Security by Cloud
Can the Cloud improve security resilience anywhere?

ISSE, November 2016

johan.fontaine@be.pwc.com
@jfte
From Cloud Security ...
Cloud Security as we know it

Trust in Cloud computing is soaring: PwC GSISS numbers

% of organizations using some form of Cloud computing

- 2012: 38%
- 2013: 47%
- 2014: 55%
- 2015: 64%

November 2016
... over cloud-enabled cybersecurity ...

Cloud computing is adopted for security reasons:

• PwC in 2015: 59% of businesses reported that their information security program has improved by using Cloud services

• Clutch.co security-trends-in-enterprise-cloud-computing March 2016:
  • 64% of enterprises consider cloud infrastructure a more secure alternative to legacy systems
  • Security is the top Primary Cloud Computing Benefit

Use the broad Cloud to implement security controls
... to Security by Cloud
Using the Cloud to improve security resilience

Use CSPs own provided security capabilities and controls:

• In an Architecture of simplicity
• To improve security capabilities across Cloud, On-Premise and in Hybrid models
• Limit the need for change and impact on organizations
• Well enough to deter or detect most attacks, not best of breed
• With the already most used CSPs, who will not vanish overnight
**Select top 3 CSPs**

Top 3 most used CSPs according to Clutch.co, December 2015

- Microsoft Azure (MSA): 23%
- Amazon Web Services (AWS): 22%
- Google Cloud Platform (GCP): 21%

Gartner Magic Quadrants: IaaS & Public Cloud Storage

- Top leader: AWS
- Second and only other leader: MSA
- Only visionary: GCP
- All others are niche players.
**Security Controls**
classification: main defence capabilities categories

- Preventive
- Detective
- Corrective
29 available services providing Security by Cloud

# per defence capability & CSP

<table>
<thead>
<tr>
<th>Service</th>
<th>Preventive</th>
<th>Detective</th>
<th>Corrective</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS</td>
<td>4</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>GCP</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>MSA</td>
<td>12</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
Completeness of security controls: On-Premise

# per level & CSP

- AWS
- GCP
- MSA

Low | Medium | High
---|---|---
0 | 1 | 8
Completeness of security controls: Cloud

# per level & CSP

Security by Cloud
PwC

November 2016
Completeness of security controls: Hybrid

# per level & CSP

Security by Cloud
PwC
November 2016
Suited for size of organisations

# per level & CSP

Security by Cloud
PwC
November 2016
Ease of implementation

# per level & CSP
Ease of implementation vs completeness
Average completeness score per ease level

- Easy: 3.1
- Moderate: 5.75
- Harder: 7

Max completeness score: 9, when all 3 environments score high
What’s missing in MSA  
CIS 20 Critical Security Controls

CSC 4  Continuous Vulnerability Assessment and Remediation  
CSC 7  Email and Web Browser Protections: an option in Office 365  
CSC 9  Limitation and Control of Network Ports, Protocols, and Services  
CSC 11  Secure Configurations for Network Devices such as Firewalls, Routers, and Switches  
CSC 12  Boundary Defense  
CSC 15  Wireless Access Control  
CSC 17  Security Skills Assessment and Appropriate Training to Fill Gaps  
CSC 19  Incident Response and Management  
CSC 20  Penetration Tests and Red Team Exercises

**Bold** = real world importance  
*Italic* = less relevant  
*Underlined* = part of own security program
The concept holds value but is incomplete. Microsoft is actively implementing it in Azure, and partially in Office 365. Cloud Enabled Cybersecurity can help to fill the gaps. Momentum by the ’classic’ security vendors.