

Did you know that online crime is bigger than the illicit drug trade?

Thank you for your time, as discussed please find below information on the latest release of TrustDefender™.

Pixel IT is the Australian and New Zealand distributor for award winning online transaction security solution, TrustDefender™.

TRUSTDEFENDER is a unique next generation 'Online ID Protection & Transaction Security solution' integrating customers' devices into the overall security infrastructure by securing their device prior to logging in to the enterprise's web services, before any Username, Password, ID or or two factor token is entered. TrustDefender then checks for vulnerabilities providing real time health verification of customers' devices allowing enterprises to apply on demand transaction policies based on the assessment, securing the transaction process from end to end, for the entire session. Providing peace of mind for both parties.



Survey:

I.D Theft

45% of Australians believe ID theft is likely to occur as a result of using the Internet.

Online Privacy

50% of Australians are more concerned about giving personal information over the Internet than they were two years.

Business Trust

36% of Australians would not deal with a company or charity because of concerns over its protection or use of their personal information.

(The Office of the Privacy Commissioner, National Survey, 2007) **Free Call 1800 674 935 for WebEx Demonstration**

Inadequate Security for Current Online Banking

"**One-in-five online transactions is vulnerable** despite added security methods such as SMS passwords. It is worrisome that obvious attacks were successful in **21%** of cases, and stealthy attacks in **61%** of cases."

"According to our study only **79%** of users would be able to avoid realistic attacks, which represents an inadequate level of security for online banking."

Mohammed AlZomai of the Information Security Institute at the Queensland University of Technology.

At a Glance:

1. Provides a security health check of customers PC prior to input of username and password or other confidential details ensuring:

- No keyloggers, trojans, rootkits, malware or spyware is running
- AV is switch on and up to date
- Firewall is enabled, etc.

2. Security policies and rules are enabled prior to login and during period of online transaction with financial institution.

3. Enables financial institution to apply security policies and rules based on PC security health status, which may include:

- Restrict transaction destinations, limits or types
- Alert recommended action i.e. update AV, enable firewall
- Run in Safe&Secure mode

4. Real-time Audit & Reporting:

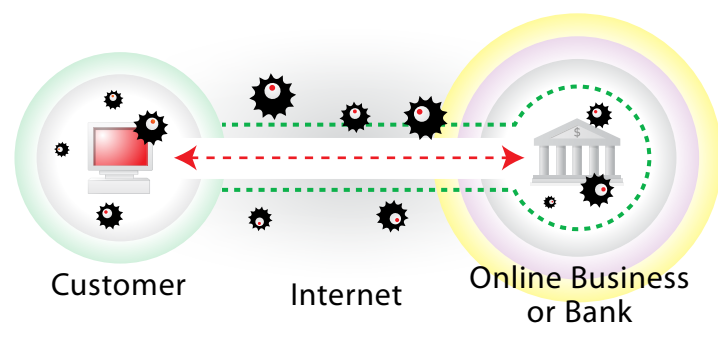
- Antivirus Status
- Firewall Status
- Windows Update Status
- Safe&Secure Mode, etc.

Benefits:

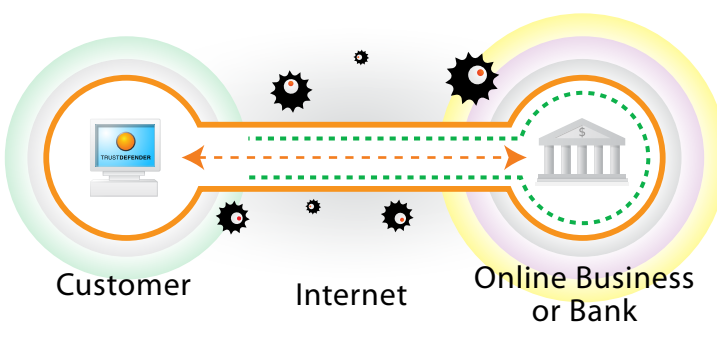
- ✓ Stop Online Fraud (including credit card fraud)
- ✓ Extend reach of anti-fraud capabilities
- ✓ Mitigate Fraud Risk
- ✓ Enhance Online Security
- ✓ Real-Time Audit and Reporting

- ✓ Compliance
- ✓ Reduce Online Merchant Risk
- ✓ Increased Member Confidence
- ✓ Brand Protection
- ✓ Peace of Mind

Without Trustdefender



With Trustdefender



Features:

Safe&Secure Mode (Whitelisting approach)

Secures and ensure all running applications on members PC are legitimate for the entire duration of the online transaction session. More importantly, non-trusted or malicious applications are immediately recognised and disabled.

End to End Online Transaction Security

Integrates customer and financial institutions security into a single security chain. Eliminating weak links and backdoors from 'Man in the middle' attack.

Auditing and Reporting

Comprehensive reports include breakdown of customers:

- Antivirus Products
- Firewall Products
- Windows Update Status
- Safe&Secure Mode.

Guaranteed Authentication Program (GAP)

TrustDefender knows all SSL Certificate Fingerprints and URL's of the banks online offering and can therefore provide previously unseen possibilities, such as:

1. Automatically detect a particular online offering before any confidential information (e.g. username / password & token) is transmitted and load the policies.

2. Once activated, TrustDefender then shows a non-forgable transparent browser-independent window with the Image and Name of the connected online offering.

3. The GAP-mode incorporates the IP-Address AND the SSL certificate fingerprints making it invulnerable to any DNS-spoofing, Man-In-The-Middle or other Pharming and Phishing Attacks!

Two Factor Authentication

Complementing existing Two Factor Authentication, TrustDefender will also provide the customer with Two independent Factors to Authenticate the Website. The First Factor is the GAP Window and the second Factor is the Personalised Login.

'Quiet Mode'

The TrustDefender™ Client runs transparently on the customers PC.

Secure Lockdown

Based on the SSL Certificate and URL information from the GAP database, TrustDefender can secure the customers PC also on a network level for the period of the transaction (from logon to logoff). An On-Demand Personal Firewall will automatically block all internet requests that do not belong to the online offering – thus mitigating any key loggers, cross-site scripting- and man-in-the-middle attacks.

Browser Independent

TrustDefender™ works with every browser, regardless of the user's preference. Furthermore TrustDefender™ does not run within the Security Context of the Browser (increased Security).

Automatic Client Deployment

The automatic client deployment feature will deploy to all different types of environments. It's unique Fallback Mechanism deploys TrustDefender via to ActiveX, JAVA, Flash and Javascript, supporting every possible environment.

One Time Download

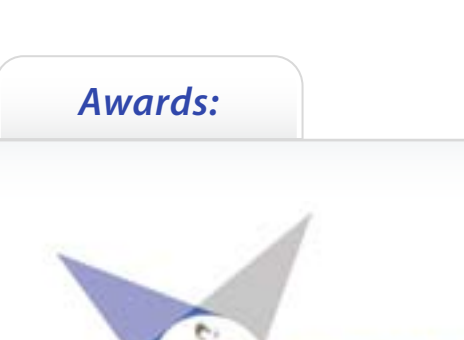
The base technology of all the TrustDefender™ agent is the same, whether deployed specifically via an online business, or independently installed as the consumer version (Gold Edition). There is no need to redeploy the TrustDefender™ client for each company who uses TrustDefender™.

Kernel Forensics Engine

Designed as a more general approach to solve any Windows Kernel modifications, not just rootkits. So no software goes undetected.

- Includes a kernel mode Rootkit Scanner
- Detection of hidden applications (Userland Rootkit Scanner)
- Detection of hidden kernel drivers (Kernel Rootkit Scanner)
- Detection of hooked ServiceDescriptorTable
- Detection of hooked native GDI APIs in Shadow ServiceDescriptorTable
- Detection of hooked Import Address Table
- Detection of hooked kernel Drivers.

Awards:



AUSTRALIAN INFORMATION INDUSTRY ASSOCIATION

FINALIST-2007 : eGovernment & Services Category; Financial Applications Category; Security Category.

WINNER-Prestigious 2007 iAward: In the Financial Applications Category.

Editions:

Gold Edition:

A consumer focused online transaction security application available via download providing the confidence & peace of mind knowing that they can securely and safely bank online with ANY bank as part of TrustDefenders "Guaranteed Authentication Program".



Enterprise Server Edition:

Ideal for larger enterprise organisations who wish to host, manage and integrate the key aspects of TrustDefender into their existing anti-fraud system. Providing the necessary tools for full visibility of the online session to keep ahead of cyber crime.

Managed Service Offering:

Ideally suited to small medium sized financial institutions, the managed service covers the enterprise server edition offering hosted by TrustDefender in their "ASIO T4 Accredited" Secure Data Centre. The managed service is easily integrated into the financial institution website with full access to management console provided for management of security policies and rules for each customer online transaction instance. Allowing organisations to lower total cost of ownership whilst providing the full benefits of ensuring the online banking experience is safe and secure at all times for their customers.

For further information call 1800 674 935

PixelIT

Network Solutions