## **NetIQ Change Guardian**

Monitor the activities of privileged users to reduce the risk of insider or targeted attacks

### Introduction

Every day, organizations face increased information security risks when privileged users make unauthorized changes to critical files, systems and applications within their IT infrastructures.

NetlQ<sup>®</sup> Change Guardian<sup>™</sup> monitors critical files, systems and applications in real time to detect unauthorized privileged-user activity, helping you significantly reduce organizational risk to critical assets. It also helps you achieve compliance with regulatory and privacy standards such as the Payment Card Industry Data Security Standards (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH), the International Organization for Standardization's latest standards (ISO/IEC 27001), the EU Privacy Directive and others.

#### **Product Overview**

NetlQ Change Guardian gives you the security intelligence you need to rapidly identify and respond to privileged user activities that could signal a security breach or result in compliance gaps. It helps security teams detect and respond to potential threats in real time through intelligent alerting of unauthorized access and changes to critical files, systems and applications.

NetIQ Change Guardian integrates seamlessly with your existing security information and event management (SIEM) solution to extend its ability to detect and respond to threats. The solution provides enriched detail that pinpoints the *who*, *what*, *when* and *where* of an event, significantly reducing the risk of a targeted attack.

Used in conjunction with NetlQ Secure Configuration Manager<sup>™</sup> for compliance and entitlement reporting and NetlQ Sentinel<sup>™</sup> for security event management, log aggregation, and forensic analysis, NetlQ Change Guardian is an important component of a powerful, integrated and automated solution for security and compliance management.

#### Capabilities

To combat an increasingly sophisticated threat landscape and complex computing environment driven by such technologies as BYOD, mobility and cloud, organizations must take a layered and integrated approach to defending their critical systems and sensitive data. NetIQ Change Guardian products provide the following essential protection measures:

 Privileged-user monitoring – audits and monitors the activities of privileged users

# $\bigcirc$

**SOLUTION** Security Management

**PRODUCT** NetlQ® Change Guardian™

NetlQ Change Guardian delivers the right information at the right time to the right stakeholder – to help identify and mitigate security threats and protect corporate assets.



Organizations face increased information security risks when privileged users make unauthorized changes to critical files, systems and applications. NetlQ Change Guardian helps IT security professionals manage file and system integrity to protect sensitive data and ensure compliance with regulations and internal security policies. to reduce the risk of insider attacks.

- **Real-time change monitoring** identifies and reports on changes to critical files, platforms and systems to help prevent breaches and ensure policy compliance.
- **Real-time intelligent alerting** provides immediate visibility to unauthorized changes that could lead to a breach, enabling the fastest threat response.
- Compliance and best practices
  attainment helps satisfy compliance
  mandates by demonstrating the ability to
  monitor access to critical files and data.

#### **Features and Benefits**

Beyond simply identifying changes, NetlQ Change Guardian provides the forensic reporting you need to make intelligent security decisions that will effectively limit the risk of corporate data loss.

#### Key features and benefits:

- Provides a detailed audit trail of privilegeduser activity across your Microsoft Windows and Active Directory, UNIX and Linux environments
- Has the ability to specify monitoring policies in familiar, everyday language, making it easy for your security teams to associate NetlQ Change Guardian

policies with technical controls required by multiple regulations, mandates and internal policies

- Provides enhanced security event detail that pinpoints the *who*, *what*, *when*, *where* and authorization status of a change or activity, including before- and after- details of the change
- Identifies managed versus unmanaged changes, with real-time alerting on unauthorized changes
- Identifies changes in key file systems to help meet compliance requirements for file integrity monitoring
- Integrates seamlessly with all major SIEM solutions, including NetIQ Sentinel, enabling event correlation and significantly reducing the risk of an undetected breach
- Delivers the reporting tools necessary to clearly demonstrate compliance to internal and external auditors

#### **Key Differentiators**

• **Comprehensive, integrated approach** to monitoring privileged-user activity helps protect your growing enterprise from attack. Because dynamic, mixed IT environments typically do not allow for a holistic view of risk and compliance, you need a comprehensive security

	ardian	
File integrity w	as changed	
	epity changed by 'ad-administrator' with outco	me Surress.
	and a subject of an and a subject of the subject of	
UNIO CHEW	and and	
E User	a dramati alter	
- Application	adutopia webg.com C. Vilindewsis.com/329VC1EPHC/EDIE	
	C ANDREAD FORMATION OF A CAR	
and a second second	e	
Contigener	C COAge Confu Files	
Oterct	topenet conto	
- Copera	of an end of the second	
	Turnetin 2010/Wards 26 10 44 24 URD-5	
Event Seve	Tuesday, 2012/18/09/29 10 44/24 0/10/5	
Contract of Contra	and the second second	
7 most	6/5-#2008/10/21 117 128/	
T Patient	adultiplainelig.com Othersould //imdees Server 2008 R2 Enterprise I	the state of the s
a Observer	Change Guardian for Windows	Longe Denke Pace 1 (part 1001), the de
	Unange countrale for conditives	
CLASSINGATION.	And the Annual Prove	
5 Policy	CiGree Contry Free	
E Activity E Outcome	Ormanaged Suzzens	
- Severity	5	
CONTEXT ACTINUMES		
CARLOOM		
Rok Domain	operational continuity	
CARLOOM		
Carloone Rok Domain Rok	operational continuity	-
Rok Domain	operational continuity	Minist and Sources
CARLORN Risk Domain Risk	operational continuity	Bing and Second
Colfocers Risk Duman Risk DILTA Cr\COllege Costlug 7	operational continuity sign	
CARLORD Rok Domain Rok Citta C	operational continuity stigh Lider\Suptort.conflig source	witter
Colfocers Risk Duman Risk DILTA Cr\COllege Costlug 7	operational continuity sign	
CARLOOK Rok Doman Rok Cittle Cittle Cittle Deloffie	operational continuity stigh Lider\Suptort.conflig source	witter
CARLORD Rok Domain Rok Citta C	operational continuity stigh Lider\Suptort.conflig source	witter
CATLORY Rea Densan Rak DILL. C:\/Capp Costly P Krissoft Did offic Costly() APTORISCI	operational continuity stigh Lider\Suptort.conflig source	NYTER
Categorie Reak Domain Reak DELSA C:\COLUMN Category of Armemetr Dec of the Contrast percension Contrast percension 2 = stoghtere	opendenst outlandy style Liter/Lapitest, next/lip strone fibi EXPCME	NTON 1520 AFTER Ubgsheets
CATLORY Real Donain Real DISA. Crivelage castra P Announty Ded in the Contrast personnect 2 stophens 1 st. Configure large	opendenst outlandy style Liter/Lapitest, next/lip strone fibi EXPCME	NYTER 1580 AFTER skaplant af-Configure Inging
CATEGORY Reak Domain Reak DELSA. CriteCology Countrie P Arramenty Del of the Control Definition CC Control Definition CC Control Def	operational continuity stags LEAR's Lapitant, manifest title table	NTER 1520 AFER Visplano «- Configure leging = accor
CARLODER Reak Domain Reak DELS. C:\COLOGY Custory F Creating Custory F CONTENT PRESENCE CONTENT PRESENCE Standards Standards	operational continuity stage Line (Lapitant, contra) tilat tilat tilat tilat tilat tilat tilat tilat	NYTER 1580 AFTER 158pSant 14_Configure logging = Nextor Nexton
CATEGORY Real Contain Real DELS. C:\Clags Control P Control Control P Control Control P Control Contro	operational continuity stags LEAR's Lapitant, manifest title table	NYTH 1920 AFTER Noglaws 4°- Carligate Staging - A Notes Market Audio-Tala" Ja
CARLODER Reak Contain Reak DELSA. C:\CORep Coastrap F Creation CONTINUE (INTERNOCE Deal of the CONTINUE (INTERNOCE CONTINUE (INTERNOCE CONTINUE (INTERNOCE) CONTINUE (INTERNOCE)	operational continuity stage Line (Lapitant, contra) tilat tilat tilat tilat tilat tilat tilat tilat	NYTER 1580 AFTER 158pSant 14_Configure logging = Nextor Nexton

NetIQ Change Guardian delivers intelligent alerts that answer key security and audit questions clearly and simply, enabling the fastest response to threats.

NetlQ Change Guardian enables early identification and disruption of security breaches through real-time detection of unauthorized changes and access to critical files, systems and applications.

solution that helps detect and respond to unauthorized change, activity and access. NetIQ Change Guardian simplifies security and compliance processes by eliminating the need to manage multiple tools across disparate systems. It centralizes security information, which allows organizations to extend their existing ability to manage risk, and prevent and respond to business disruption. NetIQ Change Guardian supports heterogeneous environments consisting of multiple servers, operating systems, devices and applications, including Microsoft Windows, Active Directory, UNIX and Linux.

#### • Extends the capabilities of SIEM to

close the security intelligence gap. SIEM solutions do not provide the security event detail required to detect an insider or targeted attack nor the level of file integrity change reporting that some compliance mandates demand. When integrated with SIEM solutions such as NetIQ Sentinel, NetlQ Change Guardian works to enrich the "actionable intelligence" provided by the SIEM solution with the security event detail you need to identify and react quickly to threats. Armed with this comprehensive security intelligence, you will be better able to mitigate the impact of an attack before serious damage or compliance gaps can occur.



To learn more about NetlQ Change Guardian, or to start a trial, go to www.netiq.com/cg.

- Intelligent alerting helps reduce risk from insider and targeted attacks due to the misuse of privileged access. NetlQ Change Guardian helps you to detect and respond to potential threats in real time through intelligent alerting of unauthorized access and changes to critical files, systems and applications. The alerts contain enriched security information with the detail necessary to identify threats and record change. They include specifics such as who performed the action, what action was performed, when the action was taken, and where the action was taken. They also indicate whether or not the action was authorized, and include before-and-after details of the change.
- Policy-based monitoring helps you to demonstrate compliance simply and at lower cost. NetIQ Change Guardian helps you to demonstrate compliance with various regulations, mandates, best practices and internal policies through policy-based change auditing and monitoring. The solution provides the ability to specify monitoring policies in familiar, everyday language. This makes it easy for you to associate NetlQ Change Guardian policies with technical controls, simplifying meaning and intent. NetIQ Change Guardian presents activity in straightforward and simple terms, diminishing the effort required for audit preparedness and proof of compliance.

#### Worldwide Headquarters

1233 West Loop South, Suite 810 Houston, Texas 77027 USA Worldwide: +1 713.548.1700 U.S. / Canada Toll Free: 888.323.6768 info@netiq.com www.netiq.com http://community.netiq.com For a complete list of our offices in North America, Europe, the Middle East, Africa, Asia-Pacific and Latin America, please visit



www.netiq.com/contacts.

NetIQ, the NetIQ logo, Change Guardian, Secure Configuration Manager and Sentinel are trademarks or registered trademarks of NetIQ Corporation in the USA. All other company and product names may be trademarks of their respective companies.