

# **EmpMonitor Rules Guide**

Version 1.2



# Table of Contents

## 1. About This Guide

## 2. Related Resources

## 3. Rules Overview

### 3.1. Common Use Cases

#### 3.1.1 Preventing Data Loss

#### 3.1.2 Detecting Insider Threats\

#### 3.1.3 Identifying Abusive Behavior and Accidental Threats

#### 3.1.4 Detecting Malicious Intent

#### 3.1.5 Improving Productivity and HR Management

#### 3.1.6 Conforming with Regulatory Compliance

## 4. Steps For Creating Rule

### 4.1 Why are You Creating the Rule?

### 4.2 What Activity, Content or Behavioral Anomaly You Want to Detect?

### 4.3 Where is the Activity Performed or Content Located?

### 4.4 When Should the Rule be Active?

### 4.5 Whom Should it Apply to?

### 4.6 What Makes the Data Sensitive?

### 4.7 What Scenarios Violate the Rule?

### 4.8 What Action(s) Do You Want to Take?

## 5. Understanding Common Rule Elements

### 5.1 Rule Name and Description

### 5.2 Tags

### 5.3 Schedule

### 5.4 Rules Condition

### 5.5 Rule Logic

#### 5.5.1 Condition Logic:

- Each value in a rule condition is considered as an 'OR' logic. In the above example, the rule will trigger if the 'Application Name' matches with 'regedit.exe' or 'pseditor.exe'.
- Each condition parameter is considered as an 'AND' logic. In the above example, the rule will trigger if the 'Application Name' and the 'Launch from CLI' parameters meets the condition.

- If you have multiple condition blocks, each new condition is considered as an 'OR' logic. In the above example, if either the Condition 1 or Condition 2 meets the criterion, the rule will be triggered.

You can see how the rule condition logics relate to each other on the Rule's Summary panel.

#### 5.5.2 Content Logic

#### 5.6 Risk Level

##### 5.6.1 Setting the Risk Levels in a Regular Rule

##### 5.6.2 Setting the Risk Level in an Anomaly Rule

#### 5.7 Rule Summary

## 6. Creating Regular Rules

### 6.1 Setting Up the Rule Basics

### 6.2 Selecting Rule Categories and Types

### 6.3 Defining Users

### 6.4 Defining Detection Criteria

#### 6.4.1 Agent Schedule Rules: What Schedule Violations Can You Detect?

##### Daily Work Time

Used to detect if there are any discrepancies in the employee's daily work time. You can detect if their work hour is less than or more than a specified hour(s).

Used to detect if the employee is working longer or shorter than scheduled.

Choose either IS SHORT BY or IS OVER BY and enter a minute value in the SPECIFY VALUE field.

##### Starts Early

#### 6.4.2 Activity Rules: What Activities Can You Detect?

If you choose the 'Any' file operation without any other criteria, EmpMonitor will trigger the rule for any file operations.

##### 6.4.2.4.1 Rule Examples

This criterion is not supported in Download and Upload operations.

##### RDP File Transfer

Detects if the file copy operation is done over an RDP (Remote Desktop Protocol) session. This happens when you connect to a remote computer and copy files to/from it.

You can select either YES or NO.

This criterion is only supported in the Copy operation.

##### Attachment Name

##### Bytes Sent

Used to specify the number of bytes sent over the network connection.

You can enter a byte value in the CONDITION field and use the '=', '>', or the '>=' logics.

Similarly, you can use the EXCEPT field to specify an exception.

#### Bytes Received

Used to specify the number of bytes received over the network connection.

You can enter a byte value in the CONDITION field and use the '=', '>', or the '>=' logics.

Similarly, you can use the EXCEPT field to specify an exception

### 6.4.3 Content Sharing Rules: What Contents Trigger the Rules?

#### 6.4.3.1 The Content Tab

#### 6.4.3.2 OCR

##### 6.4.3.2.1 Rule Examples

##### 6.4.3.2.2 Rule Criteria

#### 6.4.3.4 Files

##### 6.4.3.4.1 Rule Examples

##### 6.4.3.4.2 Rule Criteria

#### 6.4.3.5 Emails

##### 6.4.3.5.1 Rule Examples

##### 6.4.3.5.2 Rule Criteria

## 7. Creating Anomaly Rules

### 7.1 Rule Examples

### 7.2 Setting Up the Rule Basics

### 7.3 Detection Criteria - What Behavioral Anomalies Trigger the Rules?

## 8. Defining Rule Actions

### 8.1 Customizing the Rule Messages and Alerts

#### 8.1.1 Configuring the Alert Template

#### 8.1.2 Changing the Email Notification Settings

#### 8.1.3 Changing the Alert Wait Time

#### 8.1.4 Changing the Alert Log Limit

#### 8.1.5 Changing the Task Selection Timeout

## 9. Using the Prebuilt Rule-Templates

### 9.1.1 Using the Regular Rule Templates

### 9.1.2 Using Anomaly Rule Templates

## 10. Enforcing the Rules

### 10.1 Automatic Enforcement

### 10.2 Manual Enforcement

## **11. Investigating the Rule Violation Incidents**

11.1 Using the Alerts Report & the Alerts Log Widget

11.2 Using the Session Player

11.3 Using the Risk Report & the Risk Widget

## **12. Sample Rules Walkthrough**

12.1 Rule Sample 1: User logs in during off hours

12.1.1 Rule Summary

12.1.2 Setting up the Rule

12.1.3 Viewing the Rule Alerts

12.1.4 Viewing the Session Recording

12.2 Rule Sample 2: User sending emails with attachments to non-business address

12.2.1 Rule Summary

12.2.2 Setting up the Rule

12.2.3 Viewing the Rule Alerts

12.2.4 Viewing the Session Recording

12.3 Rule Sample 3: User attempting to upload a sensitive file to a cloud drive

12.3.1 Rule Summary

12.3.2 Setting up the Rule

12.3.3 Viewing the Rule Alerts

12.3.4 Viewing the Session Recording

12.4 Sample Rule 4: User attempting to share files containing sensitive content

12.4.1 Rule Summary

12.4.2 Setting up the Rule

12.4.3 Viewing the Rule Alerts

12.4.4 Viewing the Session Recording

12.5 Sample Rule 5: Employee productivity anomaly

12.5.1 Rule Summary

12.5.2 Setting up the Rule

12.5.3 Viewing the Rule Alerts

12.5.4 Viewing the Session Recording

## **13. Appendix**

13.1 List of Prebuilt Rule Templates

13.2 List of Prebuilt Anomaly Rule Templates

13.3 List of Pre-Defined Classified Data

# 1. About This Guide

In this guide, you will learn how to utilize EmpMonitor's behavioral-based rules to detect insider threats and protect your business from any malicious anomalies or accidental security incidents, avoid data breaches, prevent data loss and also help you with regulatory compliances. Here explained the rule structures, conditions, logic, data types, etc. It shows you the steps for creating rules, their use cases, best practices, and advanced capabilities.

It's specially designed to give configurational and processing knowledge about EmpMonitor to the Management, Administrators, and IT security personnel of your organization.

## 2. Related Resources

- **EmpMonitor User Guide**- shows you the detailed information about the EmpMonitor's user interface. You can also refer to it as a manual to use EmpMonitor on a day to day basis. To the relevant section, this Rule Guide contains context-sensitive links wherever needed.
- **EmpMonitor Resources Page**- contains info-resources(How to-), video tutorials, Product guide, Deployment Guide, and other resources, which might be helpful for you.
- **Guided Tour**- EmpMonitor interactive tour guide has over 100 use-cases. From this, you can learn how to utilize EmpMonitor features & capabilities. And see how some of the common rules work. Click on the link(:\_\_\_\_\_ ) to get access to the **Guided Tour**, showing you the detailed information about the EmpMonitor's rules and features.

### 3. Rules Overview

Behavioral rules are a core part of EmpMonitor's automated insider threat detection and data loss prevention capabilities. These features allow you to identify unproductive, harmful, or dangerous activity in realtime and optionally, act on your behalf to impede such threats. The Intelligent Rules Engine is thoroughly integrated into the EmpMonitor platform:

- The Rules Engine utilizes EmpMonitor's granular Activity Monitoring capabilities, like apps, websites, emails, etc. to decide what activity or content the rule should identify.
- It also uses the User Profiles to decide the rule should apply to whom.
- You can use the Configurations settings to supply additional inputs such as employee Schedule, Task Lists, Shared List, etc. with the Rules Editor to speedup the rule creation process and also to share parameters across different rules.
- The Monitoring Settings can be used to control when and how the rules should work, minimizing privacy concerns.
- You can see detailed reports on the rule violation incidents with the Alerts, Risk Report, Dashboard Widgets, Session Player, and the Notification Emails.
- EmpMonitor Agent implements the rules you create from the EmpMonitor Dashboard on the user's computer.

With hundreds of in-built rule templates, pre-defined data categories, and sample rules, you can get started with EmpMonitor right away. You can also create your own rules easily with an intuitive, visual Rules Editor. The editor allows you to apply a common language, regular expressions, shared list, and pre-built data classifications to determine what makes an activity or data sensitive and use simple conditions that will invoke a rule violation incident. If a rule is violated, you will be notified about the occurrence, and optionally, the system will take action automatically in different ways, such as: warning the user, blocking the activity, etc.

EmpMonitor keeps detailed records of each rule violation incident complete with comprehensive information and associated metadata. You can view these reports from the Alerts screen and quickly search for an incident.

EmpMonitor also records video and optionally, audio in case of a rule violation incident. You can see these recordings with the Session Player. The player allows you to view what rule notifications the user received and the trail of activities leading up to the incident. You can also export these recordings for evidence or forensic investigation purposes. These recordings are automatically analyzed and indexed by EmpMonitor's advanced OCR-engine. You can administer high-speed OCR search for on-screen content or create OCRbased rules that will activate whenever certain text is detected on the screen, in real-time.

You can conduct risk analysis and identify high-risk rules, users, or objects from the Risk report. It also gives you ideas on how to adjust your rules' detection settings to focus on pivotal areas of vulnerabilities or false positives.

Lastly, you can get scheduled delivery of rule violation reports or 'just-in-time' notifications in your inbox with the help of Email Notifications feature.

## **3.1. Common Use Cases**

### **3.1.1 Preventing Data Loss**

- Uploading reports that contain sensitive data to Cloud Storage.
- Sharing documents outside the organization that has a confidential watermark.
- Sending out emails with sensitive files to non-corporate personnel.
- Sending out emails with attachments files of large size, or if you make too many attachments, or zipped files.
- Printing on irregular hours.
- Printing a considerable number of sensitive documents.
- Taking screenshots, using screen capture or snipping tools.
- Copying CRM data and pasting it in emails, on an external site, or in an unauthorized application.
- The non-authorized use of Cloud storage drives as an attempt to exfiltrate data.
- Moving or saving files on a removable media.
- Sharing files with protected properties such as Tags, Attribute, Document Category, etc.
- Employees conversing with the company's competitors.

### **3.1.2 Detecting Insider Threats\**

- Sign of discontent, harassment, legal threats, or any other sentiment in emails or IM chats indicating underlying issues.
- Development team handling production data for testing and development.
- The IT department collecting authentication information such as credit card magnetic data, which is strictly prohibited under agreement.



- Accessing the internet from restricted servers.
- Installing RDP clients or opening ports.
- Users entering sensitive data such as passwords or personal details on potentially harmful or phishing sites.
- Employees using the browser's incognito mode very frequently.
- Clearing browser history or deleting cache files.
- Sudden change in employees' schedules or work patterns.
- External user or freelancer accessing confidential customer and employee records.
- Contractor trying to log in to database servers during off-hours or after the completion of a project.
- Using code snippets in database queries.
- A merchant trying to bypass security clearances and obtain additional access by exploiting a bug, design flaw, or configuration oversight in an operating system or software application.

### **3.1.3 Identifying Abusive Behavior and Accidental Threats**

- Violating company resources, such as, printing unnecessary copies of documents, throttling the network, etc.
- Employees looking at materials online that are ambiguous, suspicious, or otherwise dangerous. For example, hacking sites, pornography, or piracy content.
- Customer agent asking for credit card numbers in unsecured email or support chat without using the proper communications channel.
- Sharing 'not for the public' files on social media or IMs.
- Employee accessing emails that contain phishing links, viruses, or malware.
- Installing browser plugins that aren't secure or known to be problematic.
- Entering passwords or personal details on unsecured websites.

### 3.1.4 Detecting Malicious Intent

- Unauthorized users accessing a document they should not have access to.
- Users trying to hide information in an image.
- Employees participating in insider trading by sharing embargoed data such as M&A documents.
- Exploring the internet for suspicious keywords and phrases, such as: 'how to disable the firewall,' 'recover password,' 'steganography,' etc.
- Running the Tor browser or accessing the darknet sites.
- Attempting to bypass the proxy server.
- Installing a VPN client.
- Running network snooper, registry editor, or other dangerous applications.
- Running password crackers, keyloggers, or other malicious tools.
- Running software from external media or cloud services.
- Modifying the configuration of the network or system settings.
- Opening up blocked pores in the router settings.
- RDP connection attempts to forbid hosts or unauthorized use of RDP applications.
- Performing IT sabotage by deleting user accounts, files, or directories.
- Sharing source codes outside the development team.
- Creating back-door accounts or fake user credentials.

### 3.1.5 Improving Productivity and HR Management

- Get notified when workers spend too much time on Facebook, watching YouTube videos, or surfing online shopping sites.
- Flag when employees idling too much, coming to work late, frequently absent, etc.
- Warn employees when they are spending excess time on personal tasks such as applying for jobs.
- Using applications or sites that are unproductive.
- Not following prescribed policy while dealing with customers.

- Not following corporate etiquette policy, for example, visiting gambling sites.
- Contractor submitting invoices that do not match work hours or task completion status.

### 3.1.6 Conforming with Regulatory Compliance

- Prevent exfiltration of PHI (Protected Health Information) such as EHR, FDA recognized drug names, ICD codes, NHS numbers, etc. to comply with HIPAA and HITECH policies (HIPAA 164.500 - 164.532).
- Automatically log-out the user when inactive for a certain time (HIPAA 174.312).
- Block unauthorized traffic from EHR/EMR and clinical applications (HIPAA 164.306).
- Restrict access based on a user's 'need to know' clearance. For example, block IT admins from accessing cardholder data while performing support tasks (PCI-DSS 10.1).
- Use OCR-based rules to detect when a user has access to the full view of a PAN (Personal Account Number) violating PAN-masking or PAN-unreadable rules (PCI-DSS 3.4/3.5).
- Block file-write operation when credit card numbers or magnetic track data is detected that would violate the storing of authentication data rule (PCI-DSS 3.2).
- Prevent the sharing of contact lists containing EU PII (personally identifiable information) such as English names, EU addresses, or EU phone numbers (GDPR 5).
- Notify users when sharing files containing data such as DNA profile, NHS/NI number, and sexual orientation data, hence preventing the violation of processing of special categories of personal data rule (GDPR 9).
- Ensure that non-EU admins cannot access the records of EU employees, preventing the violation of transfers of personal data to third countries' rule (GDPR 44).
- Enforce security-compliant behavior and take immediate action on the detection of anomalies or rule violations and train employees with detailed rule-alerts (ISO 27001, Standard Enforcement).

## 4. Steps For Creating Rule

### 4.1 Why are You Creating the Rule?

What's your thought on creating rules? Would you like to monitor the user's activities to avoid insider threats? Or you might want to check out if there is anyone in your organization having malicious intent to commit data fraud or crime? Are you seeking help from external vendors to prevent IP leaks? Does your business need to comply with regulations like HIPAA, GDPR, GLBA, etc.?

Conceive a new policy or assign it under the existing policy that fits the rule's purpose.

### 4.2 What Activity, Content or Behavioral Anomaly You Want to Detect?

Have you discovered discrepancies in your employee's schedule? Do you want to detect employees doing time theft? Or there might be some sensitive data that you want to protect. Would you like to know if someone is trying to access it?

Select a Rule Type from the Rules Editor's General tab.

If you are trying to detect behavioral anomalies such as an employee sending an abnormal amount of emails than normal, then you should consider creating an anomaly rule.

Create an anomaly rule from the Behavior > Anomaly rule menu.

### 4.3 Where is the Activity Performed or Content Located?

Next, you'll have to figure out where the anomaly activities like data and content sharing are happening. Does it involve email or usage of any application to transfer files? Like such, there will be many ingress/egress points that you need to monitor. For example- emails, instant messages, web uploads.

Select Types of Activities or Types of Contents from the Rules Editor's General tab.

### 4.4 When Should the Rule be Active?

Would you like to run the rule 24/7 or follow a schedule? For example- The rules will be active during work hours but, it would disable during non-working hours or lunch breaks

Assigned rules can be turned on/off.

Or you can also select the time on which you want the rules to be active.

### 4.5 Whom Should it Apply to?

Do you want to create rules for certain users only? Don't want to assign similar rules to all users of different groups and departments. You can also set up a terminal server to monitor all your

external vendors and external business partners. Or you might want to exclude someone from the rule's enforcement.

On the rule editor, you have the option to choose the department or users to apply the rule. You can also select users on a policy basis by turning on the INHERIT POLICY SETTINGS

## 4.6 What Makes the Data Sensitive?

When you are trying to detect content, you need to describe the details of the data. Does it have a particular structure such as the credit card number? Or you might want to check some unstructured or dynamic data.

On the Rule's editor, specify the type of content you want to detect. You can choose from a Predefined Classified Data or create your own custom data types by selecting other options from the list.

## 4.7 What Scenarios Violate the Rule?

Next, you have to define the scenarios that will trigger the rule. You will have to implement conditions and logics to detect the rule violation. Remember, there are also multiple ways of achieving the same result.

For example, if you wanted to prevent uploading of files to a personal Cloud drive, you could use a condition to detect file operation 'upload'. And use a second condition, 'upload URL', and specify website addresses such as 'google.drive.com, dropbox.com' etc. Or, you could just select file operations for 'write' and select the 'Cloud providers' from the built-in list.

Make use of different categories (i.e Website, Application, etc) on Rule's editor to specify the conditions and scenarios.

## 4.8 What Action(s) Do You Want to Take?

What should the system do when a rule is broken? Do you want it to notify you immediately? Or, do you want it to take some preventive actions too? For example, block the action? Or do you need to take a sequence of actions? For example, block the action but also record the incident? Or, take different actions depending on how often they broke the rule? Assign a risk level to the action?

Use the Actions tab on the Rules Editor to define the action(s). Use the Advanced Mode to assign multi level thresholds and risks.

# 5 Understanding Common Rule Elements

## 5.1 Rule Name and Description

For each rule specify a unique name and optionally, give a description to the rule.

## 5.2 Tags

Tags are keywords you can assign to a rule to easily identify it. They are useful in searching for the rule and can also be used as filters (i.e. on the Risk or Alerts report).

## 5.3 Schedule

By default, a rule can remain active for 24 hours. However, you can also adjust it according to the work schedule of your employees.

For example, you can create a rule that would be active during work hours, but it disables during break time. To change the time for the rule to be active, drag the two pointers to adjust the time.

Note: Agent Schedule rules and Anomaly rules do not have this rule schedule.

## 5.4 Rules Condition

Use the CONDITION fields in a rule to specify what values to compare the rule parameters with. To specify a rule condition, start typing in the relevant CONDITION field, then select an option from the pop-up to tell EmpMonitor what type of value it is.

Here are shown some of the ways to use the conditions.

### **Contains/Equals:**

Use the Contains or Equals conditions for a partial or extract text match. For example, to block certain applications from running, you can type them in the CONDITION field and choose one of these conditions. Note that these conditions aren't case sensitive.

### **Match List:**

You can create a Shared List containing items of text, Regular Expressions, or network addresses. For example, you can create a list of websites and use the Match list condition to block multiple applications without creating a separate rule for each. Check out the Shared List section on the EmpMonitor User Guide to learn more about Shared Lists.

### **Match RegExp:**

For complex matches, such as Credit Card Numbers, Social Security Numbers etc., you can use the Match RegExp option. EmpMonitor supports the standard Regular Expression library.

## 5.5 Rule Logic

Rule logic binds two or more Conditions or Content Definitions together. So, they can be applied to both the rule Conditions and the Content Definitions.

## 5.5.1 Condition Logic

Rule conditions can have either 'OR' logic or 'AND' logic.

- Each value in a rule condition is considered as an 'OR' logic. In the above example, the rule will trigger if the 'Application Name' matches with 'regedit.exe' or 'pseditor.exe'.
- Each condition parameter is considered as an 'AND' logic. In the above example, the rule will trigger if the 'Application Name' and the 'Launch from CLI' parameters meets the condition.
- If you have multiple condition blocks, each new condition is considered as an 'OR' logic. In the above example, if either the Condition 1 or Condition 2 meets the criterion, the rule will be triggered.

You can see how the rule condition logics relate to each other on the Rule's Summary panel.

## 5.5.2 Content Logic

When creating a Content Sharing rule, you have to use 4 logic rules to bind the content definitions together. You can do so under the Advanced: Setup Logics section of the Content tab. Click on the logic between two conditions, a pop-up menu will appear where you can select a logic out of four options.

On the Rule Summary panel, you can check how Content definition logic relates with each other.

The table below explains each type of logic and how they are evaluated:

Logic	Evaluates true if	Example
<b>AND</b>	BOTH of the definitions are met.	In the above example, we are using the tagsfield from the <i>File Properties</i> in Definition 1 and the <i>title</i> field in Definition 2. The logic will return true if file tags equals the text 'CONFIDENTIAL' and the title contains 'PRIVATE'. So, basically, it will process the files that are both confidential and private.
<b>OR</b>	EITHER of the definitions is met.	Using the above example, the logic will return true if file tags equals the text 'CONFIDENTIAL' or the title contains the text 'PRIVATE'. So, basically, it will process the files that are either confidential or private.
<b>AND NOT</b>	The first definition is met AND the second definition is NOT met.	Using the above example, the logic will return true if file tags equals the text 'CONFIDENTIAL' and the title does not contain the text 'PRIVATE'. So, basically, it will process the files that are confidential and not private
<b>OR NOT</b>	The first definition is met OR the second definition is NOT met.	Using the above example, the logic will return true if file tags equals the text 'CONFIDENTIAL' or the title does not contain the text 'PRIVATE'. So, basically, it will process all files except the private ones.

## 5.6 Risk Level

EmpMonitor lets assign risk levels to the rules. Although it's optional, assigning risk levels has some advantages. It will let you analyse risk on the Risk Report, view risk trends and identify high risk users and rules.

There are two places you can assign risks.

### 5.6.1 Setting the Risk Levels in a Regular Rule

You assign risk level to a regular rule from the Advanced Mode of the Rule Editor's Actions tab. You can choose from: No Risk, Low, Moderate, High and Critical.

You can assign risk levels to each action block separately (you create action blocks by clicking the ADD THRESHOLD button).

### 5.6.2 Setting the Risk Level in an Anomaly Rule

Assign risk level to an Anomaly rule under its RULE RISK LEVEL section. You can choose from: No Risk, Low, Moderate, High and Critical. If it's turned on, the risk associated with the rule will be counted as many times as violation happens. Otherwise it will be counted once for all violations.

Unlike the regular rules which support multilevel risk assignments, you can assign only one risk level per anomaly rule.

## 5.7 Rule Summary

In the Rule editor, you have the option to check the summary of the rule in understandable language. You can see the values used in different tabs- what conditions are used, and the logical connection among them; rule actions, etc.

**Note:** Anomaly Rules panel doesn't have a summary panel.



## 6. Creating Regular Rules

The Rules Editor is an intuitive, visual editor with the help of which, you can create sophisticated threat detection, productivity optimization, or data loss prevention rules easily without going through multiple screens or coding.

To access the Rules Editor, create a new rule, or edit an existing rule from the Behavior > Policies menu.

### 6.1 Setting Up the Rule Basics

Specify the basic settings for the rule on the Rules Editor's General tab.

On the top fields, specify a Name and optionally, add a Description for the rule.

You can also define the rule's Tags on this tab. Tags are keywords that you can assign to a rule to easily identify it. They are helpful in searching for the rule and can also be used as filters (i.e. on the Risk or Alerts report).

### 6.2 Selecting Rule Categories and Types

You can choose the Rule Category and Types of Activities (for Activity-based rules) or the Types of Content (for Content Sharing rules) from the Rules Editor's General tab.

There are three types of rule categories you can choose from - Agent Schedule, Activity and Content Sharing. Each category further supports different activities or content types. The table below shows which categories support which activity/content types and their use cases:

	Agent Schedule	Activity	Content Sharing
<b>Use Cases</b>	Useful for detecting flaws in employee schedules or workflow. For example, you will receive a notification when an employee is late. Or, block remote login during odd hours or from unrecognized IPs.	Useful for detecting and controlling user activities for a range of monitored objects. For example, restricting app/website usage. Or, preventing file transfer operations (copy, upload, download etc.) on a folder/app/URL.	Useful for protecting sensitive data. For example, block and email that contains personally identifiable information, or for preventing file transfer operations when certain content is identified in the file.

<b>Type of Activity/Content</b>	• Schedule	<ul style="list-style-type: none"> <li>● Web Pages</li> <li>● Applications</li> <li>● Keystrokes</li> <li>● Files</li> <li>● Emails</li> <li>● IM</li> <li>● Browser</li> <li>● Plugins</li> <li>● Printing</li> <li>● Networking</li> </ul>	<ul style="list-style-type: none"> <li>● Content</li> <li>● OCR</li> <li>● Clipboard</li> <li>● Files</li> <li>● Emails</li> <li>● IM</li> </ul>
---------------------------------	------------	--	--

### 6.3 Defining Users

You specify the users for the rules on the Rules Editor's User tab.

Here you define which users, groups, departments, or computers the rule will apply to. If you select a computer, the rule will apply to all the users on that computer.

By default, the rule will inherit the user settings from the policy it is a part of. However, you can turn off the INHERIT POLICY SETTINGS to select users manually.

You can specify, who the rule will be applied to and optionally, exclude anyone you don't want to be included using the EXCLUDE FROM RULE field.

Check out the EmpMonitor User Guide to learn how to add users, computers, groups, and departments.

### 6.4 Defining Detection Criteria

After you have decided what type of rule you need and which users the rule will apply to, the next part is defining the detection criteria and scope. You will specify what, how or when the rule will be activated. You do this by selecting different parts of the selected Activity Type or Content-Type. For example, the URL of the Webpage activity or the Application Name of the Clipboard content, etc. You can then specify Condition Logics against the part(s) and the values you want to detect. Here's how a detection criterion may look like:

In the next sections, we will walk you through all the available options for setting detection criteria for each rule type.

#### 6.4.1 Agent Schedule Rules: What Schedule Violations Can You Detect?

You can define the detection criteria for the Agent Schedule-based rules from the Schedule tab. Agent Schedule-based rules are the easiest to define as most of it deals with only one detection criterion, schedule/time.

**i** Agent Schedule-based rules use employee schedules to determine their detection criteria. Check out the Schedules section of the EmpMonitor User Guide to learn how to configure schedules for employees.

#### **6.4.1.1 Rule Examples**

- Get notified when a user attempts to log in during abnormal hours or on off days.
- Warns users or automatically locks out their computer if they are idling for too long.
- Notify the supervisor automatically when an employee is absent or late.
- Notify HR and/or payroll if the employee's work time or scheduled work hours change.
- Create a list or range of restricted IPs and disallow login from those IPs.

#### **6.4.1.2 Rule Criteria**

The table below explains what criteria or schedule violation incidents the Agent Schedules support and what conditions you can use with them.

##### **Daily Work Time**

Used to detect if there are any discrepancies in the employee's daily work time. You can detect if their work hour is less than or more than a specified hour(s).

Select either IS LESS THAN or IS GREATER THAN and enter an hour value in the SPECIFY VALUE field.

##### **Scheduled Work Time**

Used to detect if the employee is working longer or shorter than scheduled.

Choose either IS SHORT BY or IS OVER BY and enter a minute value in the SPECIFY VALUE field.

##### **Starts Early**

Detects if the employee started their work earlier than scheduled, by specified minutes.

Enter a minute value in the DEFINE THE TIME RANGE field.

##### **Ends Early**

Detects if the employee ends their work earlier than scheduled, by specified minutes.

Enter a minute value in the DEFINE THE TIME RANGE field.

##### **Ends Late**

Detects if the employee ends their work later than scheduled, by specified minutes.

Enter a minute value in the DEFINE THE TIME RANGE field.

**Arrives Late**

Detects if the employee starts their work later than scheduled, by specified minutes. Note that, unlike the 'Is Late' condition, this will trigger the rule after the employee has logged in.

Enter a minute value in the DEFINE THE TIME RANGE field.

**Is Absent**

Detects if the employee is absent.

No other value is required.

**Is Late**

Detects if the employee is late in logging in to their computer according to their scheduled start time. Note that, unlike the 'Arrives Late' condition, this will trigger the rule before the employee has logged in.

Enter a minute value in the DEFINE THE TIME RANGE field.

**Works on Day-Off**

Detects if the employee is working on their day off.

No other value is required.

**Login**

Detects if the employee logs in during off-hours and optionally also detects if they are trying to log in from a restricted IP.

Set the off-hour range on the SETUP THE OFF HOURS slider. You can click the + / - buttons to add/remove hours. Drag the slider Circles to adjust the hours.

You can restrict IPs from where the login is not permitted in the RESTRICTED IPS field. You can enter any text in the IPv4 format, i.e.: 101.10.2.1/32, and choose a 'Equals' or 'Not Equals' conditions. Or, you can select a Shared List (Network-based) and specify a 'Match List' or 'Does Not Match' condition. Check out the Shared List section on the EmpMonitor User Guide to learn how to create shared lists.

If you check the 'Apply on screen unlock' box, then the login event will be triggered when the user unlocks their screen.

Click on the days under the EXCLUDE DAYS section to include/exclude days in the detection criterion.

**Idle**

Detects if the employee is idling (no keyboard or mouse activity) for more than specified minutes.

Enter a minute value in the DEFINE THE TIME RANGE field.

## 6.4.2 Activity Rules: What Activities Can You Detect?

You can specify the detection criteria for the Activity-based rules from their respective activity tab(s). For example, if you chose Webpages and Emails from the Type of Activity section (in the General tab), you will have two tabs called 'Webpages' and 'Emails' where you can add the rule conditions and values.

### 6.4.2.1 Webpages

Webpages activity allows you to detect web browsing activities through URL, title and query arguments, and browsing-related timing (i.e. idle/active).

#### 6.4.2.1.1 Rule Examples


- Warn users if they are spending excessive time on social media or entertainment sites such as YouTube.
- Restrict access to non-whitelisted/unauthorized websites, but allow managers to override if needed.
- Find out potential turnover by checking if employees are searching for job sites. Get notified if the time spent on such sites exceeds a threshold.

#### 6.4.2.1.2 Rule Criteria

The table below shows what criteria the Webpages activity supports and in what conditions you can use with them.

##### **Any**

Lets you detect if a web page is visited.

 If you use this option without any other criteria, EmpMonitor will trigger the rule anytime a web page is visited.

##### **Webpage URL**

Used to detect You can enter some text in the CONDITION field and choose from 'Contains', 'Equals', or 'Match RegExp'. Or, you can select a Shared List and specify a 'Match List' or 'Equals' condition. Check out the Shared List section on the EmpMonitor User Guide to learn how to create shared lists. an URL (webpage address) or part of an URL.

Similarly, you can exclude any URLs in the EXCEPT field.

##### **Webpage Title**

Similar to the *Webpage URL* criterion, just use the webpage title instead.

##### **Query Argument Name**


A query argument name is the portion of a URL where data is passed to a website. It usually starts with a '?' or '&'. For example: `www.contacts.com/saved?company=empmonitor`. Here, the `company` is the query argument name.

Using this criterion, you can create interesting detection rules. For example, by checking for the 'compose' argument in the Gmail website, you can identify if the user is composing an email. Combining this with the Webpage URL or Webpage Title criterion, you can detect more granular activities. For example, using the text 'new' in the Webpage URL and specifying 'compose' in the Query Argument Name, you can tell if a user is composing a new mail or editing an existing draft.

### **Time Active**

Used to detect how long the user has been active on the website.


You can enter a minute value in the CONDITION field and use '=', '>', '>=' logics.

 The *Time Active* criterion is only shown when you have already selected a Website Title or a Website URL criterion.

### **Time Idle**

Similar to the Time Active criterion, but shows how long the user has been idle/inactive on the site.


You can enter a minute value in the CONDITION field and use the '>' logic.

 The *Time Idle* criterion is only shown when you have already selected a Website Title or a Website URL criterion.

### **Total Time Active**


Similar to the Time Active criterion, but shows the total active time (a combination of all the active times during an entire session).

You can enter a minute value in the CONDITION field and use '=', '>', '>=' logics.

 The *Total Time Active* criterion is only shown when you have already selected a Website Title or a Website URL criterion.

### **Total Time Idle**

You can enter a minute value in the CONDITION field and use '=', '>', '>=' logics.

 The *Total Time Active* criterion is only shown when you have already selected a Website Title or a Website URL criterion.

### **6.4.2.2 Applications**

Applications activity allows you to detect the launch of any application, including the ones that are run from the command line interface or through the Windows Run command.

### 6.4.2.2.1 Rule Examples

- Detect and block when a dangerous application (i.e. Windows Registry Editor) or an unauthorized application is launched.
- Warn users if they are spending time on unproductive applications such as games, music/video players, etc.
- Detect when anonymous browsers, such as, 'Tor' is used.
- Detect when screen sharing applications, snipping tools, or peer-to-peer file-sharing/torrent software are used.

### 6.4.2.2.2 Rule Criteria

The table below explains what criteria the Applications activity supports and what conditions you can use with them.

#### **Any**

Lets you detect if an application is launched.



If you use this option without any other criteria; EmpMonitor will trigger the rule anytime, any application is launched.

#### **Application Name**

Used to detect the name or part of the name of an application. For example: 'regedit.exe.'

You can enter any text in the CONDITION field and choose from 'Contains', 'Equals', or 'Match RegExp'. Or, you can select a Shared List (Textbased or Regular Expressions-based) and specify a 'Match List' or 'Equals List' condition. Check out the Shared List section on the EmpMonitor User Guide to learn how to create shared lists.

Similarly, you can exclude any applications you do not want to track in the EXCEPT field.

#### **Application Caption**

Similar to the Application Name criterion, just use the application caption instead. For example: 'Registry Editor.'

#### **Launched from CLI**

Detects if an application is launched from the CLI (Command Line Interface).

Select YES or NO.

#### **Command Line Arguments**

Command line arguments are additional parameters, options, or values passed to an application when launching it from the CLI. They usually start with a '/', '-', or a space after the application name. For example: C:\ipconfig /renew. Here, renewal is an argument.

Using this criterion, you can, for example, disable certain functions of an application. For example, in the second screenshot on the left, we blocked the launch of the IP config application when the release or renew arguments are used. Otherwise, it will run as usual.

You can only use text value with the 'Contains', 'RegExp' or exact text match conditions for the CONDITION field.

**i** The *Command Line Arguments* criterion is only shown when you have already selected YES for the *Launched from CLI* criterion.

### **Time Active**

Used to detect how long the user has been active on an application.

You can enter a minute value in the CONDITION field and use '=', '>', '>=' logics.

**i** The *Time Active* criterion is only shown when you have already selected an *Application Name* or an *Application Caption* criterion.

### **Time Idle**

Similar to the *Time Active* criterion, but shows how long the user has been idle/inactive on an application.

You can enter a minute value in the CONDITION field and use the '>' logic.

**i** The *Time Idle* criterion is only shown when you have already selected an *Application Name* or an *Application Caption* criterion.

### **Total Time Active**

Similar to the *Time Active* criterion, but shows the total time active (a combination of all the active times during an entire session).

You can enter a minute value in the CONDITION field and use '=', '>', '>=' logics.

**i** The *Total Time Active* criterion is only shown when you have already selected an *Application Name* or an *Application Caption* criterion.

### **Total Time Idle**

You can enter a minute value in the CONDITION field and use '=', '>', '>=' logics.

**i** The *Total Time Active* criterion is only shown when you have already selected an *Application Name* or an *Application Caption* criterion.

### **6.4.2.3 Keystrokes**

Keystrokes activity is used to detect keystrokes entered by the users in applications or websites. In addition to regular keys, you can also detect the clipboard operations (copy/paste commands), use of special keys such as the Print Screen or multiple simultaneous keypresses or combo keys such as CTRL+C.



### 6.4.2.3.1 Rule Examples

- Detect if someone is taking screenshots with the intention of stealing information.
- Detect if an employee is using unprofessional language with a customer on live chat.
- A user repeating easy to guess passwords, hence, creating a security risk.
- Disable keyboard macros or select combo keys in certain applications or for some users.

### 6.4.2.3.2 Rule Criteria

The table below shows what criteria the Keystrokes activity supports and what conditions you can use with them.

#### Text Typed

Used to detect continuous text without any word break. For example, if text typed = "password", the rule will be triggered when the last letter 'd' is typed.

You can also detect special keys such as <Shift+P> or other combinations (check out the Keystrokes Monitoring Report section on the EmpMonitor User Guide to learn how you can find out the special symbols keys).

You can enter any text in the CONDITION field and choose the 'Contains' or 'Match RegExp' option.

Similarly, you can exclude any text you do not want to detect in the EXCEPT field.

#### Word Typed

Used to detect words typed with breaks. For example, if word typed = "password" the rule will be triggered when you finish typing the word and then type separation key, such as: <Space> or '!' or '.' (dot).

You can enter any text in the CONDITION field and choose the 'Contains' option.


Similarly, you can exclude any word you do not want to detect in the EXCEPT field.

#### Application Name

Specifies which applications will be tracked.

You can enter any text in the CONDITION field and choose from 'Contains', 'Equals', or 'Match RegExp'. Or, you can select a Shared List (Textbased or Regular Expressions-based) and specify a 'Match List' or 'Equals' condition. Check out the Shared List section on the EmpMonitor User Guide to learn how to create shared lists.

Similarly, you can exclude any applications you do not want to track in the EXCEPT field.

 The *Application Name* criterion is only shown when you have already selected a *Text Typed* or *Word Typed* criterion. Also, if you use this criterion, you cannot use the *Webpage URL* criterion in the same condition block. However, you can use both criteria in separate condition blocks (i.e. *Condition 1* and *Condition 2*).

## Webpage URL

Specifies which websites will be tracked. This is the same as the *Webpage URL* criterion under the Webpages activity.

**i** The *Webpage URL* criterion is only shown when you have already selected a *Text Typed* or *Word Typed* criterion. Also, if you use this criterion, you cannot use the *Application Name* criterion in the same condition block. However, you can use both criteria in separate condition blocks (i.e. *Condition 1* and *Condition 2*).

## 6.4.2.4 Files

Files activity lets you detect file operations such as access, read, write, upload, download, etc. There are ten such file operations you can detect. Each operation allows you to further specify additional detection criteria. For example, the *Download* operation lets you detect the program, file name, URL, and file size.

Note that not all criteria are available for all file operations. EmpMonitor will automatically show or hide the criteria based on which file operation you select. For example, if you select the *Insert* or the *Eject* operation, you will only see the *Program* and *Drive* criterion.

Select a file operation by clicking the CONDITION filed.

Click the '+' button to add a criterion to the operation.

**i** If you choose the 'Any' file operation without any other criteria, EmpMonitor will trigger the rule for any file operations.

### 6.4.2.4.1 Rule Examples

- Detect/block access to sensitive folders.
- Turn a folder or drive and write a proof, preventing any changes to the files in that folder.
- Get notified when files are uploaded to Cloud sharing sites such as Dropbox, Google Drive, etc.
- Block files from being copied to/from removable media such as USB drives.
- Prevent changes in program settings or tampering of configuration files.
- Block certain file transfer protocols such as FTP.
- Restrict the transfer of large files.

### 6.4.2.4.2 Rule Criteria

The table below describes the criteria you can use for the Files activity, and which file operations are supported for each criterion.

## **Program**

Lets you specify in which program/app the file operation took place.

You can choose from 'Contains', 'Equals', or 'Match RegExp'.


Similarly, you can exclude any programs you do not want to track in the EXCEPT field.

## **Network Host**

Used for network-based file operations. It detects the hostname of the file operation. For example <http://sharepoint.com>, <ftp://filevault.net>, etc.

You can choose from 'Contains', 'Equals', 'All Shares'. Or, you can select a Shared List (Network-based) and specify a 'Match List' condition. Check out the Shared List section on the EmpMonitor User Guide to learn how to create shared lists.


Similarly, you can exclude any hosts you do not want to track in the EXCEPT field.

 This criterion is not supported in: Insert, Eject, Download, and Upload operations.

## **File Path**

Used to detect a file path, folder, or extension. For example: document, c:\windows, etc. The file extension is used to identify a file type and usually starts with a '.' (dot). For example: .doc, .pdf etc. Note: you do not need to specify the '.' when entering the extension.


You can choose from 'Contains', 'Equals', 'Exact Folder'. Or, you can check for file extensions using one of the 'Extension Contains', 'Extension Equals', 'Extension Does Not Contain' options.

 This criterion is not supported in: Insert, Eject, Download, and Upload operations.

## **Drive**

Detects the local, network, or external drives.

You can choose either 'All Drives' or 'All External Drives'.

 This criterion is not supported in Download and Upload operations.

## **Cloud Provider**

Used to detect the cloud provider.

You can choose from 'All Cloud Providers', 'Dropbox', 'Google Drive', 'OneDrive', or 'Box'.

Similarly, you can exclude any providers you do not want to track in the EXCEPT field.

 This criterion is not supported in: Insert, Eject, Download, and Upload operations.

### **RDP File Transfer**

Detects if the file copy operation is done over an RDP (Remote Desktop Protocol) session. This happens when you connect to a remote computer and copy files to/from it.

You can select either YES or NO.

 This criterion is only supported in the Copy operation.

### **Download File Name**

Lets you detect the download file name.

You can choose from 'Contains', 'Equals', or 'Match RegExp'.

Similarly, you can exclude any files you do not want to track in the EXCEPT field.

 This criterion is only supported in the Download operation.

### **Download URL**

Similar to the Download File Name criterion but used to detect the download URL instead.

 This criterion is only supported in the Download operation.

### **Download File Size**

Used to detect the size (in bytes) of the file being downloaded.

You can enter a byte value in the CONDITION field and use '=', '>', '<', '>=' logics.

Similarly, you can use the EXCEPT field to specify an exception.

 This criterion is only supported in the Download operation.

### **Upload File Name**

Similar to the *Download File Name* criterion but used for Upload operation instead.

 This criterion is only supported in the Upload operation.

### **Upload URL**

Similar to the *Download URL* criterion but used for the Upload operation instead.

 This criterion is only supported in the Upload operation.

### **Upload File Size**

Similar to the *Download File Size* criterion but used for the Upload operation instead.

 This criterion is only supported in the Upload operation.

### **Upload Via**

Lets you detect what kind of application or protocol is used for the upload operation.

You can choose from 'FTP', 'SMTP', 'Outlook' or 'Browser'.

Similarly, you can use the EXCEPT field to ignore any protocol/application you do not want to track.

 This criterion is only supported in the Upload operation.

## **6.4.2.5 Emails**

Emails activity lets you detect outgoing and incoming emails, including any email attachments.

### **6.4.2.5.1 Rule Examples**


- Prevent attaching files from a certain location(s) such as a folder, a network path, or a Cloud drive.
- Restrict sending of work emails from personal email accounts.
- Prevent sending attachments to non-business addresses.
- Detect if a competitor is contacting your employees or vice versa.
- Get notified if a user is sending emails with large attachments.

### **6.4.2.5.2 Rule Criteria**

The table below shows what criteria the Email activity supports and what conditions you can use with them.

#### **Any**

Lets you detect if an email is sent or received.

 If you use this option without any other criteria, EmpMonitor will trigger the rule anytime an email is sent or received.

#### **Mail Body**

Used for detecting text inside the mail body.

You can choose from 'Contains' or 'RegExp' with any text. Or, you can select a Shared List (Text-based or Regular Expressions-based) and specify a 'Match List' condition. Check out the Shared List section on the EmpMonitor User Guide to learn how to create shared lists.

Similarly, you can exclude any text/list you do not want to track in the EXCEPT field.

#### **Mail Subject**

Used for detecting text inside the mail subject.

You can choose from 'Contains', 'Equals', or 'RegExp' with any text. Or, you can select a Shared List and specify a 'Match List' or 'Equals List' condition. Check out the Shared List section on the EmpMonitor User Guide to learn how to create shared lists.

Similarly, you can exclude any text/list you do not want to track in the EXCEPT field.

#### **Mail CC**

Detects the CC addresses in an email.

You can choose from 'Contains', 'Equals', or 'RegExp' with any text. Or, you can select a Shared List and specify a 'Match List' or 'Equals List' condition. Check out the Shared List section on the EmpMonitor Rules Guide to learn how to create shared lists.

Similarly, you can exclude any text/list you do not want to track in the EXCEPT field.

#### **Mail To**

Similar to the *Mail CC* criterion but used to detect the *Mail To* addresses instead.

#### **Mail From**

Similar to *Mail CC* and *Mail To* criterion but used to detect the *Mail From* addresses instead.

#### **Mail Direction**

Lets you detect if the mail is being sent or received.

Select either the INCOMING or OUTGOING option.

#### **Mail Client**

Used to specify the mail client you want to detect.

You can choose from 'Gmail', 'Outlook Client', 'Outlook Web Client', 'Live.com', 'Yahoo Mail', and 'Yandex Mail'. EmpMonitor keeps adding support for new clients so you might see more clients than mentioned here.

Similarly, you can exclude any client(s) you do not want to track in the EXCEPT field.

#### **Has Attachments**


Used to detect if the mail has any attachment.

Select either the YES or NO option.

#### **Attachment Name**

Used to detect the names or extensions for the attached files. A file extension is used to identify a file type and usually starts with a '.' (dot)'. For example: .doc, .pdf etc. Note: you do not need to specify the '.' when entering the extension.

You can choose from 'Contains', 'Equals', or 'RegExp' with any text. Or, you can check for file extensions using one of the 'Extension Contains', 'Extension Equals', 'Extension Does Not Contain' options.

 The *Attachment Name* criterion is only shown when you have already selected YES for the *Has Attachment* criterion.

### **Mail Size**

Used to detect the size (in bytes) of the mail.

You can enter a byte value in the *CONDITION* field and use the '=', '>', '<', '>=' logics.

Similarly, you can use the *EXCEPT* field to specify an exception.

### **6.4.2.6 IM – Instant Messaging**

IM activity lets you detect instant messaging conversations and group chats for popular IMs such as Facebook, Skype, Slack, etc. You can detect both incoming and outgoing messages, detect the participants, and search the message body for keywords or text.

#### 6.4.2.6.1 Rule Examples


- Restrict messages to/from select contacts.
- Detect if a user is in contact with suspicious people or criminal groups.
- Monitor support chat conversations to improve the quality of customer service and SLA.
- Get notified if the chat body contains specific keywords or sensitive phrases such as lawsuit threats, angry sentiments, sexual harassment, etc.

#### 6.4.2.6.2 Rule Criteria

The table below shows what criteria the IM activity supports and what conditions you can use with them.

### **Any**

Lets you detect if an IM is sent or received.

 If you use this option without any other criteria, EmpMonitor will trigger the rule anytime an IM is sent or received.

### **Message Body**

Used for detecting text inside the message body.

You can choose from 'Contains' or 'RegExp' with any text. Or, you can select a Shared List (Text-based or Regular Expressions-based) and specify a 'Match List' or 'Equals List' condition. Check out the Shared List section on the EmpMonitor User Guide to learn how to create shared lists.

Similarly, you can exclude any text/list you do not want to track in the *EXCEPT* field.

### **Message Direction**

Lets you detect if the message is being sent or received.

Select either the INCOMING or OUTGOING option.

### **Messaging App**

Used to specify the messaging app you want to detect.

You can choose from 'Facebook', 'Skype Web', 'Skype for Business', 'LinkedIn', 'Google Hangouts', 'WhatsApp Web', 'Slack Web', 'Slack', 'Microsoft Team Web' and 'Microsoft Team'. EmpMonitor keeps adding support for new apps so you might see more clients than mentioned here.

Similarly, you can exclude any app(s) you do not want to track in the EXCEPT field.

### **Contact Name**

Used to detect the contacts/participants of the IM conversation.

You can choose from 'Contains', 'Equals', or 'RegExp' with any text as conditions.

Similarly, you can exclude any contacts you do not want to track in the EXCEPT field.

### **6.4.2.7 Browser Plugin**

Browser Plugin activity lets you detect any installed browser plugins or extensions, what they are doing or what data they are accessing.

#### 6.4.2.7.1 Rule Examples


- Restrict the use of dangerous browser plugins and extensions to prevent malware infection and prevent security or privacy breaches.
- Prevent a plugin from utilizing certain permissions such as the ability to access critical proxy settings or user data.

#### 6.4.2.7.2 Rule Criteria

The table below shows what criteria the Browser Plugin activity supports and what conditions you can use with them.

### **Any**

Lets you detect if a plugin is launched/activated.

 If you use this option without any other criteria, EmpMonitor will trigger the rule anytime a plugin is launched or activated.

### **Browser**

Used to specify the browser you want to detect.

You can choose from 'Chrome', 'Opera', 'Firefox', 'Internet Explorer' or 'All Browsers'. EmpMonitor keeps adding support for new browsers so you might see more clients than mentioned here.

Similarly, you can exclude any client(s) you do not want to track in the EXCEPT field.



## **Plugin Name**

Used to specify the plugin you want to detect.

You can choose from 'Contains', 'RegExp' or exact match with any text as conditions.

Similarly, you can exclude any plugins you do not want to track in the EXCEPT field.

## **Plugin Permissions**

You can detect what permissions the plugin is using.

You can choose any of these conditions:

- Proxy VPN - detects if the plugin is accessing the browser's proxy settings.
- Request - detects if the plugin is making a web request. This permission allows a plugin to observe and analyze traffic and intercept, block, or modify web requests.
- User Data - detects if the plugin is accessing any user data such as cookies.

Similarly, you can exclude any permission you do not want to track in the EXCEPT field.

## **6.4.2.8 Printing**

The Printing activity lets you detect print jobs across local or network printers. You can use criteria such as the document and printer, and the number of pages being printed.

### 6.4.2.8.1 Rule Examples


- Prevent data leaks over hardcopies by restricting what documents can be printed.
- Warn the user about large print jobs to reduce waste.
- Restrict how many pages can be printed in a certain printer to reduce expenses when taking an expensive/color print.
- Implement printer use policies by users/departments. For example, which departments/users can use which printer, how much or what they can print.

### 6.4.2.8.2 Rule Criteria

The table below shows what criteria Printing activity supports and what conditions you can use with them.

## **Any**

Lets you detect if any print job is sent to the printer.

 If you use this option without any other criteria, EmpMonitor will trigger the rule anytime a print job is sent to the printer.

## **Document Name**

Used to specify the document names you want to detect.

You can choose from 'Contains', 'Equals', or 'RegExp' with any text as conditions.

Similarly, you can exclude any plugins you do not want to track in the EXCEPT field.

#### **Printer Name**

Used to specify the printers you want to track.

You can choose from 'Contains', 'Equals', or 'RegExp' with any text as conditions.

Similarly, you can exclude any plugins you do not want to track in the EXCEPT field.

#### **Number of Pages**

Used to detect the number of pages of the document being printed.

You can enter a page value in the CONDITION field and use the '=', '>', '<', '>=' logics.

Similarly, you can use the EXCEPT field to specify an exception.

### **6.4.2.9 Networking**

The Printing activity lets you detect print jobs across local or network printers. You can use criteria, such as the document and printer, and the number of pages being printed.

#### **6.4.2.9.1 Rule Examples**

- Implement network security-related rules, for example, restrict outgoing internet traffic from the payment server (to comply with PCI DSS regulation).
- Limit network access such as, disable login via RDP (Remote Desktop Protocol).
- Implement geo-fencing, for example, restrict access to your EU server from the US users.
- Get notified when abnormal network activity (i.e. sudden spike in network traffic) is detected which might indicate an intrusion.

#### **6.4.2.9.2 Rule Criteria**

The table below explains what criteria the Printing activity supports and what conditions you can use with them.

#### **Application Name**

You can enter any text in the CONDITION field and choose from 'Contains', 'Equals', or 'Match RegExp'. Or, you can select a Shared List (Textbased or Regular Expressions-based) and specify a 'Match List' or 'Equals' condition. Check out the Shared List section on the EmpMonitor User Guide to learn how to create shared lists.

Similarly, you can exclude any applications you do not want to track in the EXCEPT field.

#### **Remote Host**

Used to specify the network the remote host is connected to. You can enter a host address (such as google.com) in the CONDITION field and choose the 'Match List' option. Or, you can select a

Shared List (Network-based) and specify a 'Match List' condition. Check out the Shared List section on the EmpMonitor User Guide to learn how to create shared lists.

Similarly, you can exclude any network you do not want to track in the EXCEPT field.

#### **Remote Port**

Used to detect the port of the network connection.

You can enter a port value in the CONDITION field and use the '=' logic.

Similarly, you can use the EXCEPT field to specify an exception.

#### **Bytes Sent**

Used to specify the number of bytes sent over the network connection.

You can enter a byte value in the CONDITION field and use the '=', '>', or the '>=' logics.

Similarly, you can use the EXCEPT field to specify an exception.

#### **Bytes Received**

Used to specify the number of bytes received over the network connection.

You can enter a byte value in the CONDITION field and use the '=', '>', or the '>=' logics.

Similarly, you can use the EXCEPT field to specify an exception

### **6.4.3 Content Sharing Rules: What Contents Trigger the Rules?**

Content Sharing rules are used to detect content or text inside an object. The object can be a file, an email or IM chat, data in the clipboard or even any text displayed on the screen. You can use these powerful rules to prevent data exfiltration attempts, such as: block transferring of a file when it contains credit card numbers; warn a user when they attempt to send emails containing sensitive keywords etc.

You can specify the detection criteria for the Content Sharing rules in two places:

- On the special Content Tab: This tab allows you to define what makes the content sensitive and specify the data values to look for. This tab is automatically added when you select the Content Sharingrule type (in the General tab).
- On the selected Content Type Tabs: For example, if you selected **OCR** and Emails from the Type of Content section (in the General tab), you will have two tabs called '**OCR**' and 'Emails' where you can add the rule conditions and values.

The basic premise of the Content Sharing rule is: you describe the data in Content Tab and then you tell EmpMonitor where to look for that data in the Content Type Tabs. You need to use both of them for creating a Content Sharing rule.

### 6.4.3.1 The Content Tab

This tab allows you to define what makes the content sensitive and specify the values to look for. You need to select at least one Types of Content, such as:OCR, Clipboard, File etc. to be able to use the Content tab.

You can select from different data definitions depending on what Types of Content you have selected in the General tab (i.e. OCR, Clipboard, Files, Emails, IM).

For example, if you have selected the Clipboard content type, then you will see the 'Clipboard Origin' in the data definition list.

The table below shows what criteria the Content definition supports and what conditions you can use with them

#### Data Content

Data Content is a generic criterion that can be used to look for any text or binary data. For example, by using it with the OCR, you can create a rule that warns a user when it detects some text on their screen. Or, by using it with the Clipboard, you can detect anything copied on the clipboard.

You can select TEXT, BINARY or BOTH as the CONTENT TYPE.

For SELECT MATCH TYPE, you can choose 'Contains', 'Equals' or 'RegExp' and specify the text or binary values in the bottom field. Use the + button to add multiple values. Or, you can choose 'Match List Member' or 'Equals List Member' as a match type and then select a Shared List (Text-based or Regular Expressions-based) from the SELECT SHARED LIST drop-down menu. Check out the Shared List section on the EmpMonitor User Guide to learn how to create shared lists.

The Data Content criterion can be used with any content types (i.e. OCR, Files, Email etc.).

#### Clipboard

OriginClipboard Origin detects data pasted into the clipboard from a specific webpage or application. By using it you can, for example, build a rule that prevents copy pasting of customer data from your CRM site.

You can select WEB PAGE or APPLICATION as the source of the clipboard copy operation.

For SELECT MATCH TYPE, you can choose 'Contains', 'Equals' or 'RegExp' and specify the text values in the bottom field. Use the + button to add multiple values. Or, you can choose 'Match List Member' or 'Equals ListMember' as a match type and then select a Shared List (Text-based or Regular Expressions-based) from the SELECT URL or SELECT NAME drop-down menu. Check out the Shared List section on the EmpMonitor User Guide to learn how to create shared lists

The Clipboard Origin criterion can only be used with the Clipboard content type.

#### File Origin

File Origin detects file sharing based on its origin or source. It supports local, Cloud and web sharing. By using it you can, for example, build a rule that prevents sharing of files to Cloud drives.

You can select from several sharing options under the SELECT FILE ORIGIN section. SHARE= any type of network shares, CLOUD = sharing over Cloud services, such as, Dropbox and URL = sharing over any websites.

Depending on which origin (SHARE / CLOUD / URL) you selected, you can choose from 'All Share', 'Contains', 'Equals' or 'RegExp' in the SELECT MATCH TYPE field and specify the text values in the bottom field. Use the + button to add multiple values. Or, if available, you can choose the 'Match List Member' or 'Equals List Member' as a match type and then select a Shared List (Network-based) from the SELECT URL or SELECT NAME drop-down menu. Check out the Shared List section on the EmpMonitor User Guide to learn how to create shared lists.

The File Origin criterion can only be used with the Files content type

### **File Properties**

File Properties detect files based on their meta-tags (also know as 'file property' or 'field') . By using it you can, for example, build a rule that prevents sharing of any documents outside your company that has a Tag Property containing the string value of 'internal only'. You can create such tags/fields/properties from an application (such as Microsoft Word) or from the Windows Explorer.

You can select ANY, STRING, INTEGER or DATE for the FIELD TYPE.

If needed, enter the name of the field/property in the FIELD NAME.

If you select the STRING field type, you can choose from 'Contains', 'Equals' or 'RegExp' in the SELECT MATCH TYPE field and specify the text values to detect in the SPECIFY VALUE field. Use the + button to add multiple values. Or, you can choose the 'Match List Member' or 'Equals List Member' as a match type and then select a Shared List from the SELECT URL or SELECT NAME drop-down menu. Check out the Shared List section on the EmpMonitor User Guide to learn how to create shared lists.

If you choose an INTEGER or DATE value, you can choose one of the '=', '>', '<' logics in the MATCH TYPE field and provide a numeric or date value in the SPECIFY VALUE field.

The File Properties criterion can only be used with the Files content type.

### **Predefined Classified Data**

Predefined Classified Data detects content based on predefined data categories.

There are several types of data categories you can choose from: Financial Data, Health Data, Personally Identifiable Data etc. The SENSITIVE DATA TO DETECT field will have different menu options depending on what you choose in the SELECT SENSITIVE DATA CATEGORY field. For example, if you choose Financial Data in the previous field, you can choose from 'All credit card numbers', 'SWIFT code' etc. Or, if you choose the Health Data, you can choose from 'Common drug names', 'DNA profile' etc. Check out the Appendix section for a list of all the pre-defined classified data supported in EmpMonitor .

Finally, specify how often a data pattern can appear in the content before the rule is triggered in the TRIGGER ON PATTERN... field.

The PredefinedClassified Data criterion cannot be used with the OCR content type.

### 6.4.3.2 OCR

The OCR content type detects on-screen text in real-time, even inside images or videos. It works with multi-screen setups, virtual desktops and terminal servers. By default, OCR detects English text. But you can also use Hebrew, Spanish or Turkish language. Check out the Editing Screen Settings section on the EmpMonitor User Guide to learn how to change the default OCR language.

#### 6.4.3.2.1 Rule Examples

- Generate an alert when a user sees a full credit card number on the screen violating the PCI DSS compliance requirements.
- Get notified when your employees visit sites that contain illegal or questionable content, such as: hacking, pornographic or piracy related content.
- Detect if an unauthorized user is viewing a document that contains sensitive words.
- Prevent steganographic data exfiltration by detecting information hidden inside images or videos.

#### 6.4.3.2.2 Rule Criteria

The table below shows what criteria the OCR supports and what conditions you can use with them

##### Any

Lets you detect text in any applications.

If you use this option without any other criteria, EmpMonitor will trigger the rule anytime the OCR text is detected on the screen, in any applications.

##### Application Name

Used to specify the applications in which the OCR content will be detected.

You can choose from 'Contains', 'Equals' or 'Equals List' with any text as conditions. Or, you can select a Shared List (Text-based or Regular Expressions-based) and specify a 'Equals List' or 'Match List' condition. Check out the Shared List section on the EmpMonitor User Guide to learn how to create shared lists.

Similarly, you can exclude any applications you do not want to track in the EXCEPT field. The Application Name and the Webpage URL criterion cannot be used together in the same condition block.

##### Webpage URL

Used to specify the webpage URL (website address) in which the OCR content will be detected.

You can enter any text in the CONDITION field and choose from 'Contains', 'Equals' or 'Match RegExp'. Or, you can select a Shared List (Text-based or Regular Expressions-based) and specify a 'Match List' or 'Equals List' condition. Check out the Shared List section on the EmpMonitor User Guide to learn how to create shared lists.

Similarly, you can exclude any URLs in the EXCEPT field.

The Application Name and the Webpage URL criterion cannot be used together in the same condition block.

#### 6.4.3.4 Files

Files content type works in the same way as it does in the Files Activity rules. However, there are certain file operations that you cannot use in the Content Sharing rules. For example, theDownload operation is not supported.

Note that not all criteria are available for all file operations. EmpMonitor will automatically show or hide the criteria based on which file operation you select. So, if you select the Access or theDelete operation, you will only see the Program criterion. Some file operation may have additional detection criteria. For example, the Uploadoperation lets you specify the Upload URL.

Select a file operation by clicking the CONDITION filed.

Click the + button to add a criterion to the operation.

If you choose the 'Any' file operation without any other criteria, EmpMonitor will trigger the rule for any file operation where the content is detected.

##### 6.4.3.4.1 Rule Examples

- Prevent sharing of files that contain sensitive information, such as: Credit Card Numbers, Social Security Numbers, Health Records or your own custom data type.
- Prevent sharing of a file based on certain properties, such as, when a document contains a 'confidential' watermark.
- Create rules based on file origin, such as, stop all network sharing from certain applications.

These are some examples of Content Sharing rules for Files. For other examples of the Files rules, check out the Files Activity rule examples.

##### 6.4.3.4.2 Rule Criteria

The table below describes the criteria you can use for the Files sharing rules, and which file operations are supported for each criterion.

#### Program

Lets you specify in which program/app the file operation took place.

You can choose from 'Contains', 'Equals' or 'Match RegExp'.

Similarly, you can exclude any programs you do not want to track in the EXCEPTfield.

#### Network Host

Used for network-based file operations. Detects the host name of the file operation. For example: http://sharepoint.com, ftp://filevault.net etc.

You can choose from 'Contains', 'Equals', 'All Shares'. Or, you can select a Shared List(Network-based) and specify a 'Match List' condition. Check out the Shared List section on the EmpMonitor User Guide to learn how to create shared lists.

Similarly, you can exclude any hosts you do not want to track in the EXCEPT field.This criterion is only supported inthe Write And Copy Operations.

#### **Cloud Provide**

Used to detect cloud providers.

You can choose from 'All Cloud Providers', 'Dropbox', 'Google Drive', 'OneDrive' or 'Box'.

Similarly, you can exclude any provider you do not want to track in the EXCEPT field.

This criterion is only supported in Write and Copy operations.

#### **RDP File Transfer**

Detects if the file copy operation is done over an RDP (Remote Desktop Protocol) session.

This happens when you connect to a remote computer and copy files to/from it.

You can select either YES or NO.

This criterion is only supported in the Copy operation

#### **Upload URL**

You can choose from 'Contains', 'Equals' or 'RegExp'. Or, you can select a Shared List and specify a 'Match List' or 'Equals List' condition.Check out the Shared List section on the EmpMonitor User Guide to learn how to create shared lists.

Similarly, you can exclude any URLs you do not want to track in the EXCEPT field.

This criterion is only supported in the Uploadoperation.

#### **External Drive**

You do not need to specify any conditions in this criterion.

This criterion is only supported in the Write andCopy operations.

#### **6.4.3.5 Emails**

Files content type works in the same way as it does in the Email Activity rules. Except, theMail Body criterion is not supported.

Emails lets you detect content sharing over outgoing and incoming emails including any email attachments.



#### 6.4.3.5.1 Rule Examples:

- Detect sensitive information like Credit Card Numbers, Social Security Numbers, Health Records or your own custom data types inside attachments and act based on what's detected.
- Detect if an internal memo is shared outside the company.
- For example, warn the user when sending out an email that contains a document containing contacts to prevent data exfiltration or comply with privacy laws.

These are some examples of Content Sharing rules for Emails. For other examples of the Emails rules, check out the Emails Activity rule examples.

#### 6.4.3.5.2 Rule Criteria:

The table below shows what criteria the Emails sharing supports and what conditions you can use with them.

##### **Any**

Lets you detect if an email is sent or received.

If you use this option without any other criteria, EmpMonitor will trigger the rule anytime an email is sent or received.

##### **Mail Subject**

Used for detecting text inside the mail subject.

You can choose from 'Contains', 'Equals' or 'RegExp' with any text. Or, you can select a Shared List (Text-based or Regular Expressions-based) and specify a 'Match List' or 'Equals List' condition. Check out the Shared List section on the EmpMonitor User Guide to learn how to create shared lists. Similarly, you can exclude any text/list you do not want to track in the EXCEPT field.

##### **Mail CC**

Detects the CC addresses in an email.

You can choose from 'Contains', 'Equals', or 'RegExp' with any text. Or, you can select a Shared List (Text-based or Regular Expressions-based) and specify a 'Match List' or 'Equals List' condition. Check out the Shared List section on the EmpMonitor User Guide to learn how to create shared lists.

Similarly, you can exclude any text/list you do not want to track in the EXCEPT field.

##### **Mail To**

Similar to *Mail CC* criterion but used to detect the *Mail To* addresses instead.

##### **Mail From**

Similar to *Mail CC* and *Mail To* criterion but used to detect the *Mail From* addresses instead.

##### **Mail Direction**

Lets you detect if the mail is being sent or received.

Select either the INCOMING or OUTGOING option.

### **Mail Client**

Used to specify the mail client you want to detect.

You can choose from 'Gmail', 'Outlook Client', 'Outlook Web Client', 'Live.com', 'Yahoo Mail', and 'Yandex Mail'. EmpMonitor keeps adding support for new clients so you might see more clients than mentioned here.

Similarly, you can exclude any client(s) you do not want to track in the EXCEPT field.

### **Has Attachments**


Used to detect if the mail has any attachment.

Select either the YES or NO option.

### **Attachment Name**

Used to detect the names or extensions for the attached files. The file extension is used to identify a file type and usually starts with a '.' (dot)'. For example: .doc, .pdf etc. Note: you do not need to specify the '.' when entering the extension.

You can choose from 'Contains', 'Equals', or 'RegExp' with any text. Or, you can check for file extensions using one of the 'Extension Contains', 'Extension Equals', 'Extension Does Not Contain' options.

 The Attachment Name criterion is only shown when you have already selected YES for the Has Attachment criterion.

### **Mail Size**

Used to detect the size (in bytes) of the mail. You can enter a byte value in the CONDITION field and use the '=', '>', '<', '>=' logics. Similarly, you can use the EXCEPT field to specify an exception.

## **6.4.3.6 IM**

IM content type works in the same way as it does in the IM Activity rules. Except, the Message Body criterion is not supported.

IM lets you detect content sharing over instant messaging conversations and group chats for popular IMs such as Facebook, Skype, Slack, etc. You can detect both incoming and outgoing messages, detect the participants, and search in the message body for keywords or text.

### **6.4.3.6.1 Rule Examples**

- Improve productivity and data security. For example, detect if customer service agents are not responding to complaints or queries coming through your Instant Messaging channels.
- Create rules that warn the HR about angry exchanges, harassments, or other potential negative sentiments in chat conversations.

- Detect if a user is targeted for phishing or social engineering online.

**i** These are some examples of Content Sharing rules for IM. For other examples of the IM rules, check out the IM Activity rule examples.

#### 6.4.3.6.2 Rule Criteria

The table below shows what criteria the IM sharing supports and what conditions you can use with them.

#### **Any**

Lets you detect if an IM is sent or received.

**i** If you use this option without any other criteria, EmpMonitor will trigger the rule anytime an IM is sent or received where the content is detected.

#### **Message Direction**

Lets you detect if the message is being sent or received.

Select either the INCOMING or OUTGOING option.

#### **Messaging App**

Used to specify the messaging app you want to detect.

You can choose from 'Facebook', 'Skype Web', 'Skype for Business', 'LinkedIn', 'Google Hangouts', 'WhatsApp Web', 'Slack Web', 'Slack', 'Microsoft Team Web' and 'Microsoft Team'. EmpMonitor keeps adding support for new apps so you might see more clients than mentioned here.

Similarly, you can exclude any app(s) you do not want to track in the EXCEPT field.

#### **Contact Name**

Used to detect the contacts/participants of the IM conversation.

You can choose from 'Contains', 'Equals', or 'RegExp' with any text as conditions.

Similarly, you can exclude any contacts you do not want to track in the EXCEPT field.

## 7. Creating Anomaly Rules

To identify the anomaly behavior of users, you can create Anomaly Rules by deciding behavioral baselines. There you can assign risk levels to any anomaly behavior, which automatically notifies the admin or the managers handling anomaly behavior of employees.

The Anomaly Rules Editor is an intuitive visual editor where you can create sophisticated behavioral-anomaly rules on a single screen.

To access the Anomaly Rules Editor, create a new anomaly rule or edit an existing rule from the Behavior > Anomaly rules menu.

### 7.1 Rule Examples

- Detect when employees spend more than a certain percentage of their work hours on unproductive or entertainment sites such as Facebook, YouTube etc.
- Detect if an employee is idling for too long.
- Get notified if an employee's productivity drops by a certain rate.
- Get notified when a user sends an unusual number of emails than they normally do on a day-to-day basis.
- Detect if the file upload activity of a user exceeds some threshold.
- Detect if your network activity suddenly spikes or drops indicating something unusual happening.

### 7.2 Setting Up the Rule Basics

Specify the basic settings for an anomaly rule on the Anomaly Rules Editor's General Settings section. Give a name for the anomaly rule and select the user's group or department to whom you want to apply the rule. If you have selected several devices, then that rule will work for all the users of those devices. Optionally, you can exclude anyone you don't want to be included using the EXCLUDING field. You can also specify the rule's tags in the TAGS field. Tags are keywords you can assign to a rule to easily identify it. They are useful in searching for the rule and can also be used as filters on various reports (i.e. Risk or Alerts report).

### 7.3 Detection Criteria - What Behavioral Anomalies Trigger the Rules?

Define the detection criteria under the RULE TRIGGER section of the Anomaly Rules Editor. You can select an action that will trigger the rule and then specify the conditions to evaluate. There are several types of actions you can choose from: Applications, Websites, Emails, Activity, Files, Network etc.

Each action has different conditions you can select from, such as: Time, Name, Anomaly Baseline etc. After you have selected a condition, you can choose a logic, such as: '>', '<', 'Equals' etc. from the middle field.

Finally, you specify value(s) to detect in the right-most field. You can add multiple conditions to an action by clicking the ADD CONDITION button.

For example, you can create an anomaly rule using the URL condition and a Time condition with a Websites action to detect if a user spent >20% in 'youtube.com'. In the next few sections, we will walk you through all the available options for setting detection criteria for each action type.

#### **Time**

Detects time spent (%) in an application or website. Enter a percent value and use the '>' or '>=' logic for the condition.

This condition is only supported in the Applications and Web Pages actions.

#### **Name**

Used to specify a name for an application. Enter a text value and use the 'Equals', 'Contains', 'Does Not Contain', 'Regular Expression Match', or 'Regular Expression Not Match' logic for the condition. This condition is only supported in the Applications action.

#### **URL**

Used to detect the URL of a webpage. Enter a text value and use the 'Equals', 'Contains', 'Does Not Contain', 'Regular Expression Match', or 'Regular Expression Not Match' logic for the condition.

This condition is only supported in the Webpages action.

#### **Threshold Count**

Sets the threshold count for how many times an activity occurs before triggering the rule. For example, no. of emails sent, no. of download operation, no. documents printed etc.

Enter a number value and use the '>' or '>=' logic for the condition.

This condition is supported in all actions except for Applications and Web Pages.

#### **Productivity**

Detects the productivity level (in percent) of a user. To learn more about how productivity is measured in EmpMonitor, check out the Productivity section on the EmpMonitor User Guide.

Enter a percent value and use the '<', '>' or '>=' logic for the condition.

This condition is only supported in the Activity: Productivity Action

#### **Rate**

Detects the idle rate (in percent) of a user. To learn more about how idle rate is measured in EmpMonitor, check out the Productivity section on the EmpMonitor User Guide.

Enter a percent value and use the '>' or '>=' logic for the condition.

This condition is only supported in the Activity: Idle Rate action.

#### **Size**

Detects the size (in MegaBytes) of data in a network operation.

Enter a value in Mega Bytes and use the '>' or '>=' logic for the condition.

This condition is only supported in the Network: Data In And Network: Data Out actions.

### **Anomaly Baseline**

Anomaly Baseline uses an algorithm to determine if certain users are trying to crossover the behavioral baseline. This can be the user's current behavior compared to their past behavior; an employee's behavior compared to their departmental baseline; or an employee's behavior compared to the baseline of the entire organization. Using a baseline lets you detect any kind of anomaly behavior happening in your organization. For example, set an anomaly rule to notify you when a user sends an unusual number of emails than they normally do on a day-to-day basis.

You can select either the 'Company', 'Department' or the 'Self' as the rule's condition.

## 8. Defining Rule Actions

Rule Actions will let you specify what system should do when any rule gets violated. Either you can warn that user or you can also block their action. The system will also get you notified and record the screenshots of that particular user's desktop.

For regular rules, you can assign Rule Actions from the action tab in the Rule Editor. On the other hand, you can also create Rules Actions for anomaly rules using Anomaly Rule editor.

Note: Not all rule categories support rule actions:

For example, the Agent Schedule only supports the NOTIFY action for most of its schedule violation types except for the Login and Idle activities. Same way, different Types of Activity / Types of Content may also have their own special actions. For example, Webpages have an action called REDIRECT which is not available for other activities.

Also, not all actions are available on all the operation systems.

**Note that,** *Anomaly Rules only support the Notify action.*

In a few cases, you can also use multiple actions but they should not conflict with each other. For example, you can use notify and block action together, as these actions don't conflict with each other. However, you can't use BLOCK user and LOCK OUT user action together since both of these actions prevent the user from completing an activity. Rules editor will automatically cancel the action(s) that are conflicting with the currently working action(s).

Here are the actions you can use:

### **Notify**

EmpMonitor will send the email notification to the specified accounts whenever someone violates the rule.

You can manage how such notification emails are handled from the Settings screen. See the Changing the Email Notification Settings section to learn more.

### **Block**

This action blocks the user's activity and also shows the message about the activity of the user's computer. You can also use the HTML template to display the message. See the Configuring the Alert Template section to learn more.

If you are using the HTML template option, you can use simple HTML tags in the message itself. For example, you can put a link in the message to your company policy to refresh the user's knowledge, like this.

Uploading data to personal Cloud drives is prohibited. Please [click here](\"http://www.abc.com/policy\") to read the policy

In case, when Allow Bypass With Confirmation option is selected, the user will get blocked. The user will be able to bypass the block after clicking a Yes button.

If the MANGER CAN MAKE EXCEPTIONS option is selected, EmpMonitor will send an email to the manager(s) specified in the email field. The manger(s) can then allow the user to bypass the block by clicking a link in the email.

You can also specify how long EmpMonitor should wait between multiple alert messages that the user sees. See the Changing the Alert Wait Time to learn more.

### **Look Out User**

Shows a warning message to the user and then when they press the OK button, they are locked out of the system. If the user logs back in, they will be logged out automatically. An administrator has to unlock the user for them to be able login again. Check out the Employee Action Menu section on the EmpMonitor User Guide for more information on unlocking a user.

This action works only on Windows OS.

### **Redirect**

Redirects the user to a different website when they try to access certain URL(s).

This action is available to Websites-based rules only.

### **Warn**

Warns a user with a message. Similar to the message in the Block action, you can use a HTML template to display the warning message.

You can specify how long EmpMonitor should wait between multiple alert messages that the user sees. See the Changing the Alert Wait Time to learn more.

### **Set User's Active Task**

You can automatically assign the user a task based on their activities.

You can specify how long EmpMonitor will wait before assigning a new task to a user. Check out the Changing the Task Selection Timeout section to learn more.

Applicable only if the user is using a Stealth Agent.

### **Record Video**

If video recording is disabled in your Screen monitoring settings, you can still record a video of the rule violation incident with this action. The system will automatically record for the specified number of minutes before and after the incident.

### **Command**

With this action, you can execute a Windows command automatically when a rule is violated.



This is a powerful action as it allows you to run any application or script on the user's computer. For example, you can force shutdown the pc (shutdown /s /f /t 0), kill a task (taskkill -im explore.exe) and do much more.

This action works on Window only.

## 8.1 Customizing the Rule Messages and Alerts

There is an Alert tab option that allows you to define how to display rule messages or alerts to the users. You can also customize the alert messages to make it look distinctive, which match with your company's branding.

To customize the alert template, click on the Gear icon on the top right corner of the EmpMonitor dashboard, then select the Settings from the drop-down menu.

A Settings screen will appear. Select the Alerts tab from this Settings screen.

### 8.1.1 Configuring the Alert Template

Click the USE HTML USER ALERTS BY DEFAULT button to enable HTML template by default for all rules.

Customize the look of your message box by editing the HTML in the CUSTOM USER ALERT HTML field. There are a few dynamic variables such as %ALERT%, %DETAILS% you can use in your message. The variable could be replaced by the actual message and details when the message is triggered. In addition, the alert can have buttons like OK and CANCEL. You can also include base 64-encoded images in your HTML, for example, to display icons or logos.

Tap on the PREVIEW button to check the look of the alert message.

SCREEN LOCATION defines where the alert will be displayed (i.e. Center, Top-Left etc.). The WIDTH and HEIGHT fields allow you to change the width and height of the alert box.

### 8.1.2 Changing the Email Notification Settings

The Notify rule action sent the email notification to the user(s) when a rule is violated.

ALERT EMAIL LIMIT setting defines the threshold number of emails where the system collects the group notifications into a single email. The system will send this many identical alert emails, and then it will group them together into an email digest. If set to 0, EmpMonitor will send each notification alert as a separate email.

### 8.1.3 Changing the Alert Wait Time

USER ALERT THRESHOLD applies to rules with a Warnor Block action. The threshold sets the minimum time, in seconds, to wait between alerts that the user sees. If set to 0, users will see all alerts they violate, regardless of the frequency.

#### **8.1.4 Changing the Alert Log Limit**

LOG ALERT THRESHOLD sets the minimum time, in seconds, to wait between logging alerts to the EmpMonitor system. If set to 0, it will not limit the number of alerts that are logged. MAXIMUM DAILY ALERTS COUNT limits the total number of alerts which get logged by EmpMonitor on a daily basis per alert type.

#### **8.1.5 Changing the Task Selection Timeout**

You can build rules in EmpMonitor to set a user's task based on their activity. RULE TASK SELECTION ACTION TIMEOUT (SECONDS) defines the time out when switching tasks. If the user switches activity and remains in the new activity for the defined seconds, the rule will be re-evaluated.

## 9. Using the Prebuilt Rule-Templates

### 9.1.1 Using the Regular Rule Templates

While creating a rule, you can select from a list of pre-built templates. Click on **CHOOSE A TEMPLATE** drop-down menu to select a template from Rule Editor's General Tab.

EmpMonitor has many templates showing Data loss prevention, Email, Applications, Websites, File Operations etc. After selecting a template, the rest of the rules tab will be automatically populated with pre-configured settings and sample data. Of course, you can also change them as per your requirement.

Check out the Appendix section for a list of all the prebuilt regular rule templates available in EmpMonitor.

### 9.1.2 Using Anomaly Rule Templates

While creating a new anomaly rule, you can choose from a list of pre-built templates. Click the **USE TEMPLATE** button, then choose a template from the **TEMPLATE TO USE** drop-down menu to choose a template.

EmpMonitor comes with many anomaly rules templates. You can choose from a list of types such as: Applications, Emails, File Operations etc.

Check out the Appendix section for a list of all the prebuilt anomaly rule templates available in EmpMonitor.

# 10. Enforcing the Rules

## 10.1 Automatic Enforcement

While creating a new rule, by default, enforcement is automatically turned on. You can also edit the rule when it's running. With any changes to the rule, it will be enforced immediately if the user is online connected to the EmpMonitor server or as soon as they connect.

*It's always a good idea to test a rule when you create or edit it to see if it's working as intended. You can do so by checking the Alerts Report.*

Rules are enforced depending on what type of EmpMonitor Agent is installed on the user's computer:

### If the user is using a Stealth Agent:

- **Regular Rules:** The rule will be enforced according to any Rule Schedule you have setup or for 24/7 if no such schedule exists. The rule will be enforced even if the user is offline or disconnected from the EmpMonitor server.
- **Anomaly Rules:** Since an anomaly rule does not have a schedule, it will run for 24/7.

### If the user is using a Revealed Agent:

- **Regular Rules:** The rule will only be enforced when the user has logged in to the Agent and clicked the Start button to begin their shift. The rule will still follow any Rule Schedule you have set up. The rule will continue to be enforced until the user clicks the Stop button to end their shift or as soon as the rule schedule has ended – whichever comes first.
- **Anomaly Rules:** Since an anomaly rule does not have a schedule, it will run until the user clicks the Stop button on the Revealed Agent.

## 10.2 Manual Enforcement

You can also manually turn a rule on/off using the EmpMonitor dashboard.

Here are the steps to do so:

**Regular Rules:** You can manually control the rules from the Behavior Policies screen. To access the Behavior Policies screen, click the BEHAVIOR > Policies menu.

Use the ON/OFF button next to a rule's name to turn it on or off. You can also use the ON/OFF button next to the Policy's name for which the rule is a part of. If you turn off the policy, all rules under the policy will be deactivated even if the individual rules are turned on. If the policy is turned on, the rules that have the ON status will be activated and the OFF rules will remain inactive.

**Anomaly Rules:** The only way to turn off an anomaly rule is to remove it from the Anomaly rules screen. To access the Anomaly rules screen, click the BEHAVIOR > Anomaly rules menu.

Click the X button besides an anomaly rule to remove it.

# 11. Investigating the Rule Violation Incidents

With EmpMonitor you have multiple ways to investigate the rule violation incidents.

## 11.1 Using the Alerts Report & the Alerts Log Widget

It is the primary source to see all the rule violation incidents. You can use the Alerts report to view a list of rule violation incidents with all the necessary details, such as: the date/time the incident happened, the user or activity involved and other pertinent information. While you can also view a session recording of an alert, export the alerts report or schedule it for auto delivery to selected email addresses.

You can access the Alerts report from the Behavior > Alerts menu.

For more information on the Alerts report and to learn how to use its different features, check out the Alerts section on the EmpMonitor User Guide.

You can also add an Alerts Log widget to your dashboard. The widget allows you to view the most recent alerts in real-time or for the selected date range. You can add the Alerts Log widget to a dashboard by clicking the ADD WIDGETS button on the Dashboard's screen

For more information on the Widgets and to learn how to use them, check out the Widgets sections on the EmpMonitor User Guide.

## 11.2 Using the Session Player

Using the session player you can have the live view of the user's desktop-screen. It will help you to precisely locate the rule violation incident. When a user is online, you can remotely take control of their desktop or even freeze their input to prevent further incidents.

If Audio recording is enabled, you can also hear recordings of both sound outputs and inputs (speakers/line-out, microphone/line-in). Finally, you can take snapshots of the user's desktop, forward the recordings to select email addresses or download them as MP4 files.

You can access the Session Player from the Alerts screen, from any of the Monitoring Reports or even from the Dashboards. Click the Movie Camera icon, wherever you see it, to access the Session Player.

For more information on the Session Player and to learn how to use its different features, check out the Session Player section on the EmpMonitor User Guide.

## 11.3 Using the Risk Report & the Risk Widget

Risk report allows you to analyze the behavior and impact of the rule violation from the user end. It shows top risky rules, users, applications and websites.

You can drill-down each risk category to further investigate what caused the risk level to change. You can also plot the risk trend by department, severity, number of violations, tag etc. Unique risk scores help you identify high-risk rules or users so that plans can be developed for treating the risks.

You can access risk report from risk menu.

## 12. Sample Rules Walkthrough

### 12.1 Rule Sample 1: User logs in during off hours

#### 12.1.1 Rule Summary

It shows how you can create an Agent Schedule rule to detect a user attempting to login during off hours.

#### 12.1.2 Setting up the Rule

##### General

On the first tab, General, we assigned a name for the rule and a description. We have chosen an Agent Schedule rule type since we are looking to detect a user's login time.

##### To learn more:

- Agent Schedule Rules: What Schedule Violations Can You Detect?
- Understanding Common Rule Elements - names, description, tags, schedule etc.

##### User

For the users, we choose to manually add the users (by turning off the INHERIT POLICY SETTINGS). We also decided to apply this rule to external contractors only. To do so, we first created a department named 'External Contractors' and then edited the selected users' profiles and assigned them to this department.

##### To learn more:

- Defining Users
- Creating/Editing Departments
- Creating/Editing Employee Profiles

##### Schedule

We have selected the Login schedule violation type so that we can monitor the login attempts. We have also set up two time slots that will be considered as off-hours (12am-8am and 6pm-12am).

Any attempt to login in these two periods will trigger the rule.If you wanted, you could set up additional options such as restricted IPs or exclude any days you don't want to monitor.

**To learn more:**

- Rule Criteria–for Agent Schedule rules

**Actions**

Finally, for the last tab, 'Actions', we have selected to use a NOTIFY action to notify the security admin and WARN action to show a warning to the offending user. For this last action, we decided to use the HTML template option to make the alert prominent to the user.

**To learn more:**

- Defining Rule Actions
- Customizing the Rules Messages and Alerts

### 12.1.3 Viewing the Rule Alerts

You can check the Alerts report for the rule:

### 12.1.4 Viewing the Session Recording

You can see the Session Recording of how the rule message will look on the user's desktop:

## 12.2 Rule Sample 2: User sending emails with attachments to non-business address

### 12.2.1 Rule Summary

This example shows how you can create a simple Activity rule to warn a user when they send an email with attachment(s) to a non-business email address.

### 12.2.2 Setting up the Rule

**General**

On the first tab, General, we assigned a name for the rule and a description. We also used some tags to identify the rule easily.We have chosen an Activity rule type since we are looking to detect a user action (the act of sending an email) and not any content. We have selected Emails as the Types of Activities.

We left the rule schedule to its default 24-hour setting.

**To learn more:**

- Activity Rules: What Activities Can You Detect?
- Emails– emails activity rule
- Understanding Common Rule Elements - names, description, tags, schedule etc.

## User

For the users, we used the default policy settings (by leaving the INHERIT POLICY SETTINGS option turned on).

### To learn more:

- Defining Users

## Actions

Finally, for the last tab, 'Actions', we have selected to use a NOTIFY action to notify the security admin and WARN action to show a warning to the offending user. For this last action, we decided to use the HTML template option to make the alert prominent to the user.

### To learn more:

- Defining Rule Actions

## Emails

### *Mail To*

We have added three criteria to the Emails activity. For the first criterion, 'Mail to', we have specified several email domains that we would consider as 'non-business' addresses and used a contains logic to detect even a partial match.

### *Mail Direction*

For the second criterion, 'Mail Direction', we have selected OUTGOING to detect only the outgoing emails.

### *Has Attachments*

For the second criterion, 'Mail Direction', we have selected OUTGOING to detect only the outgoing emails.

### To learn more:

- Rule Conditions
- Rule Logic

## Actions

Finally, for the last tab, 'Actions', we have selected to use a WARN action to just show a simple warning to the user.

### To learn more:

- Defining Rule Actions

## 12.2.3 Viewing the Rule Alerts

Checkout the Alerts report for the rule.

## 12.2.4 Viewing the Session Recording

Check out the session recording from the user's computer in the system.



## 12.3 Rule Sample 3: User attempting to upload a sensitive file to a cloud drive

### 12.3.1 Rule Summary

This example shows how you can create an Activity rule to block a user and display a message for attempting to upload certain files to a cloud drive.

### 12.3.2 Setting up the Rule

#### General

On the first tab, General, we assigned a name for the rule and a description. We have chosen an Activity rule type since we are looking to detect a user action (the act of uploading a file) and not any content. And we have selected Files as the Types of Activities. We left the rule schedule to its default 24-hour setting.

#### To learn more:

- Activity Rules: What Activities Can You Detect?
- Files– files activity rule
- Understanding Common Rule Elements - names, description, tags, schedule etc

#### User

For the users, we choose to manually add the users (by turning off the INHERIT POLICY SETTINGS). We have also excluded the Management department from the rule's scope.

#### To learn more:

- Defining Users

#### Files

##### *File Operation*

We have added two criteria to the File Activity. For the first criterion, 'File Operation', we have selected the Upload operation.

##### *Upload File Name*

For the second criterion, 'Upload File Name', we have specified some keywords that we would like to detect in the file names.

#### To learn more:

- Rule Conditions
- Rule Logic

#### Actions

Finally, for the last tab, 'Actions', we have selected a BLOCK action to block the activity and at the same time show a message to the user. For this demonstration, we used a HTML template. This will allow us to use a customized template. We can also use simple HTML tags (such as <b>, <a> etc.) in the message itself.

**To learn more:**

- Defining Rule Actions
- Customizing the Rules Messages and Alerts

### **12.3.3 Viewing the Rule Alerts**

Check out the alert report of the rule.

### **12.3.4 Viewing the Session Recording**

Check out the session recording of how the rule message will look on the user's desktop

## **12.4 Sample Rule 4: User attempting to share files containing sensitive content**

### **12.4.1 Rule Summary**

This example shows how you can create a Content rule to block a user and display a message for attempting to upload a file containing credit card numbers. The user will be able to override the block action by clicking a 'Yes' button or cancel the operation by clicking a 'No' button. In any case, a rule alert will be recorded.

### **12.4.2 Setting up the Rule**

#### **General**

On the first tab, General, we assigned a name for the rule and a description.

We have chosen a Content Sharing rule type since we are interested in detecting sensitive content. We have selected Files as the Types of Content.

We changed the rule schedule so that it will monitor 9am-12pm and 12:30pm-5:00pm, a typical work time taking into account a 30-minute lunch break.

**To learn more:**

- Content Sharing Rules: What Contents Trigger the Rules?
- Files- files content sharing rule
- Understanding Common Rule Elements - names, description, tags, schedule etc.

#### **User**

For the users, we used the default policy settings (by leaving the INHERIT POLICY SETTINGS option turned on).

**To learn more:**

- Defining Users

#### **Content**

For content, we used a built-in template, 'Predefined Classified Data' and then deleted the 'Financial Data' category to detect 'All credit card numbers'. The rule will trigger even if there's

only one credit card number detected in a file. We did so by entering a value of '1' in the TRIGGER ON PATTERN FREQUENCY IN CONTENT field.

### **Actions**

Finally, for the last tab, 'Actions', we have selected a BLOCK action but turned on the ALLOW BYPASS WITH CONFIRMATION? option. This will show a warning to the user and block the action. But it will also show two YES and NO buttons. If the user clicks YES, they will be able to override the block.

#### **To learn more:**

- Defining Rule Actions

### **12.4.3 Viewing the Rule Alerts**

Here you can check out the Alerts report for the rule:

### **12.4.4 Viewing the Session Recording**

Check out the session recording of how the rule message will look on the user's desktop:

## **12.5 Sample Rule 5: Employee productivity anomaly**

### **12.5.1 Rule Summary**

This example shows how you can create an Anomaly rule to monitor the productivity level of employees and receive a notification when it goes below a certain threshold. You will also be able to compare this against their Departmental and Organizational average.

### **12.5.2 Setting up the Rule**

#### **General Settings**

In the first section, General Settings, we assigned a name for the rule and a description. For the users, we have selected All employees. We have also used a tag to find the rule easily.

#### **To learn more:**

- Creating Anomaly Rules
- Setting Up the Rule Basics - names, description, user, tags etc

#### **Rule Trigger**

We chose the 'Activity: Productivity' as the rule trigger. For the rule's condition, we selected the Productivity criterion and chose a less than '<' logic to detect when the productivity goes below 20%.

#### **To learn more:**

- Detection Criteria - What Behavioral Anomalies Trigger the Rules?
- List of Prebuilt Anomaly Rule Templates

### **Risk Level**

We left the risk level's default settings (No Risk) and ACCUMULATES RISK option turned on so that multiple violations of the rule will add up towards the risk score for this rule.

#### **To learn more:**

- Setting the Risk Level in an Anomaly Rule

### **Actions**

Finally, for the last section, 'Actions', we have turned on the NOTIFY action to inform a manager about the productivity loss.

#### **To learn more:**

- Defining Rule Actions

### **12.5.3 Viewing the Rule Alerts**

Here you can see the Alerts report for the rule:

### **12.5.4 Viewing the Session Recording**

Anomaly rules do not have any session recordings. However, if you have enabled 24/7 recording (you can do so by Editing the Screen Settings) you can take the following steps to view the user's desktop at the time of the anomaly rule violation:

1. Take note of the date and time when the anomaly rule was triggered from the Alerts screen's Date/time column.
2. Open the Session Player for the user by any of the methods mentioned here.
3. Change the date on the Session Player to the date you noticed on the Alerts screen. Move the player head to the required time

# 13 Appendix

## 13.1 List of Prebuilt Rule Templates

<p><b>Data Loss Prevention</b></p> <p>Credit Card Number: Wide</p> <p>Credit Card Number: Narrow</p> <p>Credit Card Number: At least 50 numbers</p> <p>Credit Card Magnetic Strip Data: Wide</p> <p>Credit Card Magnetic Strip Data: Narrow</p> <p>Credit Card Magnetic Strip Data: 50 Track1 entities</p> <p>Office Document: Confidential Watermark</p> <p>Credit Card Magnetic Strip Data: 50 entities</p> <p>Health Data: Disease or Drug names</p> <p>Health Data: Drug names or NDC identifiers</p> <p>Personal Data: US SSN and Date of Birth</p> <p>Health Data: US SSN with Health Information</p> <p>Health Data: UK NHS Numbers and Medical Information</p> <p><b>Emails</b></p> <p>Outbound email with social security number</p> <p>Outgoing email to non-business address</p> <p>Email contains a CV</p> <p>Outgoing email w-attachment to non-business address</p> <p>Email contains accusative sentiment</p> <p>Email contains angry sentiment</p> <p>Email contains discouraged sentiment</p> <p>Email contains dissatisfied sentiment</p> <p>Email contains lawsuit threat</p> <p>Email contains profanity</p> <p>Email contains sexual harassment content</p> <p>Email contains unresponsive complaint</p> <p>Incoming email from competitors</p> <p>Outbound email with attachment</p> <p>Outbound email with credit card number</p> <p>Outbound email with sensitive keywords</p> <p><b>Keystrokes</b></p> <p>Screenshot taken</p> <p><b>Printer</b></p> <p>Large print job</p>	<p><b>Application</b></p> <p>Anonymous browser detected</p> <p>MSIExec program installation or removal</p> <p>Network sniffer launched</p> <p>Non-whitelisted application executed</p> <p>Registry editor launched</p> <p>Running peer-to-peer file sharing applications</p> <p>Running screen sharing applications</p> <p>Snipping tool used</p> <p><b>File Operations</b></p> <p>Access sensitive files</p> <p>Driver tampering</p> <p>Hosts file edited</p> <p>Program installation</p> <p>Write to cloud drive (native)</p> <p>Write to config file</p> <p>Write to removable media</p> <p>Copy file from RDP</p> <p>Copy file from RDP to removable media</p> <p><b>Websites</b></p> <p>Non-whitelisted website accessed</p> <p>Adult websites</p> <p>Excessive time on job search websites</p> <p>Excessive usage of social media</p> <p>Gaming or gambling sites</p> <p>Streaming movies</p> <p><b>IMs</b></p> <p>IM contains accusative sentiment</p> <p>IM contains angry sentiment</p> <p>IM contains discouraged sentiment</p> <p>IM contains dissatisfied sentiment</p> <p>IM contains lawsuit threat</p> <p>IM contains sexual harassment content</p> <p>IM contains unresponsive complaint</p>
--	--

## 13.2 List of Prebuilt Anomaly Rule Templates

<p><b>Applications</b> Application usage anomaly</p> <p><b>Emails</b> Outgoing email anomaly Outgoing email attachments anomaly</p> <p><b>File Operations</b> External storage insertion anomaly File copy anomaly File creation anomaly File delete anomaly File rename anomaly Files downloaded by browser anomaly Files downloaded by cloud client anomaly Files uploaded by browser anomaly Files uploaded by cloud client anomaly</p> <p><b>Instant Messages</b> Instant messages count anomaly</p>	<p><b>Networking</b> Network connection count (no https) anomaly Network connection count anomaly Network data in (no https) anomaly Network data in anomaly Network data out (no https) anomaly Network data out anomaly</p> <p><b>Printers</b> Documents printed count anomaly</p> <p><b>User Activity</b> Idle time anomaly User productivity rate anomaly</p> <p><b>Websites</b> Website usage anomaly</p>
--	--

## 13.3 List of Pre-Defined Classified Data

### Financial Data

<p><b>All Credit Card Numbers</b> Magnetic Data Magnetic Data (Track 1) Magnetic Data (Track 2) Swift Code ABA Route Numbers</p> <p><b>By Type</b> Visa Mastercard American Express Bankcard Dinners International Dinners USA &amp; Canada Discover En Route JCB Maestro Switch Solo RuPay</p>	<p><b>USA</b> Visa Mastercard American Express Bankcard Dinners International Dinners USA &amp; Canada Discover En Route JCB Maestro</p> <p><b>Japan</b> Visa Astercard American Express JCB Maestro</p>	<p><b>Europe</b> Visa Mastercard American Express Discover Maestro Switch Solo</p> <p><b>United Kingdom</b> Visa Mastercard American Express Discover Maestro Switch Solo</p>
---	--	---

<b>By Country</b> USA Japan Israel Europe United Kingdom Canada	<b>Israel</b> Visa Mastercard American Express JCB Maestro	<b>Canada</b> Visa Mastercard American Express Diners Discover Maestro
---	---	--

**Health Data**

Common Drug Names Common Disease Names DNA Profiles	NDC Number HICN	NHS Number ICD10 Code
---	--------------------	--------------------------

**Personally Identifiable Data**

USA Zip Code and Address UK Postal Code and Address USA Cities SSN English Names	Dates Phone Numbers IPv4 Addresses IPv6 Addresses Email Addresses	URL VIN Personal Cryptographic Keys USA Vehicle License Plates USA Driver License Number (All States)
--	---	---

**Code Snippets**

Clang C++ C# Go	Haskell Java JavaScript Objective-C	PHP Python Ruby SQL
--------------------------	--	------------------------------