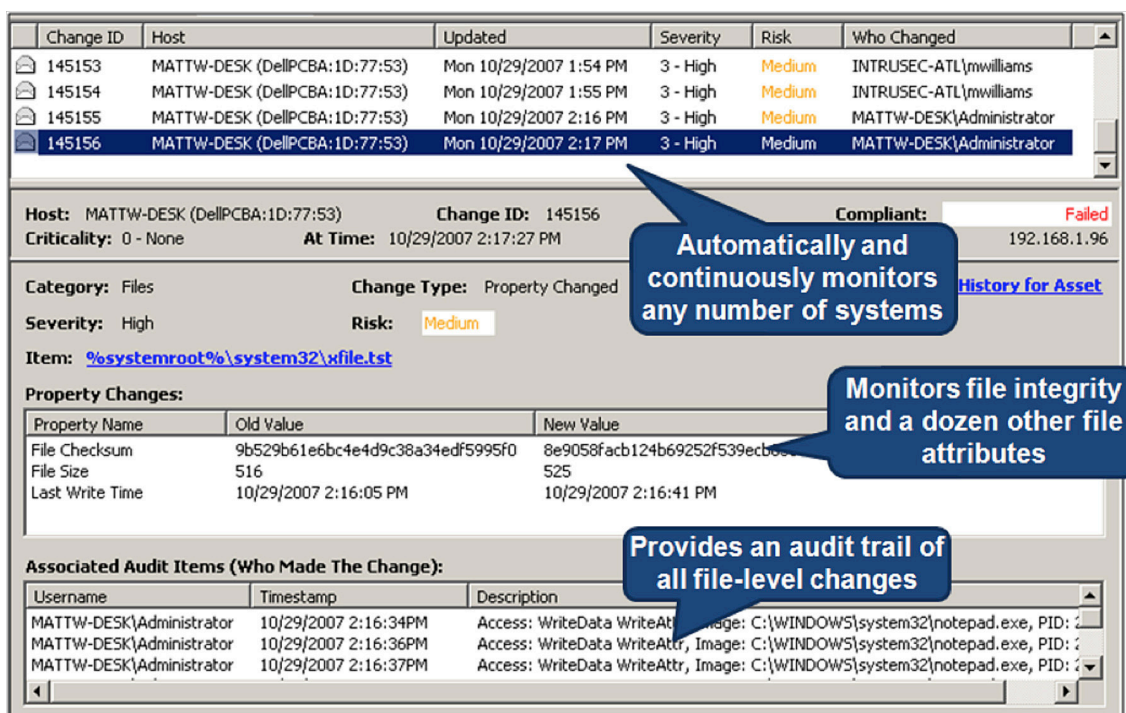


nCircle File Integrity Monitor™

Agentless File Configuration Auditing, Monitoring, and Alerting

File integrity monitoring enables organizations to detect unauthorized file system modifications and maintain host integrity, system availability and data confidentiality. This capability is critical today, especially for companies that are governed by regulations and standards that deal with data integrity and privacy such as the Payment Card Industry (PCI) Data Security Standard. Specifically, section 11.5 of the PCI regulations requires “merchants to deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system or content files.”

nCircle File Integrity Monitor provides an agentless file integrity auditing solution that gives you the ability to monitor an asset’s details all the way down to the file level without requiring software agents on the monitored system. Using DynAgent™, nCircle’s patent-pending agentless technology, File Integrity Monitor compares file details and checksums on designated hosts to stated baselines. Any deviations from the baseline are highlighted in the console, logged, and reported to administrators to intelligently address any changes and ensure continuous security and policy compliance.



Change ID	Host	Updated	Severity	Risk	Who Changed
145153	MATTW-DESK (DellPCBA:1D:77:53)	Mon 10/29/2007 1:54 PM	3 - High	Medium	INTRUSEC-ATL\mwilliams
145154	MATTW-DESK (DellPCBA:1D:77:53)	Mon 10/29/2007 1:55 PM	3 - High	Medium	INTRUSEC-ATL\mwilliams
145155	MATTW-DESK (DellPCBA:1D:77:53)	Mon 10/29/2007 2:16 PM	3 - High	Medium	MATTW-DESK\Administrator
145156	MATTW-DESK (DellPCBA:1D:77:53)	Mon 10/29/2007 2:17 PM	3 - High	Medium	MATTW-DESK\Administrator

Host: MATTW-DESK (DellPCBA:1D:77:53)	Change ID: 145156	Compliant: Failed
Criticality: 0 - None	At Time: 10/29/2007 2:17:27 PM	192.168.1.96
Category: Files	Change Type: Property Changed	History for Asset
Severity: High	Risk: Medium	
Item: %systemroot%\system32\xfile.tst		
Property Changes:		
Property Name	Old Value	New Value
File Checksum	9b529b61e6bc4e4d9c38a34edf5995f0	8e9058facb124b69252f539ecb...
File Size	516	525
Last Write Time	10/29/2007 2:16:05 PM	10/29/2007 2:16:41 PM
Associated Audit Items (Who Made The Change):		
Username	Timestamp	Description
MATTW-DESK\Administrator	10/29/2007 2:16:34PM	Access: WriteData WriteAttr, Image: C:\WINDOWS\system32\notepad.exe, PID: 2
MATTW-DESK\Administrator	10/29/2007 2:16:36PM	Access: WriteData WriteAttr, Image: C:\WINDOWS\system32\notepad.exe, PID: 2
MATTW-DESK\Administrator	10/29/2007 2:16:37PM	Access: WriteData WriteAttr, Image: C:\WINDOWS\system32\notepad.exe, PID: 2

Automatically and continuously monitors any number of systems

Monitors file integrity and a dozen other file attributes

Provides an audit trail of all file-level changes

nCircle File Integrity Monitor automatically detects any changes made to a host's files to ensure security and policy compliance

File Integrity Monitor Delivers:

- **Agentless File-Level Integrity Monitoring and Auditing** – nCircle File Integrity Monitor features DynAgent™, nCircle's patent-pending agentless technology, to help companies audit file integrity across their entire global network without requiring an agent. In addition to automatically discovering what files exist on a host, detailed information about the files is also provided:
 - File size
 - Version
 - When it was created
 - When it was modified
 - The login name of any user who modifies the file
 - Access attributes like Read-Only Access, Hidden, System, etc.

File Integrity Monitor's agentless DynAgent technology delivers the same detailed information as an agent-based solution, with none of the management overhead and complexity.

- **File Version Verification** – nCircle File Integrity Monitor utilizes its powerful Policy Compliance Engine to not only verify that files have not changed, but also verifies that files are the correct version. Loading the manufacturer-supplied checksum into the Policy Compliance Engine ensures that the critical system files on your production server are, in fact, the same ones that came from the manufacturer.
- **Cryptography-based Monitoring** – As an extra safeguard against file tampering, the solution also monitors file checksums – MD5 or SHA-1 on Windows-based systems and MD5 or any user-defined hash algorithm on Unix-based systems – providing cryptography-based monitoring for file changes.

nCircle file integrity monitoring is available as a standalone solution – [nCircle File Integrity Monitor](#) – or as part of [nCircle Configuration Compliance Manager](#).

About nCircle

nCircle is the leading provider of automated security and compliance auditing solutions. More than 4,000 enterprises, government agencies and service providers around the world rely on nCircle's proactive solutions to manage and reduce security risk and achieve compliance on their networks. nCircle has won numerous awards for growth, innovation, customer satisfaction and technology leadership. nCircle is headquartered in San Francisco, CA, with regional offices throughout the United States and in London and Toronto. Additional information about nCircle is available at www.ncircle.com



nCircle^o

nCircle
info@ncircle.com
www.ncircle.com

Corporate Headquarters
101 Second Street, Suite 400
San Francisco, CA 94105
Phone: +1 888 464 2900
Fax: +1 415 625 5982

Europe Headquarters
Venture House
Arlington Square
Downshire Way
Bracknell
RG12 1WA
United Kingdom
Phone: +44 (0) 1344 742829
Fax: +44 (0) 1344 741001
emea@ncircle.com