



Judy's Blue Team:  
Cloud SIEM + XDR

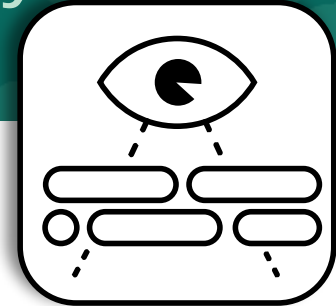
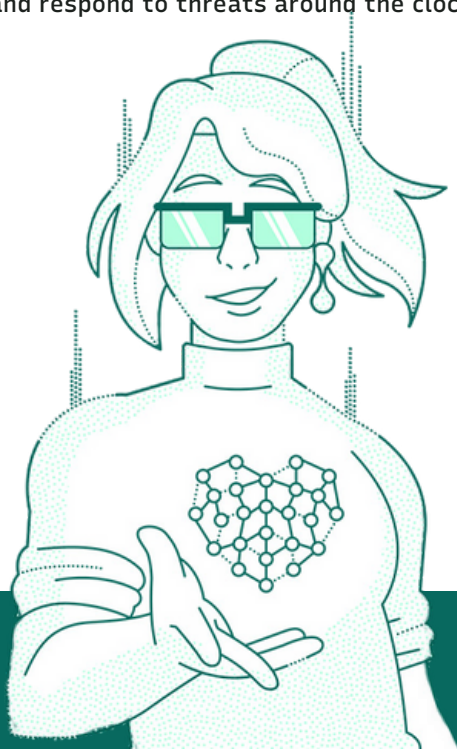
# Powerful security built for SMBs. Judy makes it easy.

## 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.

### 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:**

Name, Title | Your Company Name

Phone: XXX | Email: XXXX

# Judy helps you simplify and automate threat protection.

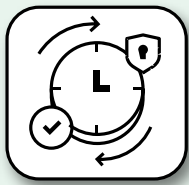
Judy's Blue Team:  
Cloud SIEM + XDR



## 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.



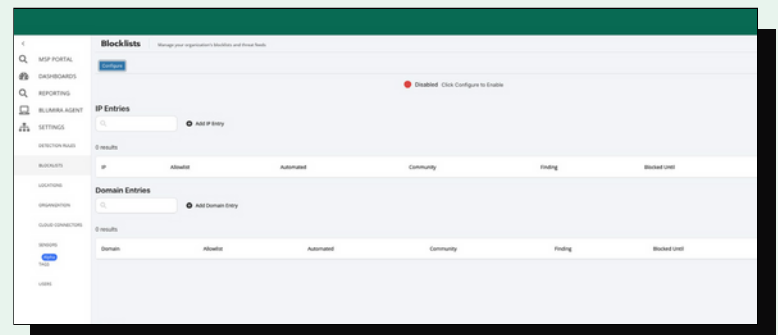
## Rapid Response in 3 Steps

The faster you resolve and incident, the lower the impact

### 1. Automated Response

#### Block threats immediately

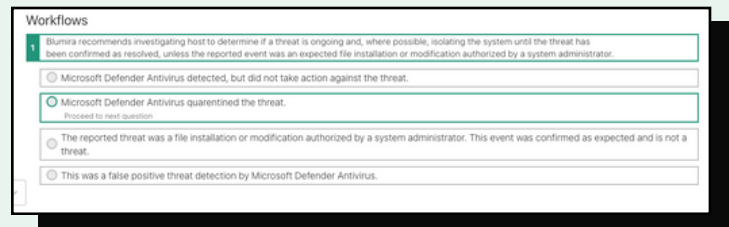
Get the fastest response times by blocking known threats automatically through Judy's platform, reducing manual remediation.



### 2. Playbooks

#### Guided, faster response

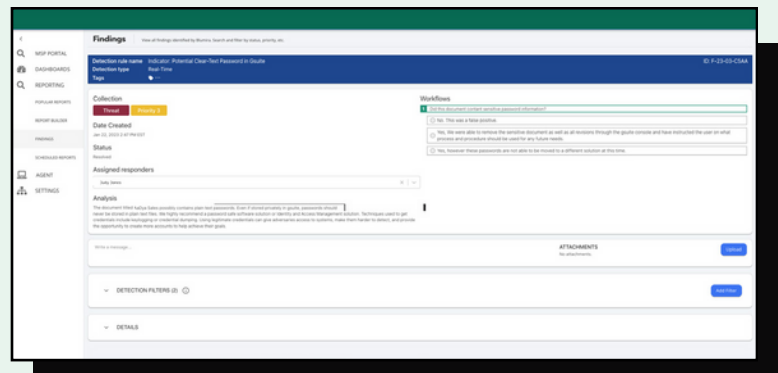
Get playbooks for every finding written by security experts for step-by-step instructions on how to respond—easy for anyone to understand.



### 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.



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

Name, Title | Your Company Name

Phone: XXX | Email: XXXX

# Get Comprehensive Coverage of Real Threats.

Judy leverages threat intelligence and behavioral analytics to detect patterns 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

Name, Title | Your Company Name

Phone: XXX | Email: XXXX

# How it works

## Judy analyzes threats faster to prevent breaches

### 1. User onboarding & log transmission



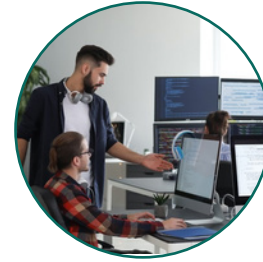
Sign up



Collect logs



### 2. Data processing & threat protection



Parse Data

Deploy Rules

Analyze threats

Surface

Findings

### 3. Three-step response



SOC  
Support

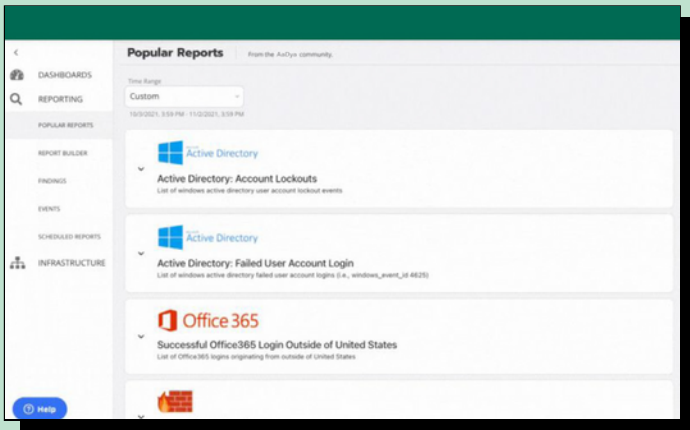


Playbooks



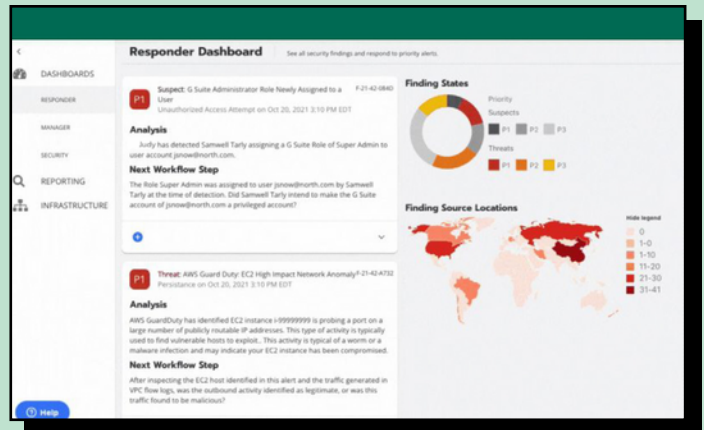
Block  
Threats

## Actionable, Automated Threat Detection & Response



- 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



- 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

Name, Title | Your Company Name

Phone: XXX | Email: XXXX

# How it works

Judy's Blue Team:  
Cloud SIEM + XDR

## Judy Integrates With Any Service

### Cloud Infrastructure



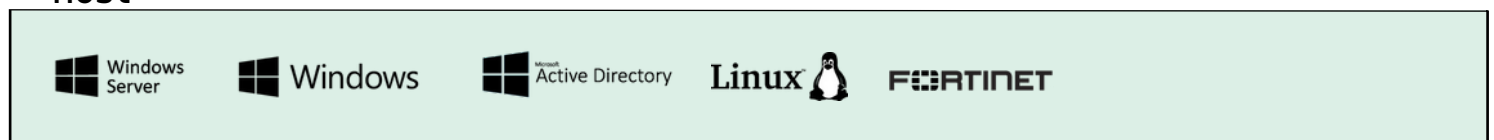
### Endpoint



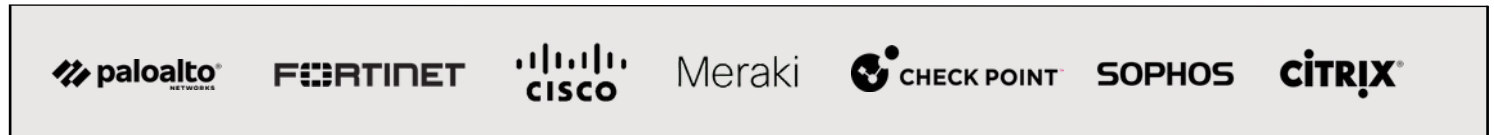
### Productivity



### Host



### Firewall



### Additional Integrations



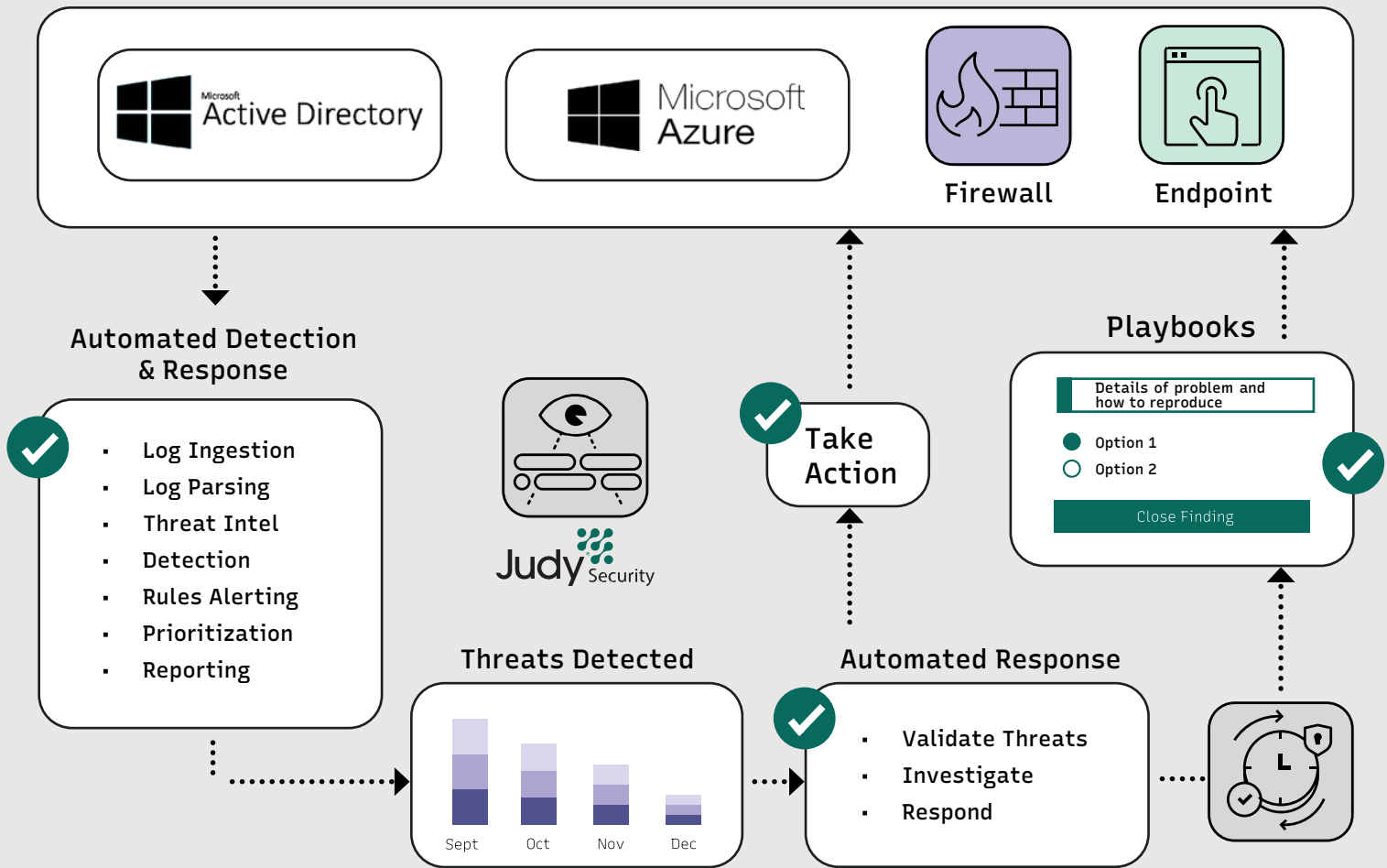
Learn More About Judy's Blue Team: Cloud SIEM + XDR

Name, Title | Your Company Name

Phone: XXX | Email: XXXX

# How it works

## Judy's Detection & Response



### 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

Name, Title | Your Company Name

Phone: XXX | Email: XXXX

