AWS Security and Networking

Configuration and Vulnerability Analysis

aws marketplace

DevSecOps

Overview

Configuration and Vulnerability Analysis

Effectively monitoring and managing cloud infrastructure configuration changes and performing on-going vulnerability analyses through forensics, troubleshooting, audits, and automation are key activities to help secure your AWS environment.

Table of Contents

In order to help maintain security with your AWS solution, it's important to make sure that your organization is on top of managing configuration settings and changes, and is performing necessary vulnerability analyses. You need a detailed view of the configuration of AWS resources in your AWS account. This includes how the resources are related to one another and how they were configured in the past so that you can see how the configurations and relationships change over time.

Specifically, your organization will want to be able to:

Evaluate your AWS resource configurations for desired settings.

Get a snapshot of the current configurations of the supported resources that are associated with your AWS account.

Retrieve configurations of one or more resources that exist in your account.

Receive a notification whenever a resource is created, modified, or deleted.

View relationships between resources. For example, you might want to find all resources that use a particular security group.

In addition, conducting ongoing vulnerability analysis and assessment is a key activity for securing your AWS environment. You should assess the security of your AWS resources via forensics, troubleshooting, and active auditing either as you progress through the development of your infrastructure or on a regular basis in a stable production environment. Automating activities for the overall security and vulnerability assessment of your infrastructure will allow you to focus on more complex security problems.

General Focus Areas

Configuration & Change Management

When you run your applications on AWS, you usually use AWS resources, which you must create and manage collectively. As the demand for your application keeps growing, so does your need to keep track of your AWS resources. Being aware of how change affects a system allows you to plan proactively, and monitoring allows you to quickly identify trends that could lead to capacity issues or service-level agreement (SLA) breaches. In traditional environments, change-control processes are often manual and must be carefully coordinated with auditing to effectively control who makes changes and when they are made.

Using AWS, you can monitor the behavior of a system and automate the response to key performance indicators (KPIs). For example, by adding additional servers as a system gains more users, you can control who has permission to make system changes and audit the history of these changes.

When you architect a system to automatically add and remove resources in response to changes in demand, this not only increases reliability but also ensures that business success doesn't become a burden. With monitoring in place, your team will be automatically alerted when KPIs deviate from expected norms. Automatic logging of changes to your environment allows you to audit and quickly identify actions that might have impacted reliability. Controls on change management ensure that you can enforce the rules that deliver the reliability you need.

Finally, you might be working with data that requires frequent audits to ensure compliance with internal policies and best practices. To demonstrate compliance, you need access to the historical configurations of your resources, thus configuration and change management is again important.

Vulnerability Analysis

Every Information Security Management System (ISMS) must ensure regular reviews of the effectiveness of security controls and policies.

To guarantee the efficiency of controls against new threats and vulnerabilities, and to ensure that the infrastructure is protected against attacks, verifying existing controls is key, and doing so requires testing.

AWS customers should undertake a number of test approaches:

- External Vulnerability Assessment: A third party evaluates system vulnerabilities with little or no knowledge of the infrastructure and its components.
- External Penetration Tests: A third party with little or no knowledge of the system actively tries to break into it, in a controlled fashion.
- Internal Gray/White-Box Review of Applications and Platforms: A test engineer who has a sound understanding of the system validates the efficiency of controls in place, or evaluates applications and platforms for known vulnerabilities.

This testing should cover the network, file system, and process activity within the specified target. A wide set of activity and configuration data should be collected, including details of communication with AWS services, use of secure channels, details of the running processes, network traffic among the running processes, and more. The collected data should be correlated, analyzed, and compared to a set of specified security rules. A completed test assessment run produces a list of findings—potential security problems of various severity—that should be remediated.

Solution Highlight: Alert Logic

Alert Logic Threat Manager with ActiveWatch allows you to continuously assess your attack surface with unlimited internal and external vulnerability scans. Security experts monitor your environment 24x7x365 so you can focus on your business. Out-of-band IDS avoids chokepoints to application performance and availability, while lightweight agents self-configure upon deployment and register/deregister for no-touch support of Auto Scaling.

Tips from the Pros

Real-World Advice from Experts that Live Cloud Everyday

Cloudticity

Cloudticity helps healthcare organizations leverage ground breaking automation and cloud expertise to design, build, and manage HIPAA-compliant solutions on the public cloud

To minimize vulnerability, you definitely need a strong defense with an in-depth, multi-layered approach to security. So you need to lock the house but also make sure that you've got an alarm. Make sure that if the alarm goes off, that people are notified. Make sure that if people are notified, there are standard operating procedures that are followed. Leverage new technology like machine learning to automatically identify anomalous behavior. An overall layered threat prevention infrastructure is very important.

In addition, when systems become vulnerable to be easily exploited, it is usually not technical factors, but rather by social engineering means. To help mitigate this issue, we hire an outside company that periodically calls my team and pretends to be somebody else, trying to get them to reveal information, passwords, and secrets – that sort of thing.

So, it's a multi-layered security approach, and continuous testing and training of appropriate behaviors when you're managing a secure environment, that are critical for maintaining resilience to the big, bad world that we live in these days.

Gerry Miller, Founder/CEO/CTO

Key Insight

Automation is Important

Because many IT security breaches are attributable to human error, automation is therefore key to maintaining a robust cloud security infrastructure. Automated software-based security mechanisms for both configuration management and vulnerability assessments, improve your ability to securely scale more rapidly and cost effectively.

Some other security-related automation suggestions include:

Set-up automated monitoring. Monitoring metrics should be used to raise alarms when thresholds are breached.

Mitigate deployment risks using automated deployments and patching when possible.

Treat operations procedures as code, and automate procedures where appropriate.

Use automatically-scalable services such as Amazon S3, Amazon CloudFront, Auto Scaling, Amazon DynamoDB, AWS Elastic Beanstalk, etc.

Set up automated response for when failure is detected (e.g., need to replace failed components).

Automate backups using AWS features, AWS Marketplace solutions, or third-party software.

Tips from the Pros

Real-World Advice from Experts that Live Cloud Everyday

Dome9

Dome9's SaaS platform allows enterprises to visualize and assess the network security posture, detect misconfigurations, actively protect against attacks, and conform to security best practices and compliance requirements across hybrid clouds

> *It's important to make sure that you have the right configurations in place to implement the security posture that you want. This is the challenge that faces a lot of enterprises. If you look at all the data exposures, at least once a week we have seen someone expose very sensitive data to the outside world. This is not surprising when you have hundreds of knobs to turn (essentially configurations and parameters that you need to set in your environment) in order to implement and maintain security posture. Really, if you try to do this manually, if you try to go set it, it's going to be easy to make mistakes.*
>
> *We have seen that time and again. It's not a problem of not knowing what to do. It's just that when you have a lot of different things to configure, it's a problem of scale and it's easy to get something wrong when it's done manually. So, really what you need are automated tools that help you manage configurations, identify vulnerabilities, and that are able to go and set the right parameters and fix any misconfigurations before they become exposures or breaches.*

CloudCheckr

Developed by a team of first-adopter cloud security practitioners, the Evident Security Platform (ESP) is a comprehensive platform for identifying and remediating security in the cloud. ESP operates as a continuous, automated solution that identifies, in real-time, when organizations are out of compliance and not adhering to security best practices.

> *There is just a consistent lack and shortage of skilled security experts and resources. It is a problem across the globe. We can't depend on manual intervention for everything. Not only do we have to automate the monitoring and alerting of all our configurations and settings, but we also have to automate the remediation and fixing of these things when problems occur*
>
> Steve Hall, Vice President of Strategic Marketing

Cloudticity

Cloudticity helps healthcare organizations leverage ground breaking automation and cloud expertise to design, build, and manage HIPAA-compliant solutions on the public cloud

> *The number one thing that to focus on to prevent threats is automation, because people make mistakes and almost every successful hack attempt is the result of a human error. The recent Equifax hack was based on somebody forgetting to patch an Apache Struts vulnerability. People forget to change default passwords. People manually configure firewall rules and forget to close a port. That is far and away the single biggest factor to successful penetrations and so, you need to approach things by saying "We're going to have hardened, tested templates that we're never going deploy by human fingers, we're only going to deploy with automation." And because humans are taken out of the equation, it's significantly less likely that human errors will leave vulnerabilities in place.*
>
> *And the cool thing with AWS, everything is automatable. There's literally nothing you can't do by writing code.*
>
> Gerry Miller, Founder/CEO/CTO

Evident.io

Developed by a team of first-adopter cloud security practitioners, the Evident Security Platform (ESP) is a comprehensive platform for identifying and remediating security in the cloud. ESP operates as a continuous, automated solution that identifies, in real-time, when organizations are out of compliance and not adhering to security best practices.

> *Enterprise cloud risk is a result of a mix of things, including poor management of configurations and settings of cloud resources, the absence of rigorous policies, and lack of insight into security controls. To really create a defensible security posture, DevOps principles need to be applied across all aspects of the cloud environment so security is continuously validated and applied. This ultimately gives your organization greater control over your data and operations.*
>
> Michaline Todd, Vice President of Marketing

Specific Solutions

Managing Change and Assessment

Configuration Management

To exercise better governance over your resource configurations and detect resource misconfigurations, you need fine-grained visibility into what resources exist and how these resources are configured at any time. You'll want to set-up automation to:

- Notify you whenever resources are created, modified, or deleted without having to monitor these changes by polling the calls made to each resource.
- Continuously evaluate the configuration settings of your AWS resources as they are created, changed, or deleted, while flagging violations if a resource is noncompliant and sending notifications.
- View how resources you intend to modify are related to other resources and assess the impact of your change.

To analyze potential security weaknesses, you need detailed historical information about your AWS resource configurations, such as the AWS Identity and Access Management (IAM) permissions that are granted to your users, or the Amazon EC2 security group rules that control access to your resources.

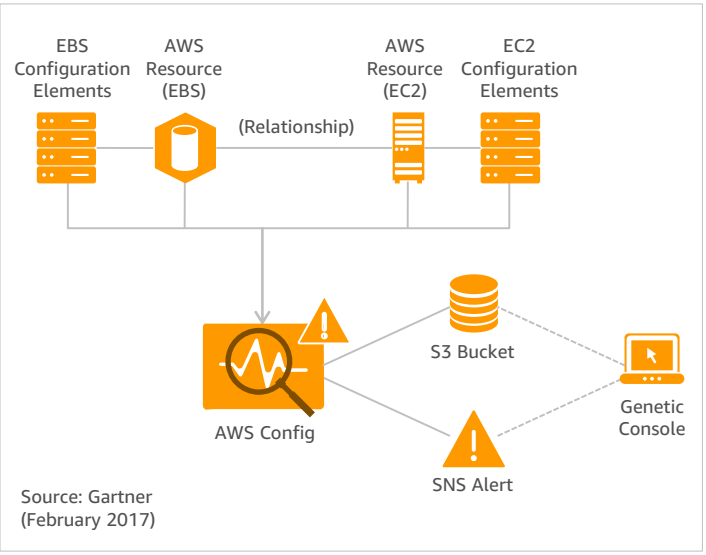
For example, you may want to view the IAM policy that was assigned to an IAM user, group, or role at any point in time. This information can help you determine the permissions that belonged to a user at that specific time: for example, you can view whether the user John Doe had permission to modify Amazon VPC settings on Jan 1, 2015.

You'll also want to view the configuration of your EC2 security groups, including the port rules that were open at a specific time. This information can help you determine whether a security group blocked incoming TCP traffic to a specific port.

Overall, you'll want to implement a change and configuration management system and processes that allow:

- **Continuous configuration change monitoring, recording, and inventory of your AWS resources**, as well as software configurations within EC2 instances at any point in time.
- **Continuous auditing and assessment** of the overall compliance of your AWS resource configurations with your organization's policies and guidelines.
- **Definable rules** for provisioning and configuring AWS resources.
- **Tracking of relationships** among resources and review resource dependencies prior to making changes.

"One of the more powerful assessment tools available from AWS is AWS Config. The power of AWS Config comes from its ability to identify resource inventory, keep configuration history and provide notification when configurations are changed. AWS Config also allows customers to write their own logic and rules to be applied against configurations of AWS services beyond what AWS itself provides." – Gartner



Vulnerability Analysis

Analyzing security vulnerabilities has a lot to do with identifying and mitigating risk. In fact, there are even ways to score and quantify the severity of risk. For example, the Common Vulnerability Scoring System (CVSS) provides a way to characterize vulnerabilities and quantify severity with a numerical score. Translating this quantitative score into qualitative representations of risk such as low, medium, and high can help assess and prioritize risk.

In order to get to the point of understanding security risks at that level, you should select a risk assessment methodology based on input from groups in your organization about the following factors:

- Business needs
- Information security requirements
- Information technology capabilities and use
- Legal requirements
- Regulatory responsibilities

Because all cloud infrastructure operates differently from legacy environments, it is critical to set criteria for accepting risks and identifying the acceptable levels of risk (risk tolerances). We recommended starting with a risk assessment and leveraging automation as much as possible. AWS risk automation can narrow down the scope of resources required for risk management.

There are several risk assessment methodologies, including OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), ISO 31000:2009 Risk Management, ENISA (European Network and Information Security Agency), IRAM (Information Risk Analysis Methodology), and NIST (National Institute of Standards & Technology) Special Publication (SP) 800-30 rev.1 Risk Management Guide.

We recommend that you create a risk register by mapping all of your assets to threats, and then, based on the vulnerability assessment and impact analysis results, creating a new risk matrix for each AWS environment.

Here is an example risk register:

- Assets
- Threats to those assets
- Vulnerabilities that could be exploited by those threats
- Consequences if those vulnerabilities are exploited

We also recommend that you analyze and evaluate the risk by calculating business impact, likelihood and probability, and risk levels. Once complete, select options for addressing identified risks. Options include applying security controls, accepting risks, avoiding risk, or transferring risks.

In addition to a number of robust third-party offerings available on AWS Marketplace, Amazon offers a number of security assessment and mitigation services. Two such services are Amazon Inspector and Amazon GuardDuty.

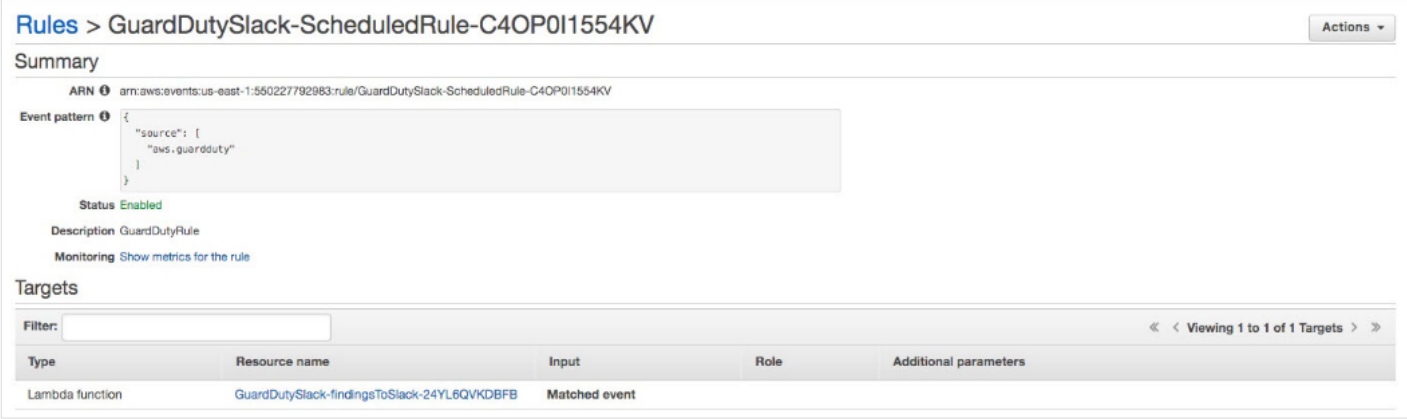
Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for vulnerabilities or deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity.

To help you get started quickly, Amazon Inspector includes a knowledge base of hundreds of rules mapped to common security best practices and vulnerability definitions. Examples of built-in rules include checking for remote root logins being enabled, or vulnerable software versions installed. These rules are regularly updated by AWS security researchers.

Amazon GuardDuty is a managed threat detection service that provides you with an accurate and easy way to continuously monitor and protect your AWS accounts and workloads. Here's an example of what GuardDuty can do.

Example vulnerability analysis: Working with GuardDuty findings

With just a few clicks, GuardDuty immediately begins analyzing billions of events from multiple AWS log sources. It uses threat intelligence feeds, such as lists of malicious IPs and domains, and machine learning to detect threats more accurately. For example, GuardDuty can detect compromised EC2 instances serving malware or mining bitcoin. It can detect attackers probing your web servers for known application vulnerabilities, or accessing your AWS resources from unusual locations. It also checks your AWS accounts for signs of compromise, such as unauthorized infrastructure deployments or unusual API calls. When a threat is detected, GuardDuty sends you a detailed security alert so you can take steps to address the threat. With GuardDuty, you get intelligent threat detection and actionable alerts in an easy-to-use, pay-as-you-go cloud security service.



Most security teams have ticketing systems, chat operations, security information event management (SIEM) systems, or other security automation systems to which they would like to push GuardDuty findings. For this purpose, GuardDuty sends all findings as JSON-based messages through Amazon CloudWatch Events, a scalable service to which you can subscribe, and stream system events with AWS services. To access these events, navigate to the CloudWatch Events console and create a rule that subscribes to the GuardDuty-related findings. You then can assign a target such as Amazon Kinesis Data Firehose that can place the findings in a number of services such as Amazon S3. The following screenshot is of the CloudWatch Events console, where a rule pulls all events from GuardDuty and pushes them to a preconfigured AWS Lambda function.

The following example is a subset of GuardDuty findings that includes relevant context and information about the nature of a threat that was detected. In this example, the instance ID (i-00bb62b69b7004a4c) is performing Secure Shell (SSH) brute-force attacks against IP address 172.16.0.28. From a Lambda function, you can access any of the following fields such as the title of the finding and its description, and send those directly to your ticketing system.

You can use other AWS services and solutions in AWS Marketplace to build custom analytics and visualizations of your security findings. For example, you can connect Amazon Kinesis Data Firehose to CloudWatch Events and write events to an S3 bucket in a standard format, which can be encrypted with AWS Key Management Service and then compressed. You also can use Amazon QuickSight or TIBCO Spotfire to build ad hoc dashboards. Similarly, you can place the data from Kinesis Data Firehose in Amazon Elasticsearch Service, with which you can use tools such as Kibana to build your own visualizations and dashboards.

Tips from the Pros

Real-World Advice from Experts that Live Cloud Everyday

Optiv

Optiv is one of the market-leading provider of end-to-end cyber security solutions

> *An organization may have a lot of vulnerabilities identified but if they're not necessarily going to be exposed, they may be mitigated by something else. What you don't want to do is blindly apply vulnerability management to areas across the cloud that aren't necessarily business risk-aligned.*
>
> *You want to manage your true enterprise risk and align that enterprise risk to your vulnerability management practices. What are some of the things from that enterprise perspective that need to be managed? Where does that risk in the cloud manifest itself, and when you think about vulnerability management, where do you need to focus?*
>
> *Many CISOs out there understand that is isn't just about mitigating risk, it's actually balancing risk and agility. Everything you do is literally, 'How do you balance your agility with your INFOSEC risk?' You cannot have your cake and eat it too. You cannot make everything completely secure, unplugged from the network, and be that agile at the same time.*

Specific Solutions

Applying Best Practices

After mitigating risks and putting the proper processes into place, controlling future risks via monitoring is key to success, and measuring control effectiveness is an integral process to each ISMS. Metrics provide visibility into how well controls are protecting the environment. Risk management often depends on qualitative and quantitative metrics. The following table outlines recommended measurement and improvement best practices:

Best Practice	Improvement
Monitoring and reviewing procedures and other controls	• Promptly detect errors in the results of processing • Promptly identify attempted and successful security breaches and incidents • Enable management to determine whether the security activities delegated to people or • implemented by information technology are performing as expected • Help detect security events and thereby prevent security incidents by the use of indicators • Determine whether the actions taken to resolve a breach of security were effective
Regular reviews of the effectiveness of ISMS	• Consider results from security audits, incidents, and effectiveness measurements, and suggestions and feedback from all interested parties • Ensure that the ISMS meets the policy and objectives • Review security controls
Measure controls effectiveness	• Verify that security requirements have been met
Risk assessments reviews at planned intervals	Review the residual risks and the identified acceptable levels of risks, taking into account: • Changes to the organization, technology, business objectives and processes, and identified threats • Effectiveness of the implemented controls • External events, such as changes to the legal or regulatory environment, changed contractual obligations, and changes in social climate
Internal ISMS audits	• First-party audits (internal audits), are conducted by, or on behalf of, the organization itself for internal purposes
Regular management reviews	• Ensure that the scope remains adequate • Identify improvements in the ISMS process
Update security plans	• Take into account the findings of monitoring and reviewing activities • Record actions and events that could affect the ISMS effectiveness or performance

AWS MARKETPLACE

As IT continues to play a more central role in the modern enterprise, security is a greater concern than ever before. AWS Marketplace has a vast selection of security solutions offered by hundreds of ISVs, spanning infrastructure security, identity and access management, data protection, logging and monitoring, configuration and vulnerability analysis, and more. These pay-as-you-go offerings can be integrated with existing technologies, enabling you to deploy a comprehensive security architecture across your AWS and on-premises environments.

Popular solutions in AWS Marketplace for configuration and vulnerability analysis include:

Alert Logic Threat Manager with ActiveWatch

Threat Manager with ActiveWatch is a managed IDS service that comes with 24x7x365 security monitoring and threat analysis to help ensure your security in AWS.

Threat Manager with ActiveWatch helps streamline security in AWS by deploying lightweight agents on EC2 instances for network traffic inspection. These agents mirror all traffic to virtual appliances that route suspicious packets through an encrypted channel to our cloud-hosted analytics platform. Our Global Information Assurance Certification (GIAC) security analysts located in global Security Operations Centers (SOC) investigate, remove false positives, prioritize, add context, and escalate security threats that could threaten your security in AWS.

https://aws.amazon.com/marketplace/pp/B06XXSB16J

Dome9 Flex for AWS

The Dome9 SaaS platform delivers verifiable cloud infrastructure security and compliance to enterprises, offering functionality across three key security areas: Network Security, IAM Protection, and Compliance and Governance. Businesses use Arc for faster cloud security operations, pain-free, and rugged DevOps practices

- Visualize security groups, policies, VPC network traffic, etc.
- Assess network security posture and risk.
- Actively control authorizations and enforce Principle of Least Privilege.
- Model "gold standard" network security best practices.
- Monitor and track changes against security best practices with fine-grained logging.
- Prevent deviations from gold standard with tamper protection and region lock.
- Proactively track, report and remediate compliance posture.

https://aws.amazon.com/marketplace/pp/B01MAWGOUH

Symantec – Cloud Workload Protection

Symantec Cloud Workload Protection automates security for AWS cloud workloads, enabling business agility, risk reduction, and cost savings for organizations, while easing DevOps and administrative burdens. Rapid discovery, visibility, and elastic protection of AWS workloads enables automated security policy enforcement to protect applications from unknown exploits.

Cloud Workload Protection provides strong security for your AWS instances and assets with application protection, intrusion detection/prevention, and real-time file integrity monitoring (RT-FIM). Cloud-native integration allows DevOps to build application protection directly into deployment workflows, while support for Chef and Puppet automates configuration, provisioning, and patching. In addition, Docker security enables protected deployment of containers on AWS.

https://aws.amazon.com/marketplace/pp/B0722D4QRN

Cisco – Stealthwatch Cloud

Public Cloud Monitoring is an AWS Native Security Visibility Service, providing security monitoring and visualization services for AWS infrastructure using advanced modeling and machine learning techniques. This service learns normal behavior for a resource or a user. When a behavior change is observed that should be investigated, Stealthwatch Cloud will generate an alert with various details.

The service consumes VPC flow logs and models all IP traffic generated by your resources, both inside the VPC and to external IP addresses. New Remote Access, Geographic Unusual Remote Access, Excessive Access Attempts, and Potential Database Exfiltration are examples of Stealthwatch Cloud alerts. In addition, network reports like top IPs, top ports, active subnets with traffic statistics, etc., are available.

The service is also integrated with additional AWS log sources like Cloud Trail, Cloud Watch, Config, Inspector, IAM, Lambda, etc. Abnormal User, Geographically Unusual AWS API Usage, Permissive AWS Security Group activity, and Inspector Findings are examples of alerts produced from these other AWS sources.

https://aws.amazon.com/marketplace/pp/B075MWZVBM

CloudCheckr

CloudCheckr Security and Cost Management provides comprehensive coverage of your AWS environment. Features include: RI purchasing recommendations, idle resource warnings, cost tracking allocation, CloudTrail reporting, change monitoring, security group mapping, and perimeter assessments.

Includes hundreds of best practice checks covering security, availability, cost, and usage, the ability to discover and visualize what's running in AWS, and AWS cost optimization.

https://aws.amazon.com/marketplace/pp/B072LXGVZ5

CrowdStrike FALCON

CrowdStrike Falcon Prevent NGAV uniquely combines an array of powerful methods designed to provide prevention against the rapidly changing tactics, techniques and procedures (TTPs) used by today's adversaries to breach organizations - including commodity malware, zero-day malware and even advanced malware-free attacks. Falcon Insight relies on CrowdStrike's revolutionary cloud-native architecture, providing a communications fabric unlike other products. Using an advanced graph data model, the CrowdStrike Threat Graph® database collects and inspects event information in real time to prevent and detect attacks on your endpoints.

As part of the Falcon endpoint protection platform, Falcon Insight records all activities of interest on an endpoint for deeper inspection - on-the-fly and after-the-fact - allowing users to quickly detect, investigate and respond to attacks - even those that evade standard prevention measures.

Falcon OverWatch provides an additional layer of oversight and analysis such that threats don't get missed and ultimately to help you prevent the mega breach. This offering is comprised of an elite team of security experts who proactively hunt, investigate and advise on threat activity in your environment.

https://aws.amazon.com/marketplace/pp/B0779JP1D9