Cloud Security: The 360° Shared Responsibility Model

December 2019

Nigel Hawthorn
EMEA Cloud & Privacy Spokesperson
@wheresnigel
Nigel_hawthorn@mcafee.com
Why Are We Here?
Everyone Is Going To The Cloud – All That Differs Is Speed … and How Safely
November 2019 Cloud Research - Methodology

The research was conducted by Censuswide.
1310 senior IT staff and 755 employees in companies with over 250 employees, in three markets; UK, Germany and France.

Censuswide abide by and employ members of the Market Research Society which is based on the ESOMAR principles.
Articles From Research (UK)

Computer Business Review 40% of Large UK businesses to be Cloud-Only by 2021: McAfee
National Technology News Security fears persist as the UK moves to cloud
Channel Eye McAfee warns of struggle with cloud security
Computer Weekly Enterprises muddled over cloud security responsibilities
IT Pro Portal Growing number of UK businesses will be cloud-only in two years
Verdict Who is responsible for cloud security? It's a bit foggy, finds McAfee
CloudTech McAfee notes the gap between cloud-first and cloud-only – yet optimism reigns on success
Professional Security Magazine Cloud first concern
Techerati UK organisations struggling with cloud security responsibilities
When Did You Implement Your First Cloud App?

- 2019: 4%
- 2017-18: 13%
- 2015-16: 28%
- 2012-14: 18%
- 2010-11: 12%
- 2009 or earlier: 0%

Responses
What Benefits Have You Seen In Your Job? (employees)

- More efficient
- More fulfilling
- Improved data security
- More varied services
- Increased productivity
- Increased innovation

- Strongly Agree
- Agree
Does Your Business Plan To Move More Sensitive Data To The Cloud?

- Yes: 93%
- No: 7%
If Not Planning To Move More Sensitive Data To Cloud, Why Not?

- Security Fears: 50%
- Compliance Concerns: 40%
- Data Access Concerns: 30%
- Cost: 10%
Who In Your Business Is Ultimately Responsible For Cloud Security?

- IT Manager: 34%
- CIO: 19%
- CEO: 14%
- DPO: 12%
- Head of Risk: 6%
- CISO: 5%
- Compliance: 4%
- CDO: 3%
- COO: 2%
- Other: 12%
Who’s Responsible For Cloud Security?

“Through 2023, 99% of cloud security failures will be the customer’s fault”
How Many Cloud Services Are We Using?

McAfee Survey Data – Cloud Adoption 2018

Estimated
How Many Cloud Services Are We Using?

McAfee Real Traffic Patterns – Cloud Adoption & Risk Report 2019

Reality (McAfee Cloud Adoption & Risk Report – April 2019)
We Already Use Lots of Cloud Services – Here are mine!

Office 365
Salesforce (CRM)
Workday (HR)
Webex
Box
Concur (Expenses)
Okta / Sailpoint (Identity)
Jira, Atlassian (Development)
Trello (Collaboration)
Zoom
Slack (Discussions)
PowerBI (Business Intelligence)
Marketo
Hoovers
Adobe Marketing Suite
Ariba (Purchasing)

Hoot (Legal)
Mindtouch (Manuals & Training)
Loopio (Database to answer Qs)
LinkedIn
Twitter
YouTube
ServiceNow (IT Support)
Clari
Digideck
BriefingEdge (Meeting Arranger)
Smartsheet (Shared Spreadsheet)
Yammer (Communications)
Skype (Communications)
Skype for Business (Communications)
Zendesk (ticketing system for marketing)
ServiceNOW (ticketing system for IT)
Security Controls Vary by Provider

- **44.4%**: Specify that customer owns all data uploaded
- **18%**: Delete data immediately on account termination
- **9.1%**: Encrypt data at rest
- **0.9%**: Encrypt data with customer-managed keys
- **6.9%**: Commit to not share data with 3rd parties
Security Controls Vary by Provider (2)

- **97%** Do not allow anonymous access
- **58%** Of services provide user activity logging
- **1%** Offer data access logging
- **25%** Provide integration with enterprise identity
- **19%** Support multi-factor authentication
- **10%** Provide identity federation using SAML, OAuth or similar services
Cloud Assessment
But, it’s not just shadow cloud use ...
However ... Where is enterprise sensitive data in the cloud?
Cloud Security Network Diagram

Employees
Partners
Customers
Vendors

Sanctioned
Shadow
Custom

Managed
Unmanaged

On-Network
Off-Network
The 360° Shared Responsibility Model
The Car Rental Shared Responsibility Model

- **Driver / Renter**
  - Speed / Quality of driving
  - Safely tie in packages
  - Insurance (General & Add-On)
  - Fuel, Oil, Water
  - Seat belts for passengers
  - Up to date servicing (brakes, tyres etc.)
  - Seat Belts
  - Airbags
  - Build quality - Handling, won’t fall apart at first corner

- **Owner (Rental Co.)**

- **Manufacturer Feature, driver responsibility**

- **Manufacturer**
Example: Network Control

- Configuration Audit
- DLP for Confidential Data
- Compromised Accounts, Malware
- Admin User Threats
- Data Anomaly Detection/Remediation

User Responsibility

Enterprise Responsibility

Service Provider feature, enterprise configuration

Service Provider Responsibility

© McAfee 2019. OK for reuse if unedited
Example: Identity & Access Management

- Check all cloud applications
- Communicate to all owners
  - Are they integrated with SSO?

© McAfee 2019. OK for reuse if unedited
Example: File Sharing and Collaboration

- Box
- Google Drive
- Office 365
- Dropbox

Control:
- Collaboration
- User/Device/Data
<table>
<thead>
<tr>
<th>Name</th>
<th>Modified</th>
<th>Modified By</th>
</tr>
</thead>
<tbody>
<tr>
<td>1905-Cloud Security - not as they seem...</td>
<td>June 26</td>
<td>Hawthorn, Nigel</td>
</tr>
<tr>
<td>1905-Cloud Security Audit.pdf</td>
<td>September 13</td>
<td>Hawthorn, Nigel</td>
</tr>
<tr>
<td>1906-ATOS Lunch GRC-McAfee Cloud.pdf</td>
<td>June 14</td>
<td>Hawthorn, Nigel</td>
</tr>
<tr>
<td>1906-ATOS Lunch GRC-McAfee Cloud.p...</td>
<td>June 27</td>
<td>Hawthorn, Nigel</td>
</tr>
<tr>
<td>1906-Black and White for Sandip.pptx</td>
<td>July 25</td>
<td>Hawthorn, Nigel</td>
</tr>
<tr>
<td>1906-Destination Cloud-Madrid.pptx</td>
<td>September 17</td>
<td>Dambrun, Bruno</td>
</tr>
<tr>
<td>1906-Destination Cloud-Madrid-C02V20...</td>
<td>September 27</td>
<td>Hawthorn, Nigel</td>
</tr>
<tr>
<td>1906-Destination Cloud-Paris.pptx</td>
<td>July 16</td>
<td>Hawthorn, Nigel</td>
</tr>
<tr>
<td>1906-Destination Cloud-Rome.pptx</td>
<td>September 27</td>
<td>Hawthorn, Nigel</td>
</tr>
<tr>
<td>1906-ds-gdpr-solution-brief.pdf</td>
<td>September 20</td>
<td>Hawthorn, Nigel</td>
</tr>
<tr>
<td>1906-MVision Cloud Intro for partners.p...</td>
<td>September 20</td>
<td>Hawthorn, Nigel</td>
</tr>
<tr>
<td>1906-SGG-Black and White.pptx</td>
<td>July 12</td>
<td>Hawthorn, Nigel</td>
</tr>
<tr>
<td>1908-Sample Shadow Findings Report.pdf</td>
<td>September 13</td>
<td>Hawthorn, Nigel</td>
</tr>
</tbody>
</table>
Example: Device Control
Example: Application Level Security: Cloud to Cloud Traffic
6.2 Licenses you grant to Prezi for use of Public User Content and Private User Content

In order to provide the Service to you in accordance with these terms, we need certain licenses from you in order for us to, e.g., host, store and display the content. For example, we need the right to publicly display/perform the work to allow us to display it on the computer monitor of any party who is not the copyright holder. We need the right to reproduce the content so that it can be saved to our servers. We need to create derivative works and modify the content, for example, when transcoding an uploaded image into a format that will work most efficiently with the Service.

With respect to Private User Content, you hereby do and shall grant to Prezi (and its successors, assigns, and third party service providers) a worldwide, non-exclusive, revocable, royalty-free, fully paid, sublicensable, and transferable license to use, host, store, reproduce, modify, create derivative works, communicate, publish, publicly perform, publicly display, distribute and transmit the content SOLELY FOR THE PURPOSE of providing you, and those with whom you have shared your presentations, with the Service. This license ends when you delete your Private User Content or your account is closed (either by you or by us), except (i) to the extent that your Private User Content has been shared with others and they have not deleted it and (ii) that we retain a license to maintain a back-up copy of your Private User Content indefinitely.

With respect to Public User Content, you hereby do and shall grant to Prezi (and its successors, assigns, and third party service providers) a worldwide, non-exclusive, revocable, royalty-free, fully paid, sublicensable, and transferable license to use, host, store, reproduce, modify, create derivative works, communicate, publish, publicly perform, publicly display, distribute and transmit the content for the purpose of providing you, and those with whom you have shared your presentations (including the public), with the Service; and (2) in connection with promotion and marketing of Prezi products and services, including without limitation allowing third parties to search or index the content, in connection with email promotions, product demonstrations, and the like. This license ends when you delete your Public User Content or your account is closed (either by you or by us), except (i) to the extent that your Public User Content has been shared with others and they have not deleted it and (ii) that we retain a license to maintain a back-up copy of your Public User Content indefinitely.

Regardless of whether you designate content public or private, Prezi makes no claim of ownership to your User Content, and obtains no rights to your content other than as provided for herein.
Mum, Dad—Can I go to a party?
This Can Be Hard – We Need Context

Apps: Name, Configuration, Posture, Risk
Workloads: Details, Location, Posture
Data: Classification, Tagging, Metadata
Users: Role, Activity, Collaborators

Activities: Access, Read, Write, Download, Upload...
Device: Managed, Unmanaged
Location: Where, When

Cloud Context

Unmanaged Devices

MVISION Cloud

SaaS

IaaS/PaaS

McAfee
Cloud Governance Team

- Multi-function Team (GRC, IT, LOB, purchasing, finance, legal etc.)
- Responsible for overall cloud policies
- Cloud service evaluation criteria, approval and roll-out
- Define user policies for data sharing, collaboration, shadow cloud use
- Define user education methods
- Management reporting
- Define controls for approved services
- Help IT implement controls
GDPR cases and fines

<table>
<thead>
<tr>
<th>No of fines</th>
<th>30</th>
<th>14</th>
<th>12</th>
<th>11</th>
<th>7</th>
<th>4</th>
<th>1</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Insufficient legal basis for data processing</td>
<td>Insufficient information security measures</td>
<td>Non-compliance with data processing principles</td>
<td>Insufficient fulfilment of data subject's rights</td>
<td>Insufficient fulfilment of information obligations</td>
<td>Insufficient fulfilment of data breach obligations</td>
<td>Breach of duty to appoint a DPO</td>
<td>Insufficient data processing agreement</td>
</tr>
<tr>
<td>No of cases</td>
<td>€643,242</td>
<td>€50,788,674</td>
<td>€246,565</td>
<td>€678,703</td>
<td>€131,025</td>
<td>€50,000</td>
<td>€5,000</td>
<td></td>
</tr>
</tbody>
</table>

Complaints: 144,376
Breach notifications: 89,271
Others: 47,441
Real Estate Company Fined € 14.5 Million in Germany for Violating GDPR Principle of Privacy By Design

By Lars Lensdorf and Ulrike Elteste on November 6, 2019

POSTED IN EU DATA PROTECTION, EUROPEAN UNION
| Article 5 – Data Controller shall be able to demonstrate compliance to regulator | • Document policies  
• Show reporting capabilities  
• Show set up in GUI  
• Show data flows to and from the cloud |
|---|---|
| Article 24 – Appropriate technical measures implemented | • Define DLP and reporting to show policies for GDPR  
• Block access to shadow cloud with high GDPR Risk  
• Continuously review new services added  
• Report on data leaving EU/EEA (CSP data hosted outside) |
| Article 25 – Data Protection by Design & Default | • Show integration with SAML/SSO/LDAP  
• Demonstrate appropriate policies are the default  
• Reporting of anomalies, data collaboration unused accounts &privileged user behaviour  
• General reporting on data access |
| 28 – Use only processors who understand GDPR | • Set policies for trusted cloud services  
• Use mix of appropriate cloud attributes  
• ISO 27018 etc. Intellectual property ownership  
• Data location, logging available  
• Security incident notification time |
Map IT Controls To Regulations (GDPR, FCA, ECC ...)

New White Paper: Cloud Security 360° Shared Responsibility Model

Introduction
Shared Responsibility is everywhere.

For today’s cloud computing, however, the shared responsibility isn’t the responsibility of the CSP and the consuming organization, it’s between the CSP and the customer. Both parties share responsibility for securing their data.

This paper acknowledges these changes and the need to reframe shared responsibility. Cloud security is no longer just about the technology; it’s about the people, processes, and policies that underpin the infrastructure. The shared model is critical for ensuring that data is protected and that both parties are held accountable.

The cloud secu

The question “Who is responsible?” is not as simple as it was before because both answer that said, “It’s not my problem” is now more complex. The cloud service provider (CSP) and the consumer are both responsible for ensuring the security of their data.

We’ll examine this new dynamic in the context of the Cloud Security 360° model.

Dissecting the Model

To explain the "Cloud Security 360°: Shared Responsibility Model" for new and experienced cloud users, it’s important to understand the key concepts:

- **Network Security**: The network security aspect of the model focuses on securing the network infrastructure and ensuring that traffic is encrypted and secure.
- **Application Security**: This aspect is responsible for ensuring that applications are secure and that data is protected as it moves through the application layer.
- **Physical Security**: This involves securing the physical environment, including physical access controls, data centers, and other aspects of the cloud infrastructure.

Overall responsibility is shared:

- **CSP responsibilities** include:
  - **Identity and Access Management**: Ensuring that users have the right level of access to the data they need.
  - **Data Classification**: Understanding the sensitivity of data and applying appropriate security controls.
  - **Data Protection**: Ensuring data is protected both at rest and in transit.

- **Customer responsibilities** include:
  - **Identity and Access Management**: Ensuring that users have the right level of access to the data they need.
  - **Data Classification**: Understanding the sensitivity of data and applying appropriate security controls.
  - **Data Protection**: Ensuring data is protected both at rest and in transit.

The 360° Shan

The 360° Shan is a visual representation of the model. It shows how responsibilities are distributed between the CSP and the customer, highlighting the shared responsibility and the areas where both parties are accountable.

How McAfee 360° can help

McAfee 360° provides comprehensive security solutions that address the challenges of cloud computing. Whether you’re a small business or a large enterprise, McAfee 360° offers a suite of tools and services designed to protect your data and ensure compliance with industry standards.

**McAfee 360° Cloud Security**

- **Identity and Access Management**: Ensuring that users have the right level of access to the data they need.
- **Data Classification**: Understanding the sensitivity of data and applying appropriate security controls.
- **Data Protection**: Ensuring data is protected both at rest and in transit.

How McAfee 360° can help

- **Identity and Access Management**: Ensuring that users have the right level of access to the data they need.
- **Data Classification**: Understanding the sensitivity of data and applying appropriate security controls.
- **Data Protection**: Ensuring data is protected both at rest and in transit.

**McAfee 360° Cloud Security**

- **Identity and Access Management**: Ensuring that users have the right level of access to the data they need.
- **Data Classification**: Understanding the sensitivity of data and applying appropriate security controls.
- **Data Protection**: Ensuring data is protected both at rest and in transit.

**McAfee 360° Cloud Security**

- **Identity and Access Management**: Ensuring that users have the right level of access to the data they need.
- **Data Classification**: Understanding the sensitivity of data and applying appropriate security controls.
- **Data Protection**: Ensuring data is protected both at rest and in transit.

**McAfee 360° Cloud Security**

- **Identity and Access Management**: Ensuring that users have the right level of access to the data they need.
- **Data Classification**: Understanding the sensitivity of data and applying appropriate security controls.
- **Data Protection**: Ensuring data is protected both at rest and in transit.
<table>
<thead>
<tr>
<th>Technology</th>
<th>IaaS</th>
<th>PaaS</th>
<th>SaaS</th>
</tr>
</thead>
</table>
| Link control, domain check, email controls, encryption | ![Icon](icon)
| User Behavior analytics, user & device policies | ![Icon](icon)
| DLP, on demand scan                           | ![Icon](icon)
| Compromised account detection, malware scanning | ![Icon](icon)
| SSO integration                               | ![Icon](icon)
| Configuration audit                           | ![Icon](icon)
| Audit of cloud configurations                 | ![Icon](icon)
| CIS benchmarking                              | ![Icon](icon)

**Technologies Required - Cloud 360° Shared Responsibility Model**

- **Collaboration control**
- **User(Device)/Data control**
- **Data Classification & Accountability**
- **End-Point Protection**
- **Identity & Access Management**
- **Application Level Controls**
- **Network Control**
- **Host Infrastructure**
- **Physical Security**

© McAfee 2019. OK for reuse if unedited
16 Example Risk Scenarios

- What is the company’s policy and enforcement if an employee attempts to download data from a trusted cloud service to an unmanaged device?
- What is the process for lines of business to request the use of a new cloud service?
- How will IT security gain visibility and control of unsupported (shadow) cloud services?
- How does the cloud enforcement model fit with other enforcement capabilities (such as proxies, firewalls etc.)?
- Is DLP deployed on cloud-based email services, such as Microsoft Exchange online?
- Are approved cloud services integrated with the company’s identity and access management system so that if an employee leaves the organisation all cloud services are turned off together?
- What logging is provided of cloud use and is that kept for a long enough period to investigate dubious activity?
- Is user behavior analytics used to investigate possible loss of cloud credentials by employees?
16 Example Risk Scenarios

- Is collaboration with third parties controlled, such as with blacklists or whitelists?
- Are employees allowed to create open links to cloud based data?
- Are uploads to the organization’s cloud services by third parties scanned for malware as the data is being uploaded?
- Are the risks of shadow cloud services continuous monitored and controls implemented?
- How do you investigate whether there are too many admin users of a cloud service?
- Can you restrict admin users to make sure that they do not access the actual data?
- How do you check the number of IaaS services in use (AWS, Azure, Google Data Services)?
- How do you check and remediate poor security settings in IaaS services?
2019 Gartner Magic Quadrant for CASBs

Gartner names McAfee a Leader for the 3rd Consecutive Year!
<table>
<thead>
<tr>
<th>Product Name</th>
<th>Vendor</th>
<th>Reviews</th>
<th>Overall Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee MVISION Cloud</td>
<td>McAfee</td>
<td>181</td>
<td>4.6</td>
</tr>
<tr>
<td>CloudSOC (formerly Elasticar)</td>
<td>Symantec</td>
<td>69</td>
<td>4</td>
</tr>
<tr>
<td>Netskope Security Cloud</td>
<td>Netskope</td>
<td>68</td>
<td>4.5</td>
</tr>
<tr>
<td>Microsoft Cloud App Security (MCAS)</td>
<td>Microsoft</td>
<td>54</td>
<td>4.3</td>
</tr>
<tr>
<td>CipherCloud Cloud Security Broker (CSB)</td>
<td>CipherCloud</td>
<td>51</td>
<td>4.3</td>
</tr>
<tr>
<td>Prisma SaaS</td>
<td>Palo Alto Networks</td>
<td>42</td>
<td>4.5</td>
</tr>
<tr>
<td>Cisco Cloudlock</td>
<td></td>
<td>34</td>
<td>4.4</td>
</tr>
</tbody>
</table>
# CASB Solution Comparison

## Assessment Criteria

<table>
<thead>
<tr>
<th>Architecture and Deployment</th>
<th>Bitglass</th>
<th>McAfee</th>
<th>Microsoft</th>
<th>Netskope</th>
<th>Symantec</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deployment Modes</td>
<td>H</td>
<td>M</td>
<td>M</td>
<td>H</td>
<td>M</td>
</tr>
<tr>
<td>Geographic coverage</td>
<td>M</td>
<td>L</td>
<td>M</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td>DDoS protection</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>Scaling and resilience</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td>Apps onboarding</td>
<td>M</td>
<td>L</td>
<td>M</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td>Cloud apps supported in API mode</td>
<td>M</td>
<td>H</td>
<td>M</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td>Cloud apps supported in forward proxy mode</td>
<td>H</td>
<td>H</td>
<td>N</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>Cloud apps supported in reverse proxy mode</td>
<td>H</td>
<td>M</td>
<td>H</td>
<td>M</td>
<td>M</td>
</tr>
</tbody>
</table>

## Data Security

| Data loss prevention (DLP)  | M        | H      | M         | M        | H        |
| Client-side encryption and EDRM integration | L    | H      | H         | H        | M        |
| Key management capabilities | M        | H      | M         | H        | L        |
| Precloud encryption and tokenization | H    | H      | L         | H        | H        |

## Threat Protection

| Adaptive access control     | H        | H      | H         | M        | H        |
| User and entity behavior analytics (UEBA) | M    | H      | M         | M        | H        |
| Malware protection          | M        | M      | H         | H        | H        |

## Visibility and Risk Rating

| Cloud service risk rating   | M        | H      | H         | M        | H        |
| Unapproved cloud visibility and policy enforcement | H   | H      | H         | H        | H        |
| Compliance capabilities     | H        | H      | H         | H        | H        |

## Management and Operations

| Configuration UI capabilities | M        | M      | M         | M        | H        |
| Logging and retention        | L        | H      | H         | M        | H        |
| Incident response            | M        | M      | M         | M        | H        |
| Automation                   | H        | H      | H         | H        | H        |
| Low touch operations         | H        | H      | H         | M        | M        |
| Customizable operations      | M        | M      | M         | M        | M        |
| CSPM                         | L        | H      | L         | M        | M        |

---

Assess Your Cloud Risks
Thank You

+44 7801 487987
@wheresnigel
Nigel_hawthorn@mcafee.com