

EventTracker WhatChanged Features

Within the Windows architecture monitoring and reporting on what changed, who changed it and when the change occurred is, for all practical purposes, impossible. EventTracker WhatChanged provides unmatched insight and control of a Windows infrastructure by enabling security and system administrators to quickly identify configuration changes that represent security and operational risks while at the same time continually monitoring for compliance against policy based configuration standards such as FDCC.

How EventTracker WhatChanged Works

WhatChanged monitors hundreds of thousands of objects within a Windows system by taking a quick, periodic snapshot evaluation of each system and comparing it against either a master snapshot of the correct configuration, or a comparison of change from a previous snapshot. The comparison is performed on the monitored system and only the detected changes are forwarded to the WhatChanged Console, minimizing network overhead. Change history is maintained on the WhatChanged Console so reporting and analysis can be performed offline.

Change Audit

- Support for both business state (compliance) and object state (security) models
- Quickly identify changes that represent security risks to your infrastructure
- Improve problem determination performance through integration of change data for root-cause analysis; leads to increased IT service availability

Configuration Assessment

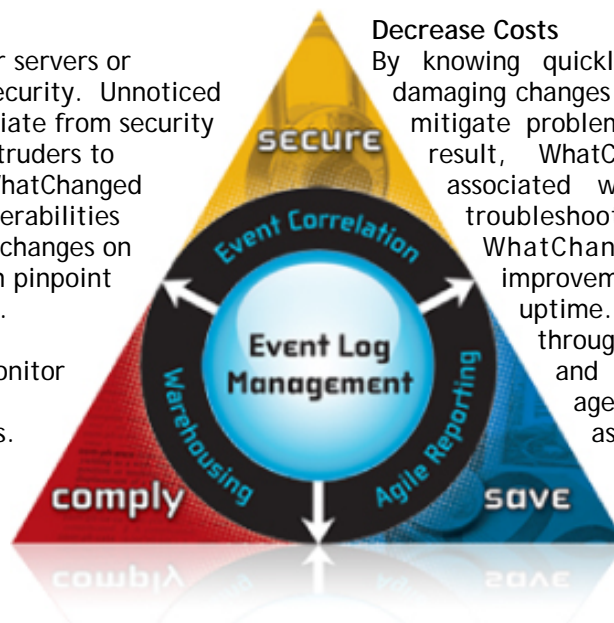
- Define standard trusted states and monitor compliance on all Windows systems
- Improve availability through reduced downtime due to misconfigured systems
- Improve overall security by minimizing vulnerable systems
- Reduce help-desk calls and cost through proactive action

Increase Security

Knowing what has changed on your servers or Workstations radically enhances security. Unnoticed and unauthorized changes can deviate from security guidelines and provide ways for intruders to penetrate your corporate data. WhatChanged monitors and alerts on known vulnerabilities and black listed files. It monitors changes on a system over time so that you can pinpoint exactly when the change occurred. WhatChanged provides a valuable independent control so you can monitor and police your change and configuration management process.

Decrease Costs

By knowing quickly that there have been potentially damaging changes made to your IT infrastructure, you can mitigate problems before they get out of hand. As a result, WhatChanged dramatically reduces costs associated with unplanned outages as well as troubleshooting and recovery times. Using WhatChanged you will see immediate improvements in operational stability and system uptime. WhatChanged provides rapid ROI through a powerful centralized configuration and deployment capability that enables agents to be quickly deployed and updated as standards and policy evolve.



Achieve Compliance

Many organizations are moving to policy-based configuration standards to enhance security and improve overall stability of the Windows environment. These Standards can be either internally defined or based on standards such as the US government's FDCC standard for Windows desktops. WhatChanged supports continuous monitoring against a policy defined configuration standard enabling users to ensure continuous compliance.

EventTracker WhatChanged Framework

- Centralized console provides a single view of the state of an organization's infrastructure by displaying summary of changes detected, vulnerabilities found and policy drifts on all systems
- Scheduled or on demand snapshot on any managed system from the WhatChanged console
- Comparison processing can be done both online and offline
- Vulnerability, configuration and policy management data is maintained only on the manager to avoid duplication and risk of corruption
- Create alerts; take action on detection of any system change or policy drift
- Create custom groups according to your organizational structure
- Monitor file-system integrity by checking file attributes and contents using either a FIPS compliant SHA-1 or MD-5 checksum algorithm
- Configurable audit provides ability to create global and system based filters for file and registry items
- Powerful centralized agent configuration and deployment architecture enables rapid deployment and updating of agents

Policy Enforcement

- Scheduled/Automated or On-Demand policy assessment for continuous compliance
- Policy Management: Create, edit, customize and import/export security configuration policies
- Policy Assessment: Assess and apply appropriate policies to applicable systems
- Policy Compliance: Monitor systems that have drifted out of compliance through a centralized UI
- Record event details of all policy deviations for forensic and audit purposes
- Criteria based rule assessment: Assess a rule only if the system exhibits a particular state
- Analyze results and remove false positives and accepted risks from reporting
- Tune and apply policy according to the role of a system or group of systems
- Create and apply custom checks by using policy editor to quickly add new checks as necessary to comply with changing requirements
- View the exact reason of failure of a rule by viewing the desired and actual state of every item

Minimum System Requirements

- 2.8GHz Pentium-based machine
- Windows 2003 Server
- >1GB RAM
- Approximately 5 GB per 100 systems required for the storage for change data

