PC University NYS OGS HP Printer / Scanner– Contract # PT66605

Secure Your School's Open Environment Network

Breaches Cost More than Money

Networks configured within education organizations of all types and sizes have increasingly become lucrative targets for cyber criminals, due to the massive amounts of personal information stored about applicants, students, faculty, employees and alumni—to name a few. By the very nature of these organizations, their networks have been built as open environments for the free exchange of information between multiple entities. And unlike private enterprises, security is difficult to centralize. The risks are many, and pose serious challenges for IT management accountable for securing these networks.

Data on cyber threats in education organizations trend closely to general market trends:

- 73% of CISOs expect to experience a major security breach within a year[1]
- It is estimated that hacking attacks cost global firms an average of $7.7 million/year, while U.S. firms average $15.4 million/year[2]
- 64% of IT managers believe their printers are likely infected with malware[3]

With the advent of the Internet of Things (IoT), a plethora of devices are now connecting to the internet anytime, anywhere within K-12, colleges and universities. Risk levels have heightened. The amount of damage caused by a cyberattack has increased exponentially.

Routine use of printers and imaging devices, previously connected to computers by cables, are now immediately accessible across a broad spectrum of users and environments via Wi-Fi. The increased complexity of printer and imaging devices means that attackers have even greater opportunities to compromise a device, and with it an entire network. The potential costs associated with even one breach can be staggering. Unfortunately, 56 percent of participants in an annual nationwide survey admit they ignore printers in their endpoint security strategy.[3]

The time has come to close the printer/imaging security gap for education organizations.

Let HP LaserJet and PageWide printers and MFPs manage your security processes

HP Secure Managed Print Services (MPS) takes the burden off you by:

- Assessing risks
- Securing and managing entire imaging/printing devices
- Maintaining printer security compliance
- Providing updated protections

HP LaserJet and PageWide Enterprise printers and MFPs enable robust protection through embedded security features. This means you can have the deepest levels of printer security in the market with HP Enterprise devices featuring HP FutureSmart Firmware.[4] When teamed with a complete range of HP JetAdvantage solutions and services, it's possible to create a strategic base of assessment, management and sustained security for:

- Imaging and printing fleets
- Data in transit and at rest
- Printed documents
- Cloud access
- Printing from mobile devices

HP LaserJet and PageWide Pro printers and MFPs

HP LaserJet and PageWide printers and MFPs include features that protect you from all angles:

- Secure boot validates the integrity of the boot code at every boot cycle
- Firmware integrity validation authenticates firmware updates prior to being loaded
- Real-time code integrity stops intruders from introducing malicious code while the printer is running

Exclusive HP Enterprise Self-Healing Print Features Automatically Repel Cyber Crime Offensives

HP LaserJet and PageWide Enterprise printers and MFPs offer three unique technologies to obstruct cybercrime efforts and self-heal.[5] Reboots are triggered at the time of attack or anomaly. Then, following a reboot, HP JetAdvantage Security Manager routinely assesses and, if necessary, remediates device security settings aligned with prior accepted company policies[6] – without IT intervention.

These three key technologies are:

- **HP Sure Start** – a behind the scenes safeguard against attacks on your device while printing and imaging devices power on
- **Whitelisting** – ensures that authentic HP FutureSmart Firmware, signed digitally by HP, has not been tampered with prior to loading into memory
- **Run-time intrusion detection** – helps to safeguard devices while operational and connected to the network – at the very time the majority of cyberattacks typically occur

The World's Most Secure and Manageable PCs[7]

A complete selection of security technologies has been built into every HP Elite PC. These technologies are called HP ProtectTools, tasked with optimizing IT security. HP Elite PCs enable users to determine who gets in and who is kept out through encrypted hard drives which permanently delete unwanted data. Corporate security policies can be easily applied with integrated hardware and software encryption, as well as iris and fingerprint authentication to help secure your data.

HP Elite PCs feature smart card keyboards as well as power-on and drive-lock passwords, plus facial recognition, ensuring that HP Elite PCs work only with authorized users. And with one of the most secure encryption standards in the industry – the embedded Trusted Platform Module – users rest easy knowing their data, email and user credentials are protected.

HP Elite PCs safeguard device, data, and identity with products and features to include:

- Exclusive HP Sure Start with Dynamic Protection, helping reduce concerns over malware or security breaches, securing HP Elite PCs at the BIOS level
- Applied corporate security policies that help secure authorized user data with integrated hardware and software encryption, as well as iris and fingerprint authentication
- Windows 10 Pro to protect business networks and resources as well as hardware security features like fingerprint readers and smart cards

About PC University Distributors, Inc.

Founded in 1996, PC University, an HP Market Star Partner, is a full-service technology solutions provider. We deliver today's best technology solutions and educational programs, as well as competitive pricing from more than 500 leading manufacturers – giving you or your organization the technology tools you need to succeed. With a combined 60+ years of experience selling to the education and government markets, at PC University we are confident that we can be of assistance in finding solutions to fit your needs and your budget.

To learn more about making HP printers, imaging, and HP Elite PCs an integral part of your organization's overall IT security strategy, contact PC University Distributors Inc. at 516-596-1500 or sales@pcuniversity.com

www.pcuniversity.com | 99 West Hawthorne Avenue, Suite 521, Valley Stream, NY 11580

[1] Hewlett Packard Enterprise, "35 Cyber Security Statistics Every CIO Should Know in 2017."
[2] Ponemon Institute LLC, "Cost of Cyber Crime 2016: Reducing the Risk of Business Innovation," sponsored by Hewlett Packard Enterprise, October 2016.
[3] Ponemon Institute, "Annual Global IT Security Benchmark Tracking Study", March 2015.
[4] Based on HP review of 2016 published security features of competitive in-class printers.
[5] Based on HP review of 2015 published embedded security features of competitive in-class printers. Only HP offers a combination of security features for integrity checking down to the BIOS with self-healing capabilities.
[6] HP JetAdvantage Security Manager must be purchased separately.
[7] Based on HP's unique and comprehensive security capabilities at no additional cost and HP Manageability Integration Kit's management of every aspect of a PC including hardware, BIOS and software management using Microsoft System Center Configuration Manager among vendors with >1M unit annual sales as of November 2016 on HP Elite PCs with 7th Gen Intel® Core® Processors, Intel® integrated graphics, and Intel® WLAN.

Partner First
Silver

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.