The State of Cloud Security: How Does Your Organization Compare?
Introduction

• We’ve seen an increasing number of data breaches and incidents related to cloud
  – S3 buckets galore
  – Open Kubernetes APIs: Cryptomining!
  – Microsoft’s outage in 2019
• Has the state of cloud security changed?
  – More controls? Better processes?
• Believe it or not, there’s some good news this year
About the Survey

• Several hundred respondents
  – In tech, finance/banking, cybersecurity, and more
• A wide range of small, mid-size and large/large++ organizations
• A broad array of roles responded:
  – Architects, ops, and executives
• Most responses from the US, Europe, and Asia
Key Findings from 2019

• A significant increase in unauthorized access by outsiders into cloud environments or to cloud assets;
  – 31% of organizations in 2019, in 2017 this was only experienced by 19% of organizations

• More than 55% of respondents stated that they were frustrated trying to get low-level logs and system information for forensics in 2017, and only 30% said as much in 2019

• ISO 27001 reports continue to be the most valuable audit reports made available by cloud providers, and more organizations are able to perform pen tests of their cloud provided environments than in the past.
What We’re Using in the Cloud

• Business apps and data top the list (76%)
  – Big drop in the use of workforce apps such as Dropbox.
  – Only 45% said they were using such apps today versus 84% in 2017

• Overall storage/archival of data: 48%
• Server workloads: 46.9%
• Security services: 46.5%
What We’re Using in the Cloud

What applications do you have in the public cloud? Select all that apply.

Business applications and data: 75.5%
Storage/Archiving data: 48.0%
Server virtualization: 46.9%
Security services: 46.5%
Managed services: 45.4%
Workforce applications (Dropbox, etc.): 44.7%
Backups and disaster recovery: 41.8%
Hosting network services: 34.8%
Desktop virtualization: 21.6%
Other: 4.0%
More Stats on Cloud Use

• Top number of cloud providers: 2-3
  – Consistent from 2017-2019
  – Roughly 1/3 of respondents

• A higher percentage of respondents were using only one provider in 2017 (17%) versus today (16%)

• 7.4% use more than 20 cloud providers
  – 4% in 2017
Sensitive Data in the Cloud

- **Short answer:** Yes

Are you currently storing any of the following sensitive or regulated (compliance-related) data in the public cloud? Select all that apply.

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business intelligence</td>
<td>48.2%</td>
</tr>
<tr>
<td>Intellectual property</td>
<td>47.7%</td>
</tr>
<tr>
<td>Customer personal information</td>
<td>42.7%</td>
</tr>
<tr>
<td>Business records (finance and accounting)</td>
<td>41.7%</td>
</tr>
<tr>
<td>Employee records</td>
<td>37.7%</td>
</tr>
<tr>
<td>Customer financial information</td>
<td>25.6%</td>
</tr>
<tr>
<td>Customer payment card information</td>
<td>17.6%</td>
</tr>
<tr>
<td>Health records</td>
<td>12.1%</td>
</tr>
<tr>
<td>Other</td>
<td>11.1%</td>
</tr>
<tr>
<td>Student records</td>
<td>9.1%</td>
</tr>
<tr>
<td>National security or law enforcement data</td>
<td>5.0%</td>
</tr>
</tbody>
</table>

©2019 SANS™ Institute | www.sans.org
Have privacy regulations such as the General Data Protection Regulation (GDPR) impacted your organization’s existing or planned cloud strategy?

- Yes: 53.7%
- No: 34.4%
- Unknown: 11.9%

Privacy: A Growing Concern
New Security Tools in the Cloud?

- Are organizations using more cloud-centric security technologies?

![Bar chart showing usage of security tools in the cloud.](image-url)
As in 2017, unauthorized access to data by outsiders topped the list of concerns at 56% (slightly lower than in 2017 but still the highest category).

In second position, inability to respond to incidents (52%) moved up from seventh position in 2017, where 48% chose this concern.

Other major concerns were lack of visibility into what data is being processed and where (51%, up from 48% in 2017) and unauthorized access to data from other cloud tenants at 50%, also (very similar to our responses in 2017)
Concerns and Threats in the Cloud

• For the issues that were actually realized, downtime was fairly consistent from the last survey (up slightly from 18% to 21%).

• The biggest change overall this year was a significant increase in unauthorized access by outsiders at 28%—in 2017 only 12% of respondents’ organizations reported this problem.

• We also saw an increase in misconfiguration issues with application components and APIs.
Actual Breaches in the Cloud

Has your organization experienced an incident or actual breach with the past 12 months involving your public cloud applications and/or data?

- 72.1% Yes
- 10.5% Think so, but can't prove
- 10.5% Not that we know of
- 7.0% Unknown

©2019 SANS™ Institute | www.sans.org
What was Involved in the attack(s)? Select all that apply.

- Account or credential hijacking: 48.9%
- Misconfiguration of cloud services and/or resources: 42.2%
- Privileged user abuse: 37.8%
- Unauthorized (rogue) application components or compute instances: 31.1%
- Insecure API or interface compromise: 28.9%
- Shadow IT: 28.9%
- DoS attacks: 28.9%
- Sensitive data exfiltration directly from cloud apps: 24.4%
- Exploit against cloud provider vulnerability or APIs: 20.0%
- Misconfiguration or vulnerability of hypervisors and/or other virtualization attacks: 17.8%
- Crossover from other hosted cloud applications: 13.3%
- Adversary pivoting from cloud to internal systems: 11.1%
- Other: 8.9%
Cloud Security Controls in Use

Which of the following technologies have you successfully implemented to protect sensitive data and access in your public cloud environment(s), whether internally managed and/or in the form of Security-as-a-Service?

- Anti-malware
- VPN
- Log and event management
- Multi-factor authentication
- Vulnerability scanning
- Network access controls
- IDS/IPS
- Network traffic analysis
- Identity management (IDM) and identity and access management (IDM/IAM)
- Forensics and incident response (IR)
- Data loss prevention (DLP) [host- or network-based]
- Agent-based remote workload monitoring of cloud-based applications
- Cloud encryption gateways and/or CASBs
- Software defined perimeter (SDP)
- Other

©2019 SANS™ Institute | www.sans.org
Key Takeaways: Controls

• the majority of controls across the board are still being managed internally
• Growth: CASBs and encryption gateways (as much as 18% for hybrid management) and identity management solutions (as much as 22% in hybrid management)
• Altogether, the numbers are low!
More Cloud Maturity?

• **Positive**: Today, 68% of organizations have cloud security and governance policies in place,
  – Up from 62% in 2017
  – 24% stated that they didn’t, and 8% weren’t sure

• **Negative**: Only 44% of respondents stated they were leveraging cloud provider APIs in the cloud to implement security controls (a critical element of automation and cloud security maturity)
  – Almost unchanged from 2017 (43 %)
Use of CSP APIs...

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

- Configuration management and control: 74.7%
- Logging and event management: 71.6%
- Identity and access management: 59.0%
- Vulnerability scanning and pen testing: 50.5%
- Encryption and data protection: 49.5%
- Local host monitoring: 47.4%
- Forensics and IR: 27.4%
Controls Integration

• More than 50% have integrated network access controls (52%) and 47% have integrated network traffic analysis

• Another 45% have integrated SIEM and event management tools, too

• Future Controls:
  – Endpoint detection and response (EDR) tools (32%)
  – Forensics and IR tools (28%)
  – Event management once again with 26%
 Controls Integration

Which of the following security technologies have you been able to integrate between your in-house environment and public cloud? Which are you planning on integrating within the next 12 months? Select only those that apply.
Single Vendor Options?

- Multifactor authentication
- Vulnerability scanning
- Network traffic analysis
- Event management and SIEM platforms
- Anti-malware
- IDS/IPS
- Network access controls
- Encryption and key management
- Endpoint detection and response (EDR)
- DLP (host- or network-based)
- Forensics and IR tools
- Other

Current vs. Next 12 Months
IR and Forensics Challenges

- Biggest challenge: A lack of real-time visibility into events and communications involved in incidents
  - EDR tools and network “taps” may help
- Other major challenges cited include:
  - Difficulty correlating events between on-premises and cloud environments
  - Immature forensics and IR processes
  - Inability to acquire forensic evidence
  - Also: Getting logs and low-level system data (55% in 2017 vs 30% today)
Additional IR & Forensics Challenges

- Lack of access to underlying log files and low-level system information usually needed for forensics examination: 30.0%
- Inability to correlate indicators to threats: 29.4%
- Difficulties because of multitenancy: 24.1%
- Inability to maintain chain of custody: 24.1%
- Inability to consume the collected forensic evidence: 23.5%
- Compatibility issues with forensics tools: 17.7%
- Inability to obtain information because of limitations in agreement with cloud provider: 17.7%
- Other: 5.9%
Another Big Challenge: IAM

- IAM is a major element of all cloud deployments
- Directory sync is becoming a “must have” control
- IDaaS and SSO align with this, too
Which of the following automation and orchestration tools are you leveraging to aid in security controls implementation or processes? Select all that apply.

- Infrastructure-as-code (and security-as-code) in templates (e.g., Terraform and AWS…) 51.7%
- Security orchestration, automation and response tools 49.0%
- Configuration orchestration tools (e.g., Chef and Ansible) 48.3%
- Serverless technologies (e.g., AWS Lambda or Azure Functions) 46.4%
- Plugins for continuous integration (CI)/CD tools (e.g., Jenkins or TeamCity) 40.4%
- Other 4.0%
Audits and Pen Tests

- Top audit reports are ISO 27001, NIST/FedRAMP, and SOC 2
- Pen testing:
  - 54.7% Yes
  - 24.2% No, but we get reports
  - 10% No
  - 11% Unknown/etc.
Wrapping Up

• There are lots of takeaways from the survey this year:
  – Cloud use is growing, more sensitive data is in the cloud, and number of providers is basically stable at the low end and higher with 20+
  – IR and forensics is still frustrating
  – Use of hybrid solutions is growing
  – We need more automation & API integration