OpenText Change Guardian

Monitor privileged user activities and detect unauthorized changes in real time across critical systems to prevent security breaches and ensure compliance

Benefits

- Detect threats fast to reduce risk and breach impact
- Monitor privileged-user activities in real time
- Swiftly identify unauthorized access and changes across critical assets

IT security teams face growing challenges in detecting unauthorized access and changes to critical systems and applications before they lead to breaches. Without real-time visibility, threats go unnoticed, increasing risk and compliance gaps. OpenText™ Change Guardian helps security and IT operations teams proactively monitor and respond to suspicious activity across their environments.

Real-time threat detection

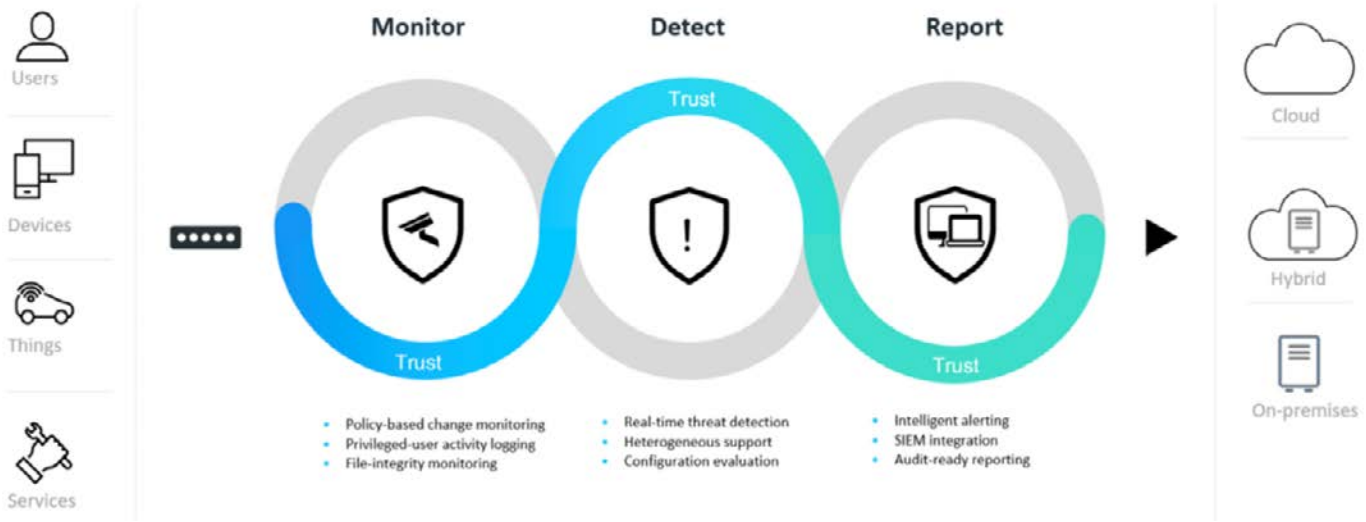
Swiftly identify unauthorized access and changes across critical systems, files, and applications, enabling rapid response to potential threats and minimizing the risk of data breaches.

Detailed security insights

Receive comprehensive information with each alert, including who performed the action, what changes were made, when they occurred, and where they took place, ensuring IT teams have the necessary context to assess and respond appropriately.

Enhanced compliance and auditing

Simplify the auditing process by providing before-and-after details of changes and indicating whether actions were authorized, streamlining compliance with various regulations and internal policies.



Streamlined incident response

Facilitate more effective incident response with actionable alerts that highlight critical changes and potential threats, enabling IT security teams to prioritize their responses, reduce response times, and manage incidents more effectively.

Conclusion

OpenText Change Guardian provides real-time visibility to detect and respond to threats, enhancing incident response, auditing, and compliance. It integrates with SIEM solutions, such as OpenText Core Behavioral Signals and Splunk for seamless threat intelligence correlation, improving detection and response times. It offers unmatched control over privileged-user activity and critical system changes without adding complexity.

Product features	Description
Policy-based change monitoring	Tracks and reports unauthorized changes to critical files and systems, helping prevent breaches and ensure compliance.
Privileged-user activity logging	Monitors privileged users to detect unauthorized changes and access, deterring malicious activity and distinguishing managed from unmanaged changes.
File-integrity monitoring	Identifies and alerts on changes to critical files and systems, helping meet regulatory requirements and keeping audit trails secure.
Real-time threat detection	Quickly identifies and reports unauthorized changes, giving IT time to investigate and prevent breaches.

Product features	Description
Heterogeneous support	- Detects unauthorized changes across various servers, operating systems, and apps, including Windows®, Active Directory®, Azure Active Directory™, Office 365®, Amazon Web Services® IAM, UNIX®, Linux, NetApp®, and EMC®.
Configuration evaluation	Monitors configuration changes over time to help meet compliance requirements for file integrity.
Intelligent alerting	Provides immediate alerts on unauthorized changes, enabling quick threat response with detailed event information.
Audit-ready reporting	Offers detailed logs and customizable reports of privileged-user activity to simplify compliance and auditing.

Copyright © 2025 Open Text • 02.25 | 260-000385-001