

Secure Access to Enterprise Networks From Unmanaged Computers

Remote employees, contractors and partners all require access to a growing number of enterprise applications from various endpoints. Before giving these unprotected computers access to your network, it's critical to ensure that malware residing on them cannot use the browser to gain access to sensitive corporate data and restricted systems – no small task considering the increasing sophistication of malware today. Silently distributed by millions of compromised websites, malware fly under the radar of anti-virus solutions. As a result, between 2% and 5% of endpoints are infected with botnets and other sophisticated malware. Remote access to enterprise networks and applications is therefore the loophole allowing malware to easily reach sensitive enterprise data.

Current solutions do not address this threat effectively. NAC rely on anti-virus and are therefore rendered ineffective. Tokens and other authentication devices used by SSL - VPN are easily bypassed by advanced malware such as Zeus which operate in real-time once the connection is already authenticated. Virtual environments are vulnerable when their client is hosted on infected computers, in addition to being expensive and difficult to scale while having varied user experience issues.

A new solution that can effectively secure access to enterprise networks from potentially insecure computers is needed.

Trusteer Secure Web Access for Enterprises – Tens of Millions of Users Worldwide

Trusteer Secure Web Access prevents malware from accessing your network resources and sensitive information through SSL - VPN connections and unmanaged computers.

Leading banks around the world are using Trusteer Secure Web Access to protect millions of business and

retail users against advanced malware such as Zeus, Clampi, Torpig, Yaludle and more.

Trusteer Secure Web Access is comprised of lightweight security software that creates a virtual firewall inside the user's computer, isolating browser sessions with the enterprise from other activities on that computer. Malware and exploitable vulnerabilities on the computer cannot bypass Trusteer's virtual firewall and influence protected web sessions with the enterprise. The virtual firewall can also take action to remove the malware completely once identified and is comprised of technologies including keystroke encryption to evade keyloggers, communication protection to guard against unauthorized modifications, browser process and add-on protection as well as API blockage to prevent unauthorized access.

The Secure Web Access Service is intuitively activated when the user connects to enterprise applications and is otherwise transparent. When a malware infected machine tries to communicate with the enterprise, it is identified and access to all enterprise systems is denied until it is malware free.

The service also includes 24x7 automated investigations by Trusteer's fraud analysts. Malicious code captured by the virtual firewall during access attempts is sent to Trusteer for analysis and its results are made available to you.

Deployable in days, Trusteer Secure Web Access comes with a proprietary management application that enables effective definition of environments, triggers alerts and allows viewing and analysis of data and security management. The service is compatible with all major browsers and doesn't call for a change in user behavior.

Secure Access to Enterprise Networks From Unmanaged Computers

Features:

- Secures browser sessions to prevent malware accessing and injecting into enterprise sessions
- Allows remote access to internal applications only when a secure access session is enabled
- Deployable in days
- Fast notification of threats affecting employees
- Supports all major platforms – Internet Explorer, FireFox, Chrome Safari - on Windows and Mac

Benefits:

- Secures access between enterprises and employees even with multiple unrelated browser sessions running
- Protects against zero day and advanced persistent threats
- Protects internal and in the cloud SaaS applications
- Blocks and removes malware including Zeus, Silon, Torpig, Yaludle and more

- Transparent to employees, no change in user experience
- Automated investigation by fraud analysts 24x7
- One time download within minutes

Specifications:

Operating Systems:

- Windows XP (32 bit and 64 bit)
- Windows Vista (32 and 64 bit)
- Windows 7 (32 and 64 bit)
- Mac OSX Tiger (Intel)
- Mac OSX Leopard (Intel)
- Mac OSX Snow Leopard (Intel)

Browsers:

- Internet Explorer 6 and above
- Firefox 3 and above
- Chrome 4 and above
- Safari 4 and above

