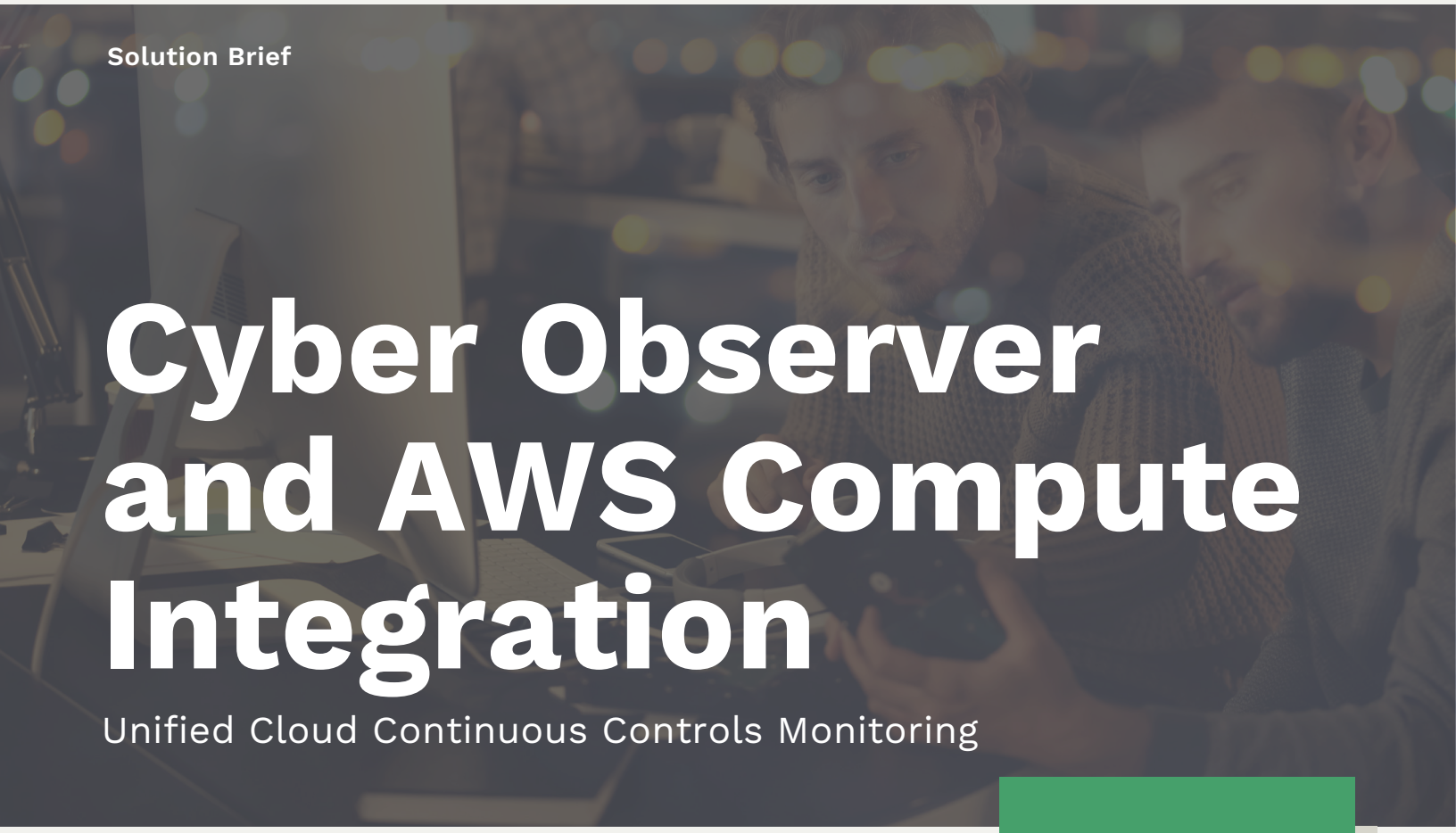
Cyber Observer Technology Partners

CYBER OBSERVER

aws



Solution Brief

Cyber Observer and AWS Compute Integration

Unified Cloud Continuous Controls Monitoring

Challenge

Today's challenging cybersecurity landscape offers an over-abundance of cybersecurity tools. As the number of breaches proliferates, so have the solutions and technologies designed to stop them. The state of cybersecurity is not getting easier to manage, despite enterprises and organizations worldwide spending more money than ever on new technologies and solutions.

Designed for CISOs and senior InfoSec managers (such as CIOs, C-level managers, risk officers, SOC managers and IT Infrastructure personnel), Cyber Observer empowers leadership with a **unified dashboard** of their entire cybersecurity ecosystem. Cyber Observer can be fully deployed within an enterprise in a few hours, enabling easy **identification** of **weaknesses**, **reduction of mean-time-to-detect (MTTD)**, **prevention of breaches**, and advancement of your organization's **cybersecurity posture** and **maturity**.

Solution

Cyber Observer's partnership with AWS enables CISOs to better manage their cybersecurity ecosystem. They receive alerts from Cyber Observer on the key aspects and issues in AWS Compute such as **EC2**, **Elastic Kubernetes Service (EKS)**, **SageMaker**, **CodeBuildand** more. This joint effort helps enterprises manage their AWS cybersecurity environment and **continuously monitor their cybersecurity ecosystem posture**.

KEY FEATURES

- Identifies cybersecurity tools that are misconfigured and malfunctioning, or missing
- Finds security gaps and provides recommendations for fixing
- Builds an ongoing security program to ensure alignment with new threats
- Uses continuous analytics to send alerts when there are deviations from normal behavior
- Automatic reporting

CYBER OBSERVER

aws

The integration between Cyber Observer and AWS offers CxOs powerful and effective **resilience visibility** along with **compliance validation** and **controls**, to secure and monitor AWS Compute in an unprecedented manner.

Cyber Observer deploys to the corporate network automatically, in a matter of a few hours, predefined with security domains and CSC measurements to deliver three unique cybersecurity ecosystem views:

- First, it provides organizations with the best indicators of the cybersecurity tools that may be **misconfigured**, **malfunctioning**, or **lacking** and should be added to provide complete cybersecurity protection.
- It then **reveals the security gaps** that exist in each security domain and **delivers continuous proactive recommendations to close these gaps**.
- Finally, Cyber Observer's machine learning analytics engine continuously calculates online measurements that represent normal behavior, and then **alerts when a deviation from normal behavior is detected**.

Fast and Secure Deployment

The Cyber Observer connector for AWS Compute receives security and configuration data from the AWS server via a secure REST API.

CYBER OBSERVER

aws

Key Features & Benefits of This Integration

- **Cyber Hygiene Analysis and Reporting for Managers:** Alerts and reporting regarding AWS Compute current configuration implementation status based on the vendor's and security standards best-practices, including security configuration issues, incidents and investigations management, admins and roles administration and more.
- **Reduced Incident Analysis Time:** Cyber Observer provides continuous alerts on deviation from normal behavior in terms of AWS Compute implementation and effectiveness as well as continuous monitoring of relevant security issues in near real-time.
- **Continuous Incident Response:** Provides the CISO and other relevant managers in the organization, as well as the AWS Compute technical owners with continuous mitigation recommendation and steps to improve, for securing and monitoring AWS implementation, effectiveness, maturity and resilience from a management perspective in an unprecedented manner.
- **Customizable Views and Reports:** Cyber Observer is highly customizable – all views and reports could be modified to the organization's needs and structure. The integration between Cyber Observer and AWS Compute offers CxOs a powerful effectiveness and resilience visibility, as well as compliance validation and controls.

Key Use Cases

1 Detailed information regarding mis-configured and insecure EC2s

- Number of EC2 network interfaces
- EC2 network interfaces with undefined name
- EC2 instances stopped for more than X minutes/hours/days
- Number of EC2 instances without IAM
- role
- EBS volumes not encrypted
  EBS snapshots publicly restorable

2 Detailed information regarding misconfigured and insecure AWS Lambda

- Number of lambda functions without
- tracing
- Lambda functions not assigned to access within VPC
- Lambda functions not prohibiting public access by other accounts
- Lambda functions with public access

3 Detailed information regarding mis-configured and insecure EKSs

- EKS clusters associated with security groups that allow any inbound traffic other than HTTPS
- EKS clusters associated with security groups that allow any outbound traffic other than HTTPS
- EKS clusters without control plane logs enabled
- EKS clusters endpoints publicly accessible

About AWS

Amazon Web Services (Nasdaq: AWS) is the world's most comprehensive and broadly adopted cloud platform, offering over 200 fully-featured services from data centers globally. Millions of customers—including the fastest-growing startups, largest enterprises, and leading government agencies—are using AWS to lower costs, become more agile, and innovate faster.

AWS is architected to be the most flexible and secure cloud computing environment. AWS supports 90 security standards and compliance certifications, and all 117 AWS services that store customer data offer the ability to encrypt that data.

About Cyber Observer

Cyber Observer is the premier critical controls monitoring (CCM) solution that simplifies the way cybersecurity tools are monitored and managed. Cyber Observer integrates hundreds of popular cybersecurity tools into a single intuitive interface that enables security and risk management executives to continuously monitor their security tools and improve their cybersecurity posture in alignment with cybersecurity, business, and regulatory frameworks.
Learn more at **cyber-observer.com**.