Wertheim Global Solutions, LLC

Guardian for OpenText Content Server

Guardian for Content Server is a data loss prevention (DLP) compliance solution for OpenText Content Server. Guardian helps minimize internal risks by enabling you to detect, investigate, and act on malicious activities in your organization. Guardian rules allow you to define the types of risks to identify and detect in your organization (such as download, email, copy, etc.), including the action the rule should take (notification and/or account disabling) when a rule is violated. Management can then quickly take any further appropriate actions necessary to make sure users' actions adhere to your organization's compliance standards.

Pain points and mitigation

Managing and minimizing risk in your organization starts with understanding the types of risks you may encounter. Internal risks, which are often overlooked, are driven by user activities, which can be detected and restrained by Guardian. The effects of a successful Phishing attack can also be minimized by using Guardian, by disabling an account that has been compromised.

There are numerous negative consequences that can result from these illegal, inappropriate, unauthorized, or unethical behaviors by users *within* your organization, or those who steal their credentials. These consequences include:

- Leaks of sensitive data
- Confidentiality violations
- Intellectual property (IP) theft
- Fraud
- Insider trading
- Regulatory compliance violations

Users typically have access to create, manage, and share data stored in a Content Server repository. In most cases, organizations have limited resources and tools to identify and mitigate internal risks to this information.

There are already many solutions available to prevent unauthorized groups or individuals from attacking your systems. But what can you do to stop an authorized person from stealing your information?

When a user decides that he or she wants to engage in malicious or illegal behavior, it is crucial for an organization to identify it and stop it while it is occurring. Too many times we hear about individuals stealing documents and making them public, while the victim didn't even know the theft occurred until they read about it in the news.

Too often, phishing attacks are successful in obtaining a legitimate user's credentials, and those credentials are then used to obtain confidential information.

Guardian monitors the activities of end-users to help you quickly identify, triage, and act on suspicious activity. By using a Predictive Analysis engine, Guardian allows you to easily define specific rules to identify these at-risk activities. These rules allow you to identify when the suspicious activities are discovered, and by whom, and to act to mitigate these risks.

Identifying potential risks with Predictive Analysis

Guardian evaluates user activities in real time, meaning that it responds to rule violations as they occur. Rule violations occur when the volume of an activity, such as download, exceeds a user's typical quantity of that activity by a certain percentage. For instance, if a user typically downloads a dozen documents a week but suddenly downloads a hundred in a day, Guardian can send a notification to his supervisor. This eliminates the need to know the volumes of activities each user typically performs, simplifying implementation.

Rule Levels

A rule can have multiple levels of actions to take. For instance, if a user exceeds activity threshold by 100%, a notification can be triggered to his manager; at 200%, notify the security department; and at 300%, disable his account pending review of the user activity. These multiple levels allow you to monitor a user at lower levels without disrupting his workflow, and can mitigate the potential damage if the user downloads these documents off-hours (such as in the middle of the night).

Rule Types

A rule can be established at either the library level (all users), group level, or individual user level. For instance, you may wish to set a delete rule for all users, a download rule for a specific group, and a view rule for a specific user.

Rule Definition

A rule can be set that includes multiple activities and for multiple users and/or groups; again, this simplifies implementation.

Alert Notifications

Alert Notifications are generated by rule violations and are sent by email, SMS text, or both. Multiple people and distribution groups can receive these notifications. Notifications include the following information:

- User
- Time detected
- Items that triggered the notification
- Status

Disabling/Enabling

When a rule violation triggers a Disable action, the user's connection to the Content Server repository is immediately broken, preventing the user from accessing any more information stored in its repository. A notification is also sent to the appropriate recipients, but not to the user. Management can then go to the Guardian Dashboard to review more details of the user's activities, further investigate the reason for the account being disabled, and, if appropriate, re-enable the user's account.

Exceptions

When a user is about to begin a project that may cause a rule to be violated, such as an eDiscovery project, you can simply use the Guardian Dashboard to temporarily suspend the rule for that user and set an end date for that project. When the project is concluded, the rule can then be re-enabled either automatically based upon that end-date, or manually via the Guardian Dashboard.

Common Scenarios

Some of the common scenarios that can be addressed using Guardian include:

- Theft by departing users

- Leak of sensitive or confidential information
- Intentional policy violations
- Phishing attacks that lead to unauthorized access to Content Server information

Next Steps

Ready to start using Guardian for OpenText Content Server? We are here to help! If you are working with an OpenText SolEx partner, they are here to help too! Contact either of us today to begin protecting your organization before it's too late.

Portions of the text in this document are based upon the following web page: https://docs.microsoft.com/en-us/microsoft-365/compliance/insider-risk-management?view=o365-worldwide