

CONTINUOUS MONITORING & CONTROL OF THE FEDERAL DESKTOP CORE CONFIGURATION

What Your CIO Needs to Know



A Triumphant WhitePaper

Background

In March of 2007, the Office of E-Government and Information Technology for the Office of Management and Budget sent a memo to all Federal CIO's. The memo, entitled "Implementation of Commonly Accepted Security Configurations for Windows Operating Systems," M-07-11, directed all federal agencies "*who have Windows XP deployed and plan to upgrade to the Vista operating system...to adopt the security configurations developed by the National Institute of Standards and Technology (NIST), the Department of Defense (DoD) and the Department of Homeland Security (DHS).*"

The memo continued: "*DoD has worked with NIST and DHS to reach a consensus agreement on secure configurations of the Vista operating system, and to deploy standard secure desktops for Windows XP. Information is more secure, overall network performance is improved, and overall operating costs are lower. Agencies with these operating systems and/or plans to upgrade to these operating systems must adopt these standard security configurations by February 1, 2008.*" This memo became known informally as the "OMB Mandate", and requires all federal government agencies to move to a single, standard, enterprise-wide managed configuration environment for desktops and laptops running Microsoft Windows XP or Windows Vista. Windows desktops and laptops of Federal government contractors that interface with federal government systems are also subject to FDCC requirements.

In June 2007, OMB released a second memorandum entitled "Ensuring New Acquisitions Include Common Security Configurations," M-07-18, encouraging agencies to use language in their software solicitations to reinforce the FDCC as a development standard and for vendors to test and certify their applications are fully compatible when operating in an FDCC environment. Since these memos were released, OMB, NIST, DoD, DHS, and private industry have partnered to develop the Federal Desktop Core Configuration (FDCC) as the standard configuration for Windows-based computers across the federal government.

"The Federal Desktop Core Configuration provides a baseline level of security, reduces risk from security threats and vulnerabilities, and saves time and resources."

*- Karen Evans
Administrator
Office of E-Government and
Information Technology*

Goals of the FDCC

The Federal Desktop Core Configuration is designed to provide a single, standard, enterprise-wide managed environment for desktops and laptops running a current Microsoft Windows operating system. By using a common configuration rather than a wide range of individually created configurations, the federal government expects to reduce costs, and reduce the problems created by application compatibility issues. In addition, the FDCC will improve IT security by reducing opportunities for outsiders to access and exploit government computer systems.

A Common Environment:

Government computing systems support a wide range of critical applications that depend on interoperability. The FDCC allows applications to be deployed in less time, reduces the time required for compatibility testing, and ensures that compatibility issues are identified and resolved in a timely manner. In addition, custom software applications developed by one government agency can reasonably be expected to work properly on another agency's Windows systems, since they will all be using a common (FDCC) configuration.

Enhanced Security

The security configuration settings in the FDCC were developed in conjunction with leading security, operations, help desk, and software engineering experts from NIST, NSA, DISA, DoD, DHS, and private industry. The FDCC removes administrative privileges for users that are not system administrators (except as required, and with prior approval for a small number of specific applications) lowering the risk of a range of malicious attacks. By restricting administrative privileges, users are barred from relaxing security settings, reducing the potential for attack. In addition, enabling a local PC firewall adds an additional layer of defense.

Reduced Support Costs

The federal government spends a significant portion of its IT budget to provide desktop support to end users. Much of this cost is due to the "one-off" nature of the Windows PC systems that are deployed across agencies. As a result of the consistent desktop configuration provided by the FDCC, the government will be able to save by reducing the volume of help desk calls and the troubleshooting time spent on each call.

Increased Agility

Upgrading existing software products, or deploying new software products, had previously been time consuming and labor intensive. The common FDCC configuration allows for accelerated testing of these products, which facilitates agency-wide simultaneous migration to new products or product upgrades. This also allows the federal government to gain greater value from its investment in software license maintenance agreements. Adopting the FDCC also allows federal agencies to significantly reduce the time required to apply security patches. With the FDCC, testing and deployment of fixes and patches can be dramatically accelerated.

Challenges of the FDCC

The FDCC Mandate requires all Federal Agencies to implement FDCC by February 2008. While the initial deadline has passed, many government agencies continue to struggle with the mandate, despite their best efforts. This lack of compliance is a clear indication of the challenges involved in driving complex requirements across large and multifaceted organizations. Some of the initial challenges include:

- user resistance due to limitations of the standard user rights mandated in the FDCC
- a legacy of multiple standards and configurations
- some FDCC-mandated settings are too restrictive for certain organizations current needs, requiring them to report FDCC deviations to the NIST and OMB

Fortunately, these are all short-term challenges that are being overcome through a combination of education, enforcement and report. The larger challenge is not how to deploy FDCC compliant systems initially, but how to ensure consistent FDCC compliance over time. The National Checklist Program (NCP) is the U.S. government repository of publicly available security checklists (or benchmarks) for the FDCC. This NIST site contains more than 160 checklists, covering more than 150 separate software products, which provide detailed low level guidance on setting the security configuration of operating systems and applications.

How do you ensure your organization is consistently in compliance with such a large and comprehensive set of requirements, across tens of thousands, or even hundreds of thousands of Windows PC's in multiple facilities? "Locking down" all your PC's might seem an attractive option at first, but the impact on user productivity would clearly be unacceptable. So how do you balance the needs of the user community with the regulatory requirements of the FDCC?

Most users start with a "clean" PC, either a new PC or one that was wiped and reinstalled for their use. These "Clean PC's" are FDCC compliant, free of unnecessary software, and fully compliant with IT policies. However, as the user begins to work with their PC, it shifts away from the initial state of compliance. In some cases, e.g. viruses or spyware, the user is not intentionally making changes to the PC. However, in many cases, intentional changes by the user result in problems, including:

- User installs file-sharing software, exposing your network
- User installs a game that overwrites shared DLL files
- User installs unlicensed commercial software product
- User installs IM software that violates organizational policy
- User uninstalls a program and deletes a shared file
- User changes email settings, deleting all "junk" emails or deleting emails from the server
- User turns off their anti-virus or firewall

These situations create both organizational risk, and increased costs. There is no practical and affordable manual approach that will ensure your agency can either maintain or demonstrate compliance when challenged. What is needed is a reliable, comprehensive and affordable automated solution that provides continuous monitoring and control over FDCC compliance and the PC environment.

Recommendations for Success

In today's highly regulated federal IT environment, the need for continuous monitoring of IT controls is more critical than ever. The risks of being out of compliance are too great. And the increasing costs (and time) of manual audits and compliance reviews are pressuring agencies to find a cost-effective, reliable, and sustainable means of validating compliance. There is a clearly identified need for technology solutions that can automate the independent and continuous monitoring and resolution (as necessary) of regulatory controls.

It doesn't make sense, either financially or operationally, to take a reactive approach to enforce compliance after problems occur. By the time support staff is involved, the damage has already been done and costs have been incurred. Manual processes put a heavy burden on IT staff and related budget. Reactive processes leave you in a position of having to clean up the damage after it has occurred. And a "one size fits all" approach isn't realistic given the diversity of user needs.

Organizations need to be able to automatically

- repair changes before they become problems;
- ensure compliance with internal policies;
- ensure compliance with external regulations; and
- avoid disruptions and damage to reputation.

There are many advantages to a continually compliant PC environment, but the most obvious are that systems perform better, and users are more productive. As a result, risks are mitigated, support costs are reduced, and the organization is able to consistently demonstrate control and compliance.

Continuous controls monitoring delivers "hard" and "soft" benefits and should be considered by any federal agency or organization looking to ensure their compliance efforts. Continuous controls monitoring and resolution software provides:

Reduced Risk

- Reassert control over your PC environment without lockdown
- Maintain security on every computer, every day
- Detect security breaches that anti-virus applications fail to recognize (e.g. "Zero Day Attack")
- Prevent malicious software from disrupting your environment
- Surgically correct problems on any machine, automatically

Lower Costs

- Reduce time to resolution for unknown problems
- Maximize and demonstrate real IT support savings due to reduction in service desk calls
- Reduction in user downtime

Better Management

- Deliver predictive, consistent service levels and improve customer satisfaction

- Increased reporting scope
- Simplified compliance baselines
- Monitoring of control effectiveness
- Document operational processes

Continuous controls monitoring and resolution software does not replace the need for regular audit processes. Instead, it reduces the time required for an audit, and ensures compliance (with both regulations and internal policies) at all times. Manually monitoring, controlling and auditing Windows computers is difficult and slow. With the right software, you can quickly and automatically:

- control Windows computers without locking them down
- repair changes before they become problems
- ensure compliance with internal policies and external regulations
- avoid damage to the reputation of your organization
- reduce the time and costs to prepare for audits
- strengthen your control environments
- reduce user downtime and help desk overload

Triumfant Corporation is the leading provider of continuous monitoring and control software for Windows computers. Triumfant products enable you to automate the process of monitoring and repairing unwanted changes to every Windows PC and server in your environment, based on the policies you determine. As a result, your Windows PC systems are in compliance and operational at all times.

Triumfant will automatically monitor and repair undesirable changes, ensuring continuous compliance between audits and strict adherence to internal controls. Triumfant provides an effective approach to your PC compliance mandates, and reasonable assurance regarding achievement of an organization's goals and objectives. Even more importantly, Triumfant also delivers a return on governance expenditures that improves organizational effectiveness and personal efficiency. Triumfant reduces the time, effort and skills required for a comprehensive audit.

Triumfant reduces the risk and complexity of your IT compliance process. And not only does Triumfant software products ensure continuous compliance with regulations such as FDCC, they reduce the risk associated with uncontrolled Windows computers before they materially affect the achievement of the organization's objectives.

Only Triumfant is:

- **Continuous:**
 - Verifies and enforces organizational policies on every PC, every day



- Ensures continuous compliance in between scheduled audits

Continuous control minimizes risks on an ongoing basis, easily produces audit evidence as needed, and resolves issues before they become problems.

- **Comprehensive**

- Creates a detailed representation of the state of each managed PC in a central database
- Widest scan scope in the industry (200,000 to 500,000 attributes per machine)
- Data collected every day from every PC

Comprehensive control ensures compliance of all PC's, not just a subset. It is simple to administer, provides detailed reporting, and serves as a "Last Line of Defense" when antivirus fails.

- **Accurate**

- Rule base automatically synthesizes "Adaptive Reference Model" that represents what is normal in your environment
- Pattern recognition technology recognizes known errors and unknown problems

Triumphant products are extremely precise, resolving both known and unknown problems. False positives are very rare, results are concise and actionable, and the customizable rule base let's you easily tune the controls to meet your precise requirements.

- **Proactive**

- Remediation responses derived on the fly to specifically address the diagnosed problem
- Missing or incorrect files and registry keys are restored using unique donor technology

Because Triumphant software is working around the clock, there is no delay while waiting for a vendor to deliver a fix or patch to protect against intrusive software. There are no backups or golden images needed, and no reboots required. And just in case, every remediation can be reversed if needed.

Through the Triumphant IT Intelligence™ platform, IT executives and their staff can automatically discover, diagnose, and precisely repair any unwanted changes in their Microsoft Windows environment (including desktops, laptops and Windows servers). From Compliance to Security to Incident and Problem Management, Triumphant offers an easy-to-use solution that helps your reduce costs, mitigate risks and increase quality of service.

As a result, Triumphant is the leading provider of automated resolution management software for personal computers. We enable organizations to easily and cost-effectively automate the process of monitoring and repairing unwanted changes to personal computers. We reduce the cost and complexity of the IT Audit process. And we reduce the level of risk associated with uncontrolled PC's.

To learn more about how Triumphant can help your organization with FDCC Compliance, please call us at 800.267.2190 or visit us at www.triumfant.com