Trusteer Apex

Enterprise Malware Protection

Trusteer

Stop Zero-Day Application Exploits and Data Exfiltration

Targeted attacks and Advanced Persistent Threats (APTs) pose a serious security threat to enterprises. In order to stop these attacks organizations must prevent advanced, information stealing malware from compromising employee endpoints. Advanced malware circumvents blacklisting detection tactics; Whitelisting approaches, which minimize malware evasion, have proven difficult to implement and manage. A new approach to effective and manageable endpoint malware protection is needed.

The Attack Vectors: Application Exploits and Social Engineering

Advanced malware compromises enterprise endpoint in one of two ways:

- **Application Exploits:** Cybercriminals use code embedded in weaponized documents and web pages to exploit application vulnerabilities, introduce malware into an employees' endpoint and penetrate the corporate network.
- **Direct User Install:** Cybercriminals use various tactics to manipulate the user to install an application that contains malware. The malicious application can be delivered via a website download, an infected USB drive, or an email attachment.

Once infected with malware, compromised endpoints can be used to access systems, collect data and send it to the Internet. Data exfiltration can take place within minutes of the malware infection, which is why it is critical to identify and mitigate the infection as quickly as possible.

Trusteer Apex applies Stateful Application Control to enable automated malware protection that is effective and easy to deploy and manage.

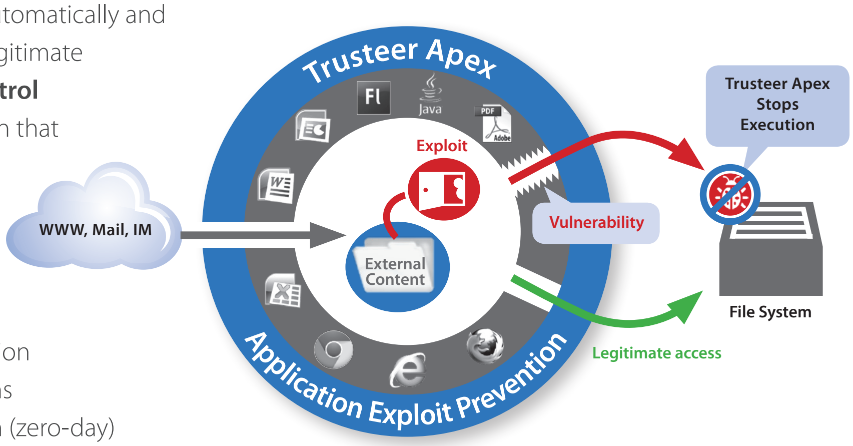
Blacklisting or Whitelisting: Current Endpoint Controls Fall Short

Despite using market-leading endpoint protection solutions, many large enterprises are constantly breached by advanced malware. Traditional endpoint protection solutions, that are based on blacklisting file signatures and malicious behaviors, have had limited impact on advanced threats that simply work around the blacklisting rules.

Application control and whitelisting solutions allow only "trusted" files to execute on the endpoints and are more resilient to evasion tactics. However, due to the dynamic nature of the user environment and frequent changes to application files, organizations have found these solutions to be extremely difficult to implement and maintain.

Trusteer Apex: Stateful Application Control

Trusteer Apex applies a new approach, **Stateful Application Control**, to stop zero day application exploits and data exfiltration. By analyzing **what** the application is doing (operation) and **why** it is doing it (state), Trusteer Apex can automatically and accurately determine if an application action is legitimate or malicious. Trusteer's **Stateful Application Control** enables automated enterprise malware protection that maximizes security while simplifying deployment and minimizing management overhead.



Trusteer Apex blocks the execution of files written to the file system through exploitation of vulnerabilities, preventing malware from compromising the endpoint.

Stopping Application Exploitation

Application exploitation occurs when an application processes malicious external content that contains exploit code. The exploit uses known or unknown (zero-day) vulnerabilities to write a file to the file system and execute it. Trusteer protects commonly exploited and widely used applications that process untrusted external content including: the browsers, Adobe Acrobat, Flash, Java and MS-Office. Trusteer Apex uses an Application State Whitelist that includes all the legitimate application states when these applications write and execute a file. It blocks the execution of files created via exploitation of vulnerabilities in these applications (i.e, when the application enters an unknown state), preventing malware from compromising the endpoint.

Preventing Data Exfiltration

Data exfiltration requires the malware to communicate with the Internet (for example, to a Command and Control (C&C) server). Trusteer Apex restricts untrusted files from executing sensitive operations that can enable external communication. For example, opening external communication channels, or tampering with other application processes to hide external communication traffic. Untrusted files are sent to Trusteer for analysis and are either approved or removed from the endpoint.

Automated Management

Trusteer's Stateful Application Control engine is easy to manage and maintain. This is because legitimate application states rarely change, even when applications are updated or patched. Automated whitelist updates are provided by Trusteer, based on research continuously performed on a network of 30 million protected endpoints. The updates occur with no end user disruption and require minimal IT staff resource involvement. If necessary, customers can whitelist specific code that would be restricted by Trusteer due to the nature of its operation.

About Trusteer

Boston-based Trusteer is the leading provider of endpoint cybercrime prevention solutions that protect organizations against financial fraud and data breach. Hundreds of organizations and millions of end users rely on Trusteer to protect their managed and unmanaged endpoints from online threats and advanced information-stealing malware.