Title

A QUALITATIVE ANALYSIS OF CLOUD ADOPTION IN THE PUBLIC AND THE PRIVATE SECTORS FROM CYBER SECURITY VENDORS' PERSPECTIVE.

Author

GUY WAIZEL

GUY.WAIZEL@GMAIL.COM

Abstract

My research explores new marketing trends in the private and public sectors concerning the adoption of native cloud applications from cybersecurity vendors. Semi-structured interviews were conducted with two marketing leaders from cybersecurity companies. One company sells to the public sector, the other to the private sector. Following qualitative and content analysis, the results showed many advantages for both sectors of shifting to native cloud applications. In the public sector, there is reluctance to adopt cloud applications primarily because of security challenges and a lack of ecosystem integration alternatives. Offering diverse deployment types was found more effective when selling to the public sector. Applying wide and flexible online marketing techniques and strategies is more effective with customers in the private sector. On-premises deployment is used more frequently in the public sector, where both the lack of ecosystem integrations in cloud applications and perceived security challenges inhibit customer adoption of native cloud applications.

Keywords

cloud, cloud security, cybersecurity, SaaS, hybrid cloud, on-premises, native cloud, cloud adoption, migration to the cloud, cloud computing, ecosystem integrations, cost saving, value proposition

Introduction

Over the last decade, organizations have shifted business applications from on-premises to the cloud. Boillat and Legner (2013) pointed out the affect of cloud computing on the business models of enterprise software vendors when moving from on-premises software to cloud services. Many enterprise software vendors saw an opportunity to increase their customers' success and to reduce costs. For example, the following studies discuss the advantages of moving to the cloud (FutureScape, I.D.C., 2022; Pugh, 2021; Chowdhury, 2018; Egbert, 2015; Walther et al., 2012). However, customers in both the public and private sectors, for differing reasons, are not all ready to shift to the cloud.

The goal of my research is to identify ways for vendors to convince customers to shift to native cloud applications and to avoid losing them as customers when development of an on-premises version is discontinued in favor of a native cloud platform. The study explores interesting marketing trends in the public and private sectors from cybersecurity vendors, which may fuel further research about value proposition plans when shifting clients from on-premises to the cloud.

Qualitative research consisted of interviews with two marketing leaders from cybersecurity companies, of which one sells to the private sector and the other to the public sector. Each interview took about 45 minutes and included ten open questions, which are detailed in Appendix A. The data analysis consisted of eight steps: reading and organizing the data; defining the unit of analysis; creation of codes and categories; selecting quotes and memos reminders; validation and verification; coding all text to its associated category; identification of themes, summarizing results: themes, their relations to categories and selected quotes and discussions.

Results show that first, both sectors perceive an advantage when using cloud-based software. Second, those vendors who sell to the private sector make greater use of online marketing strategies to get new leads. Third, the public sector is reluctant to shift to the cloud because of security concerns and a lack of ecosystem integrations, and fourth, vendors who sell to this sector can address the latter barrier for the meantime by offering diverse deployment solutions. However, to allow the public sector to leverage the advantages of cloud applications,

vendors should continue their efforts to develop other comprehensive cloud offerings and additional ecosystem integrations using hybrid modes.

This paper describes the methods, instruments used, and the eight steps of the content analysis stage. It presents the results; previous studies and literature related to the results; the meaning of the results; limitations of the research; and concludes with the contribution and implications of this paper and suggestions for future research.

Literature Review

Customers from both the public and private sectors have already raised challenges and gaps in their business environment, delaying them from adopting various cloud software solutions. For example, research by Shultz (2016) examined the question of security for application providers and found that security concerns were the most commonly cited reasons that enterprises were not interested in SaaS.

Many other studies refer to additional challenges, including small organizations that are not ready for the move, regulations readiness, training, and resources gaps (Ivan & Ille, 2021; Griffith & Stewart 2020; Meersman & Mulchahey, 2019; Taylor, 2018; Gumbi & Mnkandla, 2015; Gai, 2014; Boillat & Legner, 2013; Bhayal, 2011).

Salih et al. (2021) researched and analyzed the 16 critical success factors that impact cloud ERP adoption and identified 12 influence drivers related to security, usability, and vendors. They focused primarily on ERP adoption and not cybersecurity software and did not differentiate sector types. Gai (2014) examined how to leverage private cloud computing in financial services, focusing mainly on financial services and private cloud and not native cloud and security solutions. Dimitrakos (2014) detailed innovation versus cyber security challenges and predicted that the cloud aggregation ecosystem would be the main innovation after 2020, raising new security challenges. The migration process to the cloud, and specifically security software, was not covered. Bhayal (2011) pointed out security challenges in cloud computing, such as protecting data privacy from breaches and suggested how to avoid third party audits by applying data integrity check solutions. However, neither security software migration to the cloud nor ecosystem considerations nor sector-type differentiation were covered in the research.

In addition, many security vendors operate their solutions exclusively on-site, so in some circumstances, integration with such security tools would not be feasible in the cloud.

Boillat and Legner (2013) pointed out the affect of cloud computing on business models of enterprise software vendors when moving from on-premises software to cloud services. They suggested two options for business models, SaaS, and SaaS+PaaS, and found that vendors using PaaS compensate for the over simplicity and lack of ecosystem integrations in SaaS mode. They did not research security vendors and did not differentiate between vendors who sell to the private or the public sector.

Tawfique and Vejseli (2018) researched the decision to migrate to the cloud, focusing on the security aspects from the consumer perspective. They concluded that some organizations hesitate to make this move because of security concerns and prefer to keep their existing security tools on-site.

Concerning the public sector, the former US CIO, Vivek Kundra, published (2011) the Federal cloud computing strategy. With this strategy, he highlighted the importance of cloud adoption. The main reasons were cost-saving, reducing cost from 80 billion to 20 billion dollars in the long-term, efficiency and consolidation of data servers. The Federal Risk and Authorization Management Program (FedRAMP) was established one year after a joint effort by the NIST (National Institute of Standards and Technology, 2004, 2006, 2011, 2014, 2015, 2016, 2018, 2019) and the US CIO office to create and gather all frameworks, security guidelines, and requirements for the federal and public sector and then certify as many software and cloud vendors as possible according to the federal needs.

Figliola and Fischer (2015) pointed out many challenges concerning the implementation of the U.S. government cloud adoption plan. For example, the FedRAMP process takes lots of time, and there are only a few certified vendors to select. Another concern raised was portability, the potential for getting locked into a specific vendor's product and being dependent on them for any changes. They also identified the lack of staff with expertise in cloud solutions and implementation guidelines which were later improved over the years by the N.I.S.T. and FedRAMP. Taylor (2018) used the ECMF (Enterprise Cloud Migration Framework), which consists of five steps and nine attributes, in order to identify challenges and barriers of cloud

adoption within the government space. Neither security software migration nor ecosystem integrations were covered in the research.

Both the private and the public sectors see advantages in shifting to the cloud. These advantages were also deduced from the content analysis in this paper and align with previous cloud adoption studies: (FutureScape, I.D.C., 2022; Pugh, 2021; Chowdhury, 2018; Egbert, 2015; Walther et al., 2012).

Methods

Primary Aim

This analysis aimed to identify and explore marketing trends, from the vendors' perspective, concerning the willingness of customers in the public and private sectors to shift to a cloud application. I contacted two participants in Israel via LinkedIn and interviewed them via Zoom. The requirements for the sample were to have at least three years of experience working at a cybersecurity vendor that develops cybersecurity solutions; to be over the age of 18, and to be involved with business and marketing activity within their organization. I also aimed to have at least one participant from a company selling security solutions to the private sector and another selling security solutions to the public sector.

Participants Profile

Participant 1 is an executive sales and marketing leader in a cybersecurity company that sells security solutions to customers in the public sector and has over twenty years of experience, including about ten years in cybersecurity. Participant 2 is a digital marketing manager with six years of experience, more than three years of which is in the field of cybersecurity, who works at a cybersecurity vendor that sells security solutions to the private sector. Both interviewees are over the age of 18. They are thoroughly involved in and familiar with their companies' core business processes, marketing activity, and strategy. They both volunteered and signed a consent form to participate in this assignment. Their identity will be kept confidential and anonymous. For the interview questionnaire, see Appendix A.

Summary of the Content Analysis

The main steps for this content analysis are adopted from well-known sources, including (LibGuides N.C.U., 2022; Creswell, 2014; Zhang, et al., 2005; Mayring, 2004; O'Connor & Gibson, 2003).

Step 1: **Read and Organize the Data**

The data were collected, prepared, and organized, then holistic and floating reading was performed over the data. Both interviews were conducted with Zoom recording and took about 45 minutes. A transcript of the recording was exported and translated, and participants' identities were disguised.

Step 2: Define Units of Analysis

I minimized the data, defined the units of analysis, and detected ideas and concepts in words and phrases. Both participants' responses, comments and phrases were marked with different colors related to a specific code. Table A in the results section presents the Units of Analysis.

Step 3: Create and Refine Codes and Categories

I created and refined codes and categories for all the ideas and concepts, reviewed all answers during the interview, created codes for the replies from both participants, and selected participants' quotes related to the project's aim. Table B in the results section presents the defined codes and categories.

Step 4: Select Quotes and Memos

I wrote memos for each participant's answers so as to not forget them when gathering all of the information at the end and selected essential quotes.

Step 5: Validation and Verification

I tested codes, performed validation and correction, checked, and verified for consistency.

Step 6: Code All Text Associated to Categories and Verification

After rereading the data and the relevant associated categories, as presented in Table B, I coded all text from both interviews and verified it.

Step 7: Identify Themes and Relations to Categories and Selected Quotes

I identified themes and then defined the relations between categories and themes. For the results of this step, see Table C and Table D.

Step 8: Summarize Findings and Discussions

I documented the results summary, findings, conclusions, and discussions in both the following sections of this article and in Table E.

Results

Following the content analysis, 81 codes were created. Eight major categories associated with the codes were identified: Shift to Cloud Factors, Encouragement of Cloud, Concerns About Cloud, Value of On-Premises, Deployment Types, Diverse Deployment Offerings, Conventional Marketing Techniques, and Online Marketing Techniques. See Table A for the full relationships between defined codes and categories.

The main themes which were identified:

- There are advantages to using the native cloud for both the public and the private sectors
- On-premises deployment is used more frequently in the public sector, where both the lack of ecosystem integrations in cloud applications and perceived security challenges inhibit customers from shifting to the cloud
- Diverse deployment types are effective when selling to the public sector
- Applying wide and flexible online marketing techniques and strategies are more effective with customers in the private sector

For the results of identified themes and their relation to categories, see Table B.

For the relationships between themes and categories, see Table C.

During the interview, I wrote memos and selected meaningful quotes, then summarized the full details of both the related quotes with the themes and related categories in Table D and Table E summarizes codes, categories, themes, selected quotes, and their relations.

Table A: Units of Analysis

Units of Analysis :				
both on-premises Hybrid and native cloud option	security that they are expecting	use PPC	simplify the general complexity using our software	He can rest assured that he receives all the support that he needs
encourage them to use the cloud	high level of service.	adds on Google. And also they hire a Co-manager. In addition, we have APM account	scale their network secured in minutes	deployed easily.
security preferences.	cost saving in terms	professional conventions.	PPC, SEO media buying, and affiliates.	it's straightforward
specific security restrictions.	lot of kind of sink cost,	focus on a particular industry,	We use a wide variety of social networks to reach potential customers in the private sector.	very user-friendly
Price	enjoy access from everywhere	e public security domain	Conventions	many competitors. Some are very small as startups, some are medium, and Some
we are capable to support all options and all varieties with our product	features that only if they are on the cloud	our portfolio product can fit also wide range of industries	use a lot LinkedIn the most, and Twitter and Facebook also	They have many solutions, on-prem and cloud and integrations and everything, and enjoy stability, as they have existed for
cloud SaaS native only	It's for sure more efficient in the cloud.	Recently we are exploring a different market different opportunity. But	main reason is fear	many years in the market
promote our cloud solution	integrating with different kinds of database sources with on-premises mode with cloud much less.	all industries they don't really contact with the military, governments, or other public sectors, because most are not interested	reasons, including pricing	Yes to his customers to suggest to them our
on-premises only because of government and public sector customers	and can connect with others,	Of course, we want a realistic solution	fear of security	help him quickly
many of them stay in on-premises mode, and we keep them like that	save money and time.	in some cases, we are bringing some more value. So the answer	we sometimes see organizations that decided not to go on cloud but change their opinion after a year.	a customer point of view
These customers would not move quickly to native cloud applications if ever, and we don't intend to push them	easily with simplicity,	adding third-party partners to partner with us.	the on-premises contains more features	from our point of view, we come and decide to explore
Understanding customers' needs are crucial to us	securing against cyber security threats	we use project companies. So basically, it's been done by the system integrator we partner with	fifty users a minimum up to two, twenty, five hundred uh,	a decision to move forward
the marketing is aligned with all their need and requests	On the network.	it's not built-in with the cloud	the challenge of security concern to move to the cloud	simplicity,
on our marketing case by case.	long-term savings	There is a lot of strength in connecting with other systems.	However, most companies today understand that the cloud is the new future. It's easier in some situations and safer than on-premises.	ease of use
Linkedin and organization connections techniques	buy something that can that is like a one stop shop	We do have some built in integrations with our cloud solution but customer demanding more , it's not enough what we have	fast deployment and	cost saving
It's the customer's decision. We do not stick to something specific.	excellent service	. For example, they don't have Cosby	accessibility anywhetre ,still	we will surely make our best in order to fit to the right environment
If the customer decides on something specific, we will deploy it.	account manager	Yes, the solution is limited some on the development, but it's not live for the customers in production mode.	always available twenty-four hours, seven days	we try to provide added value features on the cloud all time to differentiate our product than other competitors
We check customers' needs very carefully.	point of contact	ability to quickly detect and defend the unified network and cyber security tools.		

Table B: Finalizing Codes and Categories for Concepts and Ideas

Code	Categories	Code	Categories
Security Restrictions	Concerns About Cloud	Using Conventions Both for Public and Private Sectors	Conventional Marketing Techniques
Security Preference		Using LinkedIn for Both Public and Private Sectors	
Trust in Cloud		Conventions (Public sector)	
Security Fears (mainly Public sector)		Tenders(Public sector)	
Breached Risk (mainly Public sector)		LinkedIn Direct (Public sector)	
Data Privacy Risk (mainly Public sector)		Future Efforts	
Lack of Integrations (native cloud for private)		Pricing Decision	Shift to Cloud Factors
On-premises Deployment	Deployment Types	Pricing Model	
Cloud Deployment		Fast Deployment	
Native Cloud Deployment		Accessibility Anywhere	
Hybrid deployment		High Level of Service	
Using PPC for Private Sectors	Online Marketing Techniques	Cost Saving	
Using Google AdWords for Private Sectors		No HW Needed	
Using SEO Media for Private Sectors		No Maintenance Needed	
Using Affiliates for Private Sectors		No Upgrades	
Simplicity Messages for Private Sectors		Cloud Efficiency	
Efficiency Messages for Private Sectors		Easy With Simplicity	
Using LinkedIn Twitter and Facebook for Private Sectors		Long Term Saving	
Account Manager		User friendly UI	
Co-Manager		Simplicity	
ABM Account		Ease of Use	
Affiliate Specialist		Cost Saving	
Product Management		UI Accessible from Outside	
Product Marketing Manager		Using Extended Features	
PPC		Customer's Decision	Diverse Deployment Offerings
PR team		Marketing Alignment	
On-premises Mainly Federal and Government	Value of On- Premises	Customer's First Approach	
On-premises -Significant Payment		Customer Needs	
Compliance (mainly important for public sector)		Case by Case Deployment Decision	
More Features and Functionalities in On- Premises (mainly for the public sector)		Comply Customer Needs	
Lower Scaling (native cloud)-up to certain amount of users		Flexibility Solution	
Higher Scaling for Public (support more users)		Competency Solution	
Military and Government		Customer's View (Public sector)	
Support in Scale		Customer's Decision (public sector)	
Not built-in Integration		Explore New Markets	
Using System Integrator		Product Fit	
Using Customizations		Realistic Solution	
Limited Ecosystem Integration on Cloud			
Cloud Encouragement	Encouragement of cloud		
Cloud SaaS			
Cloud Promotion			
Good Security Also in Cloud			
One Stop Shop			
Shifting Customer's to Cloud			

Table C: Relations Between Categories and Themes

Categories	Themes
Shift to Cloud Factors	1. There are advantages to using the native cloud for both the public and the private sectors
Encouragement of Cloud	
Concerns About Cloud	2. On-premises deployment is used more frequently in the public sector, where both the lack of ecosystem integrations in cloud applications and perceived security challenges inhibit customers from shifting to the cloud
Value of On-Premises	
Deployment Types	3. Diverse deployment types are effective when selling to the public sector
Diverse Deployment Offerings	
Conventional Marketing Techniques	4. Applying wide and flexible online marketing techniques and strategies is more effective with customers in the private sector
Online Marketing Techniques	

Table D: Relations Between Themes Categories and Selected Quotes

Themes : Relations to Categories and Selected Quotes	
1. There are advantages to using the native cloud for both the public and the private sectors	**3.Diverse deployment-types are effective when selling to the public sector**
Relation to Categories	**Relation to Categories**
Shift to Cloud Factors	Deployment Types
Encouragement of Cloud	Diverse Deployment Offerings
Selected Quotes:	**Selected Quotes:**
" Most of the companies today understand that the cloud is the new future it's easier and in some situation safer then on premises." " It's for sure more efficient in the cloud" "He can rest assured that he receives all the support that he need." "we try to provide added value features on the cloud all time to differentiate our product than other competitors"	"We're able to support all options and all varieties with our product for the public sector" "we see sometimes organizations that decided not to go on cloud but after a year they change their opinion in public sector" "but we in our case are much more flexible" "Our competitors have lots of solutions, on-prem and cloud and integrations" "We will surely make our best in order to fit to the right environment."
2. On-premises deployment is used more frequently in the public sector, where both the lack of ecosystem integrations in cloud applications and perceived security challenges inhibit customers from shifting to the cloud	
Relation to Categories	**4. Applying wide and flexible online marketing techniques and strategies are more effective with customers in the private sector**
Concerns About Cloud	**Relation to Categories**
Value of On-Premises	Conventional Marketing Techniques
Selected Quotes:	Online Marketing Techniques
"Many of them stay in on-premises mode and we keep them like that" "We are open to integrating with different kind of sources of the database with on-premises mode with cloud much less." "There is a lot of strength to connect with other systems" "We use system integrators for customizations" "the on-prem version contain more features." "We do have some built in integrations with our cloud solution but customer demanding more ,it's not enough what we have"	**Selected Quotes:** "We use a wide variety of social networks to reach potential customers in the private sector"

Table E: Summary- Codes, Categories Themes, Selected Quotes, and Their Relations

Code	Categories	Themes : Relations to Categories and Selected Quotes
Security Restrictions	Concerns About Cloud	**1.There are advantages to using the native cloud for both the public and the private sectors**
Security Preference		**Relation to Categories**
Trust in Cloud		Shift to Cloud Factors
Security Fears (mainly Public sector)		Encouragement of Cloud
Breached Risk (mainly Public sector)		**Selected Quotes:**
Data Privacy Risk (mainly Public sector)		"We explain how to simplify the general complexity using our software" " Most of the companies today understand that the cloud is the new future it's easier and in some situation safer then on premises." " It's for sure more efficient in the cloud" "He can rest assured that he receives all the support that he need." "we try to provide added value features on the cloud all time to differentiate our product than other competitors"
Lack of Integrations (native cloud for private)		
On-premises Deployment	Deployment Types	**2. On-premises deployment is used more frequently in the public sector, where both the lack of ecosystem integrations in cloud applications and perceived security challenges inhibit customers from shifting to the cloud**
Cloud Deployment		**Relation to Categories**
Native Cloud Deployment		Concerns About Cloud
Hybrid Deployment		Value of On-Premises
Using PPC for Private Sectors	Online Marketing Techniques	**Selected Quotes:**
Using Google AdWords for Private Sectors		
Using SEO Media for Private Sectors		"Many of them stay in on-premises mode and we keep them like that" "We are open to integrating with different kind of sources of the database with on-premises mode with cloud much less." "There is a lot of strength to connect with other systems" "We use system integrators for customizations" "the on-prem version contain more features." "We do have some built in integrations with our cloud solution but customer demanding more ,it's not enough what we have"
Using Affiliates for Private Sectors		
Simplicity Messages for Private Sectors		
Efficiency Messages for Private Sectors		
Using LinkedIn Twitter and Facebook for Private Sectors		
Account Manager		
Co-Manager		
ABM Account		
Affiliate Specialist		
Product Management		**3.Diverse deployment-types are effective when selling to the public sector**
Product Marketing Manager		**Relation to Categories**
PPC		Deployment Types
PR Team		Diverse Deployment Offerings
Using Conventions Both for Public and Private Sectors	Conventional Marketing Techniques	**Selected Quotes:**
Using LinkedIn for Both Public and Private Sectors		"We're able to support all options and all varieties with our product for the public sector" "we see sometimes organizations that decided not to go on cloud but after a year they change their opinion in public sector" "but we in our case are much more flexible" "Our competitors have lots of solutions, on-prem and cloud and integrations" "We will surely make our best in order to fit to the right environment."
Conventions (Public sector)		
Tenders(Public sector)		
LinkedIn Direct (Public sector)		**4.Applying wide and flexible online marketing techniques and strategies are more effective with customers in the private sector**
Future Efforts		**Relation to Categories**
Pricing Decision		Conventional Marketing Techniques
Pricing Model		Online Marketing Techniques
Fast Deployment		**Selected Quotes:**
Accessibility Anywhere		"We use a wide variety of social networks to reach potential customers in the private

High Level of Service	Shift to Cloud Factors	
Cost Saving		
No HW Needed		
No Maintenance Needed		
No Upgrades		
Cloud Efficiency		
Easy with Simplicity		
Long Term Saving		
User Friendly UI		
Simplicity		
Ease of Use		
Cost Saving		
UI Accessible from Outside		
Using Extended Features		
On-premises Mainly Federal and Government	Value of On-Premises	
On-premises -Significant Payment		
Compliance (mainly important for public sector)		
More Features and Functionalities in On-Premises (mainly for public		
Lower Scaling (native cloud)-up to certain amount of users		
Higher Scaling for Public (support more users)		
Military and Government		
Support in Scale		
Not Built-in Integration		
Using System Integrator		
Using Customizations		
Limited Ecosystem Integration on Cloud		
Cloud Encouragement	Encouragement of Cloud	
Cloud SaaS		
Cloud Promotion		
Good Security also in Cloud		
One Stop Shop		
Shifting Customer's to Cloud		
Customer's Decision	Diverse Deployment Offerings	
Marketing Alignment		
Customer's First Approach		
Customer Needs		
Case by Case Deployment Decision		
Comply Customer Needs		
Flexibility Solution		
Competency Solution		
Customer's View (Public sector)		
Customer's Decision (public sector)		
Explore New Markets		
Product Fit		
Realistic Solution		

Discussion

This study aimed to explore new marketing trends in private and public sectors concerning cloud adoption and willingness to shift from on-premises to native cloud applications from the perspective of cybersecurity vendors.

The results showed significant perception trends from the perspective of cybersecurity vendors. It seems that when a security vendor sells to the public sector, the vendor offers a diverse selection of types of deployments. The vendor encourages the customer to shift to the cloud but does not insist; the decision is left to the customer, who can decide to deploy in either on-premises or cloud mode. Such an offering has advantages and disadvantages. By letting the customer choose the deployment type, the vendor retains customer loyalty, especially if this is a top revenue and strategic account. On the other hand, the vendor invests more in developing two versions of the same product in parallel, one as a native cloud and another for on-premises, which increases the cost of development, support and sales for the security vendor. By investing resources in two platforms, over time, the quality of the vendor's product may also decline compared to other pure SaaS and native cloud vendors who devote their efforts to just one platform.

The literature shows the importance of finding solutions for security gaps by having more FedRAMP-certified vendors (Figliola & Fischer, 2015). My results identified a significant theme. The on-premises theme also aligns with previous studies mentioned in the literature review. Vendors who leverage these findings by increasing their cloud capabilities with more ecosystem integrations and comprehensive cloud offerings may increase their public sector customers' motivation to shift from on-premises to the cloud.

Based on the security vendors' perspective, another theme finding was that security vendors who sell to the private sector leverage more social networks and diverse marketing strategies. This sector also seems to adopt faster cloud and multitenancy. These findings make sense since the private sector is more open to online SaaS products and innovations to save costs and is not constrained by so many security regulations as the public sector.

Since both vendors have thousands of customers, the findings cover trends across a significantly large number of customers from the private and public sectors. However, further research with more vendors can assist in exploring more important trends.

Conclusions

The interviews and content analysis raised some interesting marketing trends and approaches. It was valuable to get perspectives from both the public and private sectors since interviewees are in the same software industry but sell to different sectors.

I detected some interesting trends:

First, both participants raised perceptions of the advantages of native cloud applications in the public and private sectors. This position is also supported by the literature today, for example, with the following studies: (Pugh, 2021; Chowdhury, 2018; Egbert, 2015; Walther et al., 2012).

Second, the importance and value of on-premises deployment for the public sector were highlighted several times, as well as trust and security concerns in cloud aspects. A central theme was that on-premises deployment type is used more frequently by the public sector, and lack of ecosystem integrations in cloud and security challenges inhibit customers from shifting to the cloud. A significant implication is that security vendors should focus more on this customer objection and consider extending their cloud integration offerings and comprehensive offerings on the cloud.

Third, I found that security vendors who sell to the public sector use diverse deployment types offered for their customers, which seem very effective and assist in retaining enterprise customers. However, vendors should consider that developing two product lines in parallel may be inefficient and increase costs.

Fourth, using social networks and online strategies to get more leads seems to work better when marketing to the private sector than the public sector, which adopts more conventional methods of getting leads, such as tenders, conventions, LinkedIn, and more direct contact.

Although the study covers trends across a large number of customers, since both vendors each have thousands of customers, it is still limited since it was conducted with just 2 vendors so further research building on this study should analyze more vendors' perspectives from various organizations. Also, additional research from the perspective of customers will allow the correlation of data with vendors' perspectives and create value proposition plans for vendors wishing to shift their customers from on-premises deployment to native or hybrid cloud.

References

Bhayal, S., 2011. A study of security in cloud computing. California State University, Long Beach.

Boillat, T. and Legner, C., 2013. From on-premise software to cloud services: the impact of cloud computing on enterprise software vendors' business models. Journal of theoretical and applied electronic commerce research, 8(3), pp.39-58.

Boyens, J., Paulsen, C., Moorthy, R., Bartol, N. and Shankles, S.A., 2015. Supply chain risk management practices for federal information systems and organizations. N.I.S.T. Special Publication, 800(161), p.32.

Carter, L. and Bélanger, F., 2005. The utilization of e-government services: citizen trust, innovation and acceptance factors. Information systems journal, 15(1), pp.5-25.

Chandramouli, R. and Chandramouli, R., 2016. Secure virtual network configuration for virtual machine (vm) protection. N.I.S.T. Special Publication, 800, p.125B.

Chowdhury, N., 2018. Factors influencing the adoption of cloud computing driven by big data technology: a quantitative study (Doctoral dissertation, Capella University).

Creswell, J.W., 2014. Qualitative, quantitative and mixed methods approaches.

Diaz, A.A. 2022, Organizational Paradoxes of Cloud Adoption in the Federal Government: A Quantitative Study of the Organizational Change Challenges Impacting Cloud Adoption, The George Washington University.

Dimitrakos, T., 2014, August. Cloud Security Challenges and Guidelines. In EIT ICT Labs Symposium on Trusted Cloud and Future Enterprises.

Disterer, G. ISO/IEC 27000, 27001 and 27002 for information security management". 2013.

Egbert, M., 2015. Driving Public Cloud Adoption through Qualitative and Quantitative Modeling (Doctoral dissertation, Pace University).

Fagan, M., Megas, K., Scarfone, K. and Smith, M., 2019. Core cybersecurity feature baseline for securable IoT devices: A starting point for IoT device manufacturers (No. N.I.S.T. Internal or Interagency Report (N.I.S.T.I.R.) 8259 (Draft)). National Institute of Standards and Technology.

Figliola, P.M. and Fischer, E.A., 2015, January. Overview and issues for implementation of the federal cloud computing initiative: Implications for federal information technology reform management. Library of Congress, Congressional Research Service.

FutureScape, I.D.C., 2022. I.D.C. FutureScape: Worldwide I.T. industry 2022 predictions.

Gai, K., 2014. A review of leveraging private cloud computing in financial service institutions: Value propositions and current performances. Int. J. Comput. Appl., 95(3), pp.40-44.

Griffith, L.D. 2020, Strategies Federal Government I.T. Project Managers Use to Migrate I.T. Systems to the Cloud, Walden University.

Gumbi, L.N. and Mnkandla, E., 2015. Investigating South African Vendors' cloud computing value proposition to small, medium and micro enterprises: a case of the City of Tshwane Metropolitan Municipality. The African Journal of Information Systems, 7(4), p.1.

I.B.M. Launches Open Technology to Speed Response to Cyber Threats Across Clouds (2022). Available at: https://newsroom.ibm.com/2019-11-20-IBM-Launches-Open-Technology-to-Speed-Response-to-Cyber-Threats-Across-Clouds (Accessed: 27 April 2022).

Ivan, T.R. and Ille, E.E., 2021. Applying Multi-Criteria Decision-Making to the Technology Investment Decision-Making Process. Acquisition Research Program.

Joint Task Force, 2018. Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and

Technology, Gaithersburg, MD), N.I.S.T. Special Publication (S.P.) 800-37 Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2

Joint Task Force Transformation Initiative, 2011. Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD). N.I.S.T. Special Publication (S.P.) 800-39. https://doi.org/10.6028/NIST.SP.800-39

Kundra, V., 2011. Federal cloud computing strategy.

LibGuides: Chapter 4: Chapter 4: Analysis and Coding Example, 2022. Available at: https://library.ncu.edu/c.php?g=1007180&p=7392331 (Accessed: 24 November 2022).

Maurya, 2019. Fortinet tightens partnership with Google Cloud to provide advanced cloud security and accelerate the cloud on-ramp. GlobeNewswire News Room. Available at: https://www.globenewswire.com/news-release/2019/12/16/1961138/0/en/Fortinet-Tightens-Partnership-with-Google-Cloud-to-Provide-Advanced-Cloud-Security-and-Accelerate-the-Cloud-On-Ramp.html [Accessed April 28, 2022].

Mayring, P., 2004. Qualitative content analysis. A companion to qualitative research, 1(2), pp.159-176.

Meersman, M.W., 2019. Developing a Cloud Computing Risk Assessment Instrument for Small to Medium Sized Enterprises: A Qualitative Case Study Using a Delphi Technique (Doctoral dissertation, Northcentral University).

Metheny, M., 2017. *Federal cloud computing: The definitive guide for cloud service providers*. Syngress.

Mulchahey, K.E. 2019, Exploration of Complexities for Migration of Software-Licensing Models, Capella University.

National Institute of Standards and Technology, 2019. N.I.S.T. Privacy Risk Assessment Methodology (PRAM). (National Institute of Standards and Technology, Gaithersburg, MD). https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources

NIST FIPS, 199.National Institute of Standards and Technology, 2018. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.04162018

O'Connor, H. and Gibson, N., 2003. A step-by-step guide to qualitative data analysis. *Pimatisiwin: A Journal of Indigenous and Aboriginal Community Health*, *1*(1), pp.63-90.

Peake, C., 2018. Accepting the Cloud: A Quantitative Predictive Analysis of Cloud Trust and Acceptance Among I.T. Security Professionals (Doctoral dissertation, Capella University).

Pub, F.I.P.S., 2004. Standards for security categorization of federal information and information systems.

Pugh, C.E. 2021, Regulatory Compliance and Total Cost Influence on the Adoption of Cloud Technology: A Quantitative Study, Capella University.

Rose, S., Borchert, O., Mitchell, S. and Connelly, S., 2019. Zero trust architecture. National Institute of Standards and Technology.

Ross, R., McEvilley, M. and Oren, J., 2016. Systems security engineering: Considerations for a multidisciplinary approach in the engineering of trustworthy secure systems (No. N.I.S.T. Special Publication (S.P.) 800-160 (Withdrawn)). National Institute of Standards and Technology.

Ross, R.S., Dempsey, K.L., Viscuso, P., Riddle, M. and Guissanie, G., 2016. Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations [including updates as of 01-14-2016].

Salih, S., Hamdan, M., Abdelmaboud, A., Abdelaziz, A., Abdelsalam, S., Althobaiti, M.M., Cheikhrouhou, O., Hamam, H. and Alotaibi, F., 2021. Prioritising Organisational Factors Impacting Cloud ERP Adoption and the Critical Issues Related to Security, Usability, and Vendors: A Systematic Literature Review. Sensors, 21(24), p.8391.

Shultz, A., 2016. Controlling the Emerging Data Dilemma: Building Policy for Unstructured Data Access. In Information Security Management Handbook, Volume 5 (pp. 229-242). Auerbach Publications.

Slade, E.L., Dwivedi, Y.K., Piercy, N.C. and Williams, M.D., 2015. Modeling consumers' adoption intentions of remote mobile payments in the United Kingdom: extending U.T.A.U.T. with innovativeness, risk, and trust. Psychology & Marketing, 32(8), pp.860-873.

Stewart, J.C.I., 2020. End-User Cloud Data Storage Experiences, Challenges, and Security Perceptions of the Emerging Technologies Security Tools among Small Businesses (Doctoral dissertation, Capella University).

Swanson, M., Hash, J. and Bowen, P., 2006. Guide for developing security plans for federal information systems (No. N.I.S.T. Special Publication (S.P.) 800-18 Rev. 1). National Institute of Standards and Technology.

Tawfique, K. and Vejseli, A., 2018. Decision to migrate to the Cloud: A focus on security from the consumer perspective.

Taylor, C.M., Sr. 2018, Identifying and Overcoming the Barriers to Cloud Adoption within the Government Space, The George Washington University.

The Smart Grid Interoperability Panel—Smart Grid Cybersecurity Committee, 2014. Guidelines for Smart Grid Cybersecurity: Volume 1 - Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements. (National Institute of Standards and Technology, Gaithersburg, MD),

N.I.S.T. Interagency or Internal Report (I.R.) 7628, Rev. 1, Vol. 1. https://doi.org/10.6028/NIST.IR.7628r1

Venkatesh, V., Morris, M.G., Davis, G.B. and Davis, F.D., 2003. User acceptance of information technology: Toward a unified view. M.I.S. quarterly, pp.425-478.

Walther, S., Plank, A., Eymann, T., Singh, N. and Phadke, G., 2012. Success factors and value propositions of software as a service providers–a literature review and classification.

Zhang, Y., & Wildemuth, B. M., 2005. Qualitative analysis of content, 1-12.

Appendix A: Interviews Questionnaire

1. Does your organization sell software security on the cloud, hybrid cloud (some components on-premises and some on the cloud), or native cloud applications to your customers? Could you describe the type of deployments offered today to your customers?

2. Does your organization have a clear marketing strategy plan for selling your cloud application\module solution to customers running a competitor solution that can be deployed just in on-premises mode?

3. Could you provide three main reasons for potential customers who decided not to purchase your cloud application module\solution?

4. Could you point out three main reasons why some of your customers decided to purchase your cloud module solution?

5. Do you see some of your on-premises competitors' solutions as direct competitors to your cloud module offering solution?

6. Does your organization try to shift customers who used to work in on-premises software (Yours or a competitor's) to your cloud application software?

7. What strategies does your organization use to get new leads for your cloud application module\solution?

8. Is your security product offered to a specific industry \sector? Do you think a security software solution such as a native cloud application module like yours should get sold to a particular industry?

9. Does your organization partner with various ecosystem integration third parties to improve your cloud application offering?

10. Does your organization provide on your cloud application platform extended features that can be used on cloud applications only or basic functionalities that can also be achieved with on-premises version, and just the U.I. is available on the cloud?