Securing and Deploying
The Enterprise Desktop

PIVX Solutions, Inc.

Overview

PreEmpt from PivX Solutions, Inc. defines a whole new approach to Windows host security. Using *Desktop Intrusion Prevention*—proprietary risk-mitigation technology in conjunction with world-class security research, PreEmpt (formerly known as *Qwik-Fix Pro*) protects all versions of Microsoft Windows (98/ME/NT/2000/XP) from known and *unknown* security threats, including worms, Trojans, Spyware and other malware. This unique capability is provided through automated repair of critical security-related software flaws and automated security configuration management. This serves to protect PreEmpt users in advance of malicious exploits - in some cases months before they are released or discovered by hackers.

Securing the Enterprise Desktop

PreEmpt's design and implementation for securely updating desktop clients requires an architecture that is flexible for mobile user support and robust to eliminate any man-in-the middle hijack attempts. Since the fixes that are delivered to the desktop include the ability to turn services off and on, monitor system processes, and write data locally, it's critical that the delivery mechanism uses military grade encryption and rock solid delivery protocols. Utilizing 2048-bit RSA keys, SSL, and multiple encrypted file handshakes, PreEmpt delivers fixes and program changes that the Enterprise can trust.

Deploying the Enterprise Desktop

Utilizing existing Microsoft Enterprise application deployment methods such as Active Directory (AD), enables PreEmpt to be efficiently deployed to the desktop. Leveraging Active Directory and Group Policy Management to create custom GPO's, the management console simplifies the creation and deployment of fix installation and configuration for each desktop. The supplied AD template allows for granularity of deployment options on a per GPO basis. This enables the organization to enforce different security policies as needed for each department or division.

Reporting and Management

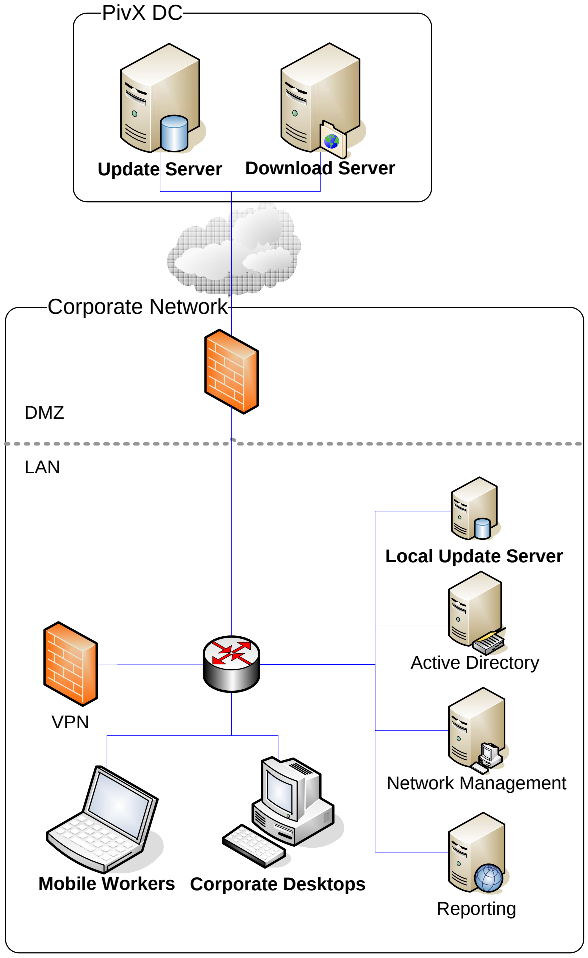
Reporting and Management of the desktop configuration and fix status of each desktop is managed through a centralized management console. Optionally, the updating of fixes can be done through a Local Update Server (LUS) that resides on the local LAN which eliminates external network traffic each time the client polls for new fix updates.

- Active Directory templates are included to quickly build group policies for enterprise deployment and management of settings, such as, which fixes are active for any given workstation or group of workstations.
- For System Administrators, PreEmpt 2.0 is designed to be managed independent of any local policy settings that are otherwise created for users across the enterprise.

- Administrators can also control whether or not the PreEmpt 2.0 user interface appears on client computers. This is often used to completely hide the PreEmpt 2.0 user interface including the system tray icon. Besides protecting the computer from new worms, viruses and other malware, many organizations find that making PreEmpt 2.0 invisible to desktop users reduces their costs by eliminating help desk calls that typically occur with any new desktop application.
- Management reports are available that describe in summary and detail:
    - Dashboard graphical view of the overall health of the deployment.
    - License Status to view seats used, expiration dates, license keys used and other license data.
    - Desktop-centric view of which PC's are installed and the fixes which are active and suspended on each desktop.
    - Detailed Fix listings with a view into which desktops have particular fixes enabled or disabled.
    - Updates status where the last update on a per desktop level can be displayed.

Update and Deployment Architecture

In summary, the update server and deployment methods in an Enterprise environment are described in the figure below.



Securing the Mobile Workforce

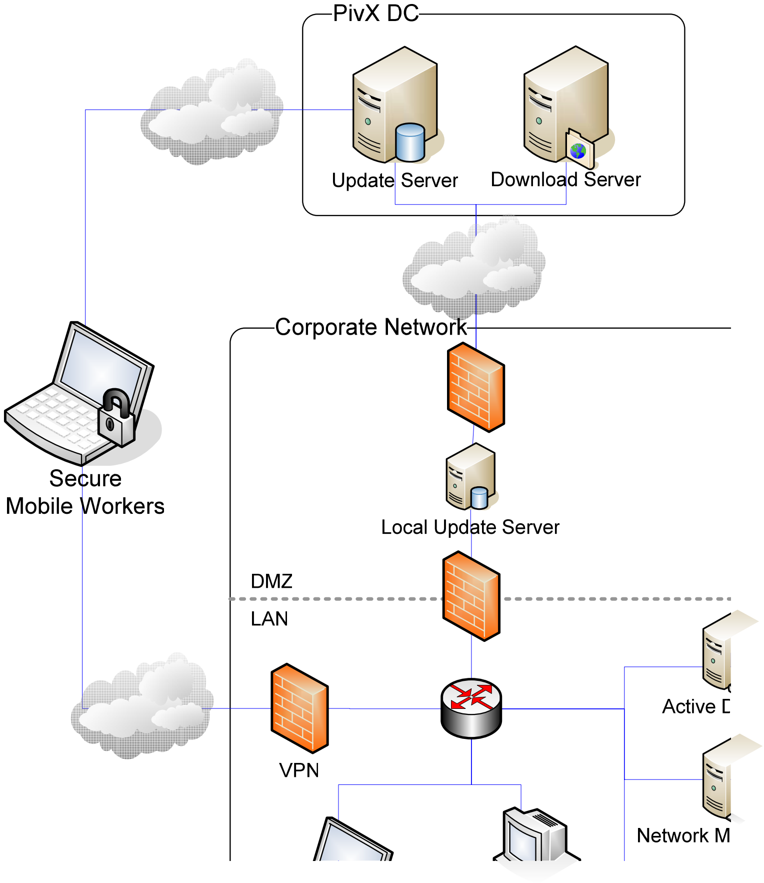
Maintaining security for users outside the corporate perimeter is hard:

- Perimeter defenses no longer apply to a growing mobile workforce.
- Mobile users are harder to troubleshoot and have different usage requirements.
- Mobile users re-connecting to the local network are frequently the infection vector for otherwise protected against exploits and malware.

PreEmpt can detect when access to the corporate LAN is unavailable and access the PivX data center directly for fix software and configuration updates. Configuration from the last time the LAN was available is maintained.

- Effective security software must preserve the same level of protection even when disconnected from IT infrastructure.

The PreEmpt desktop client is designed to work over VPNs, SSL VPNs, and firewalled access to the Local Update Server.


PivX DC
Update Server
Download Server
Corporate Network
Secure
Mobile Workers
Local Update Server
DMZ
LAN
VPN
Active D
Network M