



Taking Control of Your PC Environment

Corporate Overview

- **Software Company Founded 2002**

- New Management Team of former execs from High Tech Leaders - IBM, CA, GE, Check Point, Intuit and USAF

- **Company Accolades**

- 1,000's of customer deployments
- Strategic partnerships
 - **Microsoft, IBM, Intel, HP**
- Channel-driven business
- VARBusiness cover story

- **Award Winning Enterprise PC Solution**

- **Recognized by eWeek, ComputerWorld, NetworkWorld and Gartner**

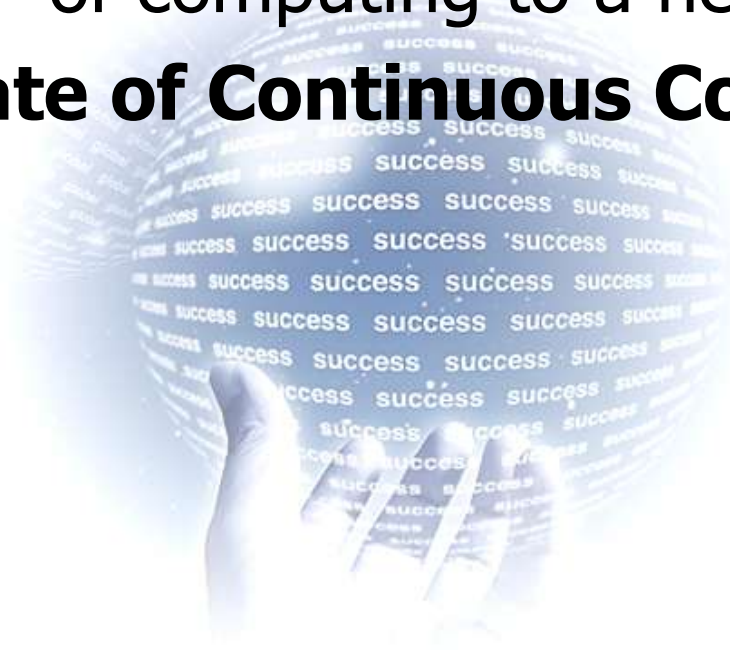


GE Healthcare



Our Mission

Transform the enterprise from
today's unpredictable and vulnerable state
of computing to a new
Solid State of Continuous Computing.



Are these Familiar Challenges?

- **PC Availability**
 - PCs down due to a variety of system problems
 - Mobile users productivity greatly reduced due to PC problems
- **Securing PCs**
- **PC Performance is degraded**
 - Mis-configurations
 - Corruptions
- **Escalating Costs to Maintain and Support PCs**
 - PCs becoming more complex
 - Require highly skilled resources
- **PCs are not in Compliance with Corporate Policy**
 - Naïve and/or Malicious abuse and use of PCs

What IT Administrators Want

Control

- > PCs with authorized configurations and applications
- > Maintain user settings and profiles
- > Flexibility and power of managing many types of PC images
- > Automated, Policy driven tools to ensure Compliance

Manageability

- > Remote PCs breaking down
- > IT staff stretched across the globe to support fully configured PCs
- > Support and ongoing maintenance of many PC/device configurations
- > Desktop backups or disaster recovery hard to implement



What End Users Want

- > A complete desktop: *their* desktop!
 - > Control over user settings
 - > Ability to install applications
 - > A PC that's updated regularly & painlessly
 - > A PC that works!
- > The flexibility to take it on the road
- > Support that can rescue them when they get in trouble



Securing Enterprise PCs - Challenges

- **Windows PCs**
 - Ship with default admin rights giving users power to make any change or modification to their system settings and download unauthorized applications such as Google Toolbar – increasing potential risks
- **Software Applications**
 - 5 years ago the average number of applications was 25-30
 - Today that number is approximately 75-85 applications
 - Requires more IT training and highly skilled PC technicians to ensure the security of enterprise PCs
- **Laptops of road warriors**
 - Multiple security vulnerabilities
 - Collect “junk” as they roam and then expose it to the network
 - Full admin rights
- **Failure to update/patch PCs on a timely basis**
- **Lack of research- not doing enough research to seek out PC tools that can address security issues today**
 - There are solutions which manage and enforce policies independent of a network connection (on a plane at 35,000 feet) and Pre-Boot of the PC's OS

Securing Enterprise PCs

- Ensure both network security and desktop security products installed, maintained and updated at all times
- Establish corporate policies spanning user rights and privileges and corporate configurations for enterprise PCs
- Ensure PC OS and related applications are maintained and that all critical security updates are applied on a timely basis
- Communicate regularly to all PC users the corporate IT policies
- Buy a PC tool that can manage and enforce the corporate policy for PCs
- A locked and well-managed PC is 42% less expensive than an unmanaged one – (Gartner, 24 January 2008)

Government PC Needs

- **FDCC: Compliance and Policy Enforcement**
 - Set and enforce PC configuration policies proactively
 - Automatically discover and remediate policy deviations
 - Visibility and reporting of any changes to FDCC standard
- **Business Continuity**
 - Reduction in downtime of desktops and laptops for end users
 - Maintain PC availability to meet service levels
- **Disaster Recovery**
- **Managing IT costs**
- **Reporting and Auditing**

FDCC Mandate

- **The Federal Desktop Core Configuration (FDCC) is a security mandate and a push toward PC standardization (OMB)**
- **Feb '08 all agencies to be on the same security configuration**
- **Federal CIOs will spend time and budget making sure their legacy applications--even ones just a year or two old--run well on their newly configured PCs**
- **Only applies to select Microsoft Windows operating systems - spec specifies nearly 300 settings in Windows**
- **This spring, eight government agencies, including the Department of Defense, the Treasury, and the Nuclear Regulatory Agency, got failing grades on the annual [computer](#) security report cards by the House Committee for Oversight and Government Reform**
- **The Department of Homeland Security got a D – gov't overall grade: C-**
- **ISSUE – Microsoft continues to ship Windows XP and Vista with default settings**

Federal Desktop Core Configuration (FDCC)

- **Approved configurations exist for Windows XP Professional (SP 2) & Vista Enterprise**
- **The XP config based on Air Force Specialized Security-Limited Functionality recommendations in NIST's Special Publication 800-68 + DoD customization of MSFT Security Guide for IE 7.0**
- **The Vista config based on DOD customization of the MSFT Security Guide — Vista and IE 7.0 — with input from the DISA, NSA and NIST**
- **Any Windows XP Professional or Vista machine in service in the federal government must be brought into compliance with the approved FDCC by Feb. 1**
- **Easy solution is re-image each PC using .INF files available from NIST and MSFT - re-imaging might be impractical, so detailed assessments and full scans of all computers must be conducted**
- **Great ROI with PE that addresses the crux of the Issue**
 - It is very difficult and costly to impose uniformity on an existing infrastructure. But in terms of testing, patching, software deployment, and re-imaging, standardization can save lots of money as well as boost security, if companies can get past the challenges and up front costs

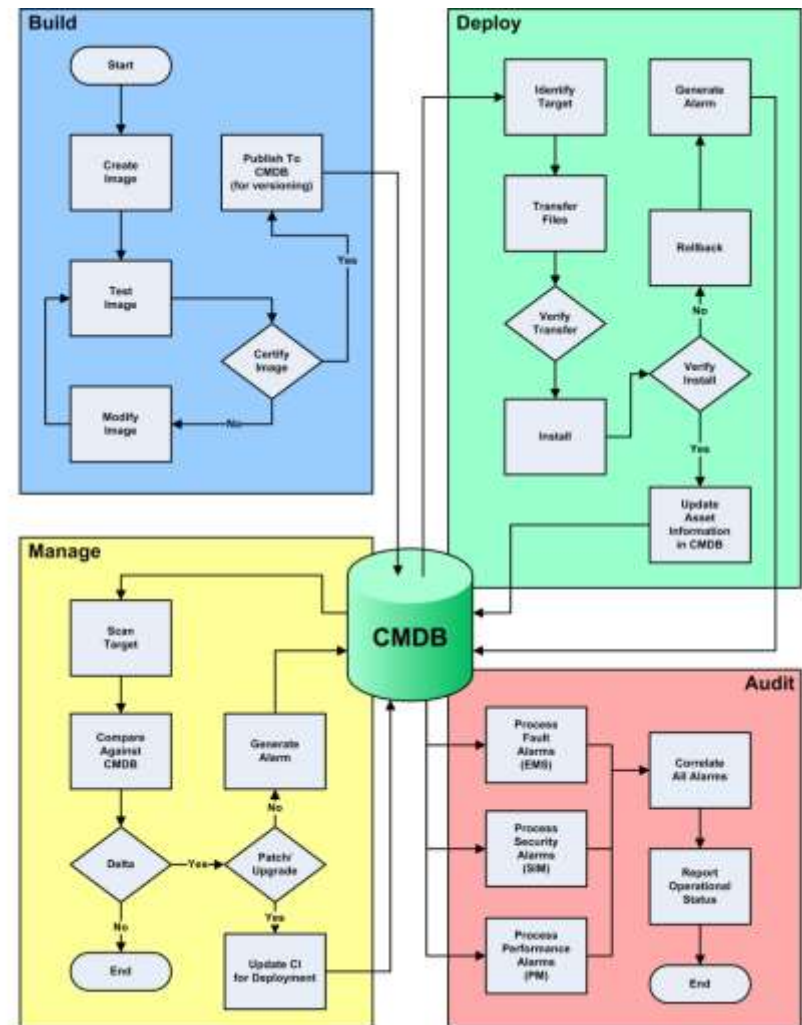
Major Government PC Challenges

- Enforcing and Managing Gold or Platinum Image
- Enforcing and Managing FDCC standard
- Managing authorized Intel Updates
- Managing and Enforcing STIGS
- Compliance
- Reporting and Auditing

PC Life Cycle Management

“The most effective way for an enterprise to reduce the TCO of its PCs is through the implementation of management best practices across all phases of the PC life cycle.” – (Gartner, 13 January 2006)

- Build
- Deploy
- Manage
- Audit



Audit – Report and Analyze

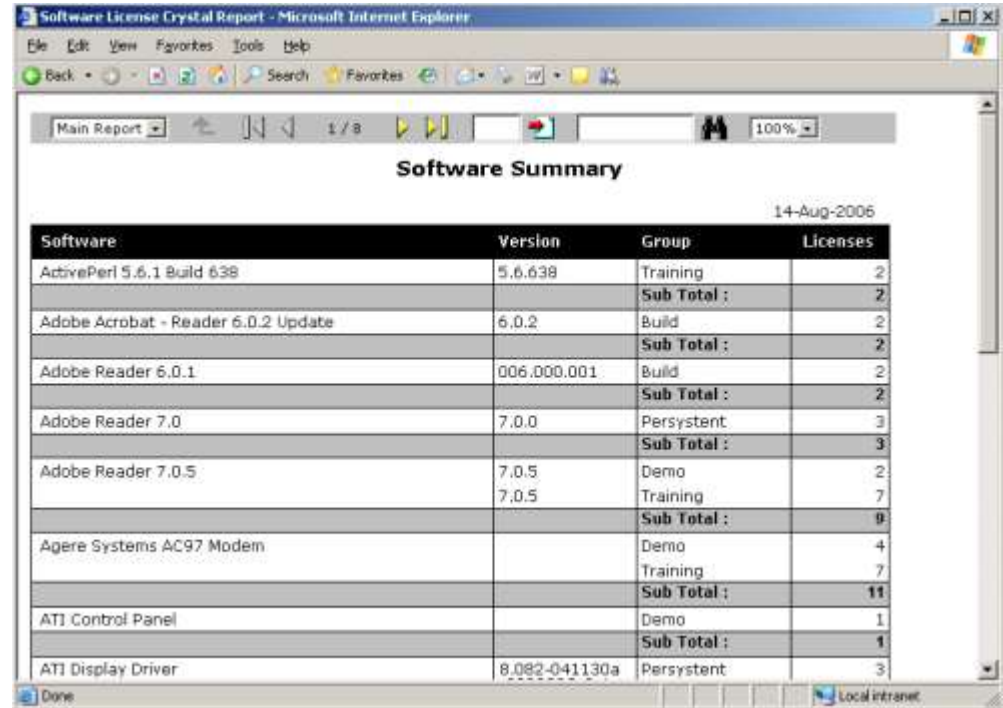
- **Analyze Policy Impact on the Organization**

- Complete reporting of device history
- Grouping at the organizational, departmental and user levels
- Software licensing

- **Demonstrate Control Over the Environment**

- Must show internal control over IT assets to achieve regulatory compliance

- **Identify Compliance and Operational Exceptions**



Software	Version	Group	Licenses
ActivePerl 5.6.1 Build 638	5.6.638	Training	2
		Sub Total :	2
Adobe Acrobat - Reader 6.0.2 Update	6.0.2	Build	2
		Sub Total :	2
Adobe Reader 6.0.1	006.000.001	Build	2
		Sub Total :	2
Adobe Reader 7.0	7.0.0	Persystem	3
		Sub Total :	3
Adobe Reader 7.0.5	7.0.5	Demo	2
	7.0.5	Training	7
		Sub Total :	9
Agere Systems AC97 Modem		Demo	4
		Training	7
		Sub Total :	11
ATI Control Panel		Demo	1
		Sub Total :	1
ATI Display Driver	8.082-041130a	Persystem	3

Thank You!



PERSYSTENT™
TECHNOLOGIES

