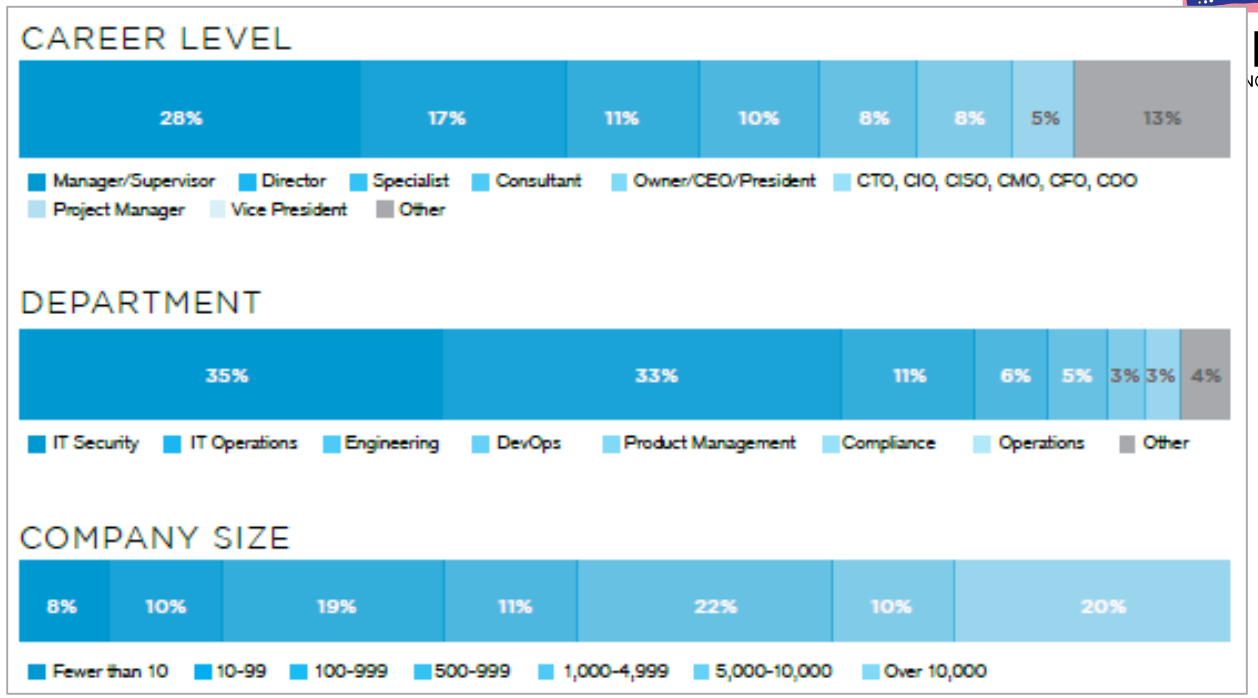
# Achieving Continuous Compliance at the Speed of Cloud

**Lee Psinakis**
**Cloud Security Specialist**
**Check Point Software Technologies**

# AGENDA

- Security Challenges in the Public Cloud
- Some Emerging Cloud Trends
- 6 Steps to Compliance Automation


This Cloud Security Report is based on the results of a comprehensive online survey of 674 cybersecurity and IT professionals, conducted in March of 2019 to gain deep insight into the latest trends, key challenges and solutions for cloud security. The respondents range from technical executives to IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.

https://pages.checkpoint.com/cloud-security-report-2019.html

# Security Challenges in the Public Cloud

## Infrastructure Challenges

- Shared Responsibility
- Minimal Visibility
- Ever-Changing workloads
- Multi-Cloud complexity

## Internal Risks

- Misconfigurations
- Compliance and Regulations
- Insider Threats

## External Threats

- Malware
- Zero-day Threats
- Account Takeover

Infrastructure Challenges

# Shared Responsibility

- Cloud providers protect their Infrastructure
- Companies must protect their Cloud Workloads

**Cloud Provider Responsibility**

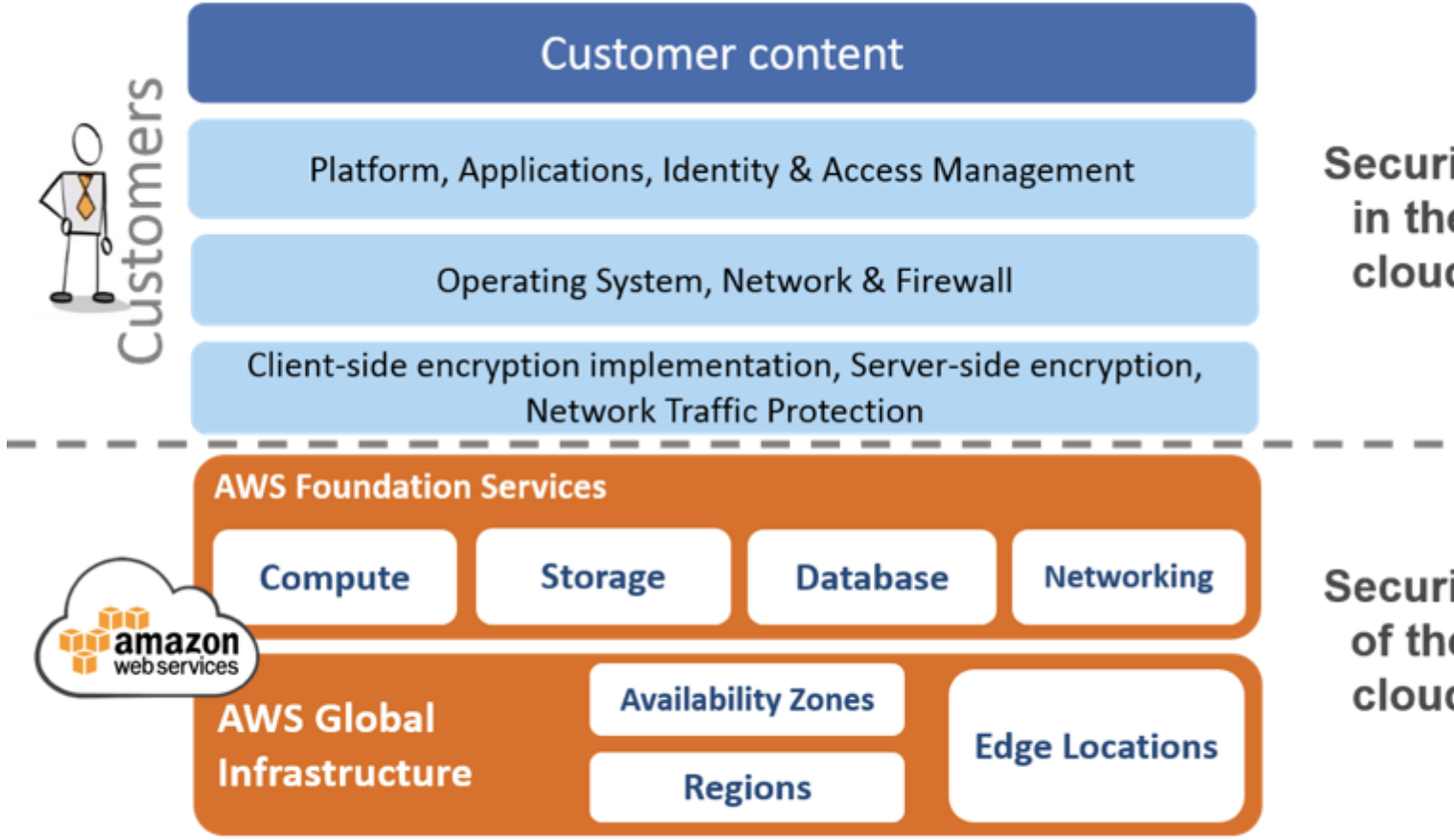
Hardware, SDN, Networking, Internet connection

**Customer Responsibility**

Application code, Application Data, Application Access, Compliance

# Public Cloud "Shared Responsibility Model"

Check Point
SOFTWARE TECHNOLOGIES LTD




Security in the cloud

Security of the cloud

Gartner

"Through 2020, **95%** of cloud security failures will be the **customer's fault.**"

**Solution: Clear Understanding of What A Customer is Responsible For**

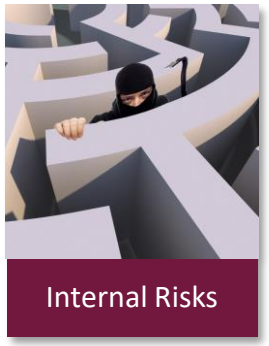
# What are your biggest operation challenges trying to protect cloud workloads?

**34%**

Compliance

**33%**

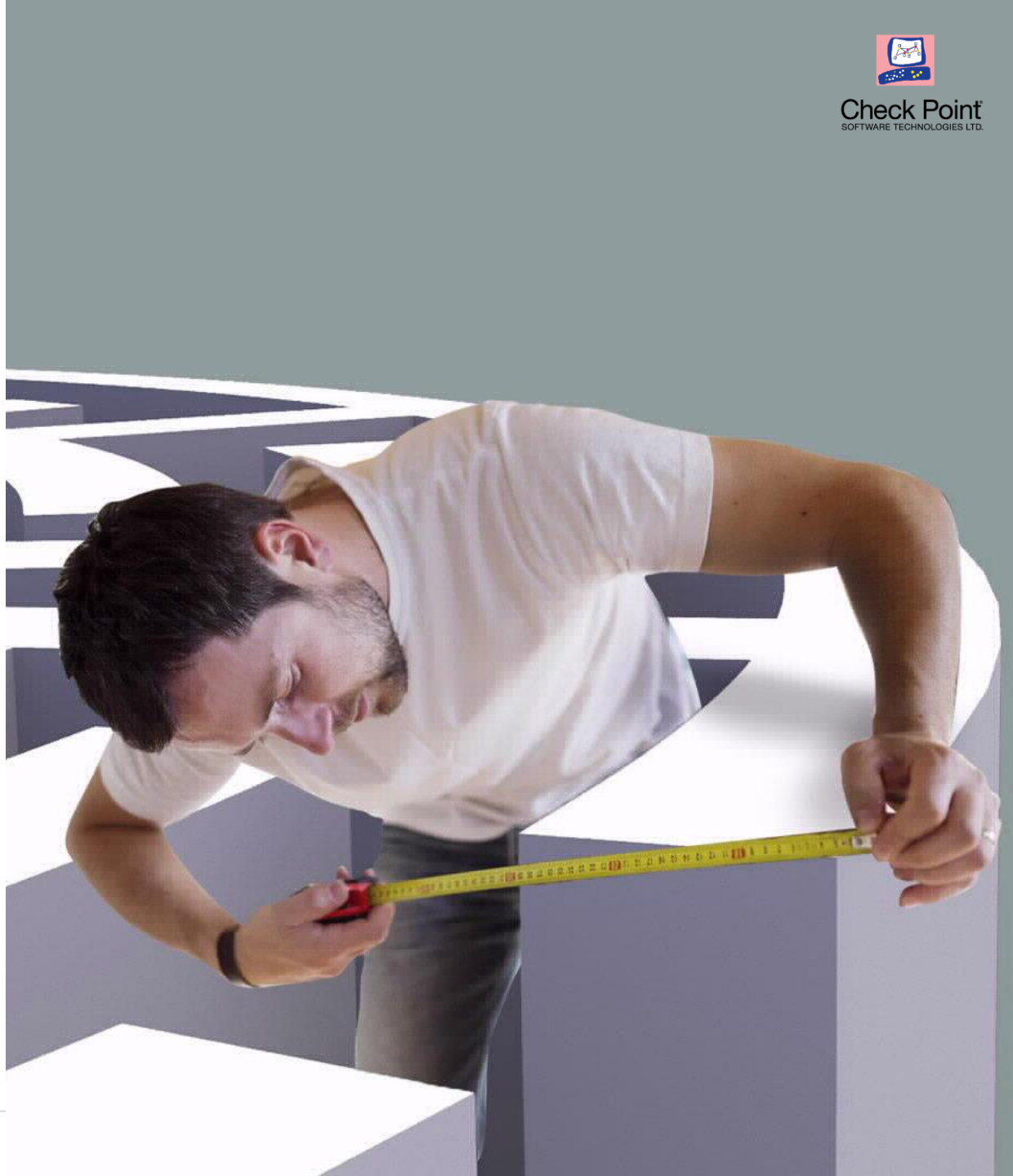
Visibility into infrastructure security




# Compliance & Regulations

- Compliance & self governance are highly focused areas for companies in regulated industries (HIPAA, PCI-DSS) or in certain geographical areas (GDPR)

- Lack of visibility, the dynamic nature of cloud and lack of certainty regarding the location of the payload, all make compliance a challenging task.



Infrastructure Challenges

# Minimal Visibility

- Cloud deployments result in challenges around identifying and quantifying assets
- Invisible and unmanaged assets create large gaps in security enforcement

> *Organizations … are struggling with visibility, making it almost impossible to determine what computing tasks are taking place where, under whose direction.*

Hype Cycle for Cloud Security, Gartner, 7/2018

Infrastructure Challenges

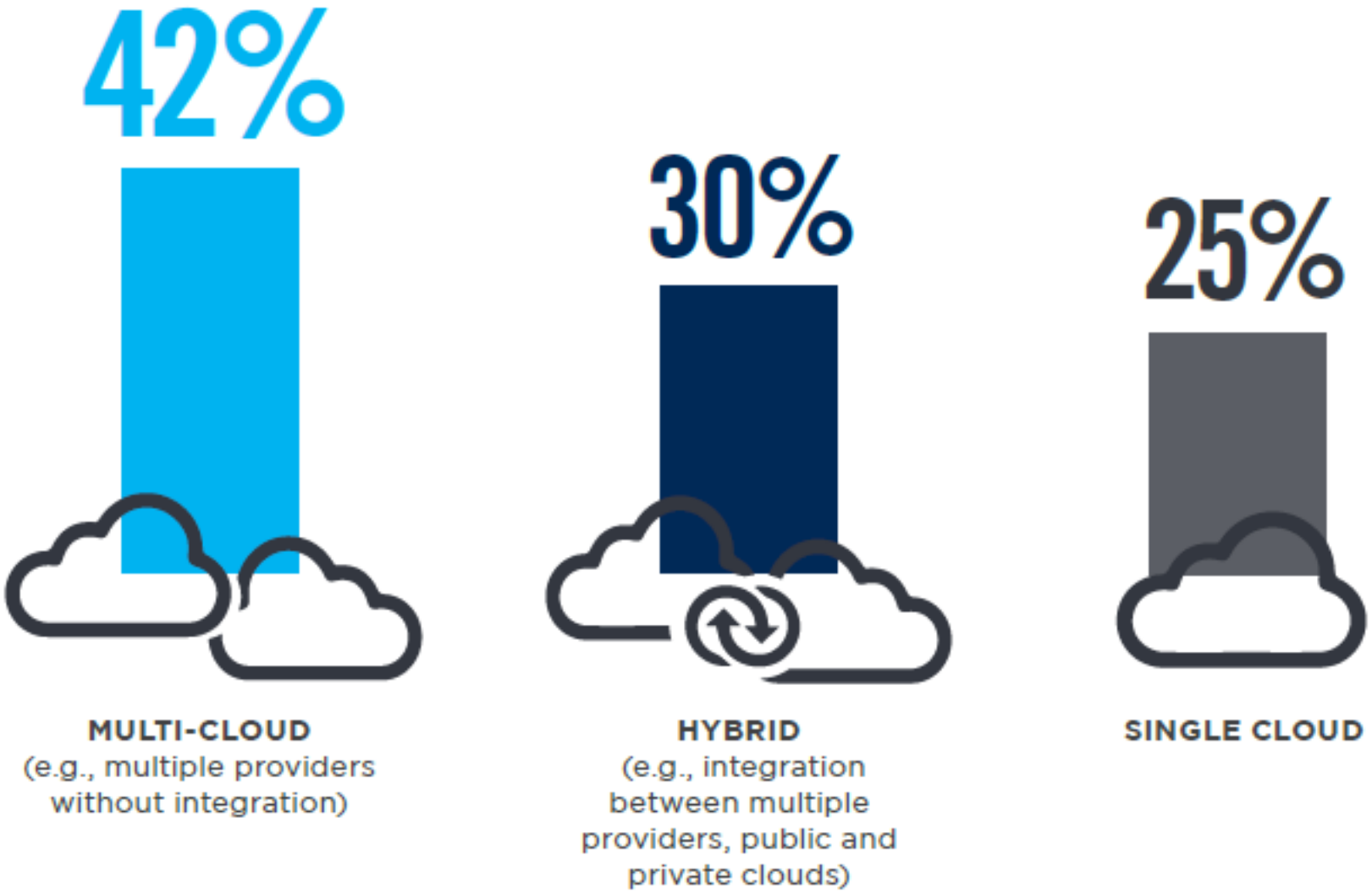
# Ever-changing Workloads

- Cloud assets are provisioned and decommissioned dynamically in large scale and fast pace
- Traditional security tools were not developed for the cloud and thus cannot  enforce policies in such a flexible environment
- Traditional security can’t work with orchestration tools

> *“Cloud computing is dynamic, with workloads spinning up and spooling down. Unprepared organizations are finding that active enforcement of policy becomes increasingly impractical.”*

Hype Cycle for Cloud Security, Gartner, 7/2018

# What is your public cloud deployment strategy?




# Multi Cloud

## Manageability

Relying on the native security controls of the cloud providers limits the ability to manage security in multi-cloud with a unified tool

## Complexity

Difficult to detect and prevent attacks across distributed applications

## Consistency

Security posture and governance policies are not consistently applied across on-premises datacenters and cloud providers

## Flexibility

Cloud environments cannot simultaneously change and apply the security enforcement in real-time

# What are the biggest security threats in the public cloud?

**42%**

Unauthorized access

**42%**

Insecure interfaces/APIs

**40%**

Misconfiguration of the cloud platform/ wrong setup

External Threats

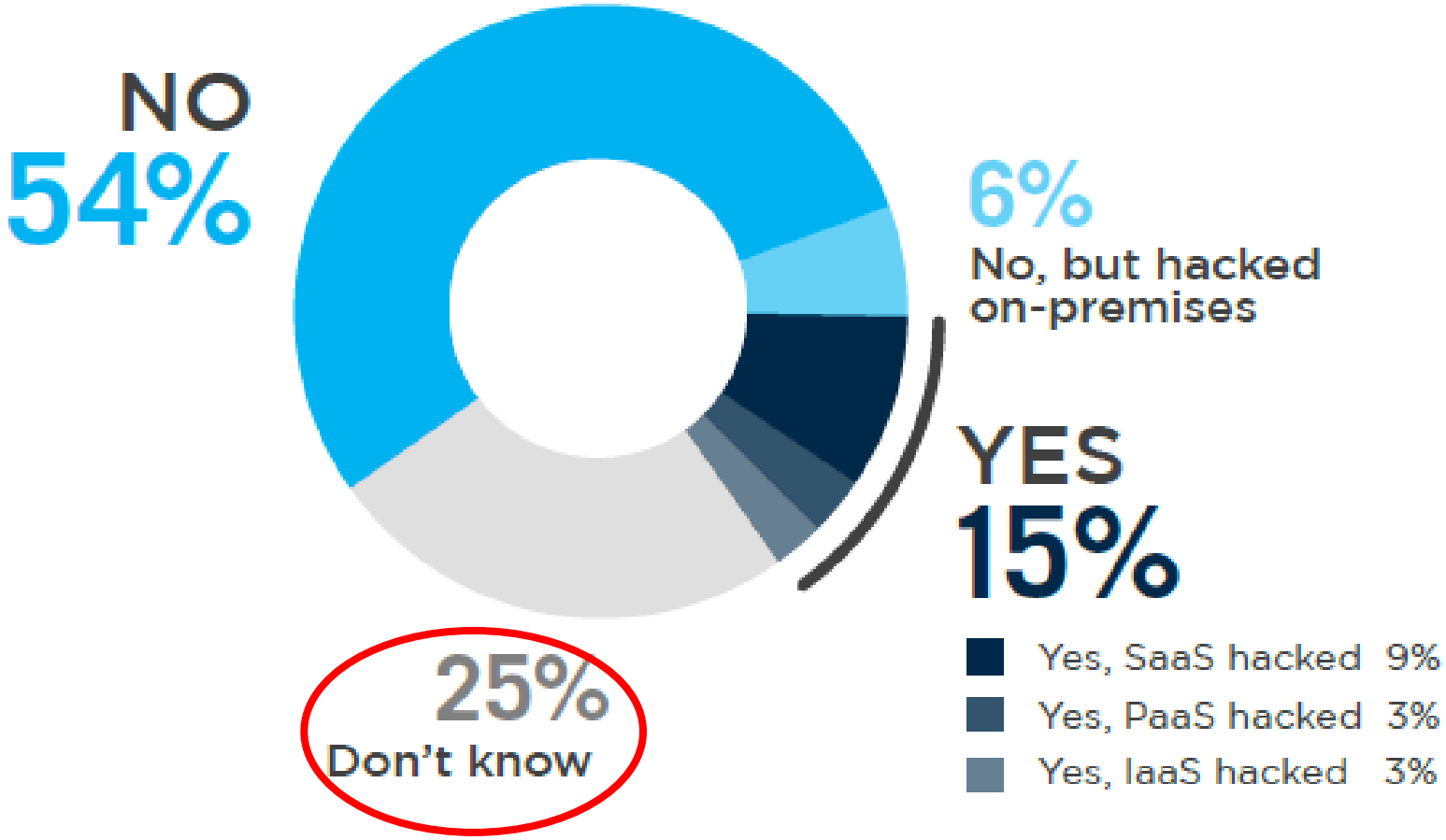
# Zero-day Attacks

- Attackers are targeting cloud workloads because they can be accessed via the internet and not hidden inside the on-premises LAN
- Thru lateral movements, once an asset gets infected, both the Cloud and On-premises infrastructures are at risk (the cloud can be a bridge to the on-premises datacenter)
- The cloud is a company's new data center. It is exposed to the same threats as the on-premises data center and even more, such as: Worms, Crypto locker, Ransomware, BitCoin mining and Bot attacks


# Insider Threats

- Rogue employees, disgruntled or recurred by attacker can leverage misconfigurations to create massive damages.
- An administrator with access to the root account of a cloud service can easily duplicate this info to other places.
- Companies are saving source code on external repositories, such as GitHub, with no access restrictions essentially open for all.
- One of the most common “worst practices” are unencrypted S3 Storage Buckets being left open in AWS

# Has your organization ever been hacked in the public cloud?

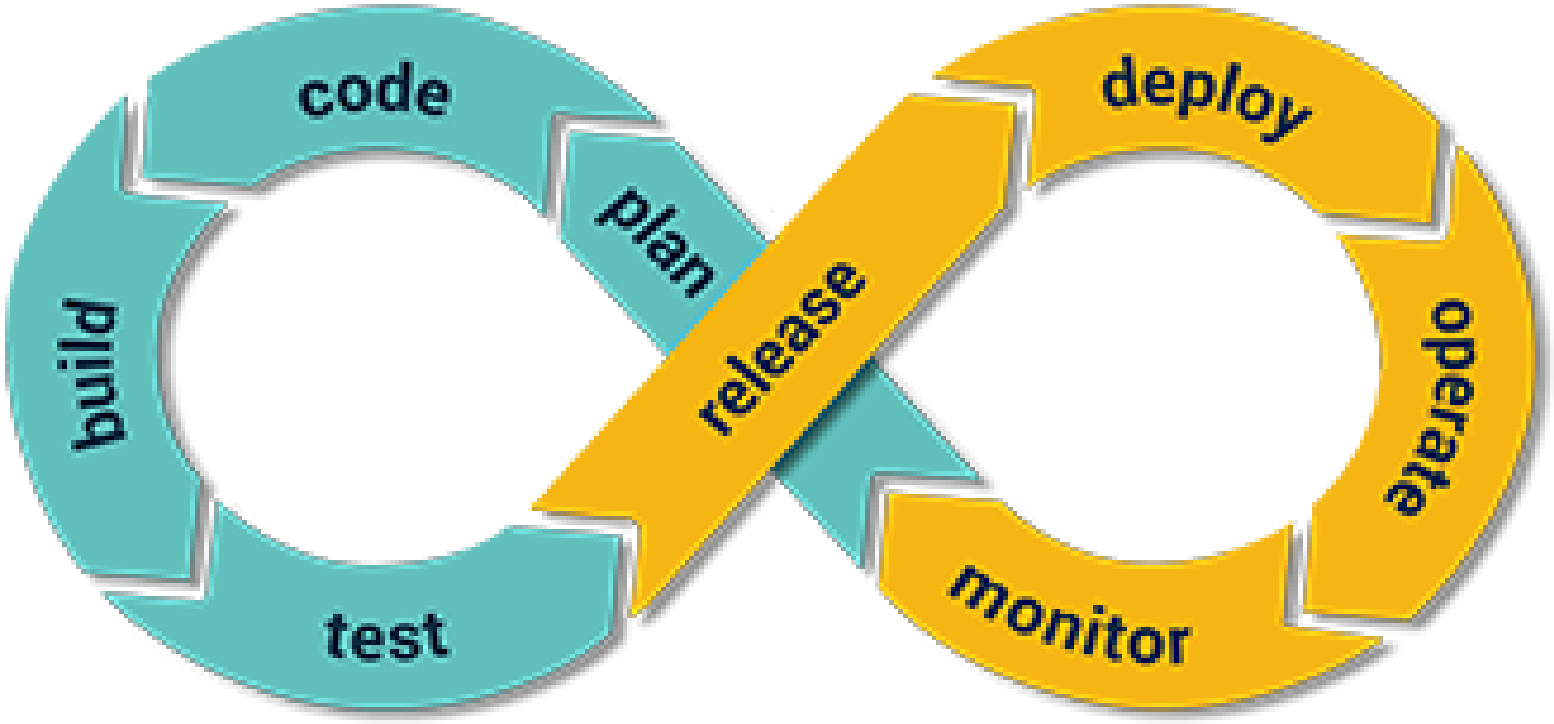


# **Key Trend:** Containers Are Growing in Popularity

"By 2023, more than 70% of global organizations will be running more than two containerized applications in production, up from less than 20% in 2019."

Gartner: 3 Critical Mistakes That I&O Leaders Must Avoid With Containers. (Available by subscription-only)

# Key Trend: "Shift Left" from Production to DevSecOps




## Always Apply Security

- Coding, Commit & Test
- Not just In Production

## More Cost Effective

- Catch problems early
- Coders hate going backwards

## Decreases Friction & Delay

- IT/InfoSec becomes an enabler

# Key Trend: Automation for Security Response & Remediation

Check Point
SOFTWARE TECHNOLOGIES LTD

## Drivers

- Reduce Time and Effort to Resolution of Issues and Alerts
- Increase Scale / Agility / Speed of Cloud Applications

## Best Practices

- Remediation should be prioritized based on Risk assessment and Threat priority
- Manual: High impact, high probability events
- Auto: industry compliance standards & common errors

# What are your cloud security priorities for the coming year?

**25%**

Defending against malware

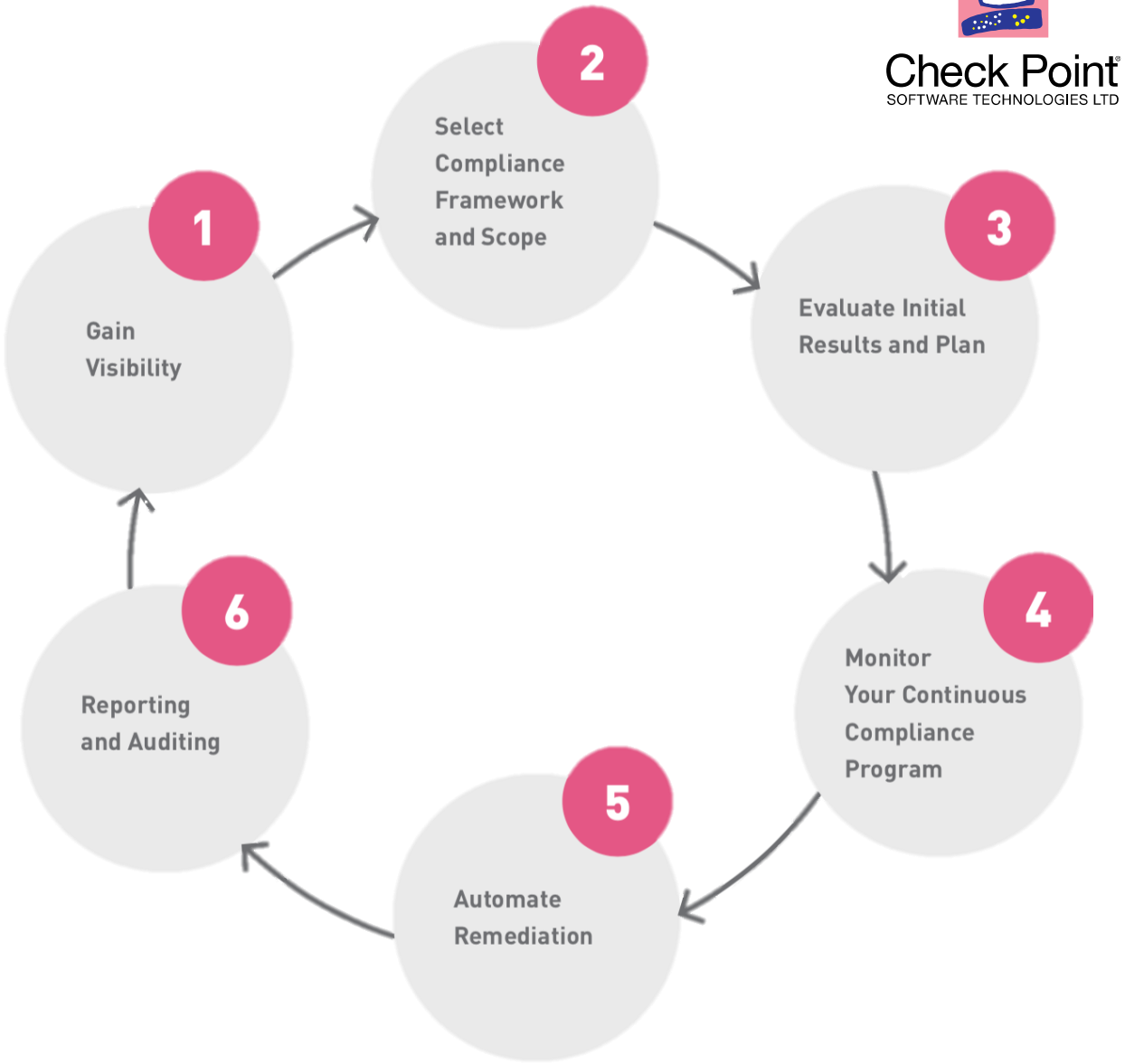
**20%**

Reaching regulatory compliance

**15%**

Securing major cloud apps already in use

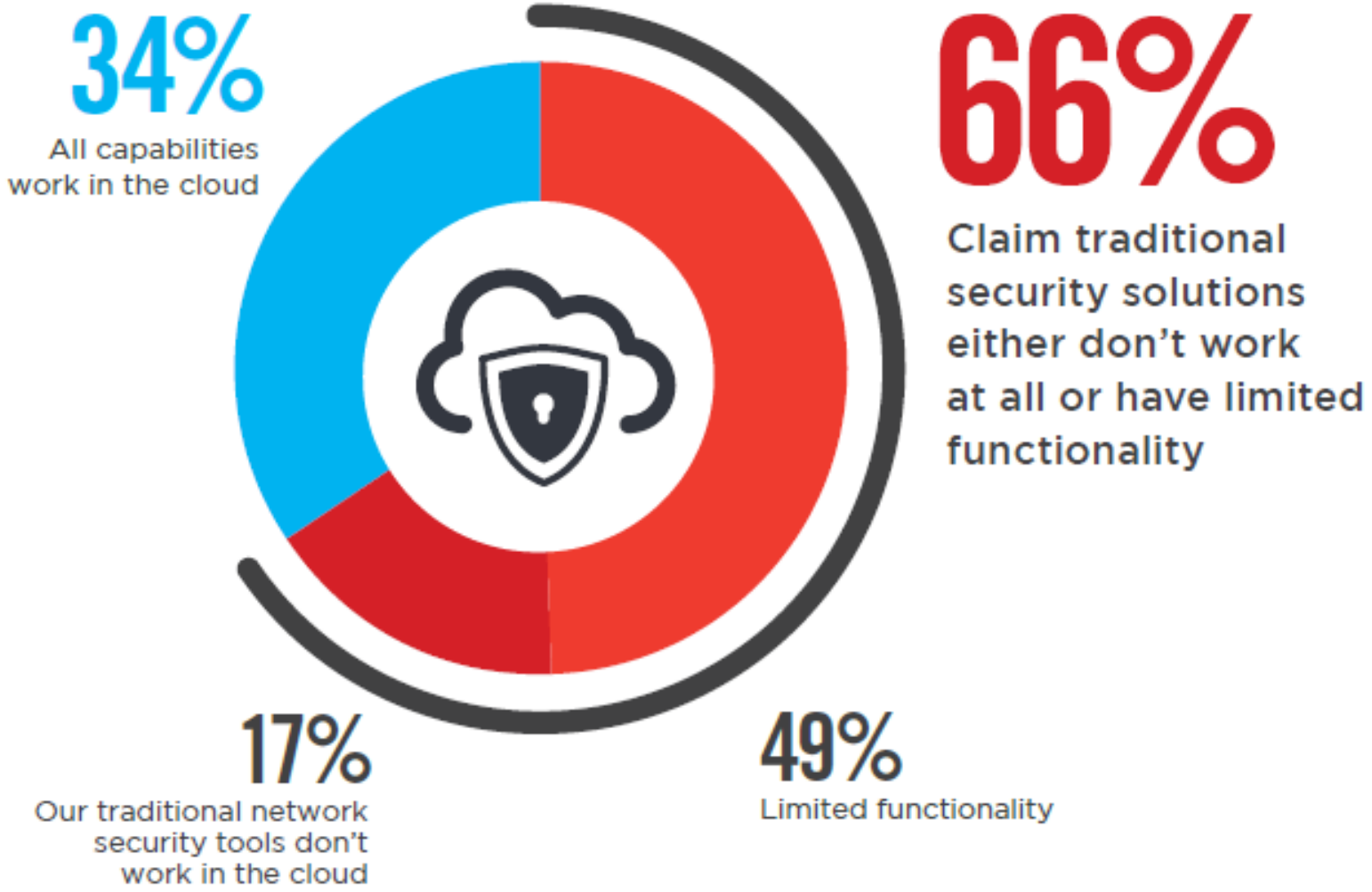

# 6 Steps to Compliance Automation




eBook from Check Point & AWS

AUTOMATE YOUR CLOUD COMPLIANCE JOURNEY IN 6 STEPS

# How well do your traditional network security tools work in cloud environments?



# Microsoft Azure security flaws uncovered

By Sead Fadilpašić 2 days ago

Flaws allowed criminals to take screenshots of banking data.

Microsoft has patched two major flaws in its Azure cloud offering that could have allowed criminals to take full control of servers and steal sensitive data.

The flaws were discovered by researchers at cybersecurity firm Check Point, who said that hackers could abuse Azure Stack to take screenshots of valuable information, such as banking or credit card information. It was also said they could abuse the Azure App Service to "take control" of entire servers.

Microsoft identified the flaws as CVE-2019-1372 and CVE-2019-1234 and worked in collaboration with Check Point on a fix.

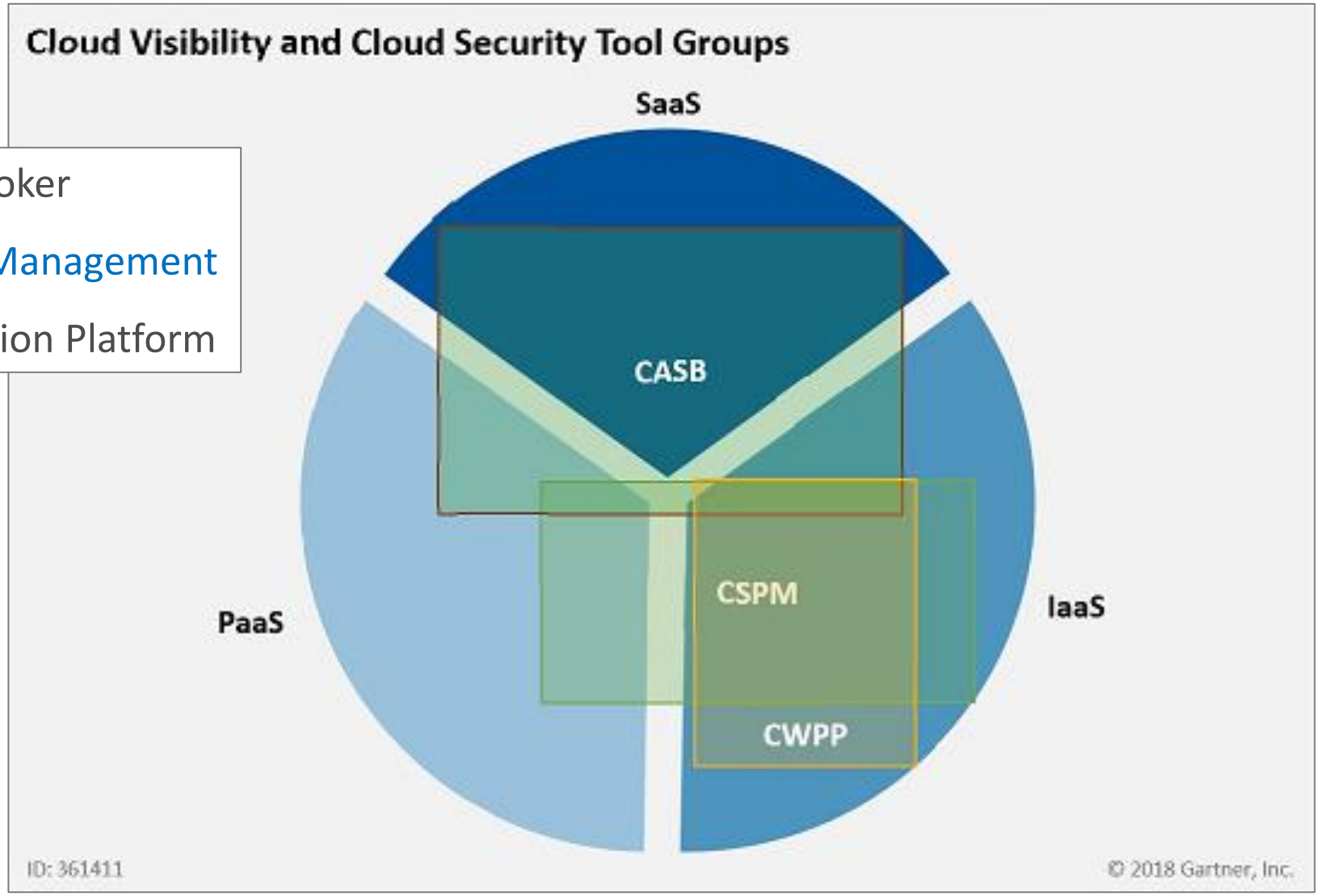
"When operating in the cloud, enterprises often behave with the wild abandon as if their services are hosted in their basement behind the safety of their trusted gateway," said Check Point, describing the problem.

# Cloud Compliance & Security Tool Groups

**CASB:** Cloud Access Security Broker

**CSPM:** Cloud Security Posture Management

**CWPP:** Cloud Workload Protection Platform



# What criteria are most important when selecting security solutions?

Check Point
SOFTWARE TECHNOLOGIES LTD

**44%**

Ability to write custom rules and remediation actions

**41%**

Integration with change management platforms

(ServiceNow, Remedy, JIRA, etc.)

**41%**

Integration with security scanner tools

(Rapid7, Qualys, Tenable, etc.)

# 1 Gain Visibility

Check Point
SOFTWARE TECHNOLOGIES LTD

### Cloud assets configuration

Identify which applications and workloads you have running on the cloud

### Public exposure levels

Understand the applications and workloads that are public-facing and more vulnerable threats

### Network topology

Review your network layout and understand areas to threat exposure

### Security groups

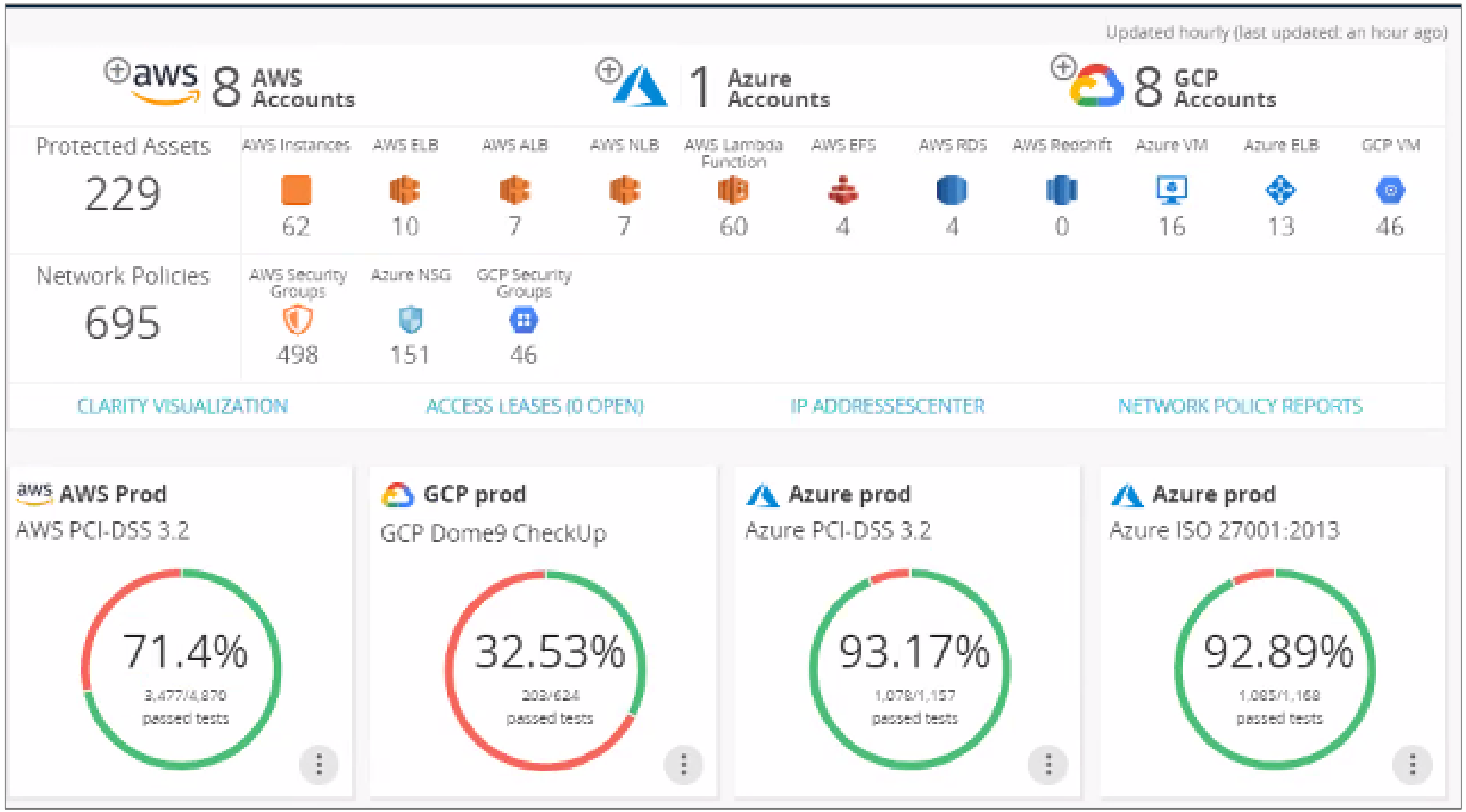
Discover and classify your security groups by varying exposure levels

### Traffic and user activity

Review how applications and workloads interact and the traffic in between them

# Public Cloud Summary Dashboard

Check Point
SOFTWARE TECHNOLOGIES LTD



# Cloud Assets Inventory

Check Point
SOFTWARE TECHNOLOGIES LTD

Cloud Inventory | Compliance & Governance | Network Security | Log.ic | IAM Safety | Administration

29 d9demo@checkpoint.c...

Protected Assets | Dashboard (Preview) | Ngnix-2SubSec | DB1 | DB2 | Notification | webapp2 | Ngnix2-2SibSec | galit-web1

## PROTECTED ASSETS DASHBOARD (Preview)

Search

Add Filters Clear All Hide Filters

Public IP Associated

Selected Dashboard Dome9 Default

ADD DASHBOARD | DELETE DASHBOARD | SAVE AS | SAVE | ADD WIDGET

### Cloud Platforms

- 72.2% AWS
- 11.5% Azure
- 8.7% Kubernetes
- 7.6% GCP

### Asset Types

- 13.4% AWS IAM Role
- 10.7% AWS IAM Us...
- 10.6% AWS VPC
- 9.2% AWS Volume
- 8.0% AWS EC2 Insta...
- 48.1% Other

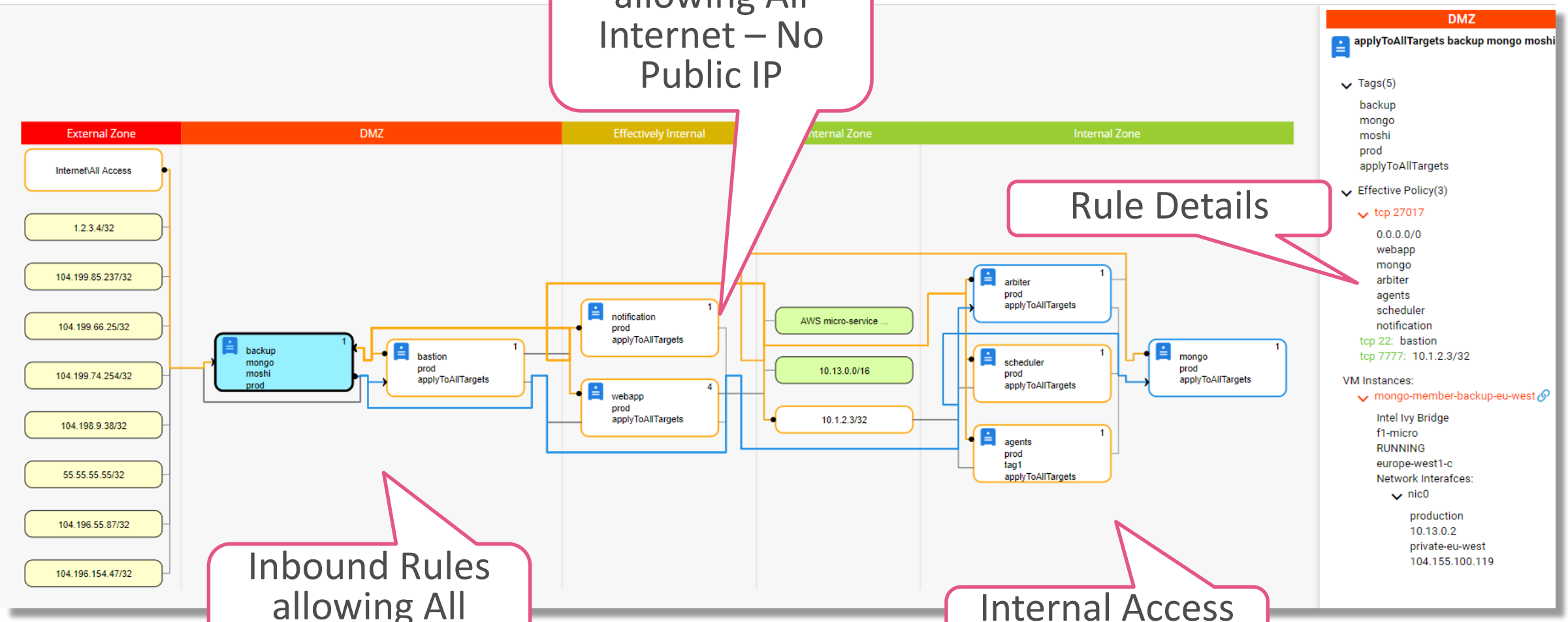
### Cloud Accounts

- 35.8% AWS Prod (0...
- 11.5% Azure prod (...
- 10.9% AWS Stage (7...
- 8.0% dont-remove-...
- 7.7% Morocco (549...
- 26.1% Other

# Network Control Plane Security for Public Clouds

Check Point
SOFTWARE TECHNOLOGIES LTD

Inbound Rules allowing All Internet – No Public IP




Rule Details

Inbound Rules allowing All Internet

Internal Access Only

# 2 Select Compliance Frameworks

Check Point
SOFTWARE TECHNOLOGIES LTD

## NIST

**Azure NIST 800-53 Rev 4**
51 RULES | 1 POLICY
Automated Validation of NIST Special Publication 800-53 (Rev. 4).

RUN ASSESSMENT

## ISO

**Azure ISO 27001:2013**
50 RULES | 1 POLICY
Automated Validation of ISO 27001:2013 Requirements for Azure.

RUN ASSESSMENT

## NIST

**Azure NIST CSF v1.1**
49 RULES | NO POLICIES
Automated Validation of NIST CSF V1.1 for Azure.
For additional reference: https://www.nist.gov/document/2018-

RUN ASSESSMENT

## SOC2

**Azure Dome9 SOC2 based on AICPA TSC 2017**
48 RULES | NO POLICIES
Automated Validation of SOC2 Compliance based on AICPA TSC 2017.

RUN ASSESSMENT

## PCI-DSS

**Azure PCI-DSS 3.2**
46 RULES | 1 POLICY
Automated Validation of Payment Card Industry (PCI) Data Security Standard Version 3.2 - April 2016.

RUN ASSESSMENT

**Azure CIS Foundations v. 1.1.0**
40 RULES | 1 POLICY
Automated Validation of Azure CIS V 1.1.0.
For additional reference:

RUN ASSESSMENT

## GDPR

**Azure GDPR Readiness**
34 RULES | NO POLICIES
Automated GDPR Assessment for Azure.
For additional reference:

RUN ASSESSMENT

## HIPAA

**Azure HIPAA**
28 RULES | 1 POLICY
Automated Validation of U.S. Health Insurance Portability and Accountability Act (HIPAA).

RUN ASSESSMENT

## CIS

**Azure CIS Foundations v. 1.0.0**
16 RULES | 1 POLICY
Automated Validation of Azure CIS V 1.0.0.
For additional reference:

RUN ASSESSMENT

# Governance – Custom Rule Building

Check Point
SOFTWARE TECHNOLOGIES LTD

Builder  Free text

VMInstance should have labels with [ key='Environment' and value

Close the scope  Undo

Operators
= != like unlike regexMatch

Functions
isPrivate() isPublic() isSecurityGroupReference() isCIDR() numberOfHosts() containedInNetworks() overlapWithNetw
isPortPrivate() isEmpty() length() in() before() after()

Test Rule

| Account | Region | Network | |
|---|---|---|---|
| GCP prod | ALL | ALL | TEST |

# 3 Evaluate Initial Results and Plan

Check Point
SOFTWARE TECHNOLOGIES LTD

### 1. Initial assessments

Based on the selected framework and scope, run an initial cloud security & compliance assessment.

Allows compliance and cloud security operations teams to evaluate initial results and better understand specific rules and policies; create a **Baseline**

### 2. Applying exclusions

Once initial findings have been evaluated, apply exclusion to **eliminate irrelevant alerts.**

This will narrow down future notifications to only those that require immediate action.

Exceptions are captured in a detailed log for future audits

### 3. Adding customizations

After applying exceptions, you can start adding customization.

- Security rules
- Internal Best Practices
- Notification policies

# Evaluate Initial Results and Plan

Check Point
LOGIES LTD

Add Filter | Clear All

Show by Rule | SHOW REMEDIATION ACTIONS | SHOW EXCLUSIONS

Cloud Inventory | Compliance & Governance | Network Security | Log.ic | IAM Safety | Administration | 29 | d9demo@checkpoint.c...

Dashboard (Preview) | Alerts | System Alerts

| Created Time | Cloud Account | Source | Rule | Entity | Entity Type | Assignee | Ack. | Exc. | Rem. |
|---|---|---|---|---|---|---|---|---|---|
| Dec 19, 2019 1:26 PM | aws Morocco (549639478491) | Compliance Engine | S3 Buckets - without loggin... | config-bucket-549639478491 (config-bucket-549639478491) | S3Bucket | Unassigned | | | |

High

**Compliance Rule**
S3 Buckets - without logging enabled

**Compliance Ruleset**
Dome9 AWS Dashboards

**Compliance rule Description**
Logging enables to track access requests to the S3 bucket. Access log information can be useful in security and access audits.

**Compliance rule Remediation**
Turn on logging. AWS reference document: http://docs.aws.amazon.com/AmazonS3/latest/user-guide/server-access-logging.html

**GSL**

```
S3Bucket should have logging.enabled=true
```

**Compliance Sections**
S3Bucket

**Remediation Actions**
N/A

**Alert ID**
V/IVTcJ29byW8W7HMjhQWQ

**Cloud Account**
aws Morocco (549639478491)

**Region**
N. Virginia

**VPC**
N/A

**Entity**
config-bucket-549639478491 (config-bucket-549639478491)

**Entity Tags**
N/A

**Entity Type**
S3Bucket

Assign User

Severity: High

**Comments**
No comments are available

EXCLUDE

Failed | S3 Bu | 74 TE | SC-13

Failed | S3 Bu | 74 TE | SC-13

Failed | Use e | 74 TE | SC-13

Failed | Ensur | 329 T | SC-7

Failed | Ensur | 329 T | SC-7

Failed | Secur | 329 T | SC-7

Failed | Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password | 30 TESTED | 23 RELEVANT | 22 NON COMPLIANT | IA-2 | IA-3 | IA-4 | IA-5 | IA-7 | SC-12 | Expand

# 4 Monitor Your Continuous Compliance

Check Point
SOFTWARE TECHNOLOGIES LTD

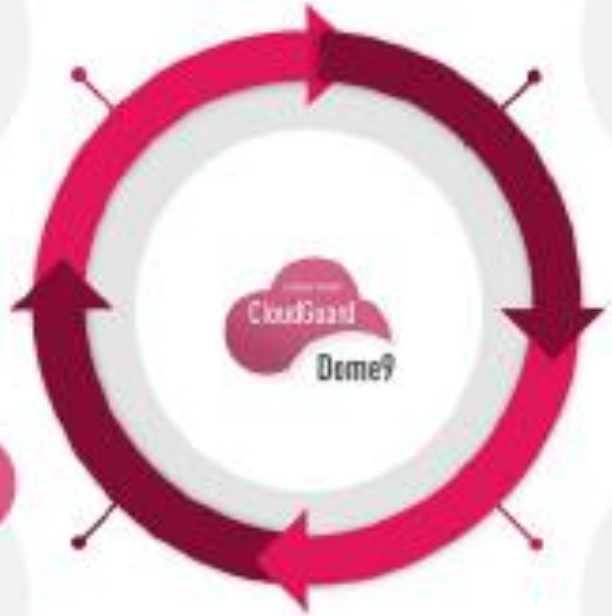
1. Define Frequency
   - Daily, Weekly, Monthly
2. Identify Owners
   - Defined by a Notification Policy
   - Different reports by account type, application, tags, compliance
   - Role-based Dashboards
3. Integrate with other internal process and support tools
   - Results and remediation plans for your Compliance Assessments can be consumed by your internal tools
   - E-mail, SNS or SEIMs like ServiceNow, PagerDuty, Jira

# 5 Automate Remediation

Check Point
SOFTWARE TECHNOLOGIES LTD

1 Compliance at the click of a button

2 Continuous Alerts and Notifications




4 Automated Remediation

3 Integration with ITMS tools

cloudbots

pd Jira servicenow slack

# Automate Remediation

Check Point
SOFTWARE TECHNOLOGIES LTD

Cloud Inventory | Compliance & Governance | Network Security | Log.ic | IAM Safety | Administration

Dashboard (Preview) | Alert

Create New Remediation

Ruleset

Dome9 AWS Dashboards

Remediate by Rule

Remediate by Cloud Account

Morocco (549639478491)

Remediate by Entity

Entity Name: config-bucket-549639478491

Entity ID

Add Cloud Bot

Add

mark_for_stop_ec2_resource
rds_quarantine_instance
s3_delete_acls
s3_delete_permissions
s3_enable_encryption
s3_enable_logging
s3_enable_versioning
sg_delete
sg_rules_delete

(0/200)

| Created Time | Cloud | Entity Type | Assignee | Ack. | Exc. | Rem. |
|---|---|---|---|---|---|---|
| Dec 19, 2019 1:26 PM | aws M (5496 | S3Bucket | Unassigned | | | |
| Dec 19, 2019 1:26 PM | aws M (5496 | S3Bucket | Unassigned | | | |
| Dec 19, 2019 1:17 PM | aws M (5496 | S3Bucket | Unassigned | | | |
| Dec 19, 2019 1:17 PM | aws M (5496 | S3Bucket | Unassigned | | | |
| Dec 19, 2019 1:17 PM | aws M (5496 | S3Bucket | Unassigned | | | |
| Dec 19, 2019 1:17 PM | aws M (5496 | S3Bucket | Unassigned | | | |
| Dec 19, 2019 12:15 PM | aws M (5496 | S3Bucket | Unassigned | | | |
| Dec 19, 2019 12:15 PM | aws M (5496 | S3Bucket | Unassigned | | | |
| Dec 19, 2019 12:15 PM | aws M (5496 | S3Bucket | Unassigned | | | |
| Dec 19, 2019 12:15 PM | aws M (5496 | S3Bucket | Unassigned | | | |
| Dec 19, 2019 | aws M | S3Bucket | Unassigned | | | |

# 6 Reporting and Auditing

Cloud Platform: Azure
Compliance Ruleset: Azure NIST 800-53 Rev 4

Azure prod (6863828a-3f21-4624-9b05-4e5f8e8f1258)

Show full report

**Entity Tests**
Score: 92.09% (Previous: 92.09%)

Previous Current

| 1117 | 1117 | 66 | 66 | 15 | 15 | 15 | 15 |
|---|---|---|---|---|---|---|---|
| | | High | | Medium | | Low | |

## Failed Tests by Rule

| Rule Name | Rule ID | Compliance Section | Findings |
|---|---|---|---|
| Ensure that 'Secure transfer required' is enabled for Storage Accounts | D9.AZU.CRY.06 | SC-13 SC-8 | 39 |
| Ensure that logging for Azure KeyVault is 'Enabled' | D9.AZU.CRY.02 | SC-13 SC-8 AU-2 AU-7 AU-11 AU-12 AU-3 AU-9 | 10 |
| VirtualMachine with administrative service: SSH (TCP:22) is too exposed to the public internet | D9.AZU.NET.AG4.VirtualMachine.22.TCP | SC-7 | 5 |
| Ensure entire Azure infrastructure doesn't have access to Azure SQL Server | D9.AZU.NET.02 | AC-14 AU-3 SC-7 AC-3 | 3 |
| Ensure that SQL server access is restricted from the internet | D9.AZU.NET.01 | AC-14 AU-3 SC-7 AC-3 | 2 |
| Ensure that the Redis Cache accepts only SSL connections | D9.AZU.CRY.05 | SC-13 SC-8 | 1 |
| Redis attached subnet Network Security Group should allow ingress traffic only to ports 6379 or 6380 | D9.AZU.NET.15 | SC-7 SC-2 AC-4 AC-17 | 1 |

# Public Cloud Summary Dashboard

Updated hourly (last updated: an hour ago)

8 AWS Accounts | 1 Azure Accounts | 8 GCP Accounts

| Protected Assets | AWS Instances | AWS ELB | AWS ALB | AWS NLB | AWS Lambda Function | AWS EFS | AWS RDS | AWS Redshift | Azure VM | Azure ELB | GCP VM |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 229 | 62 | 10 | 7 | 7 | 60 | 4 | 4 | 0 | 16 | 13 | 46 |

| Network Policies | AWS Security Groups | Azure NSG | GCP Security Groups |
|---|---|---|---|
| 695 | 498 | 151 | 46 |

CLARITY VISUALIZATION | ACCESS LEASES (0 OPEN) | IP ADDRESSESCENTER | NETWORK POLICY REPORTS

**AWS Prod**
AWS PCI-DSS 3.2
71.4%
3,477/4,870
passed tests

**GCP prod**
GCP Dome9 CheckUp
32.53%
203/624
passed tests

**Azure prod**
Azure PCI-DSS 3.2
93.17%
1,078/1,157
passed tests

**Azure prod**
Azure ISO 27001:2013
92.89%
1,085/1,168
passed tests

# Final Thoughts

Check Point
SOFTWARE TECHNOLOGIES LTD

1. Maintaining confidence in your cloud security posture depends on:
   - Your ability to keep pace with the agile nature of the cloud,
   - Having the right platform to adequately protect a multi-cloud environment,
   - Multi-cloud visibility, with rich data analytics capabilities, and
   - Upholding compliance and governance standards
2. Create a cross-functional “Cloud Center of Excellence” team
   - Representation from Network, Security, Compliance, DevOps & Cloud teams
   - Help define requirements, execute cloud strategy, recommend policies and enforce compliance
3. Evaluate third-party tools for your multi-cloud security posture management
   - Engage in a Trial or POC; SaaS solutions are easy to ty in your own environment
   - Identify your top Cloud Challenges and Key Use Cases
   - External Compliance Regulations and Internal Security Policies and best practices
   - Integration into your CICD Pipeline, SEIM, Operations

# Thank You

**Lee Psinakis**
**Cloud Security Specialist**
**Check Point Software Technologies**
**lee.psinakis@checkpoint.com**