SANS Cloud Security Survey

Dave Shackleford
Introduction

• In the SANS 2017 Cloud Security survey, we found…more of the same from 2016!
  • Well, some of it, anyway
• Key takeaways from this year:
  • More and more PII in the cloud…40% this year
  • More security controls are in use, including MFA, antimalware, and scanning tools
  • 55% are still feeling hindered from gathering evidence and performing IR in the cloud
## Use of Cloud is Increasing

<table>
<thead>
<tr>
<th>Type of Application</th>
<th>Increase by 100%</th>
<th>Increase by 70% to 90%</th>
<th>Increase by 40% to 60%</th>
<th>Increase by up to 30%</th>
<th>No Change</th>
<th>Decrease</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mission-Critical Apps</td>
<td>6.33%</td>
<td>1.89%</td>
<td>15.20%</td>
<td>26.59%</td>
<td>32.28%</td>
<td>1.26%</td>
</tr>
<tr>
<td>Applications Overall</td>
<td>7.4%</td>
<td>4.32%</td>
<td>24.69%</td>
<td>44.46%</td>
<td>17.27%</td>
<td>1.86%</td>
</tr>
</tbody>
</table>
Workforce Apps Lead the Way

What applications do you have in the cloud? Are they hosted in public clouds (outsourced to third party like Amazon), in internally managed private clouds, or both?

- **Workforce applications (Dropbox, etc.)**
- **Backups and disaster recovery**
- **Storage and archiving of data**
- **Managed services**
- **Server virtualization**
- **Security services**
- **Hosted network services**
- **Desktop virtualization**

- **Private**
- **Both**
- **Public**

0% 20% 40% 60% 80% 100%
Please indicate how many public cloud providers you use for business, communications, security, work sharing and other operations.
# Sensitive Data in the Cloud!

<table>
<thead>
<tr>
<th>Type of Data</th>
<th>2016</th>
<th>2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee Records</td>
<td>48.2%</td>
<td>47.5%</td>
</tr>
<tr>
<td>Business Intelligence</td>
<td>40.9%</td>
<td>42.6%</td>
</tr>
<tr>
<td>Business Records (Finance and Accounting)</td>
<td>37.8%</td>
<td>38.3%</td>
</tr>
<tr>
<td>Customer Personal Information</td>
<td>35.4%</td>
<td>40.4%</td>
</tr>
<tr>
<td>Intellectual Property</td>
<td>35.4%</td>
<td>34.0%</td>
</tr>
<tr>
<td>Customer Financial Information</td>
<td>24.4%</td>
<td>22.0%</td>
</tr>
<tr>
<td>Health Records</td>
<td>18.9%</td>
<td>21.3%</td>
</tr>
<tr>
<td>Customer Payment Card Information</td>
<td>18.3%</td>
<td>19.2%</td>
</tr>
<tr>
<td>National Security or Law Enforcement Data</td>
<td>11.6%</td>
<td>6.4%</td>
</tr>
<tr>
<td>Student Records</td>
<td>11.0%</td>
<td>10.6%</td>
</tr>
</tbody>
</table>
Top Cloud Threats/Concerns: 1

What are your organization’s major concerns related to the use of the public cloud for business apps? Which reflect actual incidents during the past 12 months? Leave blank those that don’t apply.

<table>
<thead>
<tr>
<th>Concern</th>
<th>Actual Incident</th>
<th>Major Concern</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access to sensitive information by insecure, unmanaged devices</td>
<td>Blue</td>
<td>Red</td>
</tr>
<tr>
<td>Unauthorized access to sensitive data by other cloud tenants</td>
<td>Blue</td>
<td>Red</td>
</tr>
<tr>
<td>Inability to respond to incidents traversing our cloud apps and data</td>
<td>Blue</td>
<td>Red</td>
</tr>
<tr>
<td>Inability to encrypt data within the environment</td>
<td>Blue</td>
<td>Red</td>
</tr>
<tr>
<td>Misuse by insiders from your organization</td>
<td>Blue</td>
<td>Red</td>
</tr>
<tr>
<td>Poor data hygiene or inability to delete data from the environment</td>
<td>Blue</td>
<td>Red</td>
</tr>
<tr>
<td>Breach of sensitive data by cloud provider personnel</td>
<td>Blue</td>
<td>Red</td>
</tr>
<tr>
<td>Not knowing with certainty where sensitive data is geographically located</td>
<td>Blue</td>
<td>Red</td>
</tr>
<tr>
<td>Lack of visibility into what data is being processed in the public cloud and where</td>
<td>Blue</td>
<td>Red</td>
</tr>
</tbody>
</table>
Top Cloud Threats/Concerns: 2

- Lack of ability to audit
- Malware intrusion from other cloud tenants
- Inability to meet compliance requirements
- Misconfiguration or vulnerability of hypervisors and other virtualization managers
- Unauthorized access by outsiders
- Inability of the cloud provider to meet service levels or SLAs
- Poor configuration and security of quickly spun-up application components (e.g., containers)
- Downtime or unavailability of applications when needed
Any real breaches? Do we know?

• Last year, just over 10% of organizations claimed they had a breach involving cloud applications and data, which was a slight increase over 2015 (9%).
• The bad news is that this number went up significantly in 2017—in fact, it almost doubled (20%).
• This is likely due to more attackers focusing on the cloud, particularly on poorly configured cloud applications and management interfaces.
• In 2016 22% didn’t know whether they had been breached, and 21% were unsure in 2017.
What’s involved in cloud attacks?

What was involved in the attack(s)? Select all that apply.

- Denial of service attacks
- Misconfiguration or vulnerability of hypervisors and other...
- Account or credential hijacking
- Exploit against hosting provider vulnerability
- Exploit against virtual server OS/application vulnerability
- Sensitive data exfiltration directly from cloud apps
- Privileged user abuse
- Crossover from other hosted cloud applications
- Adversary pivoting from cloud to internal systems
- Other
Growth in SecaaS

Which of the following technologies have you successfully implemented to protect sensitive data and control access into your public cloud environment(s), whether internally managed or in the form of security-as-a-service?
Cloud-Native Security Tools: API Integration

What types of security controls and functions are you using cloud provider APIs for? Select all that apply.

- Logging and event management
- Identity and access management
- Encryption and data protection
- Vulnerability management, including scanning and pen testing
- Local host monitoring
- Malware detection
- Forensics and incident response
- Other
What challenges have you faced in adapting your incident response and forensic analysis to the cloud? Select all that apply.

- Lack of access to underlying log files and low-level system information usually needed for forensic examination
- Lack of understanding as to what information from the cloud provider is required for analysis
- Difficulties because of multitenancy
- Inability to obtain information because of limitations in agreement with cloud provider
- Other
So what IS working?

Which of the following security technologies have you been able to integrate between the private and public cloud? Check only those that apply.

- Multifactor authentication
- Anti-malware
- Vulnerability scanning
- Network access controls
- VPN
- Encryption and key management
- DLP (host- or network-based)
- IDS/IPS
- Threat intelligence sharing /feeds
- Asset/automated configuration management
- Other