Change Guardian

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

Change Guardian at a Glance

Privileged-User Monitoring

Audits and monitors the activities of privileged users 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.

Hybrid Cloud Monitoring

Monitors AWS, Microsoft AzureAD, and Office 365 for user activities with intelligent context details.

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.

Change Guardian 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

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.

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 NetIQ Secure Configuration Manager for compliance and entitlement reporting and NetIQ Sentinel Enterprise for security event management, log aggregation, and forensic analysis, 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 defend their critical systems and sensitive data. Change Guardian products provide the following essential protection measures:

- Privileged-user monitoring—audits and monitors the activities of privileged users 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, 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 privileged user 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 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 Sentinel Enterprise, 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

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.

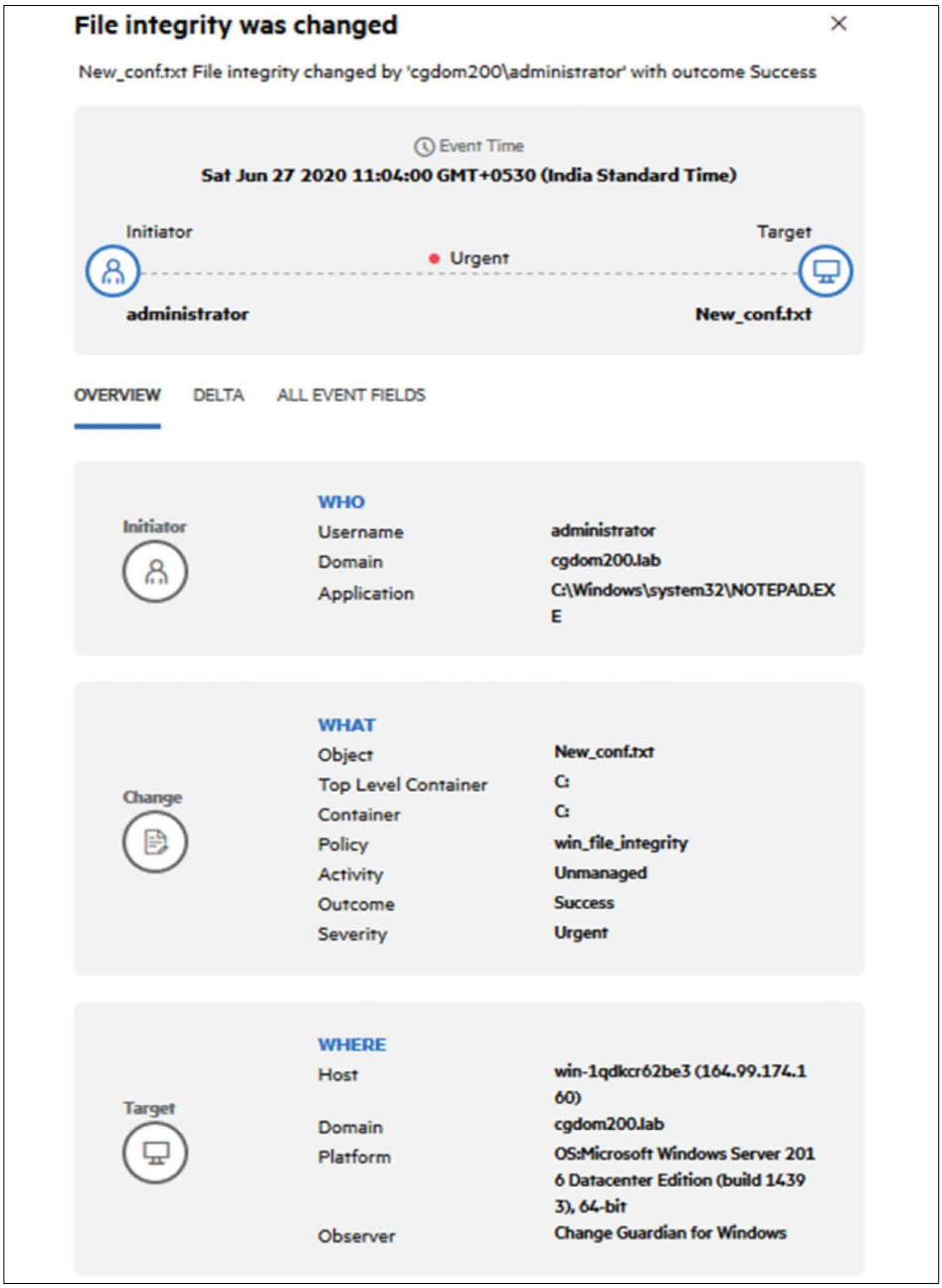

Figure 1. Change Guardian 6.0 provides a centralized view of hybrid cloud environment for changes and tracking user activities.

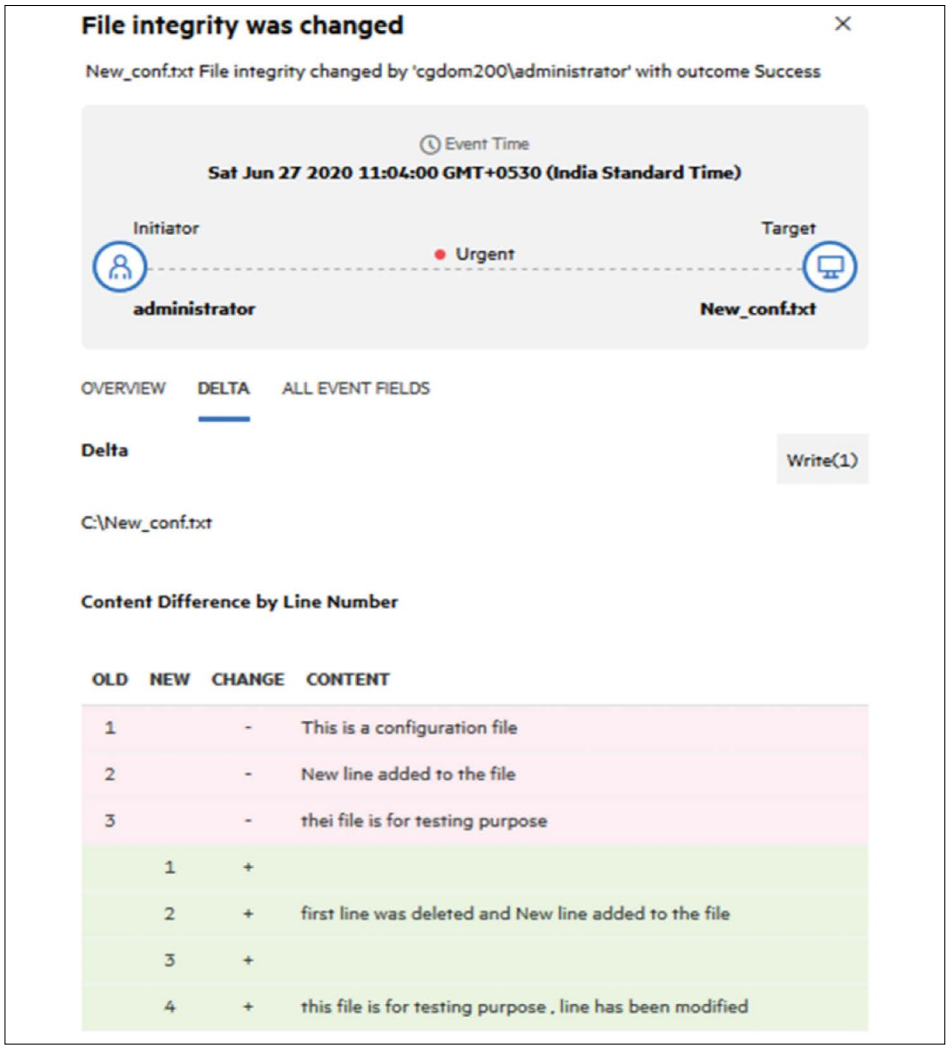

Figure 2. Change Guardian 6.0 provides the who, what, when, where and authorization status of a change or activity, including before-and after-details of the change.

Key Differentiators

- Hybrid Cloud Monitoring: Public cloud monitoring across AWS and Hybrid AzureAD and Office 365 for user activities with intelligent details around event context. Detect configuration change and monitor specialized events for identifying inside/outside attacks. Utilize preloaded templates for easy use based on industry use cases to get a faster time to deployment. Detect configuration change and unauthorized user activities across exchange online and exchange on premises.
- 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 solution that helps detect and respond to unauthorized change, activity, and access. 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. Change Guardian supports heterogeneous environments consisting of multiple servers, operating systems, devices, and applications, including Microsoft Windows, Hybrid AzureAD, Office 365, AWS, 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 ArcSight, Sentinel Enterprise, and Splunk, 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.
- Intelligent alerting helps reduce risk from insider and targeted attacks due to the misuse of privileged access. Change Guardian helps you to detect and respond to potential threats in real time through intelligent alerting of

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

Contact us at **CyberRes.com**
Like what you read? Share it.

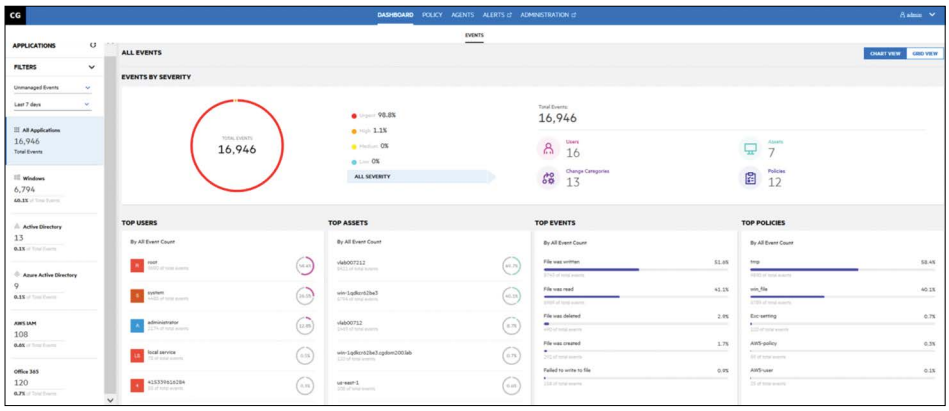

Figure 3. Change Guardian delivers intelligent alerts that answer key security and audit questions clearly and simply, enabling the fastest response to threats.

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. 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 Change Guardian policies with technical controls, simplifying meaning and intent. Change Guardian presents activity in straightforward and simple terms, diminishing the effort required for audit preparedness and proof of compliance.
- **Agent Health:** Ease day to day management by leveraging the available agent health dashboard. Change Guardian administrators the ability to check and monitor the health of its own components through a centralized dashboard, which provides visibility and an ability to diagnose issues of non-functional agents due to potential misconfiguration. Maintaining agent health helps you understand if all agents are reporting directly to Change Guardian and are monitoring the target system as expected. You can also keep track of how many agents are deployed, where they are distributed, to ensure availability and reporting changes as they take place.
- **Compliance on-demand:** Automated administration and management to help ensure the organization is adhering to regulatory requirements that mandate your organization. Change Guardian provides meaningful information, which is enriched with who, what when, where, and delta, to the security team to reduce the time and complexity of responding to suspicious activity. With this clarity of information, you have immediate visibility into changes that could lead to a breach or compliance gap. IT organizations can easily leverage these details on the infrastructure coverage for compliance and auditing purpose.

To learn more about Change Guardian, or to start a trial, go here.

CyberRes
A Micro Focus line of business