Enterprise

Trusteer Apex

Re-Defining Enterprise Endpoint Protection against Advanced Malware and Targeted Attacks

Trusteer
an IBM Company

Advanced Persistent Threats (APTs) and targeted attacks pose significant risk to enterprise organizations. Adversaries leverage multiple attack vectors to infiltrate the network and gain access to resources and data. These include exploitation of application vulnerabilities to silently infect computers; malicious Java applications which bypass existing security and exploit prevention controls; advanced malware that enables remote access and control of corporate computers; and access to corporate resources using stolen credentials obtained through spear phishing schemes or through 3rd party breach.

To protect against these attacks, organizations are implementing advanced endpoint controls to complement legacy security solutions. However, current advanced controls are point solutions focused on a single threat vector, leaving the organization exposed to other attacks. As a result, organizations are left with the inconvenient choice between accepting significant security gaps and implementing multiple stand-alone endpoint clients, an operationally untenable option.

In addition to these challenges, IT Security organizations face operational challenges which result from the limited availability of highly skilled security professionals needed for implementing and maintaining complex security controls.

There is a pressing need for a single enterprise endpoint protection solution that provides multi-layered defenses to effectively mitigate the threat vectors, but is also easy to deploy, manage and maintain, and has a low impact on the business.

Trusteer Apex prevents user endpoints from becoming the infiltration point into your organization

Breaking the Cyber Attack Chain at Strategic Chokepoints

Trusteer Apex follows the threat lifecycle applying integrated multi-layered defense to break the cyber attack chain. Through extensive research, Trusteer has identified specific stages of the cyber kill chain where the attacker has relatively few execution options, which we have termed "strategic chokepoints". By tightly controlling these chokepoints at the operating system level, Trusteer Apex breaks the kill chain and prevents the attack. Trusteer Apex leverages in-depth technical expertise and unique low level visibility into application execution paths, to apply accurate and effective controls on strategic chokepoints and prevent malicious code execution. This enables Apex to provide unique and powerful protection against both unknown, zero-day threats and known malware, without impacting user productivity.

In addition, Trusteer Apex combines defense layers that address other attack stages, strengthening the overall cyber attack chain approach and optimizing the ability to preempt attempts to compromise user endpoints with advanced malware or steal user credentials.

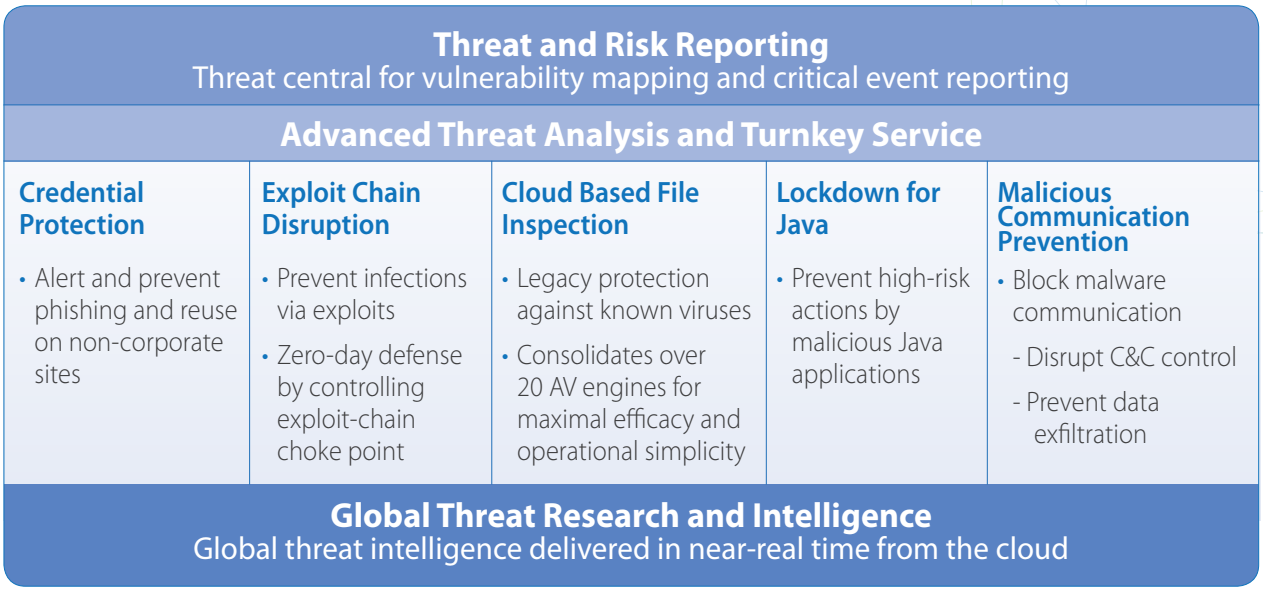

Figure 1: Trusteer Apex Multi-Layered Defense Architecture

Credentials Protection

Corporate credentials are very valuable to cyber attackers as they provide access to corporate systems. Credentials phishing schemes which manipulate users to submit their credentials on fake websites have been on the rise. Credentials have also been stolen from breached third-party databases.

Trusteer Apex prevents users from exposing their corporate credentials on phishing websites. In addition, Trusteer Apex helps enterprises enforce corporate password reuse policies by preventing employees from reusing their corporate credentials on non-corporate websites including consumer sites, social networks and more.

Exploit Chain Disruption Strategic Chokepoint!

Exploits, pieces of content embedded in weaponized documents and compromised websites, are designed to exploit vulnerabilities in end-user applications, like Java, browsers, document viewers, media players and more. The exploit chain enables the attacker to eventually infect the user endpoint with malware and compromise it. According to the **Verizon DBIR 2014**[1] 52% of infections result from exploits.

Trusteer's research mapped out the exploitation and malware delivery flow as a strategic chokepoint. Therefore, by disrupting the exploit chain, Trusteer Apex effectively prevents these stealthy infection attempts. Because this defense layer is not dependent on advanced information about the exploit, the targeted vulnerability, or the malware it's attempting to download, it effectively protects against zero-day exploits as well as exploitation of known yet unpatched vulnerabilities.

Trusteer research shows that 62% of exploits target vulnerabilities that have been known for 12 months or longer.

Cloud-Based File Inspection

About 48% of malware infections result from direct user downloads or network propagation. Many of these infections involve known malicious files that should be removed from user endpoints as soon as possible.

Trusteer Apex's File Inspection capability uses consolidated information from over 20 AV engines to provide legacy protection from known malware. If a file is detected as Should be known malware Trusteer Apex prevents the file from executing and compromising the machine. This provides maximal efficacy and operational simplicity, without requiring lengthy signature file update processes that impact network and user productivity.

[1] Verizon Data Breach Industry Report 2014

▸ Lockdown for Java **Strategic Chokepoint!**

Java exposes organizations to significant risk as it is the most targeted software platform. According to **research** conducted by Trusteer and IBM X-Force, 50% of exploits target Java vulnerabilities. Of these, 96% are malicious Java applications that manage to break Java's internal security mechanisms and gain elevated privileges (these are also known as "applicative exploits"). Because they operate maliciously inside the Java virtual machine, these attacks easily bypass OS-level controls such as Microsoft EMET which are blind to such manipulations.

Apex's Lockdown for Java enables the safe use of Java applications while preventing untrusted Java applications from executing high risk actions, such as writing to the file system or making changes to the registry. This ensures that legitimate business applications and any Java application which performs non-risky action (such as displays functions) will not be disrupted, while malicious applications will be blocked from causing harm.

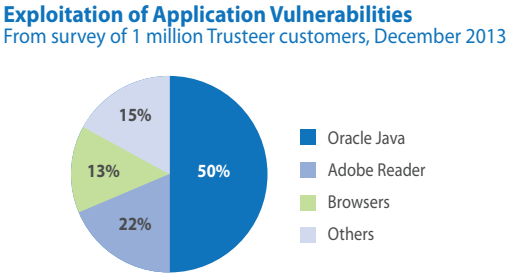

Figure 2: Exploitation of Application Vulnerabilities
Source: IBM X-Force® Research and Development

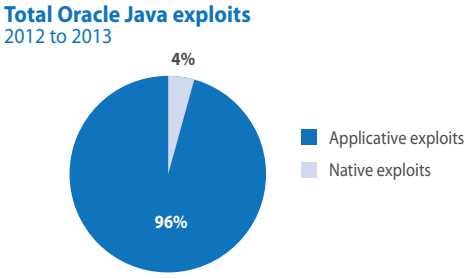

Figure 3: Total Oracle Java exploits, 2012 to 2013
Source: IBM X-Force® Research and Development

▸ Malicious Communication Prevention **Strategic Chokepoint!**

To compromise the endpoint, gain control and exfiltrate data, advanced malware must communicate with the attacker, often through a Command and Control server. Trusteer Apex prevents untrusted files from establishing communication channels outside of the corporate network. As a result, malware cannot register with the Command and Control server or get commands from its operator and therefore cannot compromise the machine or enable access to enterprise resources.

Endpoint Vulnerability Report

Vulnerable unpatched end-user applications expose the enterprise to exploitation risk. The continuous need to apply application patches, in many cases urgent critical patches, puts organizations in a never-ending rat race. And even that is not enough to prevent exploitation of zero-day vulnerabilities for which a patch doesn't exist.

Apex Endpoint Vulnerability Report provides visibility into the enterprise risk posture resulting from vulnerable applications. The report lists installations of vulnerable applications like Java and Adobe Acrobat, describes known vulnerabilities associated with them, and provides further details about each vulnerability. The report enables security professionals to make informed decisions to either patch or remove vulnerable applications (if it is possible to patch or remove them).

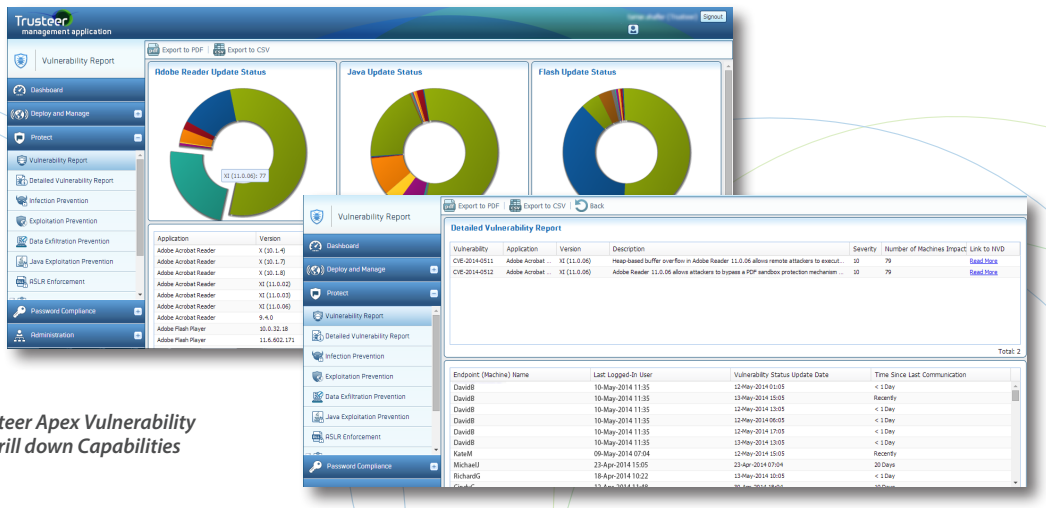

Figure 4: Trusteer Apex Vulnerability Report and Drill down Capabilities

Turnkey Service for Maximum Security and Minimal IT Overhead

Trusteer Apex installs as a software client on user endpoints. The client leverages in-depth visibility to monitor and analyze application behavior at strategic chokepoints and achieve unparalleled precision. This results in highly accurate defenses which minimize operational distractions both to the user and IT help-desk teams.

Trusteer Apex deployments are backed by Trusteer's security services which provide ongoing support to customers. Trusteer's security services help customers deal with emerging threats and security incidents dramatically boosting the customer's ability to face advanced threats and targeted attacks.

Global Threat Research and Dynamic Intelligence

Trusteer's research labs and expert team of malware researcher's work in cooperation with IBM security labs and the IBM X-force team to continuously analyze the latest security threats and targeted attacks. Threat research and intelligence data is based on dynamic security feeds provided by over 100 Million protected endpoints around the world. The combined vulnerability database is one of the largest in the industry with over 70K vulnerabilities categorized. Threat research and intelligence is translated into security updates that are automatically sent to protected endpoints.

Integration with the Wide Enterprise Security Ecosystem

Trusteer Apex fills critical gaps in the enterprise security ecosystem, protecting employee endpoints and preventing attackers from infiltrating enterprise networks and resources through compromised user endpoints. As a strategic component of the enterprise security ecosystem, Trusteer Apex is fully integrated with other enterprise security solutions, empowering organizations to streamline security operations, event correlation and forensic analysis efforts.

Trusteer Apex offers fully tested integrations with the following solutions:

- **SIEM Integration:** Trusteer Apex integrates with leading SIEM solutions, including IBM QRadar, for providing cross-organizations security intelligence and incident forensics.
- **IBM Endpoint Manager:** the integration streamlines endpoint security management
- **Palo Alto Networks WildFire:** Maximize visibility and protection by correlating information about malicious files found on the network with endpoint security events.

About Trusteer, an IBM Company

Boston-based Trusteer, an IBM company, 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.

Trusteer, an IBM Company
545 Boylston Street, 5th Floor | Boston, MA 02116
Tel: +1 (866) 496-6139 | Tel: +1 (617) 606-7755 | E-mail: trusteer.info@us.ibm.com | **www.trusteer.com**