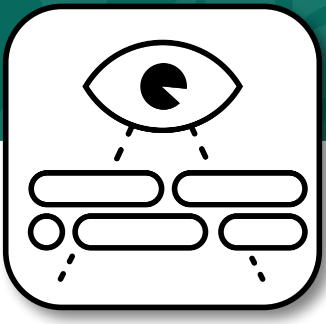
Judy's Blue Team:
Cloud SIEM + XDR

Judy Security

Powerful security built for SMBs. Judy makes it easy.



Meet Judy (and your new security team).

Get the protection you deserve—all at a price you can afford. Judy's Advanced and Premium subscriptions provide automated threat monitoring and remediation with a powerful Security Information and Event Management (SIEM) solution, along with a live team of security experts to protect your environment. Combined with Judy's next-gen Endpoint Detection and Response (EDR), you have access to a complete XDR solution—without the cost or hassle. It's streamlined, simplified security, without compromise.

We do the heavy lifting, so you can focus on building your business.

Built specifically for the needs and budgets of small and midsize businesses and their managed service providers, Judy delivers real-time visibility and reporting across your network and all of your cloud-based applications quickly, to detect and respond to threats around the clock.

Same Day Security

Get up and running in minutes (5x faster than the industry average and complete security coverage within hours.

Quickly Detect & Contain Threats

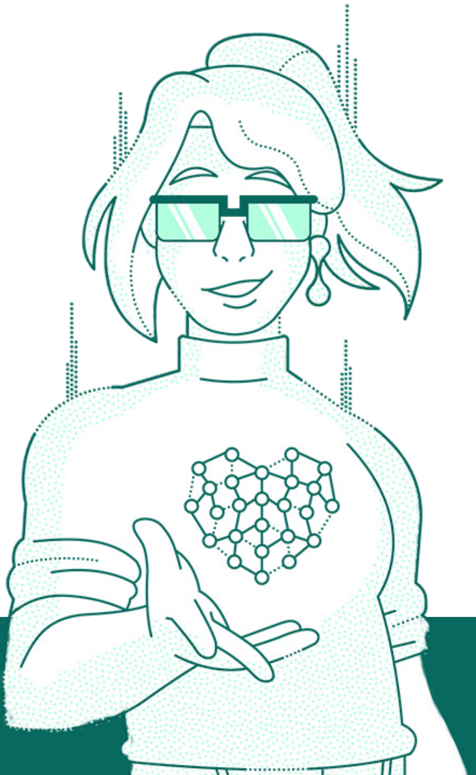
Behavior-based, 3-step detection and response cuts through the noise to prevent critical threats like ransomware and data breaches.

Unmatched Value

Streamline your offerings with threat detection and response as part of Judy's all-in-one security platform—priced per user, never data or devices.

Custom Reporting

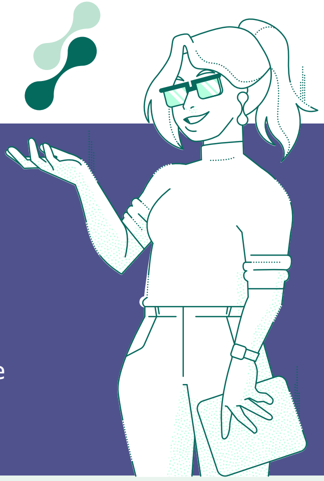
Get on demand access to the reporting you need to meet compliance and demonstrate a strong security posture.



Request a demo today to see Judy in action:
inquiries@judysecurity.ai | 800.918.9113
judysecurity.ai

Judy helps you simplify and automate threat protection.

Judy's Blue Team:
Cloud SIEM + XDR



Cloud SIEM Made Easy

Time to security is more critical than ever to quickly detect and contain threats. The powerful combination of Judy's automated platform and security experts enable you to respond to threats faster.

No hardware to deploy. No security expertise necessary. With our easy-to-use platform you'll be up and running in minutes, not days and weeks—using your existing team and infrastructure.

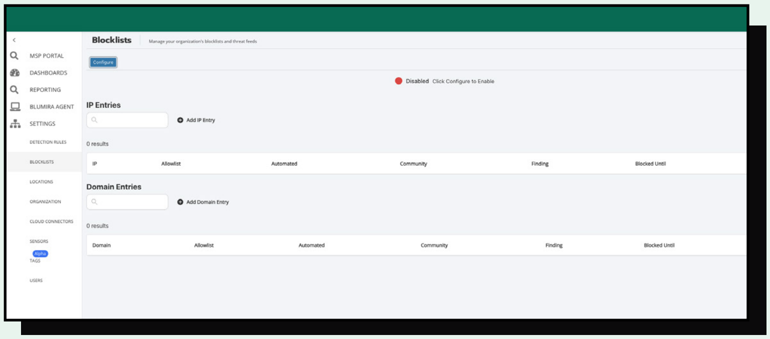
Rapid Response in 3 Steps

The faster you resolve and incident, the lower the impact

1. Automated Response

Block threats immediately

Get the fastest response times by blocking known threats automatically through Judy's platform, reducing manual remediation.



Blocklists Manage your organization's blocklists and threat feeds

Disabled Click Configure to Enable

IP Entries

0 results

IP	Allowlist	Automated	Community	Finding	Blocked Until

Domain Entries

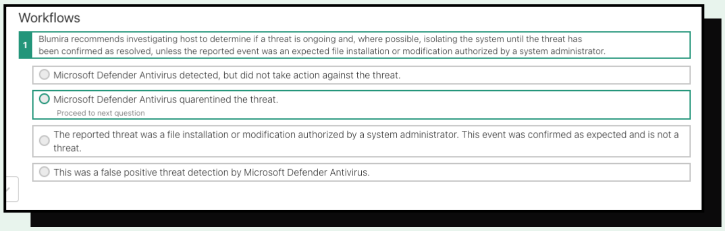
0 results

Domain	Allowlist	Automated	Community	Finding	Blocked Until

2. Playbooks

Guided, faster response

Get playbooks for every finding written by security experts for step-by-step instructions on how to respond—easy for anyone to understand.



Workflows

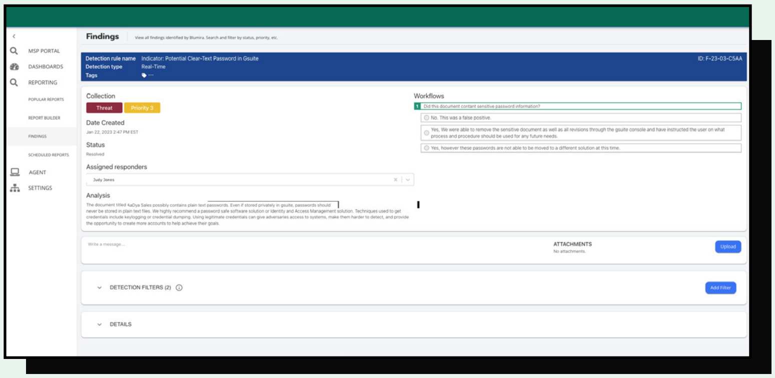
1 Blumira recommends investigating host to determine if a threat is ongoing and, where possible, isolating the system until the threat has been confirmed as resolved, unless the reported event was an expected file installation or modification authorized by a system administrator.

- ○ Microsoft Defender Antivirus detected, but did not take action against the threat.
- ○ Microsoft Defender Antivirus quarentined the threat.
  Proceed to next question
- ○ The reported threat was a file installation or modification authorized by a system administrator. This event was confirmed as expected and is not a threat.
- ○ This was a false positive threat detection by Microsoft Defender Antivirus.

3. Security Experts

Extend your security team

Our experienced and responsive security team is on standby to help answer questions, triage and assist with incident response. We continuously help improve your overall security posture.



Findings View all findings identified by Blumira. Search and filter by status, priority, etc.

Detection rule name: Indicator: Potential Clear-Text Password in Gsuite
Detection type: Real-Time
Tags
ID: F-23-03-C5AA

Collection: Threat, Priority 3

Date Created: Jan 22, 2023 2:47 PM EST

Status: Resolved

Assigned responders: Judy Jones

Analysis: The document titled AaDya Sales possibly contains plain text passwords. Even if stored privately in gsuite, passwords should never be stored in plain text files. We highly recommend a password safe software solution or Identity and Access Management solution. Techniques used to get credentials include keylogging or credential dumping. Using legitimate credentials can give adversaries access to systems, make them harder to detect, and provide the opportunity to create more accounts to help achieve their goals.

Workflows

1 Did this document contant sensitive password information?

- ○ No. This was a false positive.
- ○ Yes, We were able to remove the sensitive document as well as all revisions through the gsuite console and have instructed the user on what process and procedure should be used for any future needs.
- ○ Yes, however these passwords are not able to be moved to a different solution at this time.

Write a message...

ATTACHMENTS
No attachments.

Learn More About Judy's Blue Team: Cloud SIEM + XDR
inquiries@judysecurity.ai | 800.918.9113 | **judysecurity.ai**

Judy Security

Get Comprehensive Coverage of Real Threats.

Judy leverages threat intelligence and behavioral analytics to detect patters of attack, alerting you to high priority threats such as:

Cloud infrastructure threats

Common misconfigurations, modified security groups, malware indicating a compromised cloud instance, and attempts to connect with C2 (attacker-controlled) servers.

Identity-based attacks

Attempts to log in to your systems, including geo-impossible logins and fraudulent login attempts that could indicate the theft of usernames and passwords.

Email & document risks

Anomalous access attempts, external document sharing, email forwarding, and new inbox rules created by attackers.

Endpoint security threats

Malware, unknown or blacklisted applications, malicious executables, and compromised processes running on devices within your network.

Ransomware related risk

Judy detects indicators of a ransomware attack through any of the threats listed above then enables you to respond faster to prevent infection and a data breach.

Judy's Blue Team:
Cloud SIEM + XDR

What's Included:

1-year log retention for unlimited data

24/7 security operations support for critical issues

Detection rule management, allowlisting and customization

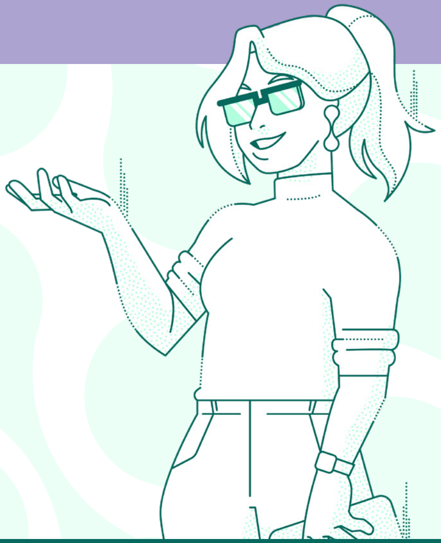
Automated blocking of threats with dynamic blocklists

Honeypots

Support for firewall and Windows/Linux logs

Custom and scheduled reporting

60+ integrations at no additional cost



Learn More About Judy's Blue Team: Cloud SIEM + XDR
inquiries@judysecurity.ai | 800.918.9113 | **judysecurity.ai**

Judy Security

How it works

Judy analyzes threats faster to prevent breaches

1. User onboarding & log transmission

Sign up

Collect logs

2. Data processing & threat protection

Parse Data

Deploy Rules

Analyze threats

Surface Findings

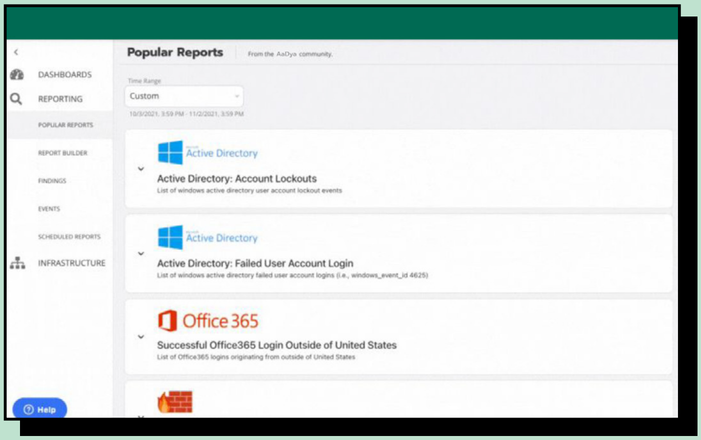
3. Three-step response

SOC Support

Playbooks

Block Threats

Actionable, Automated Threat Detection & Response



Popular Reports From the AaDya community.

Time Range: Custom

10/3/2021, 3:59 PM - 11/2/2021, 3:59 PM

Active Directory

Active Directory: Account Lockouts

List of windows active directory user account lockout events

Active Directory

Active Directory: Failed User Account Login

List of windows active directory failed user account logins (i.e., windows_event_id 4625)

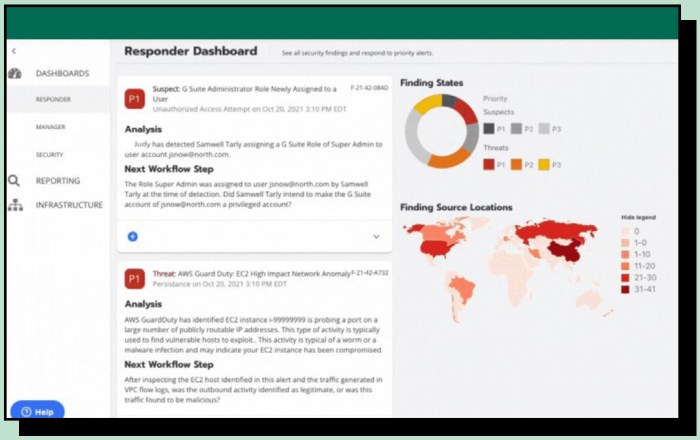
Office 365

Successful Office365 Login Outside of United States

List of Office365 logins originating from outside of United States

- Scheduled security reporting is included to help you meet compliance
- Drill down into account lockouts, failed user logins and more
- Click-through dashboards provide customizable search through your data, filtered by data source

Easy-to-Use Security Reports With Click-Through Dashboards



Responder Dashboard See all security findings and respond to priority alerts.

P1 Suspect: G Suite Administrator Role Newly Assigned to a User F-21-42-084D

Unauthorized Access Attempt on Oct 20, 2021 3:10 PM EDT

Analysis

Judy has detected Samwell Tarly assigning a G Suite Role of Super Admin to user account jsnow@north.com.

Next Workflow Step

The Role Super Admin was assigned to user jsnow@north.com by Samwell Tarly at the time of detection. Did Samwell Tarly intend to make the G Suite account of jsnow@north.com a privileged account?

P1 Threat: AWS Guard Duty: EC2 High Impact Network Anomaly F-21-42-A732

Persistance on Oct 20, 2021 3:10 PM EDT

Analysis

AWS GuardDuty has identified EC2 instance i-99999999 is probing a port on a large number of publicly routable IP addresses. This type of activity is typically used to find vulnerable hosts to exploit.. This activity is typical of a worm or a malware infection and may indicate your EC2 instance has been compromised.

Next Workflow Step

After inspecting the EC2 host identified in this alert and the traffic generated in VPC flow logs, was the outbound activity identified as legitimate, or was this traffic found to be malicious?

- Meaningful findings give you a full analysis of the threat
- Workflows for every finding tell you how to respond
- Matched evidence gives you related information to help with investigation

Learn More About Judy's Blue Team: Cloud SIEM + XDR

inquiries@judysecurity.ai | 800.918.9113 | **judysecurity.ai**

Judy Security

How it works

Judy Integrates With Any Service

Cloud Infrastructure

Microsoft Azure · Microsoft Active Directory · okta · DUO · aws

Endpoint

Judy · Carbon Black. · SentinelOne · CROWDSTRIKE · eset · TREND MICRO · SOPHOS · Symantec. · Malwarebytes · BlackBerry CYLANCE

Productivity

Microsoft 365 · G Suite · proofpoint. · FORCEPOINT · CISCO Umbrella

Host

Windows Server · Windows · Microsoft Active Directory · Linux · FORTINET

Firewall

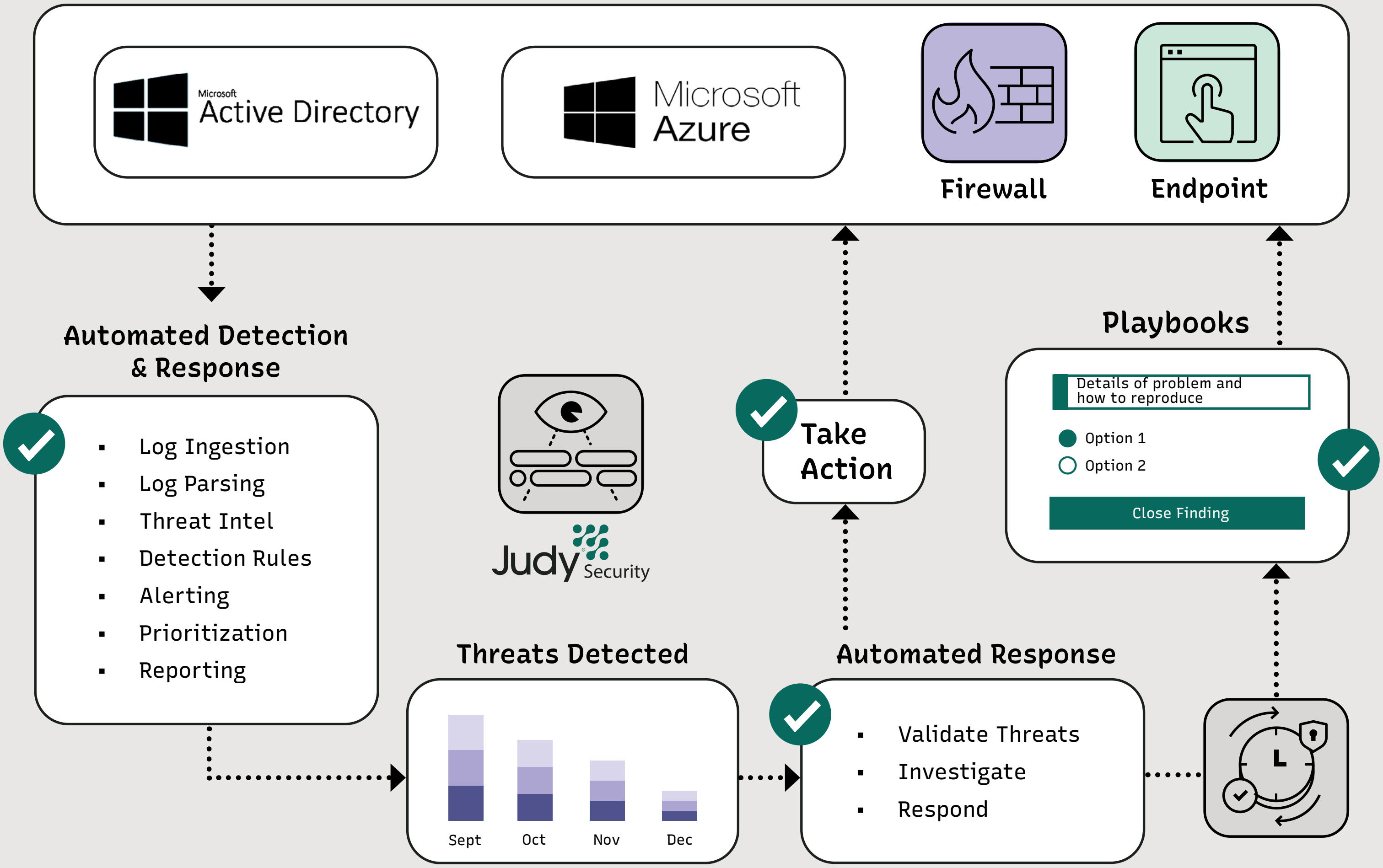
paloalto NETWORKS · FORTINET · CISCO · Meraki · CHECK POINT · SOPHOS · CITRIX

Additional Integrations

osquery · APACHE · NGINX · Mac OS · FORESCOUT · Windows Defender · proofpoint. · vmware · logstash · PhishER

How it works

Judy's Detection & Response



Automated Detection & Response

- Log Ingestion
- Log Parsing
- Threat Intel
- Detection Rules
- Alerting
- Prioritization
- Reporting

Threats Detected

Automated Response

- Validate Threats
- Investigate
- Respond

Take Action

Playbooks

Details of problem and how to reproduce

● Option 1

○ Option 2

Close Finding

5x faster to deploy.

We take care of all SIEM setup, automating tasks for our customers:

- Data parsing across integrations
- Fine-tuning to reduce noise and alert fatigue
- Rule development for the latest threats
- Finding analyses and gathering data
- Prioritize findings by severity

Learn More About Judy's Blue Team: Cloud SIEM + XDR
inquiries@judysecurity.ai | 800.918.9113 | **judysecurity.ai**

Judy Security