Solution Flyer
Security

File Integrity Monitoring and Beyond

Protecting critical systems and data from unauthorized access and change by privileged users

- **Business Challenge**

  Enterprises face increased organizational risk when privileged users make unauthorized changes to critical files and systems.

- **Solution Benefits:**

  Our file integrity monitoring solution helps you:

  - Achieve compliance with regulatory and privacy standards such as PCI DSS.
  - Integrate real-time, intelligent alerting with SIEM solutions to close the security intelligence gap.
  - Monitor activities of privileged users to detect and disrupt potential threats.
  - Detect changes on critical files, systems and applications more rapidly.

Introduction

Your organization must address the risks of unauthorized privileged-user activity if you are to protect sensitive information and critical systems. Detecting unauthorized access and changes is a difficult task requiring a security solution that provides real-time detection and alerting of changes to critical assets that could signal a security breach or compliance gap.

File integrity monitoring, as part of a broader security program, helps reduce specific risks of:

- **Data Breach**—Especially from misuse of privileged access
- **System Availability**—Caused by unplanned or unauthorized changes to files, systems and applications
- **Compliance Failure**—Resulting from an inability to demonstrate oversight of access and changes to sensitive data

Solving the Problem

For business-critical systems and data files, the best approach to solving the problem of unauthorized access and change by privileged users will include real-time alerting:

- Integrate alerting into a security information and event management (SIEM) system
- Provide highly detailed security information immediately
- Monitor the activities of privileged users

In addition, the solution should meet the requirements of compliance mandates that specifically call out file integrity monitoring solutions, and detect changes on your most important platforms.

The Micro Focus Approach

The Micro Focus® file integrity monitoring solution helps IT security professionals detect and respond to potential threats in real time through intelligent alerting of unauthorized access and changes to critical files, systems and applications.

Our real-time file integrity monitoring approach

- Monitors the activities of privileged users
- Provides real-time, intelligent alerting of unauthorized access and changes to critical files, systems and applications
- Ensures intelligent alerts deliver highly detailed security information such as when the change was made, who made the change, what was changed, where the change was made, and whether the change was authorized
- Integrates intelligent alerting into leading SIEM solutions to enable faster reaction to potential threats
- Helps achieve compliance by demonstrating the ability to monitor access and changes to sensitive data
- Detects changes on your most important platforms, including Microsoft Windows and Active Directory, UNIX and Linux

Security information is presented simply and clearly, eliminating the need for expertise in various event types and reducing the time and complexity of responding to suspicious activity. With support for heterogeneous IT environments, our solution works to simplify and centralize response to threats from across the enterprise, helping teams to quickly identify threats and respond aggressively.

Additionally, our file integrity monitoring solution works to enrich the "actionable intelligence" provided by your SIEM solution with the security event detail needed to detect and disrupt threats. SIEM by itself is limited by its dependence on native logs, which give little insight

For more information on file integrity monitoring, visit www.microfocus.com or call your local representative or partner.

Contact us at:
www.microfocus.com

Like what you read? Share it.

into the who, what, when, and where of an event. Our file integrity monitoring solution provides the enriched security information detail teams need to detect the signs of an insider or targeted attack.

Beyond File Integrity Monitoring

Beyond file integrity monitoring is the broader problem of system integrity monitoring. While it is essential to identify unauthorized access and changes to files, such monitoring must be part of a broader security and compliance management program.

Our approach to file integrity monitoring includes tight integration with SIEM solutions to present correlated, rich and relevant information to security and compliance teams. When further combined with identity management solutions, the complete solution becomes identity-aware, infused with real-time identity information that can provide additional context around user access privileges instantly, accurately, and throughout the organization. You are then able to have a complete security intelligence picture, one that enables you to more rapidly identify and respond to privileged-user activity that could be a precursor to a security breach or compliance gap.

Products

- **Micro Focus Change Guardian** provides real-time, intelligent alerting to SIEM solutions of access, changes and privileged-user activity across multiple servers, operating systems, devices and applications, including Microsoft Windows, Active Directory, UNIX and Linux.
- **NetIQ Sentinel™ Enterprise** presents a single, central location for security event management, log aggregation and forensic analysis.
- **NetIQ Identity Manager** lets you standardize user management and allows you to create a single, rich identity store for your organization.