A global 1000 organization

Deploys Trusteer Apex from IBM to help secure access to Citrix XenApp and NetScaler VPN

Overview

The need

This global 1000 organization wanted to give employees access to Citrix XenApp desktops and applications from their home computers. But, protecting these unmanaged devices from malware was critical.

The solution

The company uses IBM® Security Trusteer™ Apex™ Advanced Malware Protection with the cloud-based, on demand deployment option to protect any user PC or Mac from advanced information-stealing malware.

The benefit

The solution helps protect tens of thousands of unmanaged devices against advanced malware that can steal user credentials, PINs and enterprise data, without impacting workflows or endpoint resources.

The enterprise information technology landscape is going through a major paradigm shift. Virtualization and cloud technologies allow organizations to improve efficiency and drive down the total cost of computing. And, consumerization and BYOD (bring your own device) initiatives drive IT organizations to give employees access to cloud-based and internal enterprise applications from any device, anytime and anywhere. As these mega trends accelerate, IT security has to protect devices and applications they do not control.

Stopping information-stealing malware

A global 1000 organization sought to give its tens of thousands of employees access to Citrix XenApp desktops and applications from any device, and, specifically, from home computers that are outside the IT organization's control. A Citrix client application, called Citrix Receiver, is launched on the employee's home computer to allow the user to remotely connect to the company's work environment.

The increase in unmanaged devices, driven by consumerization, BYOD (bring your own device) and virtualization initiatives, creates new security risks. By using IBM Security Trusteer Apex Advanced Malware Protection, this global 1000 organization now can conduct a high impact rollout of its Citrix desktops and applications while protecting its intellectual property and enterprise data.

Solution components

Software

- IBM® Security Trusteer™ Apex™ Advanced Malware Protection

To help secure access to the Citrix XenApp environment, the organization used Citrix NetScaler VPN (virtual private network) gateway combined with a smart card to authenticate users. However, a key security concern still remained.

Malware can infect the underlying host and attack the Citrix VPN authentication and Citrix XenApp session. And, antivirus software can't protect the client device against malware designed to steal user credentials via keylogging, screen capturing, remote access tools (RATs) and memory injection.

The organization decided that employees' unmanaged home computers must be protected against malware to help ensure the integrity of the VPN authentication and the Citrix XenApp session.

Specifically, the organization wanted to:

- **Protect the VPN authentication,** including the smart card PIN code, one-time password and VPN credentials, to Citrix XenApp against keylogging and screen capturing. Loss of these credentials could lead to a malware-driven attack on an employee's Citrix XenApp desktop.
- **Protect the Citrix Receiver against data theft** through keylogging and screen capturing of the user session. By logging user keystrokes and display traffic, cybercriminals can access enterprise application credentials, intellectual property and financial data from enterprise applications.
- **Provide effective, on-demand and instant protection** to unmanaged devices against malware without changes to the user experience or impact to the user's machine.

The organization receives alerts on malware detection, as well as reports on adoption levels and malware infection rates.

Protecting access from unmanaged devices

The global 1000 organization turned to Trusteer software, now an IBM Security solution, to protect unmanaged device access to its sensitive Citrix XenApp environment. Trusteer Apex Advanced Malware Protection is based on IBM Security Trusteer Rapport™ software, a fraud prevention technology that helps secure tens of millions of online banking and enterprise users around the world. This solution helps protect endpoints against malware infections that attack the browser to collect personal information and conduct account takeover and financial fraud.

Trusteer Apex software extends the core protection provided by Trusteer Rapport software beyond the browser to protect client applications executing on unmanaged computers, at home or on the road, against malware infection and attacks.

The following layers of protection are provided:

- **Helps shield client applications** such as the Windows smart card user interface and the Citrix Receiver from keylogging, screen capturing, remote access tools and memory injection
- **Detects and stops browser vulnerability exploits** used to deliver malware to the endpoint from any website accessed by the user
- **Identifies and terminates malware** installation and download processes

Cloud-based, on-demand delivery

The solution uses IBM on-demand, cloud-based software delivery as a pre-requisite for accessing Citrix XenApp from an unmanaged device. The organization integrates a Trusteer code snippet into the Citrix NetScaler VPN web page to help ensure the user has Trusteer Apex software installed prior to the authentication. The installation process takes a couple of minutes and supports virtually any PC or Mac platform. Unlike legacy endpoint security solutions, Trusteer Apex software instantly protects the endpoint and the client applications without requiring a lengthy, resource-intensive file scan or signatures database update.

This hosted management application also provides visibility into the protected endpoints population. The organization receives alerts on malware detection, as well as reports on adoption levels and malware infection rates. All suspicious activity is reviewed by IBM Security intelligence, and countermeasures are created and deployed to mitigate emerging threats.

Helping keep intellectual property and enterprise data secure

The increase in unmanaged devices driven by consumerization, BYOD and virtualization initiatives is creating a new set of security risks. Securing access to enterprise applications from potentially compromised, unmanaged endpoints is a critical requirement to realizing the promised cost savings and business agility benefits. By using Trusteer Apex software, this global 1000 organization can now conduct a high impact rollout of its Citrix desktops and applications, while simultaneously protecting its intellectual property and enterprise data.

For more information

To learn more about IBM Security Trusteer solutions, please contact your IBM sales representative or IBM Business Partner, or visit the following website: **ibm.com**/security

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
August 2014

Please Recycle

WGC12364-USEN-00