

# NetIQ Change Guardian Produktfamilie

Zugriffs- und Änderungsüberwachung auf System- und Dateiebene zum Schutz von Informationen und zum Nachweis von Compliance

## PRODUKTÜBERSICHT

### Einleitung

Unsystematische Änderungen an wichtigen Objekten, Dateien, Verzeichnissen, Systemen oder Datenbanken in der gesamten IT-Infrastruktur bedrohen zunehmend die Datensicherheit in Unternehmen.

Die NetIQ® Change Guardian™ Produktfamilie ermöglicht Überwachung, Reporting und Erkennung von Änderungen. Sie trägt so dazu bei, Sicherheitsrisiken für sensible Daten und Systeme erheblich zu reduzieren und die Konformität mit aufsichtsrechtlichen Vorgaben und Datenschutzbestimmungen herzustellen, beispielsweise mit PCI DSS, HIPAA, ISO/IEC 27001 und der EU-Datenschutzrichtlinie.

### Im Überblick

Die NetIQ Change Guardian Produktfamilie unterstützt Unternehmen bei der Verfolgung von Änderungen und der Abwehr von Bedrohungen. Auf diese Weise sinkt der Zeitaufwand für die Analyse und Behebung von Problemen nach einem sicherheitsrelevanten Vorfall.

Die NetIQ Change Guardian Familie umfasst folgende Produkte:

- > **NetIQ Change Guardian for Windows** – Das Produkt dient der Überwachung von Änderungen an Dateien, Verzeichnissen, freigegebenen Ordnern, Registrierungseinträgen und Systemprozessen und zur unverzüglichen Meldung potenziell gefährlicher Änderungen an der Microsoft-Umgebung.
- > **NetIQ Change Guardian for Group Policy** – Die Lösung vermittelt die nötige Transparenz, um unsachgemäße Änderungen an Microsoft-Gruppenrichtlinienobjekten zu stoppen, bevor diese die Sicherheit oder Verfügbarkeit der Microsoft-Active-Directory-Umgebung beeinträchtigen können.
- > **NetIQ Change Guardian for Active Directory** – Das Produkt übernimmt die Active-Directory-Überwachung und Warnung vor unsystematischen Änderungen in Echtzeit, um die Konformität mit den AD-Richtlinien besser kontrollieren zu können.
- > **NetIQ Change Guardian for Databases** – Eine passive Non-Inline-Anwendung zur Überwachung des Zugriffs auf Datenbanken in Echtzeit und zum Schutz der darin befindlichen sensiblen Inhalte.

Alle Produkte der NetIQ Change Guardian Familie greifen perfekt ineinander und lassen sich reibungslos in andere SIEM-Lösungen (Security Information and Event Management) integrieren, beispielsweise in NetIQ® Security Manager™. Sie bieten damit die Skalierbarkeit, die für die ständig wechselnden Anforderungen in einer stark verteilten und anspruchsvollen Umgebung nötig ist.

In Verbindung mit NetIQ® Aegis® für die Automatisierung von IT-Sicherheitsprozessen und mit NetIQ® Secure Configuration Manager™ für die Dokumentation von Compliance und

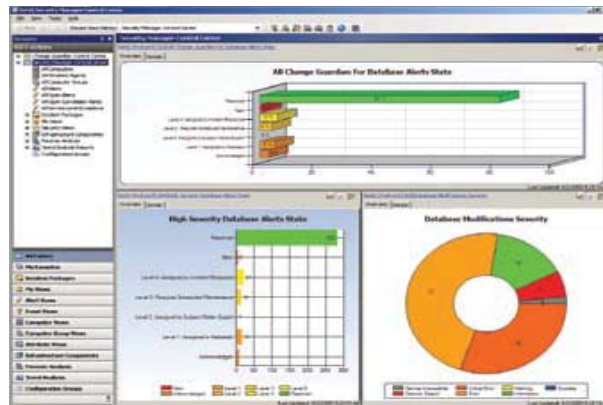
### Weitere Informationen:

Deutschland: +49 (0) 89 993510

Österreich: +42 (0) 1 595 4335

Schweiz: +41 (0) 43 399 2090

E-mail: [infode@netiq.com](mailto:infode@netiq.com) • [www.netiq.de](http://www.netiq.de)



NetIQ Change Guardian erzeugt aussagekräftige, übersichtliche Informationen über Änderungsereignisse unter Angabe der Vorher-/Nachher-Werte und mit Konzentration auf die wesentlichen Fakten.

Berechtigungen ist die NetIQ Change Guardian Produktfamilie eine unverzichtbare Komponente einer leistungsstarken, integrierten und automatischen Lösung für das Sicherheits- und Compliance-Management.

### Funktionalität

Zur Bekämpfung immer ausgefeilterer Bedrohungen und zur Konformität mit einem zunehmend komplexen Regulierungswesen müssen Unternehmen einen mehrschichtigen und systematischen Ansatz verfolgen, um ihre wichtigen Server und ihre sensiblen Daten zu schützen. NetIQ Change Guardian Produkte zeichnen sich durch folgende wesentliche Schutzmechanismen aus:

- > **Management privilegierter Benutzer** – Die Aktivitäten von privilegierten Benutzern, beispielsweise von Datenbankadministratoren, werden überprüft und überwacht, um die Gefahr von Insiderangriffen zu mindern.
- > **Überwachung von Änderungen in Echtzeit** – Änderungen an wichtigen Dateien, Plattformen, Systemen und Datenbanken werden erkannt und gemeldet, um Verstöße zu vermeiden und die Konformität mit Richtlinien zu gewährleisten.
- > **Warnung vor verdächtigen Verhaltensweisen in Echtzeit** – Verdächtige Änderungen werden unverzüglich sichtbar gemacht. In Verbindung mit SIEM-Lösungen werden aufschlussreiche forensische Informationen an die zuständigen Sicherheitsteams weitergeleitet.
- > **Konformität und Einhaltung von Best Practices** – Die Fähigkeit, den Zugriff auf wichtige Dateien und Daten zu überwachen, sichert die Konformität mit einschlägigen gesetzlichen Vorschriften.



# NetIQ Change Guardian Produktfamilie

## Merkmale und Vorteile

Über die einfache Erkennung hinaus ermöglichen NetIQ Change Guardian Produkte die detaillierte Berichterstattung, die für wirksame und fundierte Sicherheitsentscheidungen notwendig ist, um das Risiko von Datenverlusten im Unternehmen zu begrenzen. Wesentliche Merkmale und Vorteile der NetIQ Change Guardian Produktfamilie:

- Die Aktivitäten privilegierter Benutzer in Bezug auf Windows, Active Directory, Gruppenrichtlinien und Datenbank werden verfolgt und aufgezeichnet.
- Die individuelle Definition bekannter, privilegierter Benutzergruppen oder Aktivitäten, die im Unternehmen besonders sorgfältig beobachtet werden sollten, ist möglich.
- Detaillierte Informationen darüber, wer, was, wann und wie geändert oder unternommen hat, einschließlich der Vorher-/Nachher-Werte.
- Abgrenzung systematischer und unsystematischer Änderungen mit Echtzeitmeldung bei letzteren.
- Erübrigt den Einsatz der nativen Auditing-Funktionen und sorgt für hohe Leistung im Hinblick auf Auditing, Compliance und Sicherheit bei minimaler Belastung der vorhandenen Infrastruktur.
- Integrierte Ereigniserkennung und -meldung für alle gängigen SIEM-Lösungen. Abgleich der Ereignisse mit anderen Sicherheitsüberwachungslösungen, um das Risiko unentdeckter Verstöße deutlich zu senken.
- Bereitstellung aller notwendigen Reporting-Werkzeuge, um die Konformität gegenüber internen und externen Prüfern eindeutig nachweisen zu können.
- Zielgerichtete Lösungen zur Erreichung der drängenden Konformitätsziele im Bereich Identifizierung, Dokumentation und Meldung von Änderungen an Dateien, Systemen, Datenbanken, Verzeichnissen oder Objekten.

## Wesentliche Unterscheidungsmerkmale

- > **Integriertes Sicherheitsportfolio zur Unterstützung der Konformitätsziele** - Neben dem Schutz sensibler Daten tragen die NetIQ Change Guardian Produkte dazu bei, einige besonders anspruchsvolle Konformitätsanforderungen zu erfüllen. Hierzu stehen Lösungen zur Überwachung der Datenintegrität, der privilegierten Benutzer, der Datenbankaktivitäten usw. zur Verfügung.
- > **Plattformübergreifende Unterstützung für besseren Datenschutz** - IT- und Sicherheitspersonal sind für die erfolgswichtigen Ressourcen eines Unternehmens verantwortlich. NetIQ Change Guardian Produkte unterstützen auch ausgeprägt heterogene Umgebungen mit mehreren Servern, Betriebssystemen und Anwendungen.
- > **Umfassendes Änderungsberichtswesen zur Reduzierung des Risikos von Verstößen** - NetIQ Change Guardian Produkte erfassen die Vorher-/Nachher-Werte von Änderungen oder Ereignissen, erzeugen detaillierte Änderungsberichte auf Basis eines oder mehrerer Benutzer oder Computer, helfen bei der schnellen Identifizierung von Anomalien und unterstützen Nachforschungsprozesse durch detaillierte und komfortable Möglichkeiten zur forensischen Analyse.
- > **Maximale Leistung bei minimaler Auswirkung auf die Infrastruktur** - NetIQ Change Guardian Produkte überzeugen durch höchste unternehmensweite Skalierbarkeit und Lösungen, die wenig oder gar keine Auswirkungen auf die Leistung von vernetzten Anwendungen, Servern, Systemen oder Prozessen haben.
- > **Leistungsstarke Tools für Sicherheit und Compliance** - Mit einem umfassenden Portfolio an mehrfach ausgezeichneten Lösungen für das Sicherheits- und Compliance-Management gibt NetIQ Anwendern die Mittel an die Hand, ausgereifte Sicherheitsprozesse zu erstellen und zu implementieren. Dies trägt dazu bei, IT-Ressourcen zu maximieren, Compliance-Prozesse zu rationalisieren und Sicherheitsrisiken unternehmensweit zu reduzieren.

Weitere Informationen zur NetIQ Change Guardian Produktfamilie oder zu Testinstallationen erhalten Sie unter [www.netiq.com/cg](http://www.netiq.com/cg).




NetIQ Deutschland  
T +49 (0) 89 99351-0  
E [InfoDE@netiq.com](mailto:InfoDE@netiq.com)  
[www.netiq.de](http://www.netiq.de)

NetIQ Schweiz  
T +41 (0) 43 399 2090  
E [InfoCH@netiq.com](mailto:InfoCH@netiq.com)  
[www.netiq.de](http://www.netiq.de)

NetIQ Österreich  
T +43 (0) 1 595 4335-0  
E [InfoDE@netiq.com](mailto:InfoDE@netiq.com)  
[www.netiq.de](http://www.netiq.de)

Eine vollständige Liste all unserer Niederlassungen in Nordamerika, Europa, dem Mittleren Osten, Afrika, Asien und Südamerika finden Sie unter [www.netiq.com/contacts](http://www.netiq.com/contacts).

<http://community.netiq.com>

Folgen Sie uns :   

NetIQ, ein Geschäftsbereich von Attachmate.

NetIQ, das NetIQ-Zeichen, NetIQ Change Guardian, NetIQ Security Manager, NetIQ Aegis und NetIQ Secure Configuration Manager sind Marken oder eingetragene Marken der NetIQ Corporation in den Vereinigten Staaten. Alle sonstigen Firmen- und Produktnamen sind Marken oder eingetragene Marken der jeweiligen Gesellschaften.