KASPERSKY ANTI-VIRUS FOR UEFI

Advanced Anti-Rootkit Protection on EFI BIOS Level

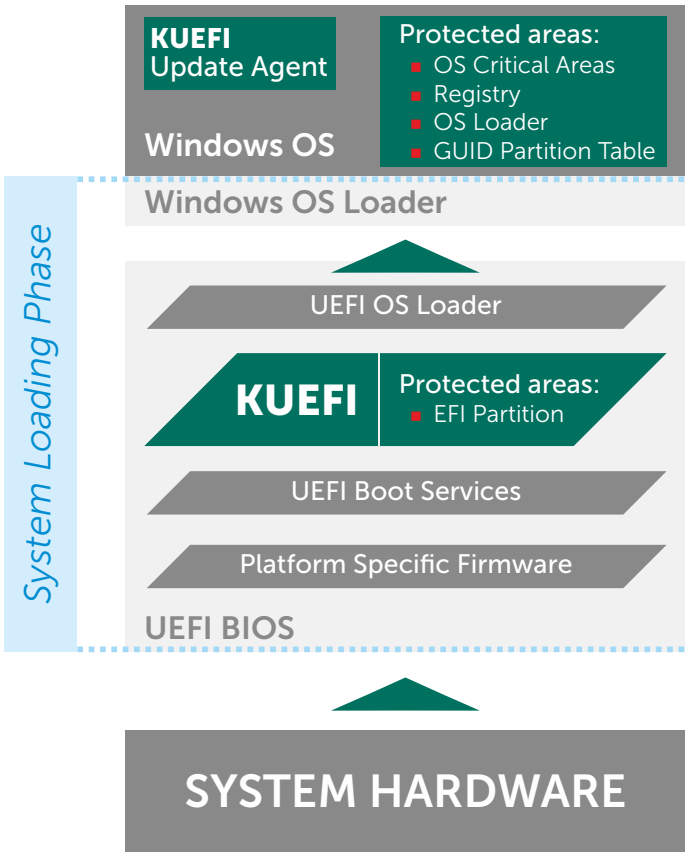
Overview

Kaspersky Anti-Virus for UEFI (KUEFI) is the only EFI BIOS level endpoint security solution providing effective protection from rootkits and bootkits and ensuring safe OS loading.

The product's unique 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 Advantages

- Designed especially for fighting complex malware, such as rootkits and bootkits capable of subverting desktop anti-malware protection.
- Based on the award-winning Kaspersky Anti-Virus 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) detection.
- Scanning module can be updated during a routine update of anti-malware bases.
- Scanning module size of less than 1 MB.

Protection Methods

Signature Analysis

This detection method is based on the search of a predefined string in the file. This also includes the detection based on the hash of the entire file. It allows to detect specific attacks with high precision and few false positives.

Links

A 'link' is a piece of binary code designed for running on the target platform. It allows to write mini-programs (usually in C/C++) to unpack, decrypt and analyze the files submitted for scanning. Any algorithm can be implemented in links. For example, Kaspersky Lab unarchivers and unpackers are implemented using this method.

Advanced Heuristics

When scanning an object, the action analyzer emulates the object's execution in a secure artificial environment (included with KUEFI). If any suspicious activity is discovered during the analysis of its simulated execution, it is considered to be malicious.

Unlike the signature method, the heuristic method aims to detect the typical behavior of objects rather than their static content, helping to detect malware that is new and/or unknown and is not yet registered in the database.

Proven Effectiveness!

Over the last two years, KUEFI has been integrated into solutions of Kaspersky Lab's partners. Even now it is providing protection for tens of thousands of workstations used by our corporate customers.

All-Round Support

- Dedicated business account managers
- Qualified 24x7 technical support
- Marketing support
- Daily Anti-Virus database updates

24x7x365 Anti-Virus Laboratory Kaspersky anti-malware technology is supported by 24x7 human analysis. The team of professional virus analysts and engineers explores the global virus weather and develops new detection methods and Anti-Virus technologies.

The combination of human analysis with latest anti-malware technologies such as advanced heuristics and automated AV engine updates provides supreme malware detection rate and ensures instant reaction to new threats.

ABOUT KASPERSKY LAB

Kaspersky Lab is the world's largest privately held vendor of endpoint protection solutions. The company is ranked among the world's top four vendors of security solutions for endpoint users*. Throughout its more than 17-year history Kaspersky Lab has remained an innovator in IT security and provides effective digital security solutions for large enterprises, SMBs and consumers. With its holding company registered in the United Kingdom, Kaspersky Lab operates in almost 200 countries and territories, providing protection for over 400 million users worldwide.

** The company was rated fourth in the IDC rating Worldwide Endpoint Security Revenue by Vendor, 2013. The rating was published in the IDC report "Worldwide Endpoint Security 2014–2018 Forecast and 2013 Vendor Shares" (August 2014, IDC #250210). The report ranked software vendors according to earnings from sales of endpoint security solutions in 2013.*