SECURING THE CLOUD WITH CLOUDGUARD DOME9

Tim Duffy
Cloud Security Sales Specialist
Don’t Envy the CISO

Jan 19, 2017 Attacker start wiping data from CouchDB and Hadoop databases

Jul 12, 2017 Cloud Security Failure: Millions of Wrestling Fans’ Personal Data Exposed

Jun 1, 2017 Booz Allen Hamilton leaves 60,000 unsecured DOD files on AWS server

Dec 19, 2017 120 Million American Households Exposed In 'Massive' ConsumerView Database Leak

Feb 16, 2017 The Era of Data-Jacking is Here. Are You Ready?

Jul 12, 2017 Misconfigured Amazon Storage Exposes 14 Million Verizon Customer Records

Apr 3, 2018 37M Panera Bread customer records found to be exposed to all and sundry in the cloud

Jul 17, 2017 Dow Jones customer data exposed in cloud error
Compliance in the Cloud - Key Challenges

What are your biggest operational, day-to-day headaches trying to protect cloud workloads?

43% Visibility into infrastructure security
38% Compliance
35% Setting consistent security policies
35% Security can't keep up with pace of change in applications

34% Lack of integration with on-premises security technologies
33% No automatic discovery/visibility/control to infrastructure security
31% Can't identify misconfiguration quickly
30% Complex cloud to cloud on-premises security rule matching

Reporting security threats 27% | Remediation threats 23% | Automatically enforcing security across multiple datacenters 23% | Lack of feature parity with on-premises security solution 21% | No flexibility 15% | Not sure/other 16%

2018 CLOUD SECURITY REPORT
Top Problems To Solve

- **Visibility of Security Posture**
  - It’s hard to grasp the state of security, especially at large scale and across multiple clouds

- **Compliance & Governance**
  - Expert knowledge is required to map security state to Compliance Requirements on an ongoing basis

- **Guardrails**
  - Shift left SDLC (Software Developer Life Cycle) trends require flexible security policies designed for cloud services and integrated into the CI/CD (Continuous Integration/Continuous Deployment) pipeline

**Operational Challenge:** Not enough experts and time to do it at scale
CloudGuard: Comprehensive Multi-Cloud Security

- Full security visibility and control
- Cloud services and applications are never exposed
- Continuous compliance for cloud native services
- Auto-remediation of security misconfigurations
- Active protection against identity theft and data loss

+ 

- Market-leading threat prevention – anti-bots, IPS, anti-malware, AV and more
- Securely connect your hybrid cloud
- Adaptive policy for macro-segmentation
Architectures are not what they used to be...
The Public Cloud Shared Responsibility Model

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

Security of the cloud
"Many cloud service providers invest heavily in incorporating higher levels of security into their products to continue building confidence that their data is more secure."

Solution: Clear Understanding of What A Customer is Responsible For
The rise of Cloud Security Posture Management (CSPM)

Top 10 Security Projects for 2018. No. 7: Cloud security posture management (CSPM): This should be considered by organizations in search of a comprehensive, automated assessment of their IaaS/platform as a service (PaaS) cloud security posture to identify areas of excessive risk.

Dome9 Security and Compliance Platform

SaaS Platform for Security and Compliance Automation in the Public Cloud

Native Support for the Big 3 Clouds

aws

Azure

Google Cloud

Comprehensive Protection Across 3 Key Security Areas

Compliance & Governance

Network Security

Cloud Security Intelligence
Where Does Dome9 Fit?

Dome9 Arc integrates into multiple phases in the InfoSec lifecycle

**Prevention before Detection**

**Assess**
- Visualize network topology
- Understand security posture
- Identify misconfigurations and threats
- Test against industry best practices

**Control**
- Enforce best practices
- Prevent unauthorized changes
- Conform to compliance standards

**Remediate**
- Fix issues with policy configurations
- Model gold standard
- Actively protect environments
Security at the Speed of DevOps

1. Validation Before Deployment: Test security and compliance posture prior to deployment – by testing intent (CFT & Terraform)
3. Secure & Trusted Deployment: Maintain a closed-by-default security posture during deployment
4. Actionable Alerts: Streamline alerts & incorporate auto-remediation capabilities
<table>
<thead>
<tr>
<th>Target</th>
<th>Pain Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Migration</td>
<td>• Wants to get started securely in the cloud</td>
</tr>
<tr>
<td></td>
<td>• Consistent security is challenging in heterogeneous cloud environments</td>
</tr>
<tr>
<td></td>
<td>• Need better visibility</td>
</tr>
<tr>
<td>Compliance</td>
<td>• Needs to comply with regulatory and/or industry compliance standards such as PCI DSS, HIPAA, SOC 2 and GDPR</td>
</tr>
<tr>
<td></td>
<td>• Manual self-assessments and proving compliance remediation is time-consuming</td>
</tr>
<tr>
<td>Security Operations</td>
<td>• Security architecture reviews</td>
</tr>
<tr>
<td></td>
<td>• Dealing with security configuration drift</td>
</tr>
<tr>
<td></td>
<td>• Lack of common tools across cloud platforms</td>
</tr>
<tr>
<td></td>
<td>• Preventing unauthorized changes</td>
</tr>
<tr>
<td>DevSecOps</td>
<td>• Security architecture reviews</td>
</tr>
<tr>
<td></td>
<td>• Dealing with security configuration drift</td>
</tr>
<tr>
<td></td>
<td>• Lack of common tools across cloud platforms</td>
</tr>
</tbody>
</table>

[Internal Use] for Check Point employees
Dome9 Clarity: Complete Network & Security Visibility

- Automatic discovery and classification of security groups by exposure level
- Intuitive visualization of topology
- Object-based IP management with IP lists
- VPC flow log overlay for traffic analysis
- Click-through remediation
Automated Compliance

Automated Remediation

Compliance in a click of a button

Integration with Ticketing & Paging tools

Notifications to your email or SNS Service
Thank You