Kaspersky Anti-Virus for UEFI

Kaspersky Anti-Virus for UEFI (KUEFI) is the EFI BIOS level endpoint security solution providing effective protection from rootkits and bootkits and ensuring safe OS loading. The product's key feature is that it starts running in the EFI environment even before the OS bootup process begins, thus preventing any resident malware from loading. By working on EFI level, KUEFI ensures reliable protection from rootkits, bootkits and other malware specifically designed to circumvent desktop anti-malware technologies.

KUEFI is provided as a small EFI module which nevertheless contains the award-winning Kaspersky Anti-Virus engine. The KUEFI architecture enables its integration into any motherboard firmware supporting the EFI standard, regardless of the vendor.

Use Cases

Motherboard, PC and tablet vendors can use KUEFI to add out-of-the-box anti-malware protection to their products, enabling them to effectively resist the following threats:

- Rootkits, bootkits and other complex malware
- Trojans, viruses, and worms
- Zero-day attacks and as-yet unknown malware
- and many other cyber-threats

When deployed on-chip, KUEFI is always on, ensuring safe OS bootup process. Thus, KUEFI integration with hardware makes it possible to meet the stricter security requirements in place in industrial and governmental institutions.
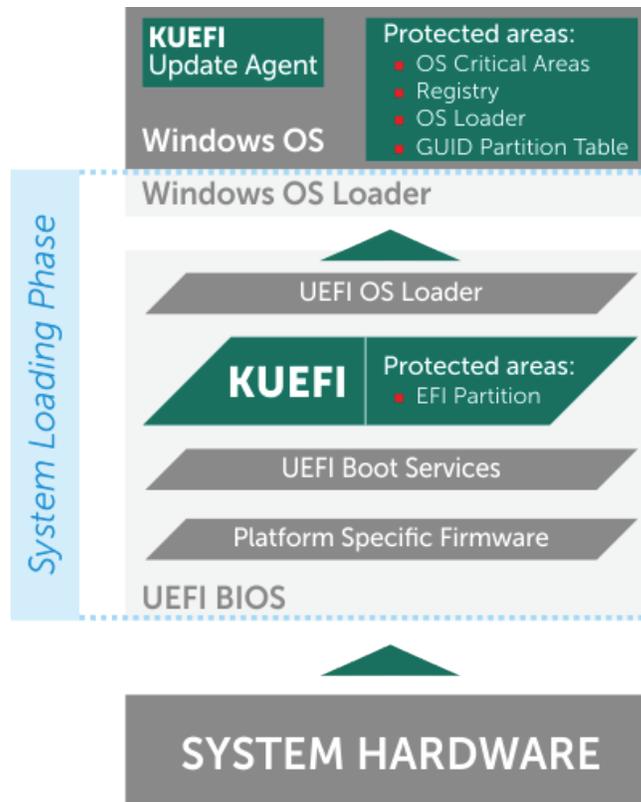
Key features

- Designed especially for fighting complex malware, such as rootkits and bootkits capable of subverting desktop anti-malware protection.
- Based on the award-winning Kaspersky AntiVirus engine.
- Thanks to motherboard firmware integration, cannot be deactivated by malware or unauthorized user.
- Supports the modern families of Windows and Linux operating systems.
- To reduce OS bootup time, scans only system critical areas: EFI, GUID Partition Table, OS loader and core, key OS files, Windows registry, and a few others.
- Provides flexible settings which can be used to set up the optimum tradeoff between performance and scanning depth as required by each customer.
- Doesn't conflict with desktop anti-malware solutions.
- Uses cutting-edge detection methods, including static and dynamic (i.e., emulator-based) detetion.
- Scanning module can be updated during a routine update of anti-malware bases.
- Scanning module size of less than 1 MB.

Contact Us

If you wish to know more, please fill in this contact form and indicate that you require more information about KUEFI, and our representative will get in touch with you shortly.

KASPERSKY‎ lab