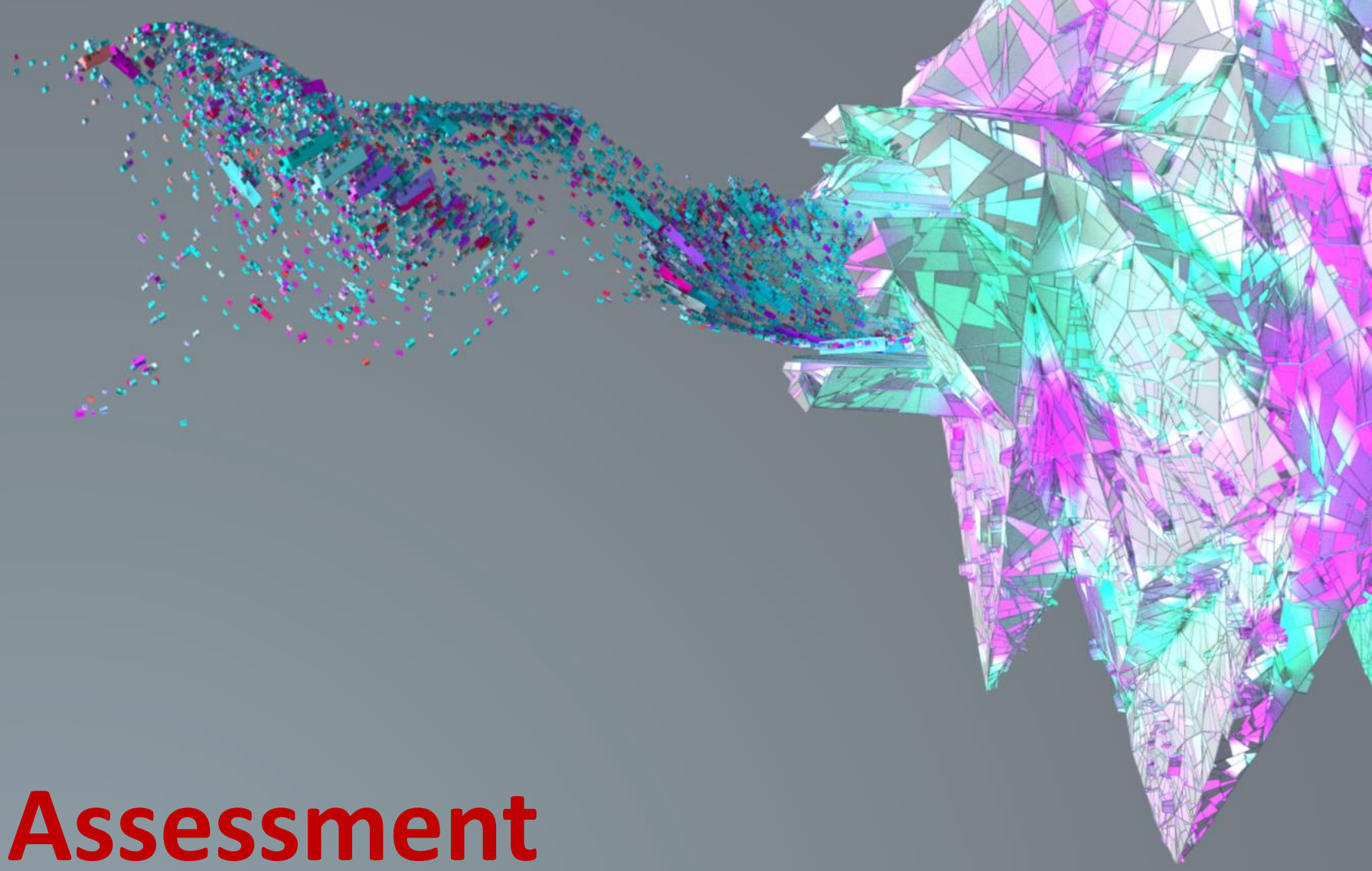
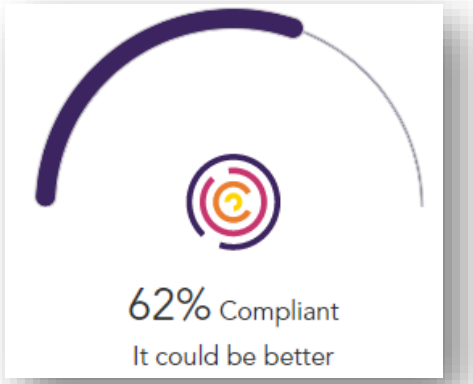
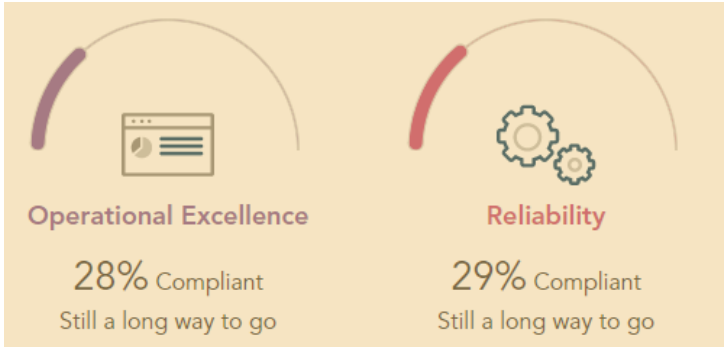


Cloud Risk Assessment

SUMMARY

General Compliance





IAM Security Failures

Rotating Identity and Access Management (IAM) credentials periodically will significantly **reduce the chances that a compromised set of access keys can be used without your knowledge** to access certain components within your AWS account.

Access Keys Rotated 90 Days	IAM	AWS	Security	High	FAILURE: 1
Access Keys Rotated 45 Days	IAM	AWS	Security	Medium	FAILURE: 1
Access Keys Rotated 30 Days	IAM	AWS	Security	Low	FAILURE: 2

Having hardware-based **MFA** protection for your root account is the best way to protect your AWS resources and services against attackers. A hardware **MFA** device signature adds an extra layer of protection on top of your existing root credentials **making your Amazon Web Services root account virtually impossible** to penetrate without the MFA generated passcode.

+ Hardware MFA for AWS Root Account	IAM	AWS	Security	High	FAILURE: 1
MFA For IAM Users With Console Password	IAM	AWS	Security	High	FAILURE: 15
+ Root MFA Enabled	IAM	AWS	Security	High	FAILURE: 1

Security

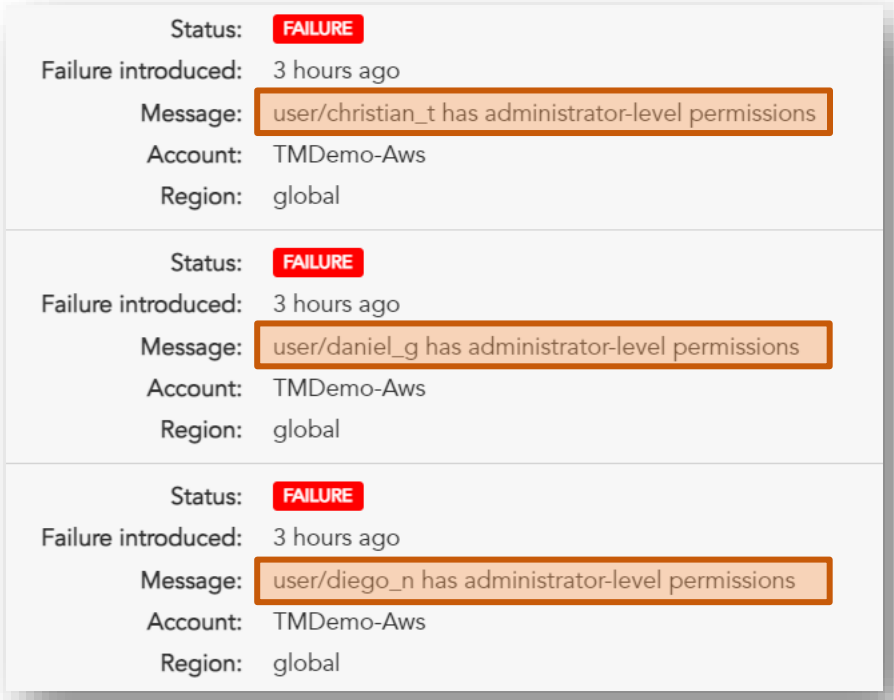
62% Compliant
It could be better

IAM Security Failures

Having MFA-protected IAM users is the best way to protect your AWS resources and services against attackers. An MFA device signature adds an extra layer of protection on top of your existing IAM user credentials (username and password), making your AWS account virtually impossible to penetrate without the MFA generated passcode.

AWS IAM Users with Admin Privileges	IAM	AWS	Security	High	FAILURE: 10

Security



When an IAM user with administrator-level permissions (i.e. has authorization to create, modify or remove any resource, access any data within the AWS environment and use any service or component) is an inexperienced person within your organization, their actions can lead to severe security problems, data leaks, data loss or unexpected charges on your AWS bill.

IAM Security Failures

Inactive IAM Console User	IAM	AWS	Security	Medium	FAILURE: 4

accountId	resource	CreateDate	PasswordLastUsed
123456789	Users.DemoCloud1	2020-01-21T21:33:55.000Z	
123456790	Users.DemoCloud2	2020-04-15T17:41:47.000Z	
123456790	Users.DemoCloud3	2020-04-15T17:49:51.000Z	
123456791	Users.DemoCloud4	2020-04-29T22:41:51.000Z	
123456791	Users.DemoCloud5	2020-04-29T22:46:04.000Z	
123456792	Users.DemoCloud7	2020-07-02T15:48:18.000Z	
123456792	Users.DemoCloud8	2020-07-02T15:48:18.000Z	
123456793	Users.DemoCloud9	2020-07-10T16:49:44.000Z	
123456793	Users.DemoCloud10	2020-07-30T16:27:39.000Z	
123456794	Users.DemoCloud11	2020-09-14T21:58:02.000Z	
123456790	Users.DemoCloud12	2020-10-01T22:07:50.000Z	
123456791	Users.DemoCloud13	2020-10-08T19:27:00.000Z	
123456791	Users.DemoCloud14	2020-10-09T20:20:41.000Z	
123456792	Users.DemoCloud15	2020-10-09T20:20:41.000Z	
123456792	Users.DemoCloud16	2020-10-26T23:31:44.000Z	
123456793	Users.DemoCloud17	2020-10-27T18:06:11.000Z	
123456793	Users.DemoCloud18	2020-12-07T22:12:04.000Z	
123456794	Users.DemoCloud19	2020-12-07T22:12:04.000Z	
123456794	Users.DemoCloud20	2020-12-07T22:12:04.000Z	
123456795	Users.DemoCloud21	2021-06-07T19:27:23.000Z	

Disabling access for inactive IAM users can reduce the risk of unauthorized access to your AWS resources and help you manage the user-based access more efficiently.

accountId	resource	CreateDate	PasswordLastUsed
123456789	Users.DemoCloud1	2020-01-21T21:33:55.000Z	d3M0.YQ92
123456790	Users.DemoCloud2	2020-04-15T17:41:47.000Z	d3M0.YQ92
123456790	Users.DemoCloud3	2020-04-15T17:49:51.000Z	d3M0.YQ92
123456791	Users.DemoCloud4	2020-04-29T22:41:51.000Z	d3M0.YQ92
123456791	Users.DemoCloud5	2020-04-29T22:46:04.000Z	d3M0.YQ92
123456792	Users.DemoCloud7	2020-07-02T15:48:18.000Z	d3M0.YQ92
123456792	Users.DemoCloud8	2020-07-02T15:48:18.000Z	d3M0.YQ92
123456793	Users.DemoCloud9	2020-07-10T16:49:44.000Z	d3M0.YQ92
123456793	Users.DemoCloud10	2020-07-30T16:27:39.000Z	d3M0.YQ92
123456794	Users.DemoCloud11	2020-09-14T21:58:02.000Z	d3M0.YQ92
123456790	Users.DemoCloud12	2020-10-01T22:07:50.000Z	d3M0.YQ92
123456791	Users.DemoCloud13	2020-10-08T19:27:00.000Z	d3M0.YQ92
123456791	Users.DemoCloud14	2020-10-09T20:20:41.000Z	d3M0.YQ92
123456792	Users.DemoCloud15	2020-10-09T20:20:41.000Z	d3M0.YQ92
123456792	Users.DemoCloud16	2020-10-26T23:31:44.000Z	d3M0.YQ92

IAM Security Failures

Unused IAM User	IAM	AWS	Security	Medium	FAILURE: 39

Security

accountId	resource	ARN
123456789	Users.DemoCloud1	arn:aws:iam::123456789:user/Users.DemoCloud1
123456790	Users.DemoCloud2	arn:aws:iam::123456789:user/Users.DemoCloud2
123456790	Users.DemoCloud3	arn:aws:iam::123456789:user/Users.DemoCloud3
123456791	Users.DemoCloud4	arn:aws:iam::123456789:user/Users.DemoCloud4
123456791	Users.DemoCloud5	arn:aws:iam::123456789:user/Users.DemoCloud5
123456792	Users.DemoCloud7	arn:aws:iam::123456789:user/Users.DemoCloud16
123456792	Users.DemoCloud8	arn:aws:iam::123456789:user/Users.DemoCloud7
123456793	Users.DemoCloud9	arn:aws:iam::123456789:user/Users.DemoCloud8
123456793	Users.DemoCloud10	arn:aws:iam::123456789:user/Users.DemoCloud9
123456794	Users.DemoCloud11	arn:aws:iam::123456789:user/Users.DemoCloud10
123456790	Users.DemoCloud12	arn:aws:iam::123456789:user/Users.DemoCloud11
123456791	Users.DemoCloud13	arn:aws:iam::123456789:user/Users.DemoCloud12
123456791	Users.DemoCloud14	arn:aws:iam::123456789:user/Users.DemoCloud13
123456792	Users.DemoCloud15	arn:aws:iam::123456789:user/Users.DemoCloud14
123456792	Users.DemoCloud16	arn:aws:iam::123456789:user/Users.DemoCloud15
123456793	Users.DemoCloud17	arn:aws:iam::123456789:user/Users.DemoCloud16
123456793	Users.DemoCloud18	arn:aws:iam::123456789:user/Users.DemoCloud17
123456794	Users.DemoCloud19	arn:aws:iam::123456789:user/Users.DemoCloud18
123456794	Users.DemoCloud20	arn:aws:iam::123456789:user/Users.DemoCloud19
123456795	Users.DemoCloud21	arn:aws:iam::123456789:user/Users.DemoCloud20
123456789	Users.DemoCloud1	arn:aws:iam::123456789:user/Users.DemoCloud21
123456790	Users.DemoCloud2	arn:aws:iam::123456789:user/Users.DemoCloud22
123456790	Users.DemoCloud3	arn:aws:iam::123456789:user/Users.DemoCloud23
123456791	Users.DemoCloud4	arn:aws:iam::123456789:user/Users.DemoCloud24

Removing unused IAM users can reduce the risk of unauthorized access to your AWS resources and help you manage the user-based access to the AWS Management Console more efficiently.

TREND MICRO

IAM Security Failures

Security

Password Policy Minimum Length	IAM	AWS	Security	Medium	FAILURE: 2
Password Policy Expiration	IAM	AWS	Security	Medium	FAILURE: 2
Password Policy Reuse Prevention	IAM	AWS	Security	Medium	FAILURE: 2
Cross-Account Access Lacks External ID and MFA	IAM	AWS	Security	Medium	FAILURE: 2
Password Policy Lowercase	IAM	AWS	Security	Medium	FAILURE: 1
Password Policy Uppercase	IAM	AWS	Security	Medium	FAILURE: 1

Enforcing AWS IAM passwords strength, pattern and rotation is vital when it comes to maintaining the security of your AWS account. Having a strong password policy in use will significantly reduce the risk of password-guessing and brute-force attacks.

EC2 Security failures

Allowing unrestricted SSH or RDP access can increase opportunities for malicious activity such as hacking, man-in-the-middle attacks (MITM) and brute-force attacks.

Unrestricted RDP Access	EC2	AWS	Security	Medium	FAILURE: 33
Unrestricted SSH Access	EC2	AWS	Security	Medium	FAILURE: 27

Status:	FAILURE
Failure introduced:	3 days ago
Message:	Security group launch-wizard-18 allows ingress from 0.0.0.0/0 or ::/0 to port 3389
Account:	TMDemo-Aws
Region:	us-east-1
Attachments:	eni-0f0ebd400e783c06d
Description:	launch-wizard-18 created 2022-01-20T10:04:39.747-06:00
Group Id:	sg-05cb85cbe1e0629b1
Group Name:	launch-wizard-18
Vpc Id:	vpc-557b7e2f

Ensure that all Amazon EC2 instances are managed by AWS Systems Manager (SSM). Systems Manager simplifies AWS cloud resource management, shortens the time to detect and resolve operational problems, and makes it easy to operate and manage your instances securely at scale. For Amazon EC2 instances to be monitored and managed with AWS Systems Manager service, they must be configured as managed instances.

EC2 Security failures

Security

Inactive IAM Console User	IAM	AWS	Security	Medium
Unrestricted FTP Access	EC2	AWS	Security	Medium
Unrestricted Oracle Access	EC2	AWS	Security	Medium
Unrestricted MySQL Access	EC2	AWS	Security	Medium

Allowing unrestricted Oracle Database, MSSQL or PostgreSQL access can increase opportunities for malicious activity such as hacking, denial-of-service (DoS) attacks and loss of data.

Status:	FAILURE
Failure introduced:	3 days ago
Message:	Security group DiegoNegretti-Traffic security group allows ingress from 0.0.0.0/0 or ::/0 to ports 20, 21
Account:	TMDemo-Aws
Region:	us-east-2
Attachments:	
Description:	Allows all inbound traffic from the internet
Group Id:	sg-0db4a6fc38214c9b8
Group Name:	DiegoNegretti-Traffic security group
Vpc Id:	vpc-0ea26c639d8cc30e5

EC2 Security Recommendations

Reliability

Security

EC2 Instance Too Old	EC2	AWS	Security, Reliability	Low	FAILURE: 95

Stopping and relaunching your old EC2 instances will reallocate them to different and possibly more reliable underlying hardware (host machine).

EC2 AMI Too Old	EC2	AWS	Security, Reliability	Low	FAILURE: 378

Using up-to-date AMIs to launch your EC2 instances brings major benefits to your AWS application stack, maintaining your EC2 deployments secure and reliable. You can go even further and automate your old AMIs update process with AWS Systems Manager or open-source tools like Packer and Netflix Animator.

S3 Security failures

Granting public FULL_CONTROL access to your Amazon S3 buckets can allow everyone on the Internet to view, upload, modify, and delete S3 objects without any restrictions. Exposing your S3 buckets to the public Internet can lead to data leaks, data loss, and unexpected charges on your AWS bill.

In some cases, it may not be clear that your device has been compromised while your info is collected and sold to others.

File Storage Security provides anti-malware scanning on files in cloud storage services such as Amazon Web Services

Used in combination with versioning, which protects objects from being overwritten, AWS S3 Object Lock enables you to store your S3 objects in an immutable form, providing an additional layer of protection against object changes and deletion. S3 Object Lock feature can also help you meet regulatory requirements within your organization when it comes to data protection.

Lambda Security failures

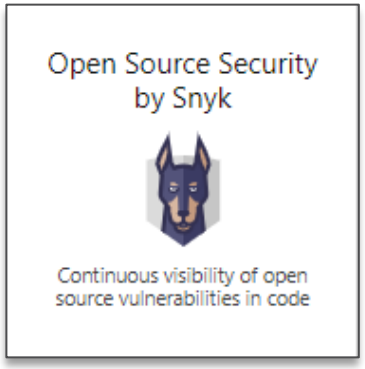
Security

Use AWS KMS Customer Master Keys for Lambda Environment Variables Encryption	Lambda	AWS	Security	High	FAILURE: 22

When you utilize your own customer-managed Customer Master Keys (CMKs) to protect the sensitive data that you pass to your Amazon Lambda functions, you achieve full control over who can use the CMKs and access the data encrypted within the environment variables. The Amazon KMS service allows you to create, rotate, disable, enable, and audit Customer Master Keys for Lambda environment variables.

VPC Access for AWS Lambda Functions	Lambda	AWS	Security	Medium	FAILURE: 34

Based on your application requirements, you can associate your Amazon Lambda functions with the appropriate Virtual Private Cloud (VPC). For example, to access the cloud resources provisioned inside a private VPC, you must provide additional VPC-specific configuration information that includes the VPC subnet IDs and security group IDs. Amazon Lambda uses this configuration information to set up Elastic Network Interfaces (ENIs) that enable your functions to connect securely to other cloud resources available within your private VPC.



Trend Micro Cloud One™ - Open-Source Security by Snyk automatically finds, prioritizes, and reports vulnerabilities and license risks in open-source dependencies used by your applications. As part of the Cloud One security platform, Open-Source Security by Snyk connects with your code repositories and CI/CD pipelines to scan projects.

Cost Optimization

Cost Optimisation

EBS Volumes Attached To Stopped EC2 Instances	EBS	AWS	Cost Optimisation, Operational Excellence	High	FAILURE: 22
Idle EC2 Instance	EC2	AWS	Cost Optimisation	High	FAILURE: 2
Underutilized EC2 Instance	EC2	AWS	Cost Optimisation	High	FAILURE: 2

Any Elastic Block Store volume created in your AWS account is adding charges to your monthly bill, regardless whether is being used or not. If you have EBS volumes (other than root volumes) that are unattached to an EC2 instance or have very low I/O activity, consider deleting them. Removing unattached/orphaned Elastic Block Store volumes will help you avoid unexpected charges on your AWS bill and halt access to any sensitive data available on these volumes.

Total Savings Cost: **USD $560**

Status:	FAILURE
Failure introduced:	3 days ago
Message:	EC2 instance i-01b58e036e46cd406 is idle
Account:	TMDemo-Aws
Region:	us-east-1
Link to resource:	i-01b58e036e46cd406
Tags:	Name: Test-env aws:clo...tack-id: arn:aws...0a92c17 aws:aut...oupName: awseb-e...L7RV7AL aws:clo...ck-name: awseb-e...y-stack aws:ec2...late:id: lt-03c3...5b4dd7e aws:clo...ical-id: AWSEBAu...ngGroup aws:ec2...version: 1 elastic...ment-id: e-d9uz2aavyy elastic...nt-name: Test-env
Cost:	$8.00
Est Cost Savings:	$8.00
CPU Utilization:	0.3%
Instance Type:	t2.micro
Network Utilization:	0 MB

Cost Optimization

Cost Optimisation

Unused AMI	EC2	AWS	Cost Optimisation	Low	FAILURE: 34

The AMIs created in your AWS account are adding charges to your monthly bill, regardless whether are being used or not. Many AWS customers will deregister their images but forget to delete the AMIs snapshots, therefore continue to incur storage costs. Cloud Conformity recommends implementing the two-step cleanup process shown in the Remediation/Resolution section in order to avoid any unexpected charges on your AWS bill.

Unassociated Elastic IP Addresses	EC2	AWS	Cost Optimisation	Low	FAILURE: 34

Amazon Web Services enforce a small hourly charge if an Elastic IP (EIP) address within your account is not associated with a running EC2 instance or an Elastic Network Interface (ENI). Cloud Conformity recommends releasing any unassociated EIPs that are no longer needed to reduce your AWS monthly costs.

Operational Excellence

Operational Excellence

Check for SSM Managed Instances	SSM	AWS	Security, Operational Excellence	High	FAILURE: 5

Launch Configuration Referencing Missing Security Groups	AutoScaling	AWS	Operational Excellence	High	FAILURE: 1
Trend Micro Cloud One™ – Conformity Insufficient Access Permissions	CloudConformity	AWS	Operational Excellence	High	FAILURE: 1

AWS Custom Rule	ConfigService	AWS	Security, Reliability, Performance Efficiency, Cost Optimisation, Operational Excellence	Medium	FAILURE: 537
Tracing Enabled	Lambda	AWS	Operational Excellence	Medium	FAILURE: 34

Reliability

Reliability

DynamoDB Continuous Backups	DynamoDB	AWS	Reliability	High	FAILURE: 29
DynamoDB Backup and Restore	DynamoDB	AWS	Reliability	High	FAILURE: 29

ELBv2 Minimum Number of EC2 Target Instances	ELBv2	AWS	Reliability	High	FAILURE: 51
ELB Minimum Number Of EC2 Instances	ELB	AWS	Reliability	High	FAILURE: 51

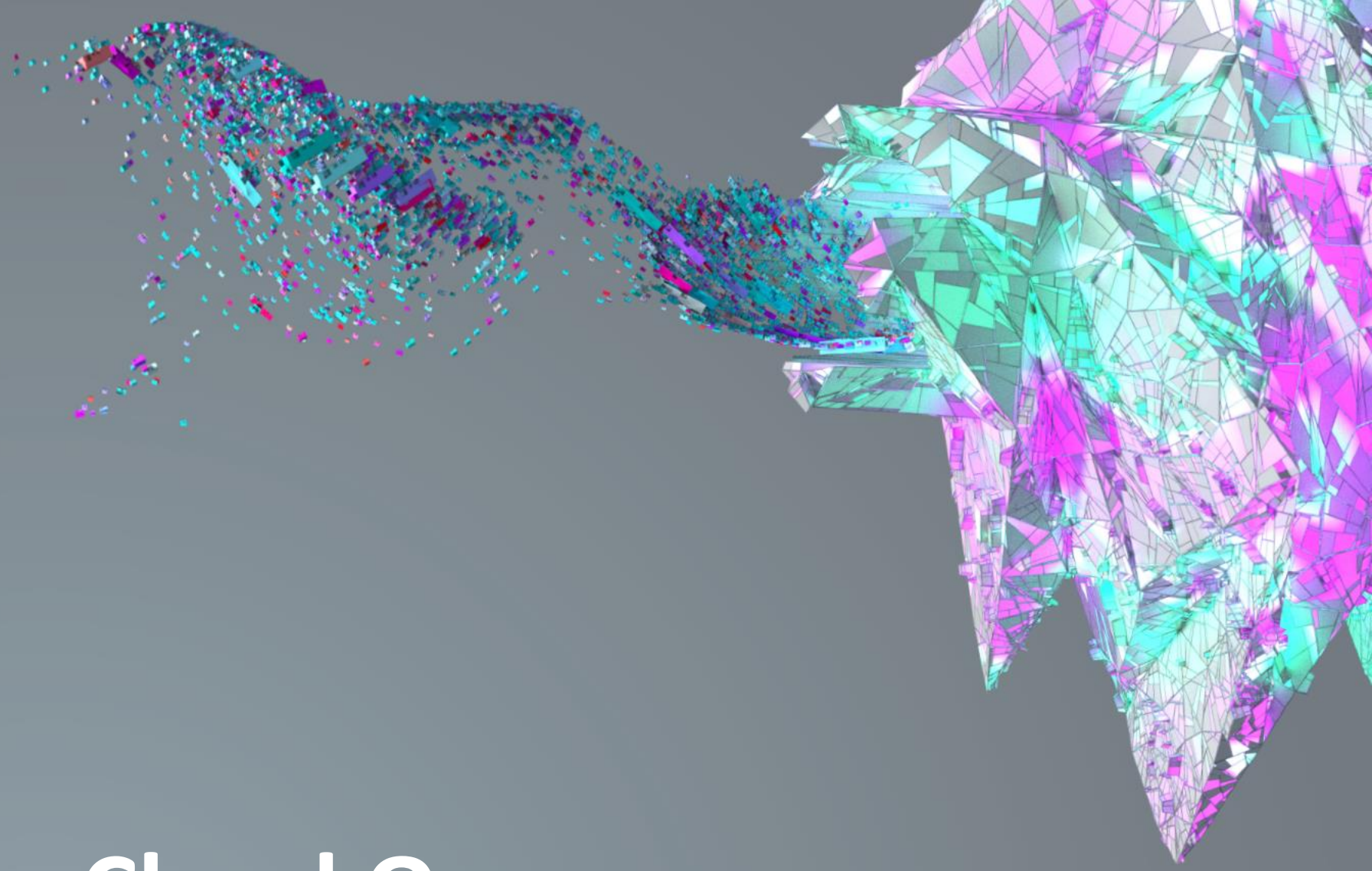
EC2 Hibernation	EC2	Reliability	Low	FAILURE: 30

EC2 Instance Termination Protection	EC2	Reliability	Medium	FAILURE: 30

Consumo estimado de Cloud One por AWS Marketplace

Cloud One Platform Calculator		
Dimension	**Cost/hr**	**Units**
Workload Security: Any Micro, Small or Medium EC2 instance types, Amazon WorkSpaces, or Other Cloud – 1 Core / hr	$0.010	
Workload Security: Any Large EC2 instance types, or Other Cloud 2 Core/ hr	$0.030	
Workload Security: Any Xlarge or larger EC2 instance types, Other Cloud 4+ Core / hr	$0.045	
Workload: Per Data Center / Not Cloud instance / hr	$0.045	
Network: Per GB (gigabyte) inspected (NOTE: estimate the number of GB per hr)	$0.013	
Application: Per 1000 Serverless function invocations / hr	$0.026	
Application: Per container or per VM /hr	$0.016	
Container: Per node / hr	$0.160	
Container: Per serverless container / hr	$0.016	
File storage: Per <21 inspected files per bucket / hr	$0.000	
File storage: Per 21-200 inspected files per bucket / hr	$0.400	
File storage: Per 201-400 inspected files per bucket / hr	$0.600	
File storage: Per 401+ inspected files per bucket / hr	$1.100	
Conformity: Per AWS account with <250 resources / hr	$0.000	
Conformity: Per AWS account with 250 to 999 resources / hr	$0.070	
Conformity: Per AWS account with 1000 to 5000 resources/hr	$0.290	
Conformity: Per AWS account with 5001+ resources/hr	$0.350	
Open Source Security by Snyk: Per project/24 hrs (15 projects free)	$0.260	
	Cost	**# of Days/Months /Years**
Cost per Day		
Cost per Month		
Cost per Year		

- El costo anual es el precio total del año que conserven la suscripción, pero este cobro se hará de acuerdo con la facturación de AWS de forma mensual.
- El valor presentado es considerando la protección y monitoreo **24/7**
- La plataforma de **Trend Micro Cloud One** cuenta con algunos **Free Tier** en los siguientes servicios:
  - **File Storage Security** – Si durante alguna hora del día se suben **< 20 archivos** al Bucket de S3 integrado con **Cloud One** no se realiza ningún cargo.
  - **Conformity** – Cuentas de AWS con < 250 recursos no se realiza ningún cargo.
  - **Open-Source Security By Snyk** - Incluye 15 proyectos gratis con la suscripción a **Cloud One**
- Igualmente pueden validar los precios directamente desde el **Marketplace de AWS**: https://aws.amazon.com/marketplace/pp/prodview-g232pyu6l55l4?sr=0-1&ref_=beagle&applicationId=AWSMPContessa



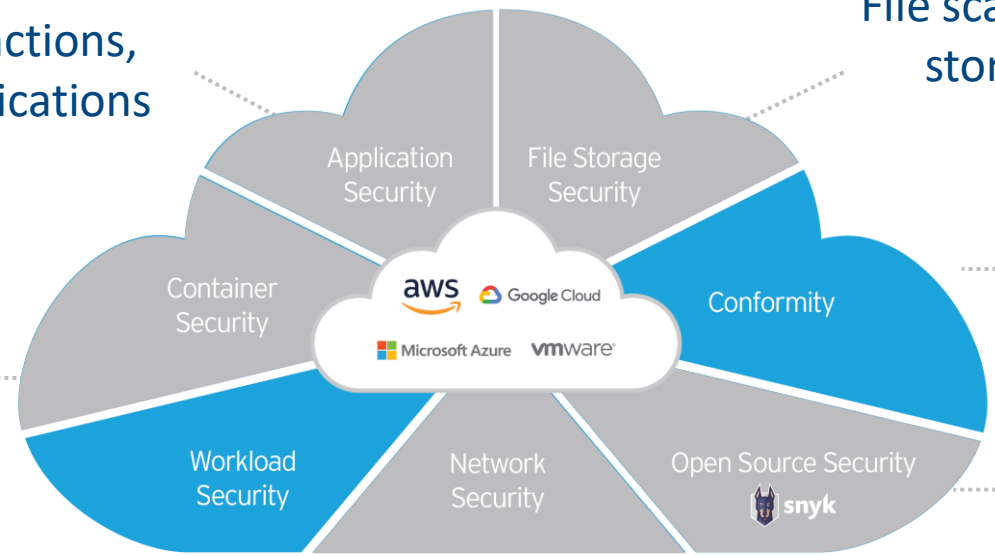
Trend Micro Cloud One

Trend Micro Cloud One™

Security Services Platform for Cloud Builders

Security for serverless functions, APIs, and applications

File scanning for cloud storage services



Container image scanning, admission control policy, and runtime protection

Assurance cloud infrastructure is configured securely

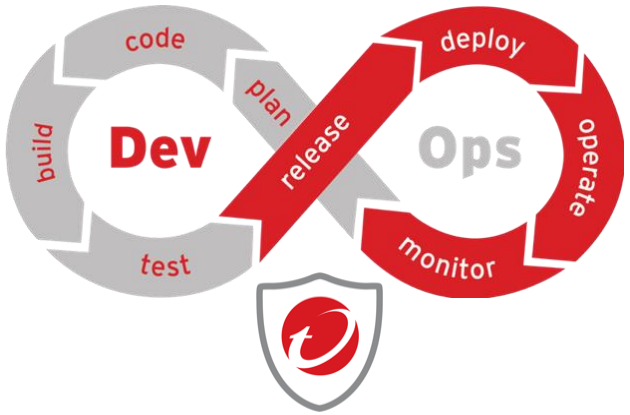
Visibility of open source vulnerabilities in code repositories

Workload & container host security

Network layer IPS to secure entire VPCs

Cloud-native, SaaS-based platform with the most extensive set of cloud security services

Cloud One – Conformity



Multi-cloud & Multi-account complete visibility

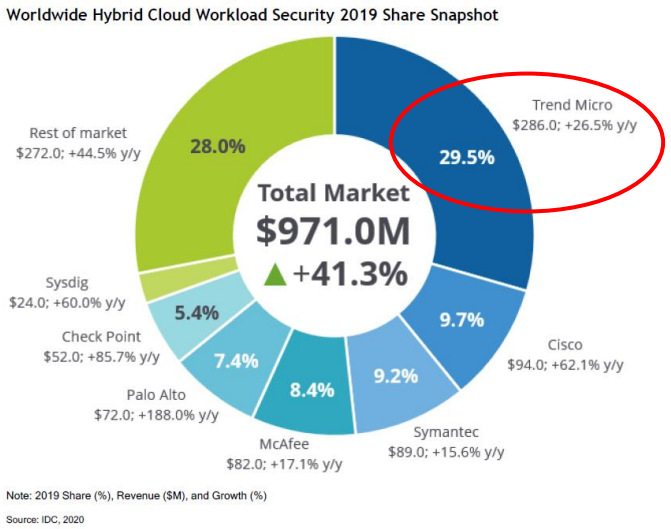
Gartner

7 of 7

Recommendations *

(April 2020)

IDC ANALYZE THE FUTURE



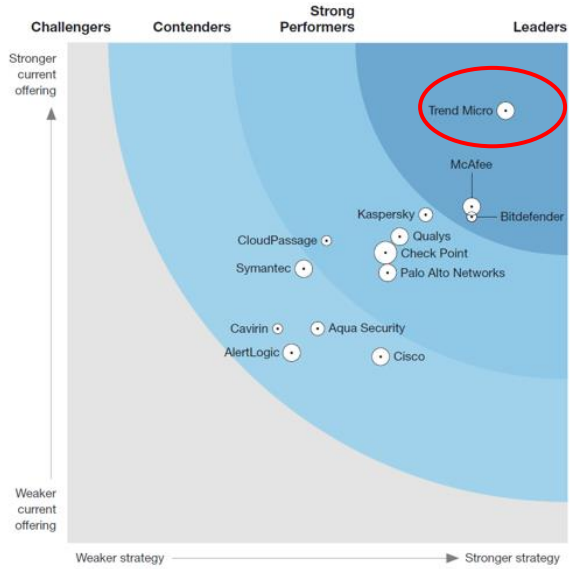
Ranked #1 for

Cloud Workload

Security market share

(June 2020)

FORRESTER®



Highest Score

for Cloud Workload

Security

(Dec 2019)

TREND MICRO

TREND MICRO™

THE ART OF CYBERSECURITY

Automated hybrid cloud workload protection via API calls to Trend Micro's cloud security platform. **Created with real data by artist Brendan Dawes.**