Check Point CHECKMATES

CloudGuard CIEM, ERM & AWP

Deep Dive

Abigael Saal Levy | Product Manager

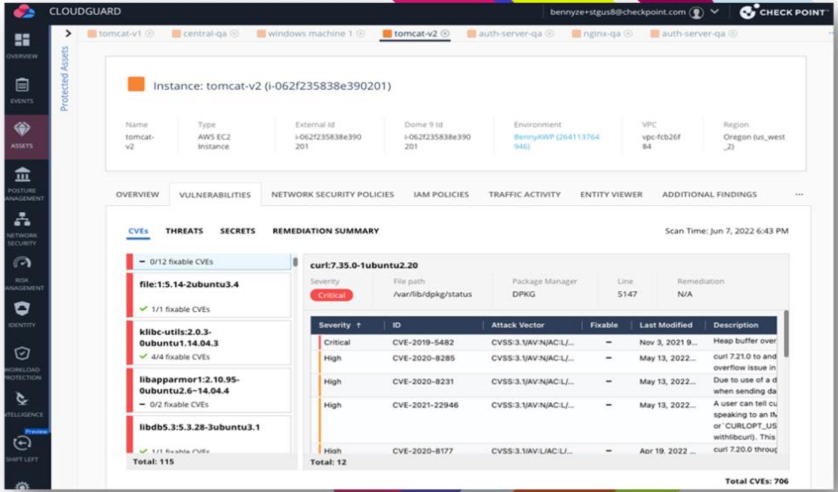
Agentless Workload Posture (AWP)

Achieve deep visibility with agentless deployment

Instant visibility into running workloads, including vulnerabilities, malware and exposed secrets

Avoid complex agent-based deployments

Maintain agility without impacting workload performance



Instance: tomcat-v2 (i-062f235838e390201)

Name	Type	External Id	Dome 9 Id	Environment	VPC	Region
tomcat-v2	AWS EC2 Instance	i-062f235838e390201	i-062f235838e390201	BennyAWP (264113764946)	vpc-fcb26f84	Oregon (us_west_2)

Scan Time: Jun 7, 2022 6:43 PM

- 0/12 fixable CVEs

file:1:5.14-2ubuntu3.4
✓ 1/1 fixable CVEs

klibc-utils:2.0.3-0ubuntu1.14.04.3
✓ 4/4 fixable CVEs

libapparmor1:2.10.95-0ubuntu2.6~14.04.4
- 0/2 fixable CVEs

libdb5.3:5.3.28-3ubuntu3.1
✓ 1/1 fixable CVEs

Total: 115

curl:7.35.0-1ubuntu2.20

Severity	File path	Package Manager	Line	Remediation
Critical	/var/lib/dpkg/status	DPKG	5147	N/A

Severity ↑	ID	Attack Vector	Fixable	Last Modified	Description
Critical	CVE-2019-5482	CVSS:3.1/AV:N/AC:L/...	–	Nov 3, 2021 9...	Heap buffer over
High	CVE-2020-8285	CVSS:3.1/AV:N/AC:L/...	–	May 13, 2022...	curl 7.21.0 to and overflow issue in
High	CVE-2020-8231	CVSS:3.1/AV:N/AC:L/...	–	May 13, 2022...	Due to use of a d when sending da
High	CVE-2021-22946	CVSS:3.1/AV:N/AC:L/...	–	May 13, 2022...	A user can tell cu speaking to an IM or `CURLOPT_US withlibcurl). This
High	CVE-2020-8177	CVSS:3.1/AV:L/AC:L/...	–	Apr 19, 2022 ...	curl 7.20.0 throu

Total: 12

Total CVEs: 706

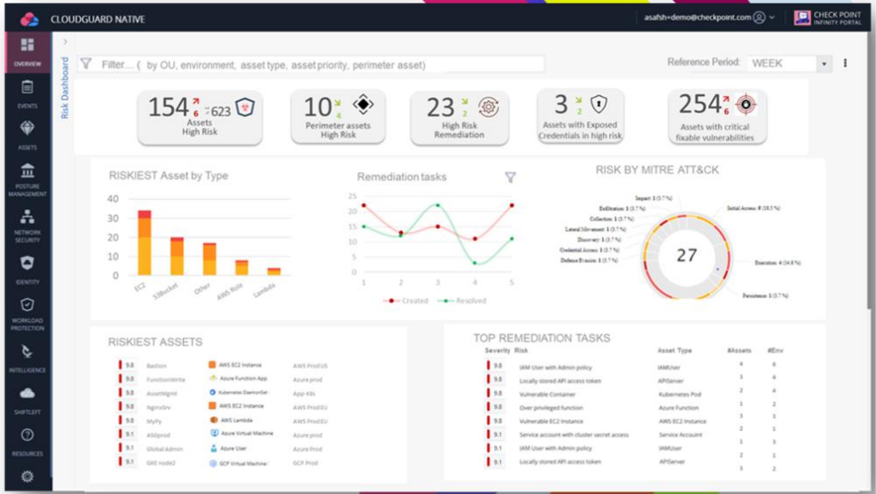
Effective Risk Management (ERM)

Focus on the 1% risks that matter

Utilize contextual AI and asset risk scoring

Reduce attack surface and focus on the highest priority risks

Automatically remediate based on “minimal effective dose” actions



RISKIEST ASSETS

9.8	Bastion	AWS EC2 Instance	AWS Prod US
9.8	FunctionWrite	Azure Function App	Azure prod
9.8	AssetMgmt	Kubernetes DaemonSet	App-K8s
9.8	NginxSrv	AWS EC2 Instance	AWS Prod EU
9.8	MyPy	AWS Lambda	AWS Prod EU
9.1	ASGprod	Azure Virtual Machine	Azure prod
9.1	Global Admin	Azure User	Azure Prod
9.1	GKE node2	GCP Virtual Machine	GCP Prod

TOP REMEDIATION TASKS

Severity	Risk	Asset Type	#Assets	#Env
9.8	IAM User with Admin policy	IAMUser	4	6
9.8	Locally stored API access token	APIServer	3	4
9.8	Vulnerable Container	Kubernetes Pod	2	4
9.8	Over privileged function	Azure Function	1	2
9.8	Vulnerable EC2 Instance	AWS EC2 Instance	3	3
9.1	Service account with cluster secret access	Service Account	2	1
9.1	IAM User with Admin policy	IAMUser	1	3
9.1	Locally stored API access token	APIServer	2	1
			3	2

Cloud Infrastructure Entitlement Management (CIEM)

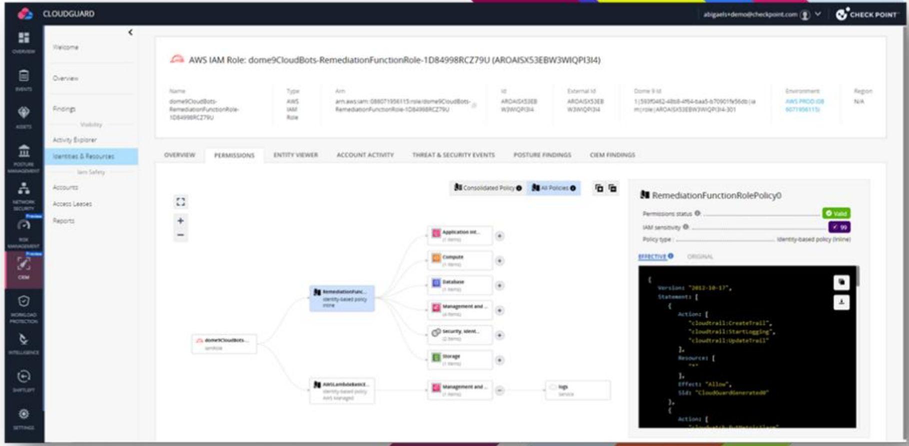
Easy and automated path to least
privileges entitlements

Entitlement mapping to provide in-depth visibility

Calculate the effective policy by analyzing all permissions directly/indirectly assigned to an entity

Automatically identify over privileged entities through account activity monitoring

Actionable remediation steps to remove excessive permissions



AWS IAM Role: dome9CloudBots-RemediationFunctionRole-1D84998RCZ79U (AROAISX53EBW3WIQPI3I4)

Name	Type	Arn	Id	External Id	Dome 9 Id	Environment	Region
dome9CloudBots-RemediationFunctionRole-1D84998RCZ79U	AWS IAM Role	arn:aws:iam::086071956115:role/dome9CloudBots-RemediationFunctionRole-1D84998RCZ79U	AROAISX53EBW3WIQPI3I4	AROAISX53EBW3WIQPI3I4	1|593f0462-48b8-4f64-baa5-b70901fe56db|iam|role|AROAISX53EBW3WIQPI3I4-301	AWS PROD (086071956115)	N/A

RemediationFunctionRolePolicy0

Permissions status: Valid

IAM sensitivity: 99

Policy type: Identity-based policy (inline)

```
{
   Version: "2012-10-17",
   Statement: [
      {
         Action: [
            "cloudtrail:CreateTrail",
            "cloudtrail:StartLogging",
            "cloudtrail:UpdateTrail"
         ],
         Resource: [
            "*"
         ],
         Effect: "Allow",
         Sid: "CloudGuardGenerated0"
      },
      {
         Action: [
```

CHECK POINT™

Thank you

YOU DESERVE THE BEST SECURITY