

Business Benefit

What is the business benefit of TrustDefender compared to other offerings?

TrustDefender delivers the greatest potential business benefit to financial organisations, not just in terms of security but also usability and customer experience. TrustDefender is very effective against the landscape of customer endpoint threats, defending against a wide range of attacks from man-in-the-middle, malware, key logging, DNS poisoning, phishing and many others. It is compatible with all browsers and has many unique features such as reporting of management information, and can be easily integrated with fraud detection or other systems thereby offering an even greater return on investment. Furthermore, TrustDefender's pricing is very competitive which allows organisations to recover a significant portion (if not all) of its costs.

Market Differentiation – What is the unique offering TrustDefender brings to the marketplace?

TrustDefender's design exploits the app-server approach to provide enhanced security, reporting and back end-integration features. In contrast, many competitors with app only solutions are faced with a number of challenges, including:

- 1) They cannot offer real-time server integration on a transactional basis;
- 2) They cannot provide the online business with information about the security state of the customer's PC;
- 3) Their end-point component can potentially (and sometimes fairly easily) be disabled by a malware; and
- 4) There is no easy independent way to verify if app software has been tampered with.

Examples of such end-user oriented components are sandbox solutions, anti-phishing toolbars, anti-fraud plugins, identity theft components, and more sophisticated malware protection systems like anti-spyware or other endpoint security systems. Financial institutions and online merchants are also often under the false impression that authentication solutions alone can deliver sufficient end-point security protection.

The following features differentiate TrustDefender from other products:

- Secures a customer's session even if the computer has already been compromised by malware.
- Utilises a whitelist approach which identifies known and unknown malware as soon as the malware appears or becomes operational on a computer.
- Prevents screen capture.
- Mutually authenticates the app and the server.
- Provides real-time audit and reporting capability for compliance and fraud monitoring.
- Provides real-time feedback to the customer on the security health of their computer.
- Supports all Windows Operating Systems from Windows 98 onwards.
- Works independent of the web-browser.
- Can be downloaded and installed onto a locked-down computer without admin rights.
- Can be centrally managed and updates or changes to policy pushed to apps.

What are the key differences in the TrustDefender approach compared to other market offerings?

One popular approach to date by competitors has been to allow any kind of malware to run and that the user's web-browser is put in a "special isolation mode" so that the malware does not affect the browser session. However, in this approach, the security software typically does not detect the presence of malware; it will just try to isolate the web-browser process as much as possible but not guarantee.

TrustDefender has taken a totally different approach based on exploiting the key basics of any malware; it needs power to run and needs to run in memory therefore TrustDefender will detect or isolate and be able to remove the malware from memory and/or disable it for the period of the transaction. TrustDefender will do this based on its flexible whitelisting approach by authenticating every single application that is running in user-mode or kernel memory.

Not all market offerings are able to determine the full period of the online transaction and will therefore not be able to stop a malicious application for its duration. This poses the risk that malware may already have started and be operating at a lower level within the OS kernel, prior to the transaction being initiated in the browser including typing in ID and password. TrustDefender is able to determine the full duration of the transaction (using TrustDefender's GAP policies) and also to remove the malware from memory and/or disable it for the full period of the transaction.

Another example is that not all market offerings are able to provide protection against key loggers. TrustDefender's approach in this scenario is to suspend, disable or remove the malware from memory so that it cannot do any harm before or during the period of the transaction. One such competitor encrypts keystrokes so that key loggers will only see the "encrypted" keystrokes. However, this will not protect the app against a key logger that is using a malicious kernel driver that sits "below" a browser based Encryption Layer. Solutions that focus on encrypting the browser based session have no knowledge that a suspicious application is running and therefore provides the impression that the session is secure when it is not. It is not sufficient to only install software onto a compromised computer without addressing the potential underlying security problems.