

# OpenText Change Guardian

Überwachen Sie die Aktivitäten privilegierter Benutzer, und erkennen Sie in Echtzeit unerlaubte Änderungen an kritischen Systemen, um Sicherheitsverletzungen zu verhindern und die Einhaltung sicherzustellen.



## Vorteile

- Schnelles Erkennen von Bedrohungen, um Risiken und die Auswirkungen von Sicherheitsverstößen zu verringern
- Überwachen der Aktivitäten von privilegierten Benutzern in Echtzeit
- Schnelles Identifizieren eines unbefugten Zugriffs und von Änderungen an kritischen Assets

IT-Sicherheitsteams stehen vor wachsenden Herausforderungen beim Erkennen von unbefugten Zugriffen und Änderungen an kritischen Systemen und Anwendungen, bevor sie zu Sicherheitsverletzungen führen. Ohne Sichtbarkeit in Echtzeit bleiben Bedrohungen unbemerkt, was zu erhöhten Risiken und Konformitätslücken führt. OpenText Change Guardian unterstützt Sicherheits- und IT-Betriebsteams bei der proaktiven Überwachung und Reaktion auf verdächtige Aktivitäten in ihren Umgebungen.

## Erkennung von Bedrohungen in Echtzeit

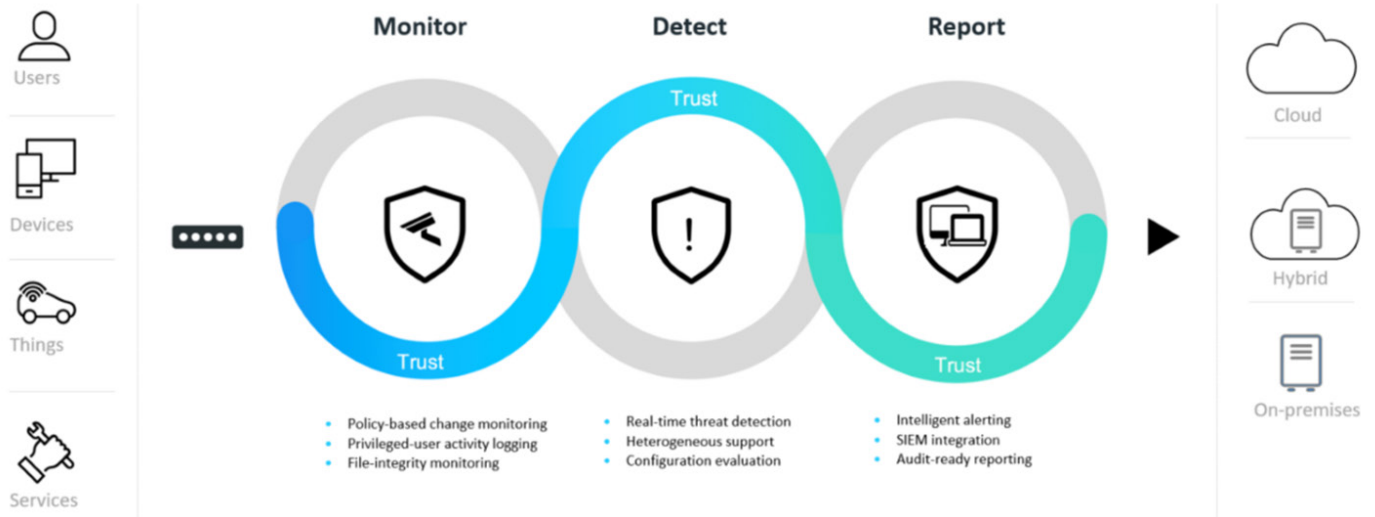
Identifizieren Sie unbefugten Zugriff und Änderungen über kritische Systeme, Dateien und Anwendungen hinweg sofort, um zügig auf potenzielle Bedrohungen zu reagieren und das Risiko von Datenschutzverletzungen zu minimieren.

## Detaillierte Sicherheitseinblicke

Erhalten Sie bei jeder Warnung umfassende Informationen, einschließlich der Person, die die Aktion ausgeführt hat, welche Änderungen vorgenommen wurden, wann sie vorgenommen wurden und wo sie stattgefunden haben. So stellen Sie sicher, dass die IT-Teams über den erforderlichen Kontext verfügen, um die Maßnahme zu beurteilen und angemessen zu reagieren.

## Verbesserte Konformität und Revision

Vereinfachen Sie den Prüfprozess, indem Sie Vorher-Nachher-Details zu Änderungen bereitstellen und angeben, ob Aktionen autorisiert wurden, um die Einhaltung verschiedener Vorschriften und interner Richtlinien zu optimieren.



## Optimierte Vorfallsreaktion

Ermöglichen Sie eine effektivere Vorfallsreaktion mit umsetzbaren Warnungen, die kritische Änderungen und potenzielle Bedrohungen hervorheben, sodass IT-Sicherheitsteams ihre Reaktionen priorisieren, Reaktionszeiten verkürzen und Vorfälle effektiver verwalten können.

## Schlussfolgerungen

OpenText Change Guardian bietet Sichtbarkeit in Echtzeit, um Bedrohungen zu erkennen und darauf zu reagieren. So werden Vorfallsreaktion, Revision und Konformität verbessert. Es kann in SIEM-Lösungen wie OpenText Core Behavioral Signals und Splunk integriert werden, um eine nahtlose Korrelation mit Bedrohungsinformationen zu gewährleisten und so die Erkennung und Reaktionszeiten zu verbessern. Es bietet eine beispiellose Kontrolle über privilegierte Benutzeraktivitäten und kritische Systemänderungen, ohne die Komplexität zu erhöhen.

Produktmerkmale	Beschreibung
<b>Richtlinienbasierte Überwachung von Änderungen</b>	Erkennung und Meldung nicht autorisierter Änderungen an kritischen Dateien und Systemen, um Sicherheitsverstößen entgegenwirken und die Einhaltung von Richtlinien gewährleisten zu können.
<b>Protokollierung der Aktivität privilegierter Benutzer</b>	Überwacht privilegierte Benutzer, um nicht autorisierte Änderungen und Zugriffe zu erkennen, schädliche Aktivitäten zu verhindern und verwaltete von nicht verwalteten Änderungen zu unterscheiden.
<b>Überwachung der Dateiintegrität</b>	Identifiziert und warnt bei Änderungen an kritischen Dateien und Systemen, hilft bei der Erfüllung gesetzlicher Anforderungen und sorgt für die Sicherheit von Revisionslisten.
<b>Erkennung von Bedrohungen in Echtzeit</b>	Erkennt und meldet schnell nicht autorisierte Änderungen und gibt der IT-Abteilung Zeit, um Verstöße zu untersuchen und zu verhindern.

Produktmerkmale	Beschreibung
<b>Heterogene Unterstützung</b>	Erkennt unerlaubte Änderungen an verschiedenen Servern, Betriebssystemen und Apps, einschließlich Windows®, Active Directory®, Azure Active Directory™, Office 365®, Amazon Web Services® IAM, UNIX®, Linux, NetApp® und EMC®.
<b>Konfigurationsbewertung</b>	Überwacht Konfigurationsänderungen im Laufe der Zeit, um die Konformitätsanforderungen für die Dateiintegrität zu erfüllen.
<b>Intelligente Warnmeldungen</b>	Bietet sofortige Warnungen bei nicht autorisierten Änderungen, um eine schnelle Reaktion auf Bedrohungen mit detaillierten Ereignisinformationen zu ermöglichen.
<b>Audit-fähige Berichte</b>	Bietet detaillierte Protokolle und anpassbare Berichte zu Aktivitäten von privilegierten Benutzern, um Konformität und Revision zu vereinfachen.