Windows 8: Kaspersky Lab is ready for new features and new threats

The arrival of Windows 8 is certainly an important milestone that plays a significant role in shaping the future of personal and mobile computing. Some of the changes in the user interface, designed with tablets and touch screens in mind, are nothing short of revolutionary. Microsoft has also presented a number of new security features designed to better protect end users. This white paper concentrates on the most significant security-related changes in the new version of Windows OS and the corresponding solutions from Kaspersky Lab.

Defending apps in the new interface

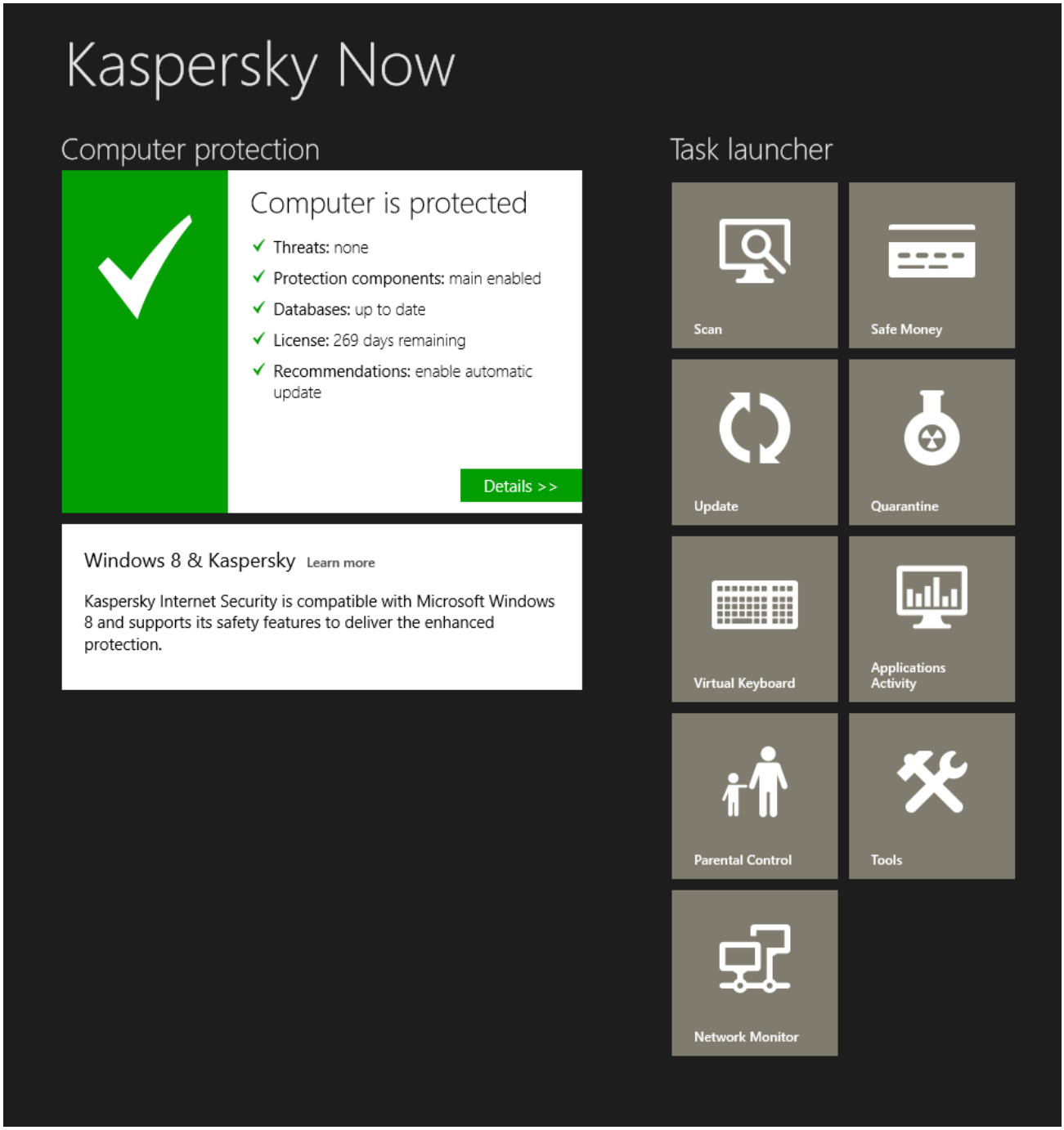
The rise of tablet devices has had the most noticeable impact on the development of the next Windows OS. Microsoft's answer to this growing trend is two different interfaces – a more or less classic one for traditional Windows applications with good old mouse-and-keyboard interaction, and a new interface designed specifically for couch surfing with a lightweight tablet device or a traditional but touch-enabled laptop. This offers end users the opportunity to share the same experience on different devices – PC, laptop or tablet – that all run the same Windows OS. This is how it looks like:

Applications, designed for the new interface, have a number of unique security characteristics, compared to traditional software. Each application can be in one of four states – operating normally, having an invalid license, modified or tampered. The last two states may point to malware infection. But with these new apps there is no need to remediate the application. Windows 8 can automatically reinstall a clean copy from its own applications store, Windows Store. To make this work, effective antivirus solutions need to know the difference between normal and new-style apps, and then alert the system of any infection to trigger reinstallation. This functionality is implemented

in Kaspersky Internet Security 2013, which can effectively inspect apps in the new interface and toggle the “Tampered” flag for those found to be infected by malware.

Kaspersky Now

To provide users with up-to-date information about security state of their Windows 8 PC, Kaspersky Lab has developed a new application called Kaspersky Now, designed specifically for the new interface of the operating system. Kaspersky Now is available to download for free at Microsoft’s Windows Store and works with the latest consumer solutions: Kaspersky Anti-Virus 2013 and Kaspersky Internet Security 2013.



It provides a uniform Dashboard with new tiled interface, where users can get all information about security status, license state and view the latest security news from Kaspersky Lab. The application also enables users to run key features of Kaspersky Lab’s security suites such as quick scan or database update without the need to switch to

traditional Windows interface, where traditional interface of Kaspersky Internet Security/Kaspersky Anti-Virus will be available.

Early-Launch Anti-Malware System

Early-Launch Anti-Malware (ELAM) is a new concept to protect the entire Windows environment from malicious activity. This is another brand new addition to the Windows operating system and it allows a certified anti-malware product to launch itself before other third-party software components. Together with Measured Boot, which gives the antivirus solution detailed information on all Windows components launched during the boot process, this new concept aims to make the whole Windows environment more secure. This system is especially important because it helps to detect and block complex malware, such as rootkits, quite efficiently.

Kaspersky Lab fully supports ELAM in its Kaspersky Internet Security 2013 solution, with a number of important additions. Not only can Kaspersky Internet Security check system and software integrity during startup, it can also remediate any active infection. At the same time, internal testing by Kaspersky Lab shows that under normal operation the early-launch driver has minimal impact on performance and startup time, introducing a delay of just a few milliseconds.

Built-In Anti-Malware Solution and General Security

Apart from new protection technologies, Microsoft is enhancing the traditional protection components of Windows 8. According to the manufacturer, the operating system includes “mitigation enhancements that further reduce the likelihood of common attacks”. In other words, Microsoft’s changes to various core system components render a large number of currently available exploits obsolete and make it harder for cybercriminals to develop new ones. These changes affect the Windows kernel with an improved PatchGuard functionality, updated Address Space Layout Randomization Technology and Internet Explorer browser.

To keep malicious code away from the user’s system, Microsoft is also enhancing its Windows Defender component, which is expected to be more efficient at detecting and blocking malware. At the same time, Microsoft believes that “all Windows 8 users should be protected by traditional anti-malware software”. Deep analysis of core enhancements of Windows 8 by Kaspersky Lab’s experts indicates that, while some changes make this operating system more secure, they still cannot be treated as a “final solution”. A good example of that is the updated PatchGuard – a feature that prevents tampering with the system kernel. Despite the improvements, it can still be circumvented – while for legal vendors, like security software companies, certain protection methods will become unusable.

The Kaspersky Lab view

Overall, the enhancements presented in Windows 8 make this system more secure against existing threats, and make it easier for security vendors to track down and block new malicious code.

- Apps for the new interface can be automatically reinstalled from the app store if they are infected, but a third-party solution is still needed to check software for malicious infections. Kaspersky Lab’s product supports this functionality in full.
- The new ELAM system, along with support for the Trusted Platform Module, provides better protection from complex malware by granting security software vendors early access to the system during startup and allowing them to check core system components.
- Further enhancements in the system reduce the possibility of infection by existing malware.
- New malicious code is blocked to some extent by the enhanced Windows Defender, but it still provides only basic protection.

In addition, Windows 8 has introduced strict requirements for software performance, including third-party security solutions. A number of new technologies developed by Kaspersky Lab address these requirements as well, increasing overall performance of the system and security software in particular.

Kaspersky Lab welcomes Microsoft's initiatives to provide secure protection mechanisms to certified third-party vendors. But the scope of the most important security-related enhancements shows us that they will only work well with an efficient security solution from a reputable vendor. Kaspersky Lab's flagship consumer product is ready for all the major changes in Windows 8.