements, and responding to security incidents. HP Thin Clients are built with security as an integral part of the product design and development process to begin protecting right out of the box.

Learn more at
hp.com/go/thin

1. Technalysis Research, Workplace of the Future: Progress, But Slowly, Feb 2017
2. Analysis of 2018 Healthcare Data Breaches, https://www.hipaajournal.com/analysis-of-healthcare-data-breaches/
3. HP SureStart Gen5 and BIOSphere Gen5 features may vary depending on the PC platform and configurations and requires 8th Gen AMD processors.
4. Based on currently available, in-market desktop thin clients as of July 2019 having AMD Memory Guard for data protection
5. Only available on Thin Clients with Windows OS
6. HP Sure View privacy screen is an optional feature and requires factory configuration at time of purchase. HP Sure View integrated privacy screen is an optional feature that must be configured at purchase and is designed to function in landscape orientation.
7. Optional features sold separately or as add on features.
8. Internet access required and sold separately
9. Only available on the HP t640 and t740 Thin Client
10. Not available on the HP t240 Thin Client
11. Mounting hardware sold separately.