Infocyte Cloud Security Use Cases

INFOCYTE FOR AWS

Infocyte

If they try it, we'll stop it.

INFOCYTE DETECTION AND RESPONSE FOR AWS

Infocyte is an agentless detection and incident response platform for cloud workloads and AWS cloud management layer. Using automated forensic inspection of cloud workloads (Microsoft Windows and Linux-based EC2 instances) and continuous IAM/ CloudTrail activity auditing, Infocyte's platform helps cloud operations and security teams proactively expose, investigate, and eliminate threats and vulnerabilities resident in their AWS or hybrid cloud environments.

With Infocyte, security teams and incident responders can quickly discover, inventory, inspect, detect, and respond to security incidents on AWS workloads — without installing agents, deploying containers, or navigating the AWS Console. Infocyte's live memory analysis, deep forensic inspection, and agentless workload interactions are designed to have minimal impact on network operations. Optionally, schedule Infocyte to run during off-peak hours or during maintenance windows without loss of efficacy.

Infocyte Detection and Response for AWS is optimized for organizations with their own SOC or partners offering security services. Your SOC benefits from our platform and KPI Dashboard which tracks improvements in mean time to detect (MTTD), mean time to respond (MTTR), attacker dwell time, and more.

Optimized for the dynamic nature of cloud environments, this product is licensed by the number of inspections per month (not related to host/instance count).

INFOCYTE MANAGED DETECTION AND RESPONSE FOR AWS

License: Command Edition

Infocyte MDR for AWS Command Edition subscribers have all the same benefits of our standard Detection and Response for AWS platform, with the additional benefit of a managed service. Subscribers have 24x7 access to Infocyte's Security Operations Center (SOC) and global network of certified partners, via support ticket, email, phone, and/or in-app chat. Our team of experts detect, analyze, respond to, report on, and prevent cybersecurity incidents.

Infocyte MDR for AWS: Command Edition includes managed services to support your security team: Incident Notification, Managed Detection, Malware Analysis, Incident Response, and Post-incident Certification to confirm your environment is secure. Optimized for the dynamic nature of cloud environments, this product is licensed by the number of inspections per month (not related to host/instance count).

INFOCYTE MANAGED DETECTION AND RESPONSE FOR AWS

License: Incident Response & Assessments

Infocyte's Incident Response & Assessment edition includes all of the same benefits of our Managed Detection and Response for AWS. IR and Assessment edition is optimized for security teams and incident responders during the critical time when you require immediate validation of a security incident or breach. Infocyte helps security teams and incident responders discover, inventory, inspect, detect, and respond to security incidents on AWS workloads and hybrid cloud environments without installing agents, deploying containers, or navigating the AWS Console. You have 24x7 access to Infocyte's SOC via support ticket, email, phone, and/or chat. Our security analysts are supported by a global network of certified partners.

Infocyte MDR for AWS: Incident Response & Assessment edition is optimized for a short duration effort by security teams focused on an incident response or during a threat and compromise assessment. Each licensed host/instance includes continuous AWS IAM / CloudTrail activity auditing and inspections over a 30-day license, enabling post-incident certification to confirm your environment is secure.

PHONE: 844.463.6298

EMAIL: sales@infocyte.com