Change Auditor Threat Detection

Proactive user threat detection for Microsoft environments

The vast majority of organizations rely on Active Directory (AD) as their primary source for authentication and authorization making it a prime target for hackers, cyberterrorists and disgruntled ex-employees. Organizations may not realize, though, that a more immediate threat to their AD security is actually insiders acting either knowingly or unwittingly. Worse yet, AD's complex nature makes it incredibly difficult to identify threats when they occur. And traditional rule-based approaches to user threat detection generate so many alerts that you can't possibly investigate them all; you risk missing the real threats altogether, leaving your organization at risk of a data security breach. So how do you analyze all the user activity occurring in your environment in real time to protect your business from disruptions and outages?

Change Auditor Threat Detection offers a unique approach to user threat detection by modeling individual user behavior patterns to detect anomalous activity that might indicate suspicious users or compromised accounts. By analyzing user activity, using proprietary advanced learning technology, user and entity behavior analytics (UEBA), and sophisticated, scoring algorithms, Change Auditor Threat Detection ranks the highest risk users in your organization, identifies potential user threats and reduces the noise from false positive alerts. You'll finally be able to overcome the gaps left behind by native auditing tools so you can keep your environment secure.

FEATURES

Real-time audit log analysis

Efficiently analyze a high volume of audit data in real-time, including AD changes, authentications and file activity. Build user baselines from these raw activity events and proactively detect when users' behavior appears anomalous so you're immediately aware of potential suspicious activity.

Change Auditor Threat Detection helps you quickly and easily detect suspicious user activity to keep your environment and users secure.

BENEFITS:

- Proactively detect threats based on user behavior patterns
- Cut down on the mountain of alerts associated with rule-based threat detection
- View security alerts in context to quickly and easily determine their severity
- Easily detect when a user acts in an abnormal way with user behavior baselines
- Identify threats based on your existing audit data to minimize impact on your infrastructure

USE CASES:

Change Auditor Threat Detection enables you to quickly and easily discover threats including:

- Abnormal AD activity
- Misuse of privileged accounts
- Brute force attacks
- Data exfiltration
- Inappropriate system or resource access
- Malware
- Privilege elevation
- Lateral movement

SYSTEM REQUIREMENTS

CHANGE AUDITOR COORDINATOR

(Server-side component)

Processor: Quad core Intel Core i7 equivalent or better

Memory: Minimum: 8 GB RAM or better Recommended: 32 GB RAM or better

CHANGE AUDITOR CLIENT

(Client-side component)

Processor: Dual core Intel Core i5 equivalent or better

Memory: Minimum: 4 GB RAM or better Recommended: 8 GB RAM or better

CHANGE AUDITOR AGENT

(Server-side component)

Processor: Dual core Intel Core i5 equivalent or better

Memory: Minimum: 4 GB RAM or better Recommended: 8 GB RAM or better

For a detailed and current list of system requirements, please visit support.quest.com/change-auditor

Automated user behavior analytics (UEBA)

Model user activity patterns without any administrator input or configuration required. User behavior baselines are automatically created using unsupervised advanced machine learning, modeling every aspect of a user's activity, including their logon patterns, administrative activity and file and folder access.

Sophisticated behavioral anomaly detection

Identify abnormal user activity by automatically comparing every user action against that user's behavioral baseline. Sophisticated threat indicator detection and multi-level risk scoring ensure that only the most egregious anomalies are highlighted, representing the riskiest user behaviors.

Pattern-based user threat detection

SMART user threat alerts are only raised when a correlated pattern of anomalous user behavior is detected. Rather than rely on rules to detect specific activities, automatically analyze all user activity as it happens and identify the most suspicious users in the environment through sophisticated user behavior pattern detection. Sophisticated global modeling ensures that only the most critical and concerning patterns of user behavior are highlighted, significantly reducing the noise caused by isolated activities and false positives.

High-fidelity user analytics

Change Auditor creates the audit logs feeding the analytics, so all of the raw event data being used to proactively detect threats in your environment inherently includes valuable information like:

- Who made the change
- What was changed
- When was it changed
- Where was it changed
- And the IP address or workstation where the change originated

Unlike native Windows event logs, Change Auditor ensures no important user actions are missed which could otherwise create critical gaps in the user behavior analytics.

Security alerts in context

View all suspicious user activity alerts in the context of the threat indicators that were discovered as part of the alert. Every behavioral anomaly is presented in the context of the user's baseline activity and with all of the raw events that triggered the alert, clearly indicating why the alert was raised and simplifying the investigation and follow-up.

Lightweight user threat detection

Leverage your existing Change Auditor infrastructure and audit data to model user behavior so there's no need to deploy unnecessarily unwieldy additional agents and servers. A single virtual appliance is the only additional infrastructure required to enable advanced user threat analytics.

ABOUT QUEST

At Quest, our purpose is to solve complex problems with simple solutions. We accomplish this with a philosophy focused on great products, great service and an overall goal of being simple to do business with. Our vision is to deliver technology that eliminates the need to choose between efficiency and effectiveness, which means you and your organization can spend less time on IT administration and more time on business innovation.

Quest
4 Polaris Way, Aliso Viejo, CA 92656 | www.quest.com
If you are located outside North America, you can find local office information on our Web site.

DataSheet-ChangeAuditorThreatDetection-US-KS-32855