

NetIQ Change Guardian™ for Windows

Benutzeraktivitäten und Änderungen in der Windows-Umgebung mit minimaler Serverbelastung überwachen

Überblick

NetIQ Change Guardian for Windows vermittelt Ihnen systemübergreifend wertvolle Einblicke in die Aktivitäten von privilegierten Benutzern sowie von ihnen durchgeführte Änderungen, und liefert die Transparenz, die Sie zum Schutz Ihrer Windows-Umgebung vor gefährlichen Bedrohungen benötigen.

Lösungen für heute

Die Überwachung von Änderungen ist eine in der Informationstechnik anerkannte Best Practice und wird zudem vom PCI-Standard (verbindliches Regelwerk für den Zahlungsverkehr über Kreditkartentransaktionen/ Payment Card Industry Data Security Standard) zwingend vorgeschrieben. Die derzeitigen Überwachungskonzepte sind für Produktionssysteme aber meist nicht praktikabel:

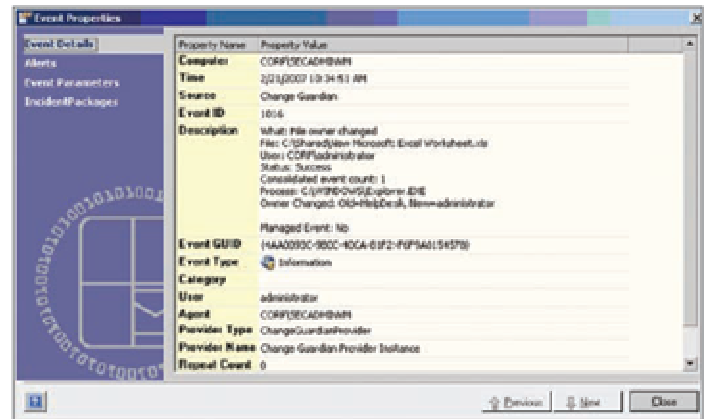
- Das native Auditing auf Objektebene beeinträchtigt die Serverleistung zu stark und erzeugt zudem irreführende und aufgeblähte Ereignisprotokolle.
- Routinen zur Prüfung der Dateiintegrität verursachen häufig eine inakzeptable Systembelastung. Ohne natives Auditing auf Objektebene lässt sich zudem nicht identifizieren, wer wann eine Änderung durchgeführt hat.
- Kernel Shims können Probleme in Bezug auf die Systemstabilität verursachen und sind bei großflächiger Implementierung problematisch.

NetIQ Change Guardian for Windows löst diese Problematik mithilfe eines eigenständigen Konzepts zur Aktivitäten- und Änderungsüberwachung. Hierzu wird ein von Microsoft unterstützter Filtertreiber verwendet, um die gewünschten Aktivitäten zu erfassen und zu verarbeiten. Dabei werden die Daten so verarbeitet, dass aussagekräftige, unkomplizierte aber dennoch leistungsstarke Ereignisprotokolle und Alarmhinweise bereitgestellt werden. Als Modul von NetIQ Security Manager™ arbeitet der Treiber eng mit dem Sicherheitsinformations- und Ereignismanagement (SIEM) zusammen, das auch eine Protokollverwaltung erfasst.

Entscheidende Vorteile

Leistungsstarke Änderungsüberwachung in Echtzeit – Überwacht Änderungen über Dateien, Verzeichnisse, Freigaben, Registrierungseinträge und Systemprozesse hinweg und meldet unverzüglich potenziell gefährliche Änderungen an Ihrer Umgebung.

Macht ein natives Auditing überflüssig – Nutzt einen von Microsoft zugelassenen Überwachungsmechanismus, um die bei nativem Auditing möglichen Leistungseinbußen zu vermeiden, während gleichzeitig hochzuverlässige Änderungsinformationen bereitgestellt werden.



Die von NetIQ Change Guardian for Windows gemeldeten Änderungsereignisse sind aussagekräftig und einfach zu lesen, so dass keine ausgesprochenen Spezialkenntnisse notwendig sind, um die Ereignisse nachvollziehen zu können. Für eine bestimmte Aktivität werden Vorher-/Nachher-Werte angegeben, wobei die Zahl der einzelnen Datensätze überschaubar bleibt. (z.B. Rechteänderung, modifizierte Datei, neuer Eintrag in die Registrierungsdatei usw.).

Validiert und erzwingt Change Control Prozesse – Identifiziert Änderungen, die über eine autorisierte Kontrollschnittstelle durchgeführt wurden, gegenüber Änderungen, die möglicherweise unter Umgehung der Change Management Prozesse erfolgten.

Protokolliert und prüft Änderungen zentral – Stellt Informationen über die in der gesamten Organisation durchgeführten kritischen Änderungen zur nachfolgenden Analyse bereit und vereinfacht die Zusammenstellung von Änderungsereignissen, die zur Erfüllung gesetzlicher Bestimmungen und zur gezielten Untersuchung von Vorfällen notwendig sind.

Liefert umfassende Änderungsberichte – Erfasst Vorher-/Nachher-Werte für Objekte, ermöglicht detaillierte Änderungsberichte auf Basis eines oder mehrerer Benutzer oder Computer, hilft bei der umgehenden Identifizierung von Anomalien und unterstützt bei der schnellen Detailsuche.

Arbeitet mit einer breiter angelegten Lösung für die Windows-Änderungskontrolle zusammen – Erweitert die Funktionalität von NetIQ Security Manager und NetIQ Change Administrator™ und stellt somit eine umfassende Lösung für die Delegation von Privilegien, die Überwachung privilegierter Benutzer und die Serversicherheit bereit.

NetIQ Change Guardian™ for Windows

Technische Merkmale

Echtzeit-Überwachung und Änderungsmeldung in Ihrer gesamten Windows-Umgebung mit detaillierten Einblicken in:

- **Dateien und Verzeichnisse** – Angaben darüber, wer eine Datei oder ein Verzeichnis erstellt, geöffnet, verschoben, bearbeitet oder gelöscht hat, und zwar zusammen mit Vorher-/Nachher-Angaben (inkl. Dateigröße und Zugangsrechten).
- **Dateifreigaben** – Kennzeichnet, wo Zugangsrechte zu Dateien oder Verzeichnissen geändert wurden.
- **Windows-Registrierung** – Hält fest, wer Änderungen vorgenommen hat, einschließlich der Vorher-/Nachher-Werte.
- **Systemprozesse** – Überwacht die Erstellung und Beendigung von Prozessen, identifiziert den Benutzer oder die Anwendung, der bzw. die die Maßnahme veranlasst hat, und protokolliert alle gestarteten Snap-Ins für die Microsoft Management Console (MMC).

Erweiterte Audit-Informationen mit höherer Zuverlässigkeit und besserer Verständlichkeit, als dies mit nativen Ereignissen möglich ist. SIDs/GUIDs werden in die tatsächlichen Deskriptoren umgesetzt und Informationen werden vor und nach der Änderung aufgezeichnet, um eine bessere Ereignisanalyse durchführen zu können.

- **Erweiterbare Rules Engine:** ermöglicht die unkomplizierte Erstellung und Anpassung von Regeln über intuitive Assistenten, um Benutzer, Computer, Dateien, Verzeichnisse, Registrierungsschlüssel und Prozesse über definierbare Zeitperioden ein- oder auszuschließen.
- **Kontrollierbare Alarmauslösung:** ermöglicht es, festzulegen, welche Änderungen einen Alarm auslösen, und wann, wo und wie diese Alarme gemeldet werden.
- **Umfassende Berichterstattung über Änderungen:** unterstützt den Nachweis der Übereinstimmung mit internen Richtlinien und gesetzlichen Bestimmungen und ermöglicht eine bessere Ursachenanalyse und Fehlerbehebung.

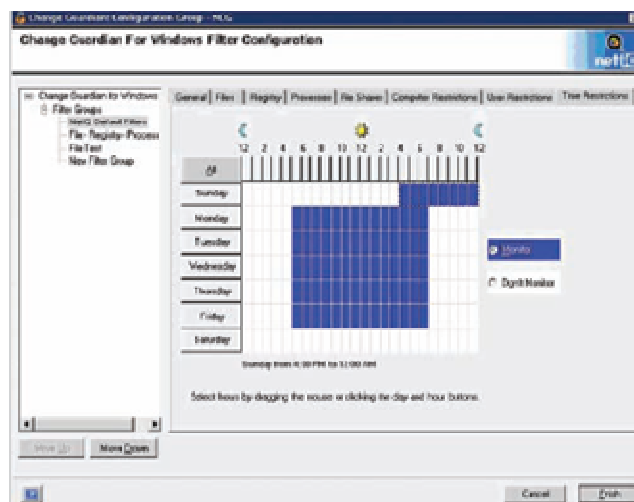
Kontakt

Internationaler Sitz
NetIQ, An Attachmate Business
1233 West Loop South
Suite 1800
Houston, TX 77027, USA
713.548.1700
713.548.1771 Fax
888.323.6768 Verkauf

NetIQ Deutschland GmbH
+49 (0) 89 99351-0
infoDE@Netiq.com
www.netiq.com

NetIQ Schweiz
+41 43399 2090
infoCH@Netiq.com
www.netiq.com

Informationen über weitere Geschäftsstellen, Partner und Wiederverkäufer finden Sie auf unserer Website unter www.netiq.com/contacts



NetIQ Change Guardian for Windows stellt flexible Überwachungsfunktionen bereit, mit denen Sie definieren können, was auf welchen Systemen und unter welchen Benutzern über welche Zeiträume überwacht (oder nicht überwacht) werden soll.

Die zentrale Erhebung und Prüfung von Änderungsinformationen auf Basis der mehrfach ausgezeichneten NetIQ Security Manager Plattform verhilft Ihnen zu einer zuverlässigen Sicherheitsinfrastruktur, die sich flexibel an den jeweiligen Bedarf Ihres Umfelds anpassen lässt.

Systemvoraussetzungen

Voraussetzungen an das Überwachungssystem:

- NetIQ Security Manager 5.6 SP1 oder neuer

Überwachte Windows-Plattformen:

- Windows Server 2003 SP1