ASUS ExpertBook P5440

Secure inside & out with BIOS-SHIELD™

BIOS SHIELD

- Data Encryption
- Time Machine Restoration
- USB Device Control
- USB Encryption
- Security Browser
- Cloud Management

Make remote work safer & more secure

Working from home is the new reality for many professionals. We may be safer at home, but cybersecurity threats have not abated—and employees may be more vulnerable to malicious actors than ever as they take their work PCs away from the centralized, managed environments of corporate campuses and into a world of untrusted devices, insecure networks, and social engineering threats.

Even as professionals move to cloud computing for collaborative work, attacks on corporate networks and local endpoints continue to pose a major threat to operations and the bottom line. Ransomware, or malware that worms its way through networks, servers, and endpoints and renders them inaccessible via encryption, is on the rise. Unless organizations pay hefty sums of money to free their systems and data, their work can be stopped cold. Even then, there's no guarantee that a malicious actor will restore access when a ransom is paid. All it takes is one unassuming user download to introduce this uniquely dangerous and costly malware to a device and possibly even to an entire network.

> “According to a report by the New York Times, ransomware attacks increased 41% in 2019[1], and the work of governments, health care providers, and major corporations alike has been stopped cold by these attacks—often for days or weeks at a time. Imagine how much money your organization could lose by being rendered idle by this type of threat. Indeed, the average cost of a single ransomware incident can be as much as $1,032,460, according to cybersecurity experts.[2] Recently, Garmin Inc. is reported to have paid as much as $10 million to regain access to its systems and restore services to its customers after a ransomware attack.[3]”

Malware isn't the only threat facing corporate PCs in our newly remote world. By their portable nature, laptops are easy targets for theft or misplacement, and that risk only grows when they're used at home. A user might forget a laptop somewhere outside the home, leave it in the car overnight where it could be a target of an opportunistic crime, or have it stolen from a remote work location like a coffee shop or library.

Without full-disk encryption or remote management technologies in place, a criminal might find themselves with vast amounts of data or proprietary information in hand that's far more valuable than the laptop hardware itself. One study found that the total cost of mitigating a stolen laptop incident costs organizations nearly $50,000, and that figure can rise to as much as $112,000 for businesses in the service industry.[4]

With all of these costly threats arrayed against endpoint PCs, you and your remote workers shouldn't put critical business data at risk on consumer systems that aren't designed with security in mind. You need a smart, durable, and reliable system with ground-up protection against these threats. That's where the ASUS ExpertBook P5440 with BIOS-SHIELD comes in.

Strong, safe, secure business partner

The ASUS ExpertBook P5440 is uniquely equipped to protect your remote workers' systems and sensitive corporate data thanks to its innovative set of hardware features and its pre-installed BIOS-SHIELD environment from Janus Technologies. The BIOS-SHIELD virtual environment delivers the security of a virtual desktop infrastructure deployment with all the native responsiveness and performance that users expect from a powerful local PC. The ExpertBook P5440 is one of the only systems to offer BIOS-SHIELD protection out of the box.

Whether you're a sole proprietor who simply wants a more secure PC, a small or medium business looking for a turn-key and manageable solution for remote workers, or a larger enterprise seeking to deploy many managed endpoints to employees at home, an ASUS ExpertBook P5440 with BIOS-SHIELD can help you and your business operate with more security and peace of mind. In tandem with other security best practices, such as keeping the operating system up to date and using a high-quality antivirus solution, BIOS-SHIELD serves as a barrier against show-stopping threats to local PCs. And if you're deploying ASUS ExpertBook P5440s as part of a centrally managed remote workforce, optional BIOS-SHIELD cloud features let your IT department take control of your endpoints from a convenient, centralized interface.†

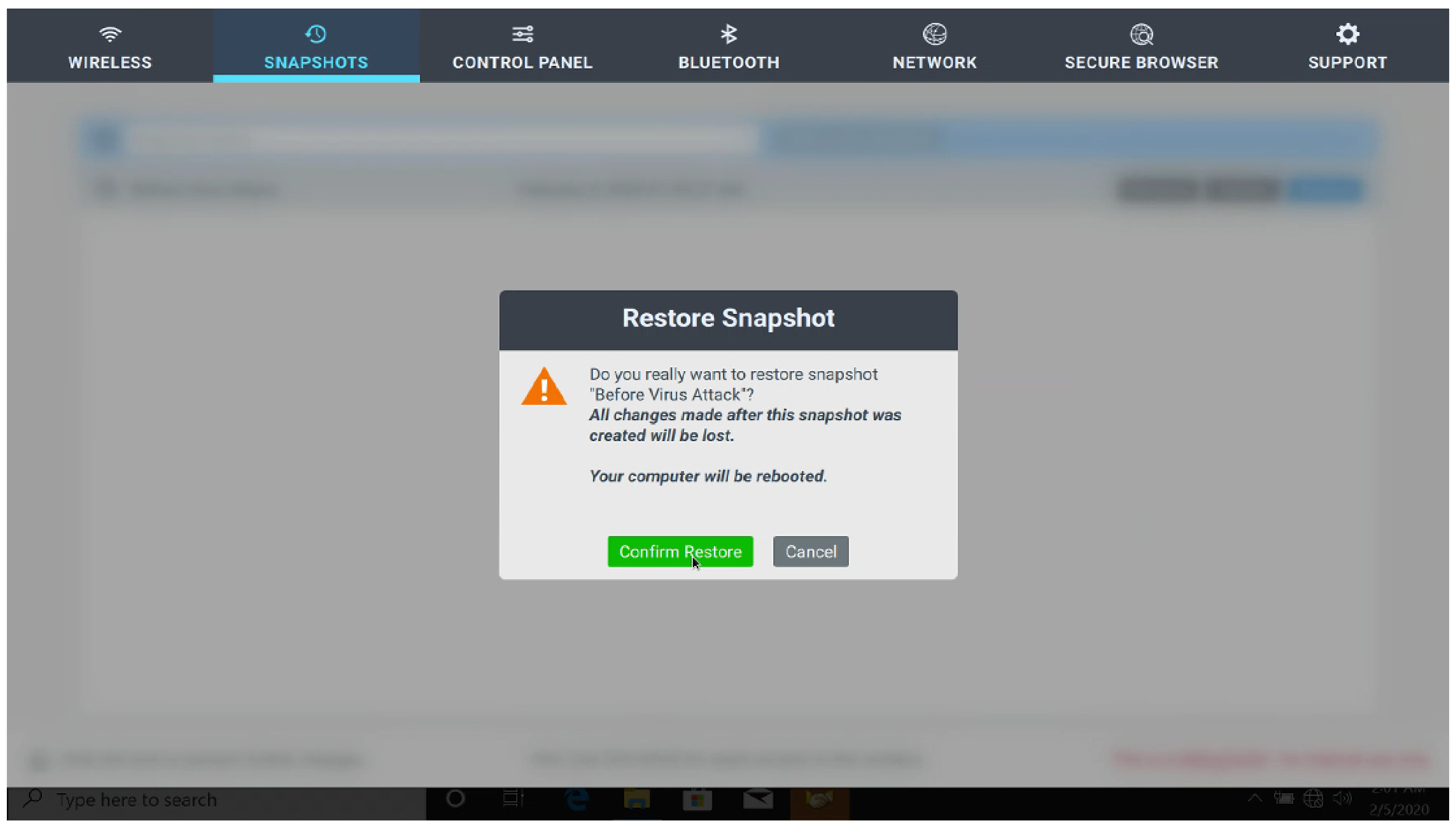
The Secure Browser keeps threats outside the box

Let's talk about some of the features that make BIOS-SHIELD such a powerful ally against the array of threats you or your remote workforce might face. The Secure Browser feature adds an extra layer of protection against the dangers of untrusted websites and downloads. Entering this sandboxed browsing environment allows you or your employees to access sensitive intranet resources or explore potentially dangerous websites without affecting or exposing the underlying Windows installation. Every time a user starts a new Secure Browser session, they get a fresh, safe browsing experience with convenient access to history and bookmarks. And in the event that a user needs to transfer a screenshot or file downloads from the Secure Browser environment to the local Windows file system, BIOS-SHIELD can screen the download for potentially dangerous embedded code and stop the transfer before that malicious code can ever run on the local PC.

Roll back to a safe setting with Time Machine

In the event that a malicious program or user mistake does affect the data stored on an ASUS ExpertBook P5440, BIOS-SHIELD minimizes the impact of that threat on local user data. Take the threat of ransomware that we discussed earlier. In the event that a user's system is infected by this pernicious type of malware, all of a user's important data might be permanently rendered inaccessible in the event that backups are unavailable.

With BIOS-SHIELD's local Time Machine Restoration snapshots, an individual user or IT department can simply roll the system back in time to a point prior to the infection, quickly restoring productivity and potentially saving the tens or even hundreds of thousands of dollars that might be necessary to unlock an infected system. Users need only to create a new snapshot at regular intervals, such as at the end of the business day, and getting back to work becomes as simple as invoking the BIOS-SHIELD interface and clicking a known good snapshot to restore. The ExpertBook P5440 includes up to 512GB of solid-state storage to ensure plenty of room for both user data and BIOS-SHIELD snapshots.



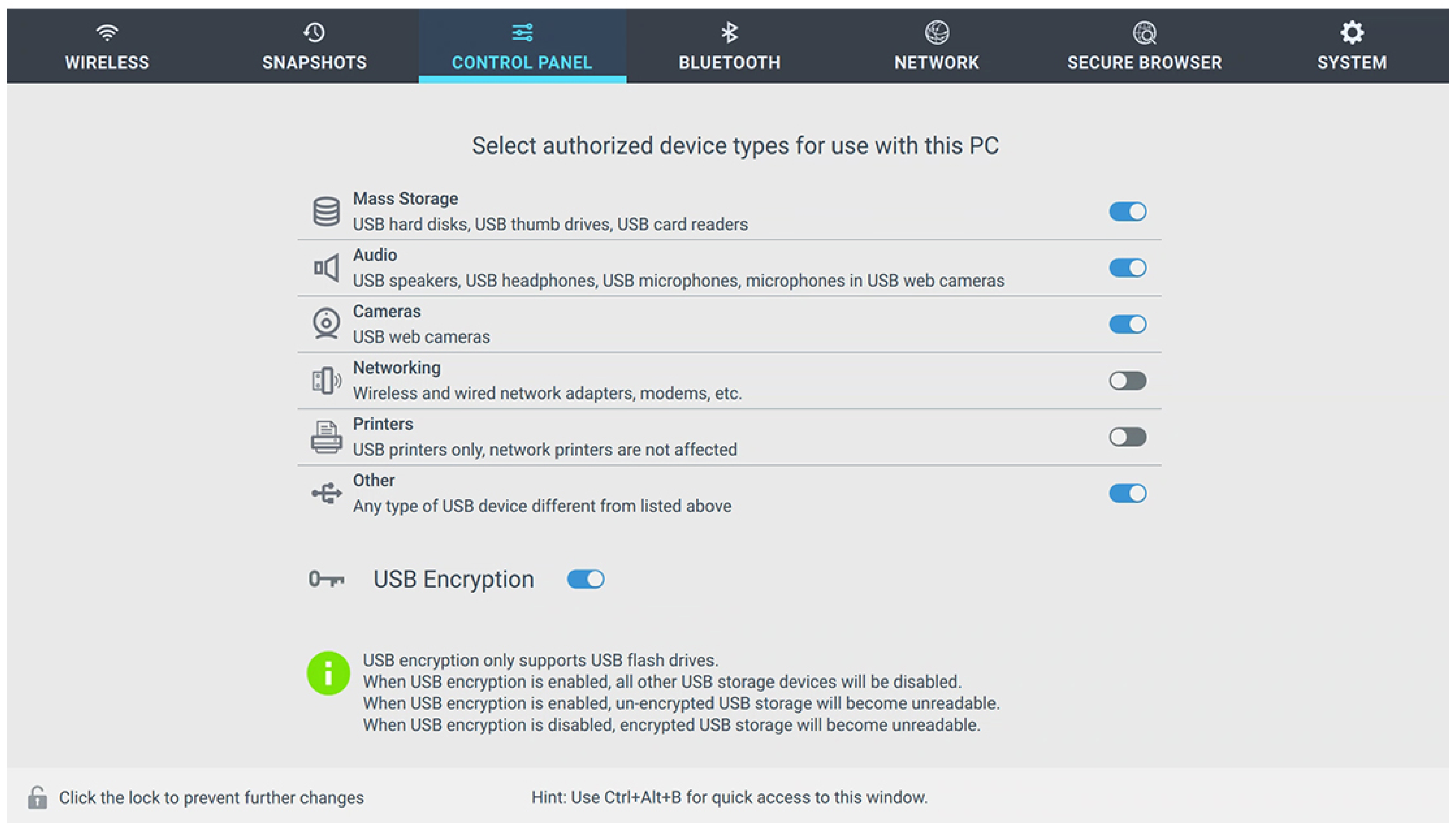
Restore Snapshot

Do you really want to restore snapshot "Before Virus Attack"?
All changes made after this snapshot was created will be lost.

Your computer will be rebooted.

Take full control of data and I/O

The ExpertBook P5440 offers a rich set of I/O ports for all the peripherals you might need to connect, including a fast and versatile USB 3.2 Gen 2 Type-C port with display and Power Delivery support. Even with this diverse connectivity, you or your IT department might want to prevent certain types of devices (like webcams or printers) from being physically connected to the system. BIOS-SHIELD offers fine-grained control over the types of peripherals a user can connect, including a blocking function for uncommon device types that might not be widely used but could still present a threat.



Select authorized device types for use with this PC

Mass Storage ●
USB hard disks, USB thumb drives, USB card readers

Audio ●
USB speakers, USB headphones, USB microphones, microphones in USB web cameras

Cameras ●
USB web cameras

Networking ○
Wireless and wired network adapters, modems, etc.

Printers ○
USB printers only, network printers are not affected

Other ●
Any type of USB device different from listed above

USB Encryption ●

USB encryption only supports USB flash drives.
When USB encryption is enabled, all other USB storage devices will be disabled.
When USB encryption is enabled, un-encrypted USB storage will become unreadable.
When USB encryption is disabled, encrypted USB storage will become unreadable.

Click the lock to prevent further changes

Hint: Use Ctrl+Alt+B for quick access to this window.

USB thumb drives present an especially vexing problem for IT administrators. These devices are undeniably useful for sharing information between employees, but they also present a threat. Stray USB thumb drives might have just been dropped or forgotten inocuously, or they may be social engineering attacks just waiting to happen.

A user could also transfer sensitive data to a personal flash drive and then lose it, potentialy exposing valuable proprietary information to the world. Worse still, an employee could transfer trade secrets to a portable storage device and share them with competitors or other unauthorized parties.

The BIOS-SHIELD environment can be used to protect against both threats. Turn on BIOS-SHIELD's protection against unknown mass storage devices, and it'll prevent untrusted devices from even being mounted by the system. For users who still need to transfer data via thumb drives in organizations using BIOS-SHIELD, they can create trusted, encrypted flash drives that can only be accessed by other BIOS-SHIELD-powered PCs with the appropriate password. And with BIOS-SHIELD's optional cloud management features[†], your organization's PCs can be assigned to functional groups like accounting or engineering departments to prevent sharing of information outside of those groups.

If a laptop is lost or stolen, any sensitive, unencrypted data on board can quickly become an embarrassment or a liability for a company. For just one prominent example, Facebook discovered as much when unencrypted hard drives containing payroll information for tens of thousands of employees were stolen from an employee's personal vehicle.[5]

BIOS-SHIELD protects against physical attacks or theft by encrypting local storage. If a malicious actor transfers the hard drive or SSD from the ExpertBook P5440 into another system in an attempt to read the data stored on it, BIOS-SHIELD's encryption will prevent sensitive information from being read. And if a malicious actor connects a stolen system to the Internet, BIOS-SHIELD's optional cloud management features[†] can remotely wipe the device's local storage and reset it to factory settings, further preventing access to sensitive data.

Speaking of passwords, even the best password policy can be defeated by crutches like Post-It notes or other well-intentioned memory aids. That's where the ASUS ExpertBook P5440 itself comes to the rescue. Users can take advantage of the Windows Hello-compatible fingerprint reader to log into the system, reducing the need for complex and hard-to-remember passwords. This biometric security layer provides another defense against unauthorized access to sensitive information.

The power and flexibility you need to stay safe, secure, and productive

On top of all of the great security features enabled by BIOS-SHIELD technology, the ASUS ExpertBook P5440 delivers the performance you need to stay productive with 8th Gen Intel Core processors, versatile storage options, a comfortable backlit keyboard, and up to 10 hours of battery life. Military-grade durability testing and a light 2.7 lb weight let this system stand up to all the challenges that working from home presents.

Contact an ASUS Representative | Learn more at https://www.asus.com/us/site/bios-shield/

End notes and Data Sources

[†] BIOS-SHIELD cloud management features require separate account registration with Janus Technologies and may incur additional charges. Please visit the vendor website for more information.

[1] The New York Times: "Ransomware Attacks Grow, Crippling Cities and Businesses."
https://www.nytimes.com/2020/02/09/technology/ransomware-attacks.html
Feb. 9, 2020. Accessed 8/7/2020.

[2] Kaspersky Lab: "New research from Kaspersky finds 45% of employees don't know how to respond to a ransomware attack."
https://usa.kaspersky.com/about/press-releases/2020_new-research-from-kaspersky-finds-45-of-employees-don-t-know-how-to-respond-to-a-ransomware-attack
April 2, 2020. Accessed 8/7/2020.

[3] Bleeping Computer: "Confirmed: Garmin received decryptor for Wasted Locker ransomware."
https://www.bleepingcomputer.com/news/security/confirmed-garmin-received-decryptor-for-wastedlocker-ransomware/

August 1, 2020. Accessed 8/7/2020.

[4] Absolute Labs: "Cost of a Lost Laptop is Nearly $50,000."
https://www.absolute.com/blog/cost-of-a-lost-laptop-is-nearly-50000/
April 4, 2009. Accessed 8/7/2020.

[5] Bloomberg: "Thief Stole Payroll Data for Thousands of Facebook Employees."
https://www.bloomberg.com/news/articles/2019-12-13/thief-stole-payroll-data-for-thousands-of-facebook-employees
December 13, 2019. Accessed 8/11/2020.