ASUS ExpertBook P5440

Secure inside & out with BIOS-SHIELD™

The ASUS ExpertBook P5440 and BIOS-SHIELD help you take control of your distributed workforce's systems and keep data safe

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.

Many prominent firms are relaxing the requirement that employees work from the office for the long term. Some are even re-evaluating the need for office space entirely, sometimes at great cost to the bottom line. For example, Pinterest canceled a future lease on top-tier facilities in San Francisco in favor of a more distributed workforce.[1] Slack is giving employees the option to work remotely on a permanent basis.[2] Facebook projects that within 10 years, over half of its employees could be remote.[3] And Twitter has granted its workers the option of staying at home "forever."[4]

Information security from the ground up and the cloud down

The shift to a remote working environment and online collaboration via cloud computing doesn't just affect how employees will live and work without a physical office. IT departments are under pressure to find new laptop PCs that are suited to the rise of the distributed office and to manage them without the convenience or assurance of frequent connections to a corporate network. Existing threats to employee PCs and the data they contain, like destruction or theft, are all the more intense in the new world of the distributed office.

Even before a wide swath of professionals began working from home, the theft of a laptop was a despairingly common occurrence. One widely-cited figure based on research from Gartner suggests that a laptop is stolen once every 53 seconds.[5] And the total financial damages of a laptop theft could extend far beyond the replacement cost of the device. According to research sponsored by Intel, the average cost of mitigating a stolen laptop is as much as $49,246 (circa 2010), and the majority of that cost comes from managing the fallout of data breaches and intellectual property losses.[6]

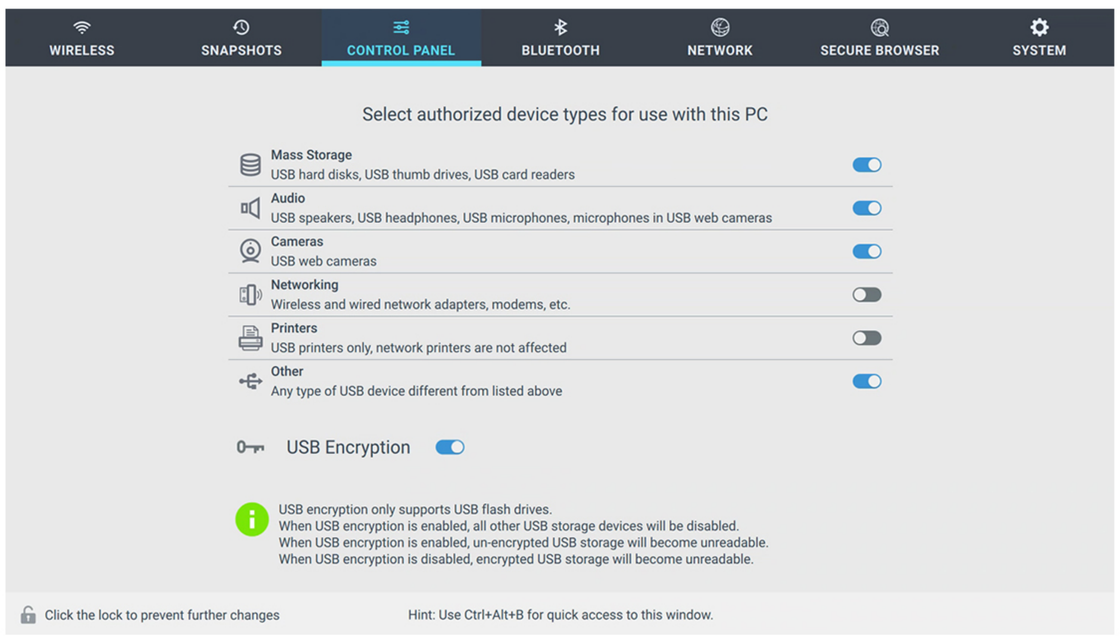
The takeaway is clear: remote workers need a laptop that's built with security in mind from the ground up, and their IT departments need remote manageability tools to make it easier to keep control over the organization's sensitive data. BIOS-SHIELD comes in.

The ExpertBook P5440 and BIOS-SHIELD form a secure foundation for remote work

The ASUS ExpertBook P5440 with BIOS-SHIELD is an ideal choice for businesses of all sizes that need a hardened, trusted laptop to get distributed office environments up and running.

BIOS-SHIELD isn't the usual suite of security tools running inside a vulnerable operating system. Instead, it's a preinstalled operating environment that combines the security of a virtual desktop infrastructure deployment with the responsive performance of a local device. It protects local data, provides the option of remote manageability to IT departments, ensures quick data recovery via system imaging and recovery, and protects against network threats through a secure browsing sandbox.

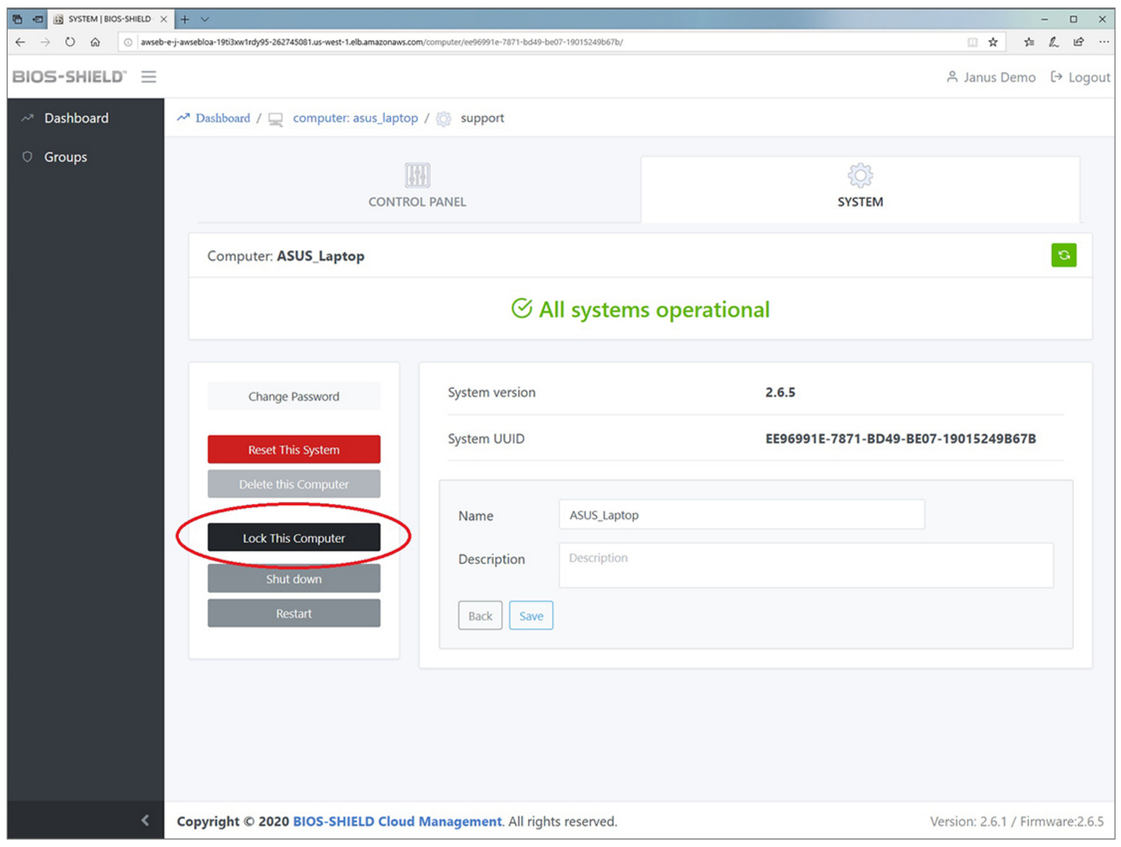
An ExpertBook P5440 with BIOS-SHIELD defends the data stored on-device against theft or loss. If a thief or attacker steals a laptop, it's usually game over for any sensitive information on the device—at least if that information isn't encrypted. By default, BIOS-SHIELD protects sensitive information on the ExpertBook P5440's local disks by encrypting them. Beyond that baseline protection, BIOS-SHIELD offers powerful controls to create and manage trusted, encrypted storage devices out of the box, and available remote management tools give administrators control over ExpertBook P5440 devices that are off-premises.



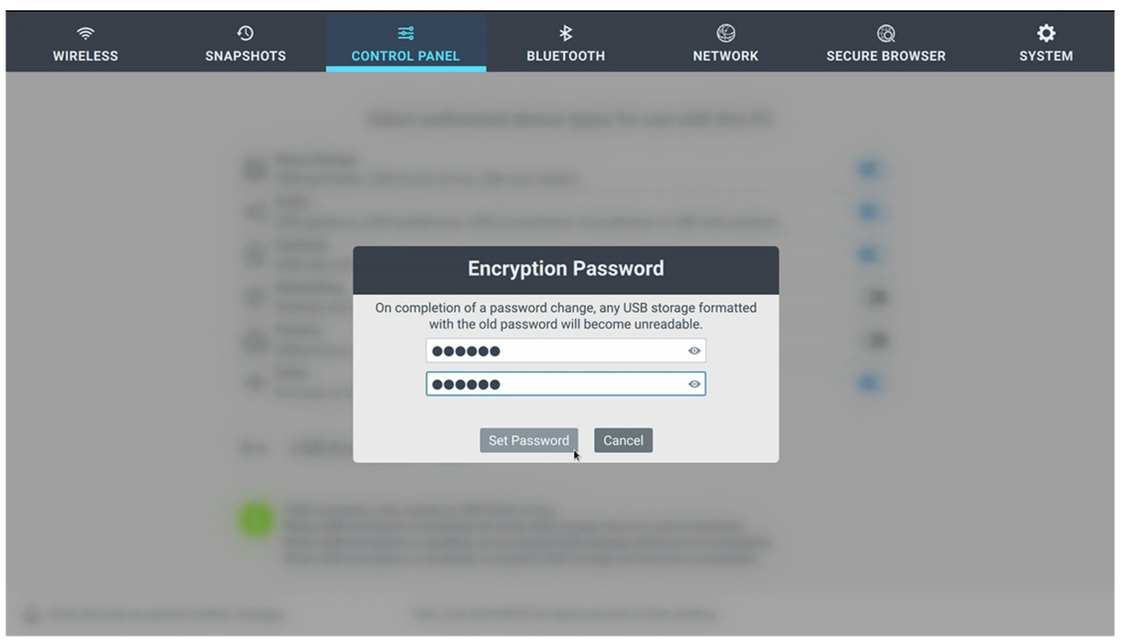
Take control of your organization's data, both on-device and off

External attackers and thieves aren't the only threat to data that an IT department might need to deal with in the distributed office. Workers' access and permissions for sensitive data naturally change over time. In a physical office, confiscating a system or locking out an employee from access to their PC is a simple enough task. In a distributed office environment, however, an IT administrator might be many dozens or even hundreds of miles away from a remote worker.

In the event that an employee's access to sensitive data needs to be revoked, BIOS-SHIELD's available remote management tools can be used to wipe all data on an ASUS ExpertBook P5440 and return it to factory settings. This remote wipe functionality is also handy in the event that the laptop is stolen and later connected to a network. And if a device is recovered or returned to your company, convenient provisioning features available through the business cloud-enabled features that come with the ExpertBook P5440 help you quickly re-deploy those laptops to the field with the proper BIOS-SHIELD security and environment settings.



Configurable USB device management within the BIOS-SHIELD interface also allows employees and administrators to create trusted, encrypted, password-protected USB flash drives. Once USB device encryption is configured, only approved storage devices can be accessed by an ExpertBook P5440 with BIOS-SHIELD. Untrusted USB storage devices are locked out before they can even be recognized by the operating system. Additional management options allow you to restrict the types of peripherals an employee can connect to the P5440 to further protect against data exfiltration.



Build your secure distributed workforce with the ASUS ExpertBook P5440 and BIOS-SHIELD

As more and more employees join distributed workforces and begin working remotely, the potential for device and data theft will only grow. Don't expose your employees and your organization to the costs and headaches of stolen data by deploying laptops that aren't built for the job. The ASUS ExpertBook P5440 with BIOS-SHIELD helps protect your sensitive data from theft with a defense-in-depth strategy that's tailor-made for the needs of distributed workforces everywhere. For more information, contact your ASUS representative.

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]SFGate. "Pinterest pays $89.5 million to terminate San Francisco office lease."
https://www.sfgate.com/business/article/Pinterest-terminate-SF-office-lease-88-Bluxome-15525421.php
8/30/2020. Accessed 10/21/2020.

[2]Fox Business. "Slack to offer permanent work from home to most employees
https://www.foxbusiness.com/technology/slack-permanent-work-from-home-most-employees.
6/14/2020. Accessed 10/21/2020.

[3]Fox Business. "Facebook to shift permanently toward more remote work after coronavirus."
https://www.foxbusiness.com/technology/facebook-coronavirus-more-work-from-home.

5/21/2020. Accessed 10/21/2020.

[4]Fox Business. "Coronavirus prompts Twitter to allow employees to work from home 'forever'."
https://www.foxbusiness.com/technology/twitter-employees-work-from-home-forever.
5/12/2020. Accessed 10/21/2020.

[5]CIO Dive. "The mobile device conundrum: Employee flexibility and security at odds."
https://www.ciodive.com/news/the-mobile-device-conundrum-employee-flexibility-and-security-at-odds/437427/
3/7/2017. Accessed 10/21/2020.

[6]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 10/21/2020.