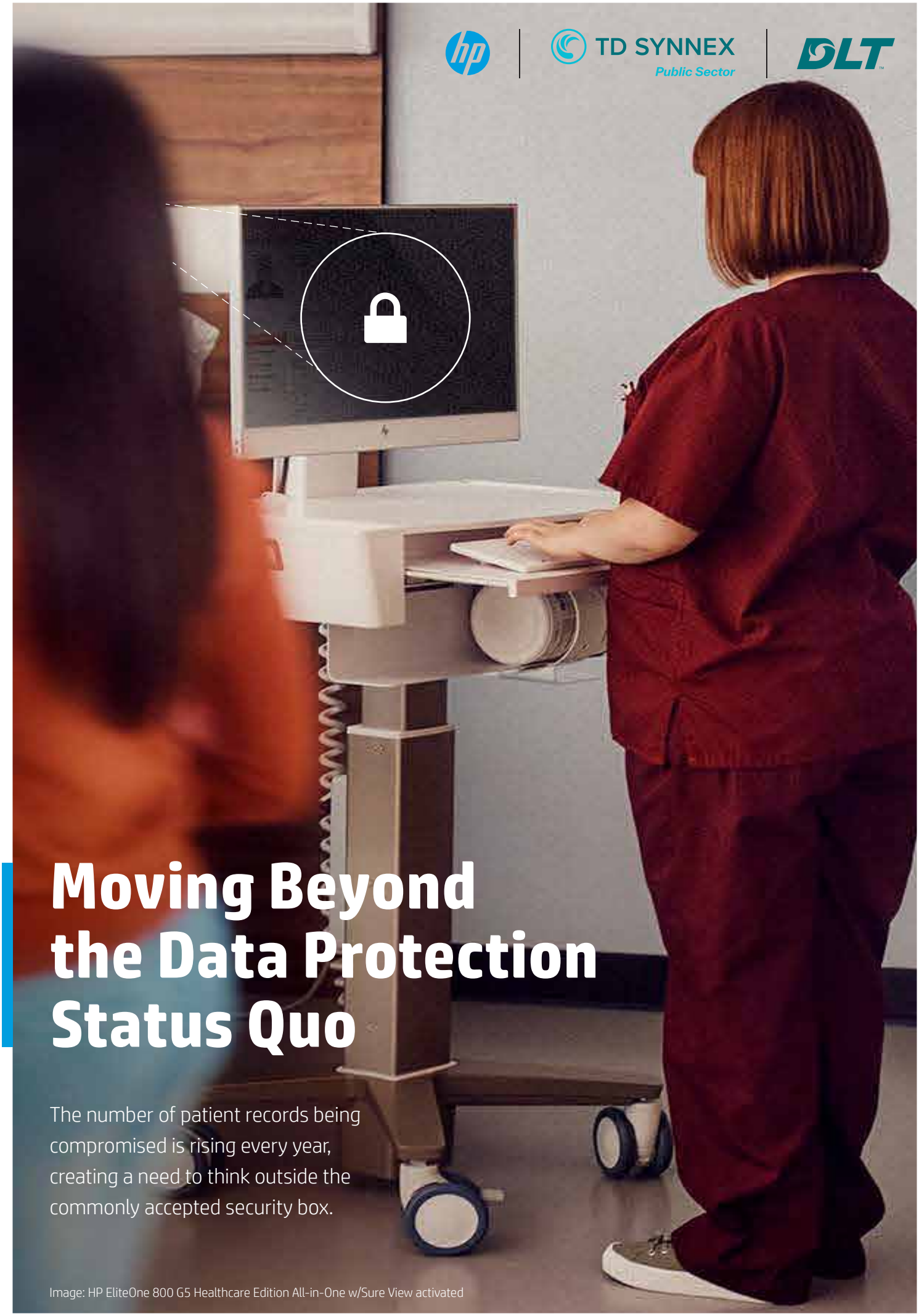

Moving Beyond the Data Protection Status Quo

The number of patient records being compromised is rising every year, creating a need to think outside the commonly accepted security box.

Image: HP EliteOne 800 G5 Healthcare Edition All-in-One w/Sure View activated

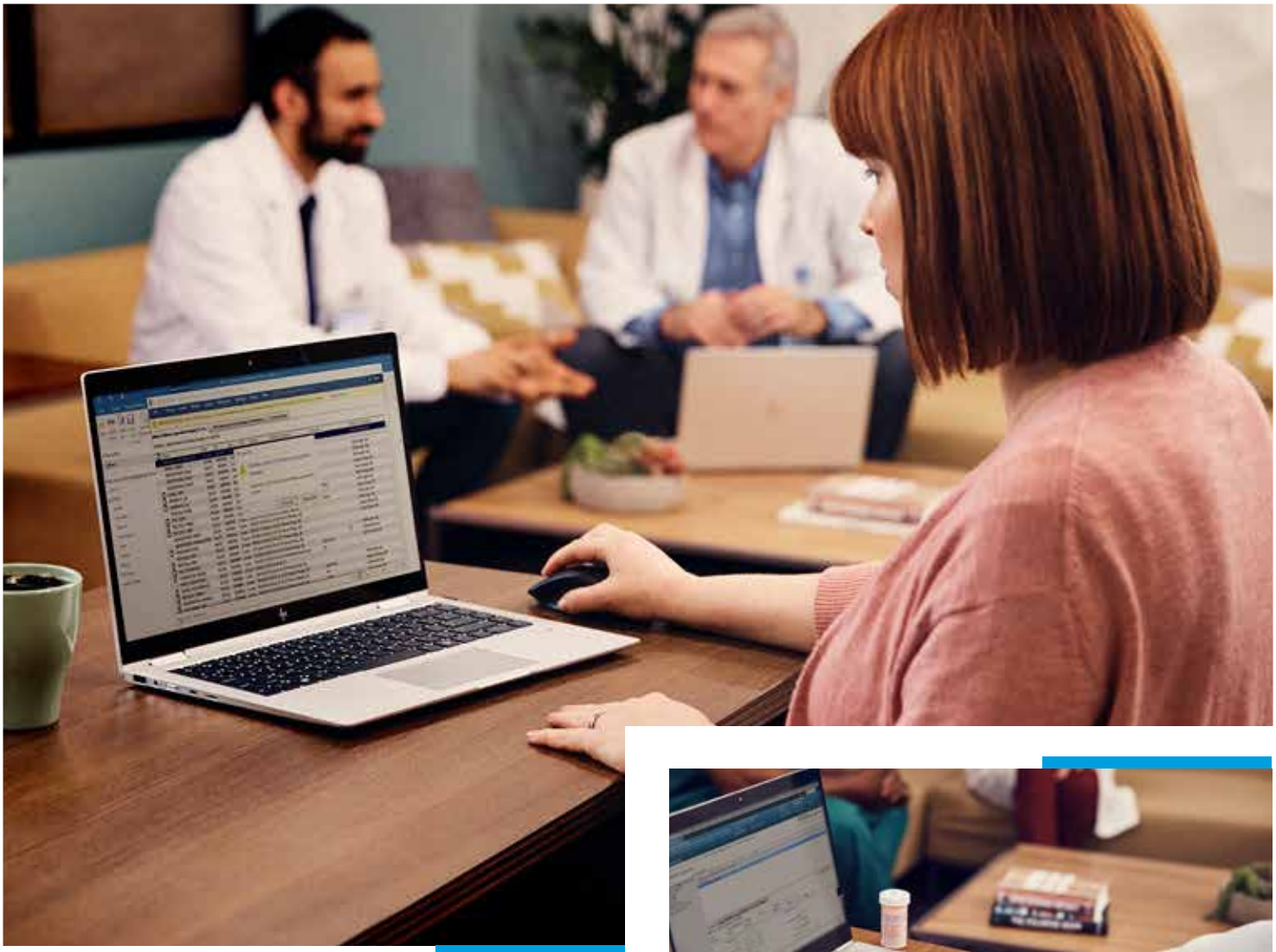

Image: HP EliteBook x360 1040 G6 w/Sure Click activated

Image: HP EliteBook 840 G6 Healthcare Edition Notebook w/optional fingerprint reader

Cybercrimes in healthcare

Some might consider the healthcare industry's response to cybercrime over the past several years "insane": many organizations keep doing the same thing over and over while data continues to be breached in large numbers.

Consider that in 2018, the healthcare sector experienced 15 million patient records compromised in 503 breaches, three times the number seen in 2017, according to the 2019 Protenus Breach Barometer. The situation seems to be getting even more dire, as about 25 million patient records have been breached in the first half of 2019.[1] Unfortunately, many provider organizations are feeling the sting. For example, more than 1.5 million patient records were breached at Inmediata Health Group, and nearly 1 million University of Washington Medicine patients had their data exposed online.[2]

"Healthcare continues to be a target that appeals to cybercriminals," said Rick Griencewic, HP Senior PC Security Advisor. "The information is valuable and, therefore, healthcare organizations are extremely vulnerable. This is nothing new, though. Healthcare organizations have been experiencing data breaches for several years now." The problem is that many healthcare organizations have "focused solely on making sure their firewalls are strong and making sure their server infrastructure is protected," he added. While such protection is necessary, it falls short of offering what's needed to help healthcare move beyond current data security results.

To better protect data, healthcare leaders need to think outside the commonly accepted security box.

Image: HP EliteBook 840 G6 Healthcare Edition Notebook w/Sure View activated

To better protect data, healthcare leaders need to think outside the commonly accepted security box. For example, they should focus on endpoints such as PCs and printers, which when unsecured are considered easy targets by hackers. Because these devices are connected to networks, when they become compromised, patient data is at risk. According to a report by the cybersecurity firm Armis, for example, WannaCry ransomware, released in 2017, is active on 145,000 devices worldwide and can attack 3,500 devices every hour.[3]

Surely, leaving endpoints open to attack creates many opportunities for cybercriminals. In a typical organization, the number of endpoints is much greater than the number of servers, sometimes as many as two devices per employee. Indeed, healthcare workers use a variety of devices, including a multitude of their personal ones, throughout the course of a typical workday.

"Just one vulnerable device can provide entry to the network, expose sensitive data, and put the entire infrastructure at risk," Griencewic said. "Because of this risk, it's obvious that healthcare organizations need to go beyond just focusing on operating systems and start to include endpoints such as computers, printers, smartphones, and IoT devices in their security plans. As such, procurement becomes a very important area to focus on. Leaders need to consider security in each device-purchasing decision they make."

Solution

Working with a vendor that builds protections into its devices can help. HP Healthcare Edition devices, for instance, offer the following:

Protection from the get-go: Both PCs and printers start up using the basic input/output system (BIOS). The BIOS, which includes time, date, and configuration settings, is responsible for controlling the basic functions of a computing device. As such, an unsecured BIOS can offer a dangerous degree of access to a hacker. BIOS-level attacks are very difficult to detect because they control the device below the operating system and cannot be removed or modified by anti-virus software. HP's Sure Start, however, monitors any changes in the BIOS. If there is a deviation, the BIOS is quarantined and replaced with its "golden image."

"The protection is built right into the hardware, which is a good thing because BIOS-level attacks can be the most devastating. With built-in BIOS protection, the BIOS is immediately replaced and your machine is healed," Griencewic noted.

Visual protection: "If somebody is walking by and inadvertently sees protected health information on a patient chart displayed on a computer screen, a healthcare organization can be subject to a huge fine," Griencewic said. HP Sure View protects sensitive information by making it difficult for onlookers to view it from the sides.

Proactive protection: More than 350,000 new malware variants are created daily. Traditional antivirus programs protect against these threats after they have already been hit. HP Sure Sense, however, relies on deep learning algorithms to instinctively recognize malware and protect against never-before-seen attacks.

"With this type of protection, it's possible to get out in front of an attack before it can do any damage," Griencewic said. "And healthcare organizations can finally move their data protection efforts forward."

Image: HP EliteOne 800 G5 Healthcare Edition All-in-One w/integrated dual-band RFID Reader, featuring HP Healthcare Edition USB Keyboard

Image: HP EliteBook x360 830 G6 w/Sure View activated

References

1. Protenus, Inc. in collaboration with DataBreaches.net. 2019 Protenus Breach Barometer Report. https://www.protenus.com/2019-breach-barometer.

2. Jessica Davis. “The 10 Biggest Healthcare Data Breaches of 2019, So Far.” Health IT Security. July 23, 2019. https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2019-so-far.

3. Ben Seri. “Two Years In and WannaCry is Still Unmanageable.” ARMIS. https://www.armis.com/resources/iot-security-blog/wannacry/.