

Active Response Made for the Cloud



True 24/7 MDR Securing Your Cloud

To support the growing shift to hybrid and cloud environments, we've added an industry-leading solution to our security stack. Cloud Response takes the power and effectiveness of our proprietary managed detection and response (MDR) technology and extends it to your cloud.

Focus on your day-to-day operations knowing that our 24/7 security operations center (SOC) leverages MDR to safeguard your cloud platform. While most solutions on the market alert you or your MSP to take action, Cloud Response provides fast, active response to adversarial threats on your behalf.

Currently, Cloud Response supports:

- **Microsoft 365:** Azure Active Directory (AD), Exchange, and SharePoint
- **Google Workspace:** Google Account and Gmail



The Criticality of Security for the Cloud

Businesses continue to take the digital journey, moving their workloads to the cloud at a rapid pace. Many organizations are using the cloud as a conduit for growth as it increases flexibility and productivity, along with reduced operating costs.

However, with the rising rate of cloud adoption and prominence of remote work, the need for robust security tailor-made for cloud technology must rise as well. In fact, we have found that cloud environments are targeted nine times more often than on-premises environments. With that, organizations' top challenges include data loss, privacy and compliance issues, and compromised credentials and resources.

Email makes up 98% of the vectors for social engineering incidents.

Verizon 2023 Data Breach Investigations Report

79% consider cloud security as their primary challenge.

Resmo

The average data breach cost for organizations using a public cloud is \$5.02m.

Resmo

See your cloud infrastructure actively secured



THE POWER OF MDR FOR YOUR CLOUD

Get peace of mind with Cloud Response which extends our MDR technology and expert SOC analysts to the cloud. Know that you are protected against even the fastest, most advanced types of cyberthreats targeting your third-party cloud platform.



ACTIVE MONITORING & RESPONSE

Cloud Response allows the 24/7 SOC to provide immediate response to adversarial threats. Rather than alerting you to take action, we take decisive actions against any malicious activity on your behalf. Trust active monitoring and unified response to protect your cloud.



STREAMLINED SETUP & ONBOARDING

Simple setup? Check. Cloud Response is seamlessly integrated with our MDR technology making the onboarding process simple. In just one day, you'll have Cloud Response guarding one of the most critical IT systems your business uses.

Why Cloud Response?

- Extends our MDR capabilities into Microsoft 365 and Google Workspace cloud environments.
- Enables our 24/7 security operations center (SOC) to see contextual data within your cloud environment and provide immediate and active response against anomalous behavior.
- Allows you to set up policy features to implement cyber hygiene processes across all users and monitor events through custom notifications.

Our Cloud Response web application has the following abilities:

MICROSOFT 365

- Manage your Microsoft Azure AD and Exchange policies
- Control and customize Azure AD, Exchange, and SharePoint event email notifications across a tenant
- Set up alerts for malicious login analytics
- Set up detection alerts for malicious email forwarding rules
- Enable our SOC's ability to disable an account, should a threat arise
- Control and customize individual user event email notifications within a specific tenant, including future travel dates.

GOOGLE WORKSPACE

- Malicious Google Account login analytics, such as Login from Unapproved Country and Suspicious Login
- Malicious Gmail detections, such as Suspicious Email Filter Rule Creation and External Email Forwarding Rule Created
- The ability to respond and disable a Google Account

Your Partner in Protection

Ready to bring active response to your cloud workflows?

► **Get started today by contacting me via phone or email.**

