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.

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
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”

Solution: Clear Understanding of What A Customer is Responsible For

“Through 2020, 95% of cloud security failures will be the customer’s fault.”

Customer content
- Platform, Applications, Identity & Access Management
- Operating System, Network & Firewall
- Client-side encryption implementation, Server-side encryption, Network Traffic Protection

Security in the cloud

Security of the cloud

AWS Foundation Services
- Compute
- Storage
- Database
- Networking

AWS Global Infrastructure
- Availability Zones
- Regions
- Edge Locations
What are your biggest operation challenges trying to protect cloud workloads?

- Compliance: 34%
- Visibility into infrastructure security: 33%
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.
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
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.”

What is your public cloud deployment strategy?

- 42% Multi-cloud (e.g., multiple providers without integration)
- 30% Hybrid (e.g., integration between multiple providers, public and private clouds)
- 25% Single cloud
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?

- Unauthorized access: 42%
- Insecure interfaces/APIs: 42%
- Misconfiguration of the cloud platform/wrong setup: 40%
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

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

1. Gain Visibility
2. Select Compliance Framework and Scope
3. Evaluate Initial Results and Plan
4. Monitor Your Continuous Compliance Program
5. Automate Remediation
6. Reporting and Auditing

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?

34% All capabilities work in the cloud

66% Claim traditional security solutions either don’t work at all or have limited functionality

17% Our traditional network security tools don’t work in the cloud

49% Limited functionality
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

Cloud Visibility and Cloud Security Tool Groups

- SaaS
- PaaS
- IaaS

CASB

CSPM

CWPP
What criteria are most important when selecting security solutions?

- **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

**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

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

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

- **Clarity Visualization**:
  - 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%
      - 1,076/1,157 passed tests
    - Azure ISO 27001:2013: 92.89%
      - 1,085/1,168 passed tests
Cloud Assets Inventory

PROTECTED ASSETS DASHBOARD (Preview)

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 User
- 10.6% AWS VPC
- 9.2% AWS Volume
- 8.0% AWS EC2 Instance
- 48.1% Other

Cloud Accounts
- 35.8% AWS Prod (Cloud...
- 11.5% Azure prod (Cloud...
- 10.9% AWS Stage (Cloud...
- 8.0% dont-remove (Cloud...
- 7.7% Morocco (Cloud...
- 26.1% Other

Welcome to the Future of Cyber Security
©2019 Check Point Software Technologies Ltd.
Network Control Plane Security for Public Clouds

Inbound Rules allowing All Internet – No Public IP

Rule Details

Inbound Rules allowing All Internet

Internal Access Only
2. Select Compliance Frameworks

<table>
<thead>
<tr>
<th>Framework</th>
<th>Description</th>
<th>Additional Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIST</td>
<td>Azure NIST 800-53 Rev 4 Automated Validation of NIST Special Publication 800-53 (Rev. 4).</td>
<td>Run Assessment</td>
</tr>
<tr>
<td>NIST</td>
<td>Azure NIST CSF v1.1 Automated Validation of NIST CSF V1.1 for Azure. For additional reference: <a href="https://www.nist.gov/document/2018-">https://www.nist.gov/document/2018-</a></td>
<td>Run Assessment</td>
</tr>
<tr>
<td>SOC2</td>
<td>Azure Dome9 SOC2 based on AICPA TSC 2017 Automated Validation of SOC2 Compliance based on AICPA TSC 2017.</td>
<td>Run Assessment</td>
</tr>
<tr>
<td>GDPR</td>
<td>Azure GDPR Readiness Automated GDPR Assessment for Azure. For additional reference:</td>
<td>Run Assessment</td>
</tr>
<tr>
<td>HIPAA</td>
<td>Azure HIPAA Automated Validation of U.S. Health Insurance Portability and Accountability Act (HIPAA).</td>
<td>Run Assessment</td>
</tr>
<tr>
<td>CIS</td>
<td>Azure CIS Foundations v. 1.1.0 Automated Validation of Azure CIS V 1.1.0. For additional reference:</td>
<td>Run Assessment</td>
</tr>
</tbody>
</table>
Governance – Custom Rule Building

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

Operators

= != like unlike regexMatch

Functions

isPrivate() isPublic() isSecurityGroupReference() isCIDR() numberOfHosts() containedInNetworks() overlapWithNet

isPortPrivate() isEmpty() length() in() before() after()

Test Rule

Account
GCP prod

Region
ALL

Network
ALL

TEST
3. Evaluate Initial Results and Plan

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
4 Monitor Your Continuous Compliance

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

1. Compliance at the click of a button
2. Continuous Alerts and Notifications
3. Integration with ITMS tools
4. Automated Remediation
5. Continuous Compliance

©2019 Check Point Software Technologies Ltd.
Automate Remediation
### Reporting and Auditing

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

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

#### Failed Tests by Rule

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Rule ID</th>
<th>Compliance Section</th>
<th>Findings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that ‘Secure transfer required’ is enabled for Storage Accounts</td>
<td><strong>D9_AZU.CRY.05</strong></td>
<td>SC-13 SC-8</td>
<td>39</td>
</tr>
<tr>
<td>Ensure that logging for Azure KeyVault is ‘Enabled’</td>
<td><strong>D9_AZU.CRY.02</strong></td>
<td>SC-13 SC-8 AU-2 AU-7 AU-11 AU-12 AU-3 AU-9</td>
<td>10</td>
</tr>
<tr>
<td>VirtualMachine with administrative service: SSH (TCP:22) is too exposed to the public internet</td>
<td><strong>D9_AZU.NET_AG4.VirtualMachine_22_TCP</strong></td>
<td>SC-7</td>
<td>5</td>
</tr>
<tr>
<td>Ensure entire Azure infrastructure doesn’t have access to Azure SQL Server</td>
<td><strong>D9_AZU.NET.02</strong></td>
<td>AC-14 SC-7 AC-3</td>
<td>3</td>
</tr>
<tr>
<td>Ensure that SQL server access is restricted from the internet</td>
<td><strong>D9_AZU.NET.01</strong></td>
<td>AC-14 SC-7 AC-3</td>
<td>2</td>
</tr>
<tr>
<td>Ensure that the Redis Cache accepts only SSL connections</td>
<td><strong>D9_AZU.CRY.01</strong></td>
<td>SC-13 SC-8</td>
<td>1</td>
</tr>
<tr>
<td>Redis attached subnet Network Security Group should allowingrass traffic only to ports 6379 or 6380</td>
<td><strong>D9_AZU.NET.15</strong></td>
<td>SC-7 SC-2 AC-4 AC-17</td>
<td>1</td>
</tr>
</tbody>
</table>
Public Cloud Summary Dashboard
Final Thoughts

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 try 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