Trusteer Apex：企业恶意软件防护

非官方中文译本 · 安天实验室 译注

文档信息			
原文名称	Trusteer Apex: Enterprise Malware Protection		
原文作者	Trusteer	**原文发布日期**	
作者简介	Trusteer 是 IBM 公司(总部位于波士顿)的下属公司，开发了一系列计算机安全软件。Trusteer 于 2006 年成立于以色列，于 2013 年 9 月被 IBM 以 10 亿美元的价格收购。 http://en.wikipedia.org/wiki/Trusteer		
原文发布单位	Trusteer		
原文出处	https://www.trusteer.com/sites/default/files/Trusteer%20Apexn_Eng.pdf		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

Trusteer Apex
企业恶意软件防护

Trusteer

防御零日漏洞和数据泄露

针对性攻击和高级持续威胁（APT）给企业造成了严重的安全威胁。为了防御这些攻击，企业必须防止先进的信息窃取恶意软件侵害企业雇员的终端。高级恶意软件绕过黑名单检测策略；减少恶意软件逃遁的白名单方法已经被证明是难以实施和管理的。需要有一个新的方法来进行有效的和可管理的端点恶意软件防护。

攻击媒介：应用程序漏洞和社会工程学

先进的恶意软件入侵企业终端的两种方式：

- **应用程序漏洞：**网络犯罪分子利用嵌入于被选为攻击武器的文档和网页之中的代码来攻击应用程序的脆弱点，将恶意软件引入一个雇员的终端机器中并渗透入企业网络。
- **直接用户安装：**网络犯罪份子利用各种手段来操纵用户去安装一个含有恶意软件的应用程序。该恶意应用程序能够通过网站下载、被感染的 U 盘或电子邮件附件来传播。

一旦感染了恶意软件，被攻陷的终端可以被用于访问系统，收集数据并将数据发送至互联网。数据泄漏会在恶意软件入侵后的几分钟内发生，这也就是为什么尽快的确定和移除感染是至关重要的。

Trusteer Apex 使用了 Stateful Application Control ,使自动恶意软件防护有效且易于部署和管理。

黑名单或白名单：当前端点控制存在不足

尽管使用市场领先的端点防护解决方案，许多大型企业仍不断地被先进的恶意软件攻破。传统的，基于黑名单文件签名和恶意软件行为的端点防护解决方案对高级威胁的影响有限。它只是简单的依据黑名单规则进行工作。

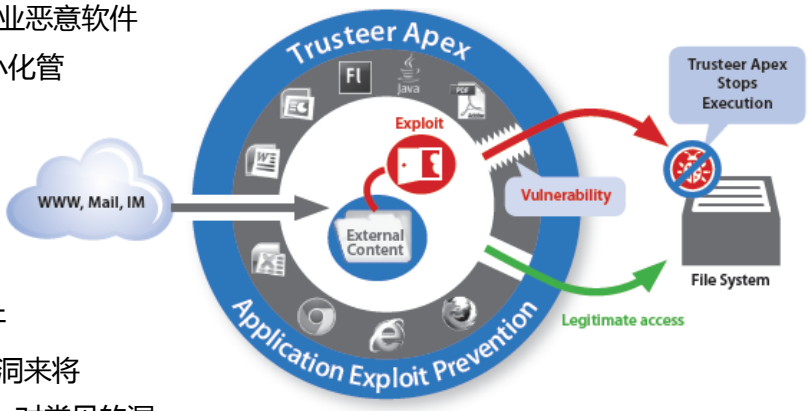
应用程序控制和白名单解决方案只允许“受信”文件在终端上执行，并且更适合恶意软件的躲避策略。然而，由于用户环境的动态特性以及应用程序文件的频繁改变，企业发现这些解决方案非常难以实施和维护。

Trusteer Apex：Stateful Application Control

Trusteer Apex 采用一个新的方法，**状态化应用程序控制**，来阻止零日应用程序漏洞和数据泄漏。通过分析应用程序正在做（操作）**什么**以及**为什么**他正在做这个（他的状态是这样），Trusteer Apex 能够自动的，准确的确定一个应用程序的行为是合法的还是恶意的。Trusteer 的 **Stateful Application Control** 提供一个自动的企业恶意软件防护方法，该方法可以在简单化部署和最小化管理开销的同时最大限度的提高安全性。

防御应用程序漏洞

当一个应用程序处理恶意的，含有攻击代码的外部内容的时候，应用程序攻击就开始了。该攻击利用已知或未知（零日）漏洞来将一个文件写入文件系统或执行它。Trusteer 对常见的漏洞和被广泛的用来处理那些不受信任的外部内容的应用程序（包括：浏览器，Adobe Acrobat，Flash，Java 和 MS-Office）进行防护。Trusteer Apex 使用一个应用程序状态白名单，该名单包含这些应用程序写入和执行一个文件时的所有合法状态。他阻断了利用这些应用程序中的漏洞来进行文件创建的操作（例如，当应用程序进入一个未知状态），阻止恶意软件对端点的入侵。



Trusteer Apex 阻断了利用这些应用程序中的漏洞来进行文件创建的操作，阻止恶意软件对端点的入侵。

防止数据泄漏

数据泄漏要求恶意软件与互联网（例如，与一个命令和控制（C&C）服务器)通信。Trusteer Apex 限制不受信的文件执行能开启外部通信的敏感操作。例如，开启外部通信通道或篡改其他应用程序进程来隐藏外部通信流量。不受信的文件被发送到 Trusteer 以供其分析，然后或者被放行或者被从终端移除。

自动化管理

Trusteer 的 Stateful Application Control 引擎是易于管理和维护的。这是因为合法的应用程序状态很少改变，甚至是在应用程序升级和打补丁后。Trusteer 提供自动白名单更新。该更新基于对一个拥有 3000 万受保护终端的网络进行不断研究而实现的。该更新不受最终拥护干扰并且所需的 IT 人力资源环境最小。如果有必要，客户可将特定代码列入白名单，Trusteer 将基于其操作的特性对其进行限制。

关于 Trusteer

总部位于波士顿的 Trusteer 是终端网络犯罪防护解决方案的主要的供应商。该方案防止企业遭受金融欺诈和数据泄漏。数百个企业和数以百万计的最终用户依靠 Trusteer 来防护他们托管的和非托管的终端，使其免予遭受网络威胁和先进的信息窃取恶意软件的侵害。

Trusteer, Inc.
545 Boylston Street, 5th Floor | Boston, MA 02116
电话: +1 (866) 496-6139 | 电话: +1 (617) 606-7755 | 邮箱: info@trusteer.com
www.trusteer.com