



CryptoGen Nepal

 Saycure.

# Solution Sheet

## SayCure Components

#Made4Security


















[www.cryptogennepal.com](http://www.cryptogennepal.com)



SayCure is a modern threat detection and response platform with threat detection capabilities which helps organizations neutralize threats before they have a negative impact on your business(s). Active response and vulnerability management capabilities out-of-the-box makes Saycure a one-stop solution for Threat life cycle management.






We focus on 3 key features:

- Cyber risk focused alerts
- Active monitoring and Response
- Compliance Monitoring
- Vulnerability Detection

Critical Cases					Search:
Name	Team Name	Members	Status	Actions	
CASE : #4051 10 Jan 2024	Nirmal Poudel	  	<div><div></div></div> 38%	⋮	
CASE : #4052 03 Jan 2024	Nirmal Poudel	  	<div><div></div></div> 45%	⋮	
CASE : #4053 12 Jan 2024	Simran Karki	  	<div><div></div></div> 92%	⋮	
CASE : #4054 19 Jan 2024	Rishav Pandit	  	<div><div></div></div> 56%	⋮	
CASE : #4055 08 Jan 2024	Bishesh Shrestha	  	<div><div></div></div> 25%	⋮	
Rows per page: 5					1-5 of 10 < >

#### Cases By Assignee

Total Cases

	Shreenkhala Bhattarai SOC Lead
	Nirmal Poudel SOC Analyst
	Simran Karki Sr. SOC Analyst
	Nayan Bhattarai SOC Analyst
	Aaditya Khati SOC Manager

## Saycure.

SayCure is a modern unified security platform with threat detection capabilities which helps organizations neutralize threats before they have a negative impact on your business(s). Active response and vulnerability management capabilities out-of-the-box makes SayCure a one-stop solution for Threat life cycle management. The platform focuses on these key features:

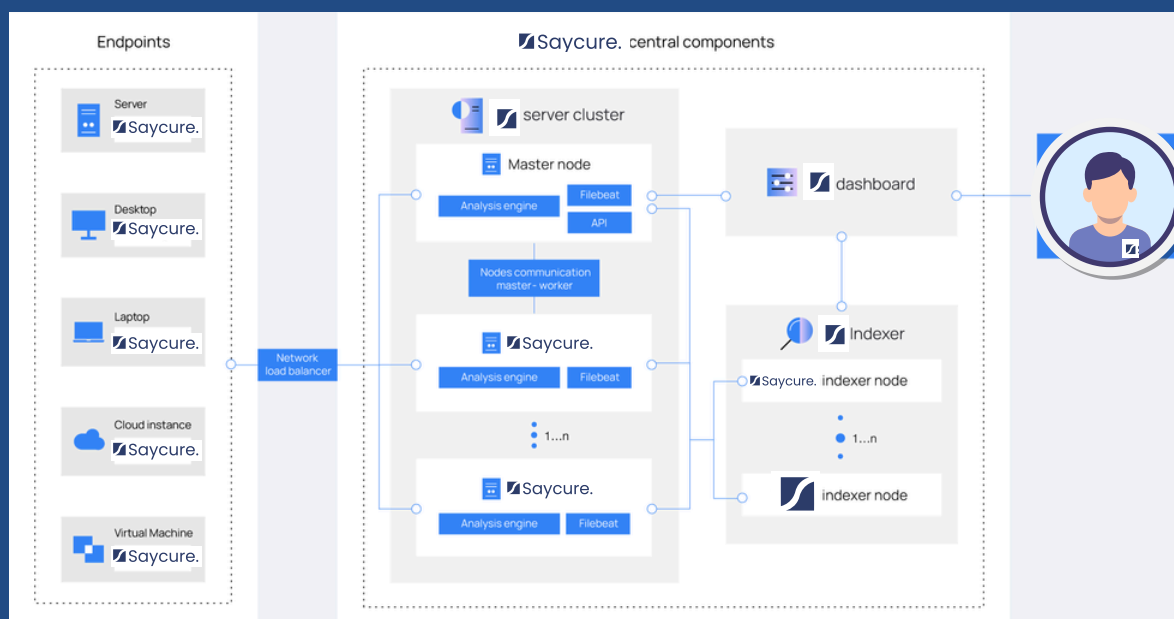
1. Endpoint Configuration Assessment
2. File and Registry Integrity Monitoring
3. Regulatory Compliance
4. Vulnerability Detection
5. Threat Analysis
6. Log Analysis
7. Alerting



### Licensing and Architecture:

SayCure is based on number of nodes and the components are designed to support based on the architecture that can be deployed on-prem or on the cloud. The saycure platform is divided into multiple clusters and is able to scale both vertically and horizontally.

Logs from Windows, Linux, cloud, network and security can be ingested directly on the saycure without any additional components.



## Saycure.

### Integrations

SayCure has the capabilities to integrate with multiple third-party platform with access to API. The integration are but not limited to, SOAR, Threat Intelligence, Case Management, Email and more.



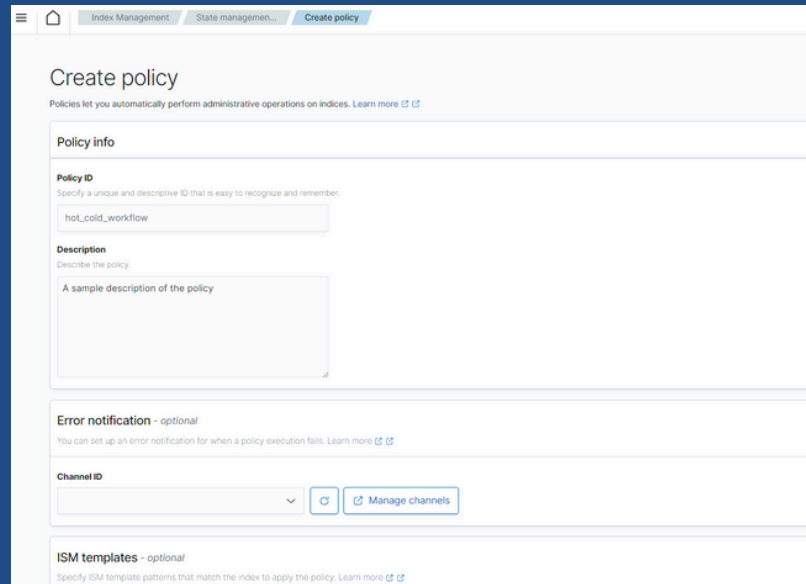
## Index Life Management (Log Retention)

Security standards require keeping data available for audits for a minimum period of time. For data older than this retention period, you might want to delete it to save storage space.

You can define specific policies to handle deletions automatically. You might also find these policies useful for index rollovers.

### Applying the retention policy to alerts index

1. Choose **Indices** in **Index Management**.
2. Select the index or indices to attach the policy.
3. Click **Actions** › **Apply policy**.

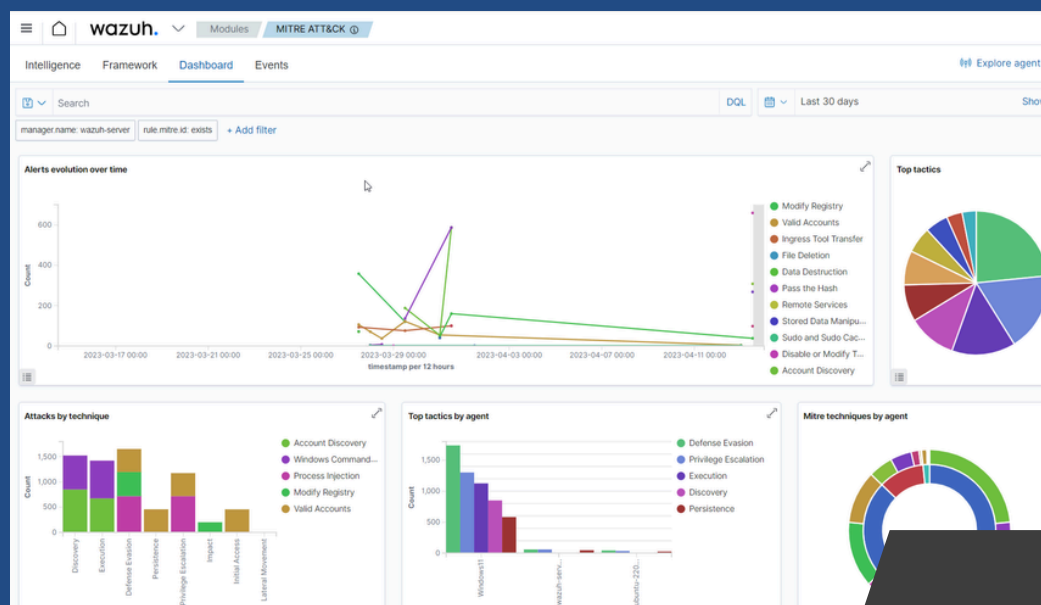


The screenshot shows the 'Create policy' form with the following sections:

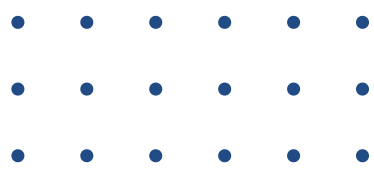
- Policy info**:
  - Policy ID**: A text input field containing 'hot\_cold\_workflow'.
  - Description**: A text area containing 'A sample description of the policy'.
- Error notification - optional**:
  - A text input field for an error notification.
  - A 'Manage channels' button.
- ISM templates - optional**:
  - A text input field for ISM templates.

## MITRE Framework

This tab provides an overview of the current state of your infrastructure with respect to known adversarial Tactics, Techniques, and Procedures (TTPs) in the MITRE ATT&CK framework. The dashboard displays key indicators such as the total number of events, alerts, and a summary of the top 10 TTPs detected within your environment.



# Contact Us



## Cases by type

My Cases

Open Cases

Open Incidents

Closed Cases



SENDER

Multiple Bruteforce Attempt

#4058-0987-2193



SENDER

URL Matched to Threat Intel

#4050-7261-9836

## Case Activity



Possible Malware De

Case Updated



Multiple Bruteforce A

Case Resolved



URL Matched to Thre

Case Updated



New Vulnerability De

Awaiting Response



+977 980-112-8471



sales@cryptogennepal.com



www.cryptogennepal.com



Naxal, Kathmandu, Nepal

# # Stay SayCure