Marketing insights when shifting cybersecurity technologies to the cloud or hybrid cloud in the context of smart cities

Guy WAIZEL,
Alexandru Ioan Cuza University of Iasi, Romania
guy.waizel@gmail.com

Abstract

This research aims to identify marketing insights that can assist marketing departments at cybersecurity vendors in persuading their customers to transition from on-premises deployment to a cloud application when the vendor decides to develop a new product on the cloud and discontinue the on-premises version. With the global trend of customers migrating to the cloud and vendors adapting their technologies accordingly, the need for such marketing insights in developing a strategic marketing plan is evident. Its purpose is to deter customers from abandoning the service and switching to competitors offering on-premises solutions. Previous studies indicate that the global rise in customer migration to the cloud is primarily driven by cost savings and efficiency. However, other studies have shown that while vendors develop and adjust their technologies for the cloud, many organizations are not yet ready for such a shift and prefer to maintain on-premises deployments. There is also an extensive body of literature that describes challenges related to security concerns, small organizations unprepared for migration, regulatory readiness, and issues with training and resource availability. Moreover, numerous cybersecurity research papers, frameworks, and methodologies are associated with cloud adoption. In this research, a qualitative analysis is conducted through in-depth interviews with 13 security professionals, focusing on a case study of active defense cybersecurity. Through the use of content analysis and thematic analysis, we aim to identify the primary themes that will contribute to a more comprehensive future model for researching and explaining consumer behavior during the transition of cybersecurity technologies from on-premises to the cloud or a hybrid cloud environment.

Keywords: cloud adoption, marketing plan, migration to cloud, security professionals, deception technology.

1. Introduction: Bridging the Knowledge Gap in Cybersecurity Cloud Migration

In the rapidly evolving landscape of cybersecurity and smart cities, the literature has extensively explored the benefits of cloud adoption in various sectors, highlighting efficiency gains and cost savings, as well described in [1], [2], [3], [4], [5]. However, a critical gap exists in the specific realm of cybersecurity enterprise software vendors and their migration strategies to the cloud, particularly in the context of smart cities. While vendors strive to adapt to cloud technologies, a significant number of organizations remain hesitant, opting for on-premises deployment due to security concerns, regulatory issues, and resource constraints, as well covered by [6], [7], [8], [9], [10], [11], [12], [13], [14], [15].

This research aims to address this knowledge gap by delving into the specific challenges faced by cybersecurity vendors in migrating clients from on-premises to cloud solutions within the context of smart cities. The literature lacks a focused exploration of migration plans and marketing strategies tailored to the unique needs of cybersecurity clientele, especially in the context of smart city infrastructure. Additionally, gaps persist in understanding comprehensive cloud features, ecosystem integrations, trust issues, and perception factors influencing customers' willingness to migrate in the specific context of smart cities.

1.1. Motivation and Significance: Enhancing Marketing Strategies in Cybersecurity

Motivated by the necessity to fill this void, this research seeks to contribute to the decision-making processes of enterprise security vendors. The significance lies in aiding these vendors to make informed marketing decisions, particularly in developing tailored marketing strategy plans for transitioning clients from on-premises to Software as a Service (SaaS) or hybrid cloud deployments. Such strategic plans are crucial for retaining customers, preventing revenue loss, and safeguarding the vendor's reputation.

The chosen case study focuses on active cyber defense technology, specifically the shift from on-premises deployment to hybrid or full SaaS models. Understanding how organizations perceive this transition is essential for vendors looking to convince their clients to embrace the cloud platform. This move promises immediate cost reductions for customers but poses risks for vendors in terms of subscription renewals and potential customer churn. Addressing these challenges requires an early adoption of the right marketing strategy.

The shift to cloud-based solutions also influences organizational behavior, requiring new training and skill sets, potential workforce changes, and challenges in adapting to cloud-oriented functionalities as indicated also by Stewart [8] and Meersman [9]. This research explores these social and organizational impacts, providing valuable insights for both vendors and organizations contemplating the shift.

Furthermore, the research extends its significance beyond the cybersecurity domain by contributing to universal strategic marketing methodologies. The development of primary data instruments, including open-ended questionnaires for security leaders.

1.2. Research Problem: Navigating the Complex Landscape of Cloud Adoption in Cybersecurity

The research problem stems from the ongoing debate surrounding on-premises versus cloud adoption in various industries. While some sectors have embraced cloud technologies for cost-saving reasons, the cybersecurity domain, especially in federal and government industries, exhibits hesitancy due to security concerns [13]. This hesitation prompts cybersecurity vendors to invest in alternative solutions, such as hybrid cloud or fully SaaS models, leading to a myriad of challenges.

Our research focuses on the dilemma faced by cybersecurity vendors in migrating on-premises customers to the cloud. The potential loss of customers, profitability, and trust looms large as vendors transition to new business and pricing models. The shift not only affects customers' perceptions of cost-saving but also raises concerns about security, data privacy, and the ability to integrate with other ecosystem security software.

Strategically managing this transition is critical for vendors to avoid customer churn and loss of trust. This qualitative analysis research is the first stage in a wider research which aims to develop and execute a comprehensive strategic marketing plan that addresses these challenges, ensuring a smooth migration process for both vendors and clients.

1.3. Research Questions, Aims, and Objectives: Unveiling Perceptions in Cybersecurity Cloud Migration

The research questions guide our exploration into organizations' perceptions of the shift from on-premises software to cloud applications in the realm of cyber-active defense technology. We aim to uncover insights related to extended features, new cloud ecosystem integrations, cost-saving perspectives, and the impact of trust in cloud security.

The objective of this first stage research are:

- To examine how organizations using cyber-active defense technology perceive the shift from on-premises software to a cloud application concerning extended features and functionalities.
- To explore organizations' perceptions of the shift from on-premises software to a cloud application when leveraging new cloud ecosystem integrations.
- To investigate how organizations utilizing cyber-active defense technology view the shift from on-premises installation to a cloud application from a cost-saving perspective.
- To assess organizations' perceptions of the shift from on-premises software to a cloud application based on their trust in cloud security.

1.4. The Context of the Research: Active Defense Cybersecurity Technology

The research contextualizes the investigation within the realm of active defense cybersecurity technology, focusing on solutions like deception technology. Traditionally deployed on-premises for network segmentation, vendors are now steering clients toward hybrid cloud or fully SaaS environments. This context provides a rich case study for understanding the dynamics of transitioning from on-premises solutions to cloud applications.

1.5. Literature Review: Navigating Challenges and Advantages in Cloud Adoption

A comprehensive literature review identifies the challenges and advantages of cloud adoption across public and private sectors. Security concerns, regulatory readiness, training gaps, and resource constraints have been cited as barriers to adoption [6], [7], [8], [9], [10], [11], [12], [13], [14], [15]. While studies acknowledge the benefits of cloud adoption in various sectors [1], [2], [3], [4], [5], there remains a dearth of literature addressing the specific challenges and marketing strategies for security software migration to the cloud.

1.6. Theories Related to the Study: A Theoretical Framework for Informed Decision-Making

Theoretical frameworks such as transaction cost theory, diffusion of innovations theory, resource dependence theory, UTAUT, stakeholder theory, theory of reasoned action, theory of planned behavior, and theory of buyer behavior provide a robust foundation for understanding the complexities of cloud adoption and marketing strategies [16], [17], [18], [19], [20], [21], [22], [23], [24], [25], [26], [27]. These theories offer valuable insights into the factors influencing customers' decisions, trust in the cloud, and the development of effective marketing strategies for cybersecurity vendors navigating the transition from on-premises to cloud solutions.

In conclusion, this research endeavors to bridge the knowledge gap in the specific context of cybersecurity enterprise software vendors, providing actionable insights to guide informed marketing decisions in the dynamic landscape of cloud adoption.

2. Method

2.1. Pilot

A pilot study aimed to improve data collection quality by refining questions for relevance and appropriateness adopted from similar pilot method previosely used by Teijlingen, E. R., & Hundley, V [28]. The study also measured interview time alignment and ensured meaningful responses to each question [28]. Additionally, it confirmed the accurate interpretation of responses for required data collection and the provision of sufficient data for subsequent research stages, facilitating deductions related to research concepts, aims, and objectives as suggested by Berg, B. L [29].

In the pilot study phase, three carefully selected participants (Participants 1-3) met specific criteria for the first stage of the research, representing various industries, being over 18, with at least two years of cybersecurity software experience and decision-making authority in procurement. An additional participant (Participant 4), a Social Science Psychology and Communication student with two years of experience, offered a unique perspective on the questionnaire's structure, question order, clarity, language, and communication. In this pilot study phase, Participant 1 was an IT & Security Team Leader with six years of experience in the education sector, Participant 2 is a Security Project Manager with three years of experience in government, and Participant 3 is an IT & Security Engineer with eight years of experience in the high-tech industry.

Insights from these pilot interviews informed the revised questionnaire. (Appendix A)

2.2. Participant Selection and Data Collection

After the pilot study, a combination of stratified sampling and purposive sampling was employed to select participants for the main study. Recruitment was carried out through LinkedIn, resulting in a sample of thirteen Israeli security leaders across diverse industries. The criteria for inclusion were individuals aged eighteen or above, possessing a minimum of two years of experience with cybersecurity software, and familiarity with cyber active defense solutions. Additionally, participants were required to have decision-making authority for cybersecurity software procurement within their organization, including the potential transition from on-premises security software to the cloud. A detailed participant demographic profile is provided in Appendix B.

The sample size aligns with the recommendations from similar qualitative studies, suggesting that between ten and fifteen participants are adequate for meaningful analysis [7]. Data collection involved semi-structured interviews lasting 45 minutes, conducted uniformly using the same interview protocol. These interactions occurred either over Zoom or via field notes for participants who objected to recording. A voluntary consent form was administered, granting participants the right to withdraw from the research at any point. Additionally, permission to record remote interviews using Zoom was sought.

2.3. Data Analysis Procedures

In this phase of content analysis, several steps were undertaken to derive meaningful insights from the collected data.

Step 1: Data Collection and Organization: Zoom sessions were conducted, lasting approximately 45 minutes each, and the recorded content was meticulously collected, prepared, and organized. A comprehensive review of the data involved both holistic and floating reading approaches. Transcripts were created, and participant identities were anonymized.

Step 2: Identification of Units of Analysis: To streamline the analysis, the data were minimized, and units of analysis were defined. Ideas and concepts expressed in words and phrases were carefully identified.

Step 3: Code and Category Development: A systematic process of code and category creation and refinement ensued. Codes were generated for responses from all participants, emphasizing those aligned with the research's objectives. Participant quotes relevant to the study were also selected during this step.

Step 4: Quote Selection and Memo Writing: Memos were written for each participant's responses to ensure comprehensive data gathering at the conclusion. Essential participant quotes were carefully selected to capture key insights.

Step 5: Validation and Verification: A rigorous validation process was implemented, involving code testing, correction, and thorough checks for consistency in the coding structure.

Step 6: Coding and Verification of Associated Text: All text from both interviews was coded based on the identified categories, and a meticulous verification process was carried out.

Step 7: Theme Identification and Relation Mapping: Distinct themes emerged, and their relationships with categories were defined. This step involved a comprehensive analysis of the connections between identified themes and selected participant quotes.

Step 8: Results Documentation: The findings, conclusions, and discussions were documented in a summarized format, providing a cohesive overview of the content analysis results.

This detailed methodological approach ensured a thorough exploration of the collected data, offering valuable insights into the research's aim and objectives.

3. Results

The content analysis conducted in this research followed a systematic approach encompassing seven key steps. In Step 1, data collection and organization set the foundation for the subsequent stages. Step 2 involved the identification of units of analysis,

followed by Step 3, which focused on code and category development. Step 4 encompassed quote selection and memo writing, while Step 5 concentrated on validation and verification. The subsequent steps, Step 6 and Step 7, involved coding and verification of associated text and theme identification with relation mapping.

A total of 234 codes emerged from this comprehensive analysis, as illustrated in Figure 1. Additionally, 24 categories were identified, each linked with pertinent quotes. The synthesis of these categories led to the derivation of five overarching themes in response to the defined research questions.

For Research Question 1, exploring organizations' perceptions of the shift to the cloud with extended features and functionalities in the context of cyber-active defense technology, two themes emerged. Theme 1 highlighted the empowerment of AI-enhanced and other advanced cloud capabilities for efficiency, security, and organizational evolution during the transition. Theme 2 focused on innovative cloud deception solutions and strategic approaches for seamless migrations.

Addressing Research Question 2 regarding organizations' perspectives on the shift to the cloud with new cloud ecosystem integrations, Theme 3 emerged—emphasizing integrated cloud security and orchestrating the cloud security ecosystem for resilience.

Research Question 3, delving into organizations' perceptions of the cloud shift from a cost-saving perspective, resulted in Theme 4—optimized cloud operations and a unified approach to economic efficiency.

Finally, Research Question 4, investigating organizations' perceptions of the cloud shift based on trust in cloud security, revealed Theme 5—trust in cloud security, navigating risks, challenges, compliance, and buyer dynamics during the transition from on-premises to the cloud or a hybrid cloud in the context of cyber-active defense technology. These findings are visually represented in Figures 2, 3, and 4, alongside corresponding categories and quotes, providing a comprehensive overview of the thematic outcomes derived from the content analysis.

The findings presented herein constitute preliminary results from the initial stage of a broader and more comprehensive research initiative. As the first stage of an ongoing investigation, these themes are subject to refinement and improvement pending review and recommendations from the researcher's committee. Given the iterative nature of the research process, subsequent stages and committee input are anticipated to enhance the precision and depth of the identified themes.

3.1 Results- Selected Codes

Cloud Adoption and Future Trends	Maturity of Cloud Security	Hybrid Cloud Complexity	System Health and Decoy Functionality	Reduced Infrastructure Costs	Data Security
Benefits of Cloud	Integration with On-Premises	Quick Adoption	Mapping and Customization Complexity	Scalability	Compliance Requirements
Security Concerns	Evolving Understanding of Cloud Risk	Training for Adoption	Initial Mapping of the Network	Pay-as-You-Go Model	Data Privacy and Sovereignty
Hybrid Cloud Approach	Customization and Vendor Selection	Transition from On-Premises	Challenges in Network Mapping	Lower Maintenance Overhead	Access Control and Identity Management
Use Cases and Specific Applications	Value of Native Cloud Solutions	Noise During Implementation	Resource Allocation for Deployment	Enhanced Security Features	Third-Party Security
Organizational Priorities	Focus on Cloud Assets	Technical User Adoption	Bureaucracy and Administrative Efforts	Global Reach	Incident Response
Transition to Cloud Services	Importance of Reputable Vendors	Control and Security in On-Premises	Resource Involvement for On-Prem Deployment	Improved Disaster Recovery	Vendor Lock-In
Complexity and Integration	Security in Specific Industries	High-Tech Industry Process	Agentless Implementation	Efficiency in Resource Allocation	Data Residency
Cloud Vendor Selection	Multi-Cloud Environment	Simplicity and Scalability	Effective Threat Detection	Impact on IT Staff Workload	Cloud Configuration
Value and Expertise	Data Encryption and Compliance	Vulnerability Scanning	Reduced False Positive Alarms	Initial Capital Expenditure Reduction	Cost and Resource Management
Industry-Specific Considerations	Threat Detection and Incident Response	User Feedback for Refinement	Early Threat Detection	Cost-Benefit Analysis	Policy Adherence
Data Privacy and Compliance	User Education and Vendor Assessments	Access Controls and Permissions	Enhanced Security Posture	Data Transfer and Subscription Costs	Multi-Tenant Concerns
Cloud Management and Resources	Security Posture and Defense Layers	Cloud Center of Excellence (CoE)	Strategic Placement of Decoys	Impact on Energy and Cooling Expenses	Audit and Compliance Checks
Challenges in Transition	Importance of Access Controls	Efficiency and Flexibility of Cloud Services	Dynamic Adaptation for Changing Threat Landscape	Flexibility in Resource Allocation	Network Security
Public Sector Considerations	Data Protection in Transit and at Rest	Data Migration for Minimal Disruption	Regulatory Compliance Considerations	License Management	Privacy Regulations
Vendor Relationship and Trust	Vendor Selection and Solution Integration	Change Management for Smooth Transition	Infrastructure Maintenance	Security Check	Mindset Change
Demand-Driven Adoption	Continuous Monitoring and Compliance	Monitoring and Optimization for Efficiency	Scalability and Resource Allocation	Immediate Adoption	Saving Time, Resources, Maintenance
Transitioning and Skill Development	Security Challenges in High-Tech Industry	Vendor Selection and Evaluation	Automated Backup and Recovery	Hybrid Model Preference	Management in the Cloud
Data Security in Cloud	Identification and Monitoring of Cloud Activities	User Training and Awareness	Security Patching	Critical vs. Non-Critical Data	Pricing Pays Off
Multi-Cloud Strategy	Balancing Security and Efficiency	Adoption Due to COVID-19	Global Accessibility	Resilience Perspective	Scalability and Cost Efficiency
Use of Cloud in Pandemic	Staff Education and Awareness	IT and Security Collaboration	Incident Response	Combining Elements	Scalability
Government Data Store Marketplaces	Due Diligence with Cloud Service Providers	Real-Time Monitoring for Compliance	Enhanced Security Features	Strategic Consideration	Cost Savings
Transition Challenges	EDR (Endpoint Detection and Response)	Integration with Anomaly Systems	Compliance Tools	Maintaining Control	Accessibility
Collaboration and Expertise	SIEM (Security Information and Event Management)	Integration Must Be Easy	Resource Optimization	Worthwhile Migration	Automatic Updates
Rapid Changes in Cloud	Attack Simulations	Importance of Ecosystem Integration	Real-Time Monitoring	Flexibility and Gradual Transition	Disaster Recovery
Compliance with Regulations	XDR (Extended Detection and Response)	All Systems Playing Together	Reduced Hardware Costs	Aligning with Specific Needs	Data Privacy and Compliance
Cloud for Business Continuity	NAC (Network Access Control)	Cautious Approach to Integrations	Automation of Repetitive Tasks	Balancing Control and Flexibility	Security Risks
Cloud for Real-Time Data	Firewall	Benefits of Third-Party Integrations	Reduced On-Site Presence	Data Sensitivity and Compliance	Internet Dependency
Threat Intelligence Integration	Sandbox	Challenges of Integration	Centralized Reporting and Analytics	Vulnerability Assessment and Management	Data Transfer Costs
Scalability and Auto-scaling	Proxy	Compatibility and Security	Data Center Maintenance	IAM (Identity and Access Management)	Integration Complexity
Cloud-Native Integration	Antivirus (AV)	Ease of Integration	Dynamic Scalability	Encryption	Vendor Dependency
Real-time Threat Intelligence Feeds	Sunblast	Vendors Offering Integrations	Enhanced Accessibility and Remote Management	Multi-Factor Authentication (MFA)	Latency
Behavioral Analysis	Mail Filter	Advantages of Integration	Cost Savings	Security Awareness and Training Programs	Data Sovereignty and Compliance
Threat Attribution	SOAR (Security Orchestration, Automation, and Response)	Integration Complexity	Regulatory Compliance Simplification	API Protection	Security Trust
Machine Learning and AI	IDPS (Intrusion Detection and Prevention System)	Customization and Tailoring	Streamlined Log Management	Data Exfiltration Monitoring	Reduced Physical Footprint
Automation and Orchestration	DLP (Data Loss Prevention)	Multi-Layered Defense	Advanced Security Features in the Cloud	Geographic Diversity	Reduced Chain of Approvals
User and Entity Behavior Analytics (UEBA)	Active Defense and Deception Technology	Data Privacy and Protection	Global Threat Intelligence Feed Integration	Geo-Fencing	Ongoing Maintenance and Updates
Incident Response Integration	Intune	Incident Response Efficiency	Reduced Time Spent on Troubleshooting	Compliance Orchestration	WAF (Web Application Firewall)
Enhanced Reporting and Analytics	Anomaly Detector	Flexibility and Adaptability	Improved Security Patch Management	Dynamic Scalability	Cloud-Native SIEM Integration

Fig.1. Selected Codes

3.2 Results- Selected Categories Themes and Quotes

Research Question 1: How do organizations perceive the shift to the cloud when leveraging extended features and functionalities in the context of cyber-active defense technology/deception technology?	
Theme 1 **Empowering AI-enhanced and other advanced and cloud capabilities for efficiency, security and organizational evolution when shifting from on-premises to the cloud or a hybrid cloud**	**Theme2** **Innovative Cloud Deception Solution and Strategies Approach for Seamless Migrations from on-premises to the cloud or a hybrid cloud**
Related Categories:	**Related Categories:**
Cloud Adoption and Future Trends:	Advantages and Strategic Planning of Deception Technology
Cloud Deployment Strategies:	Early Threat Detection
Cloud Infrastructure Management and Security:	Reduction in Dwell Time
Quick Adoption:	Mimicking Actual Network
Efficiency and Flexibility of Cloud Services:	Migration Decision Factors
Infrastructure Maintenance:	Migration Approaches
Scalability and Resource Allocation:	Security Check
Automated Backup and Recovery:	Strategic Consideration
Security Patching:	Worthwhile Migration
Global Accessibility:	Hybrid Model Preference
Adaptive Security:	Critical vs. Non-Critical Data
Organizational Change Management:	Flexibility and Gradual Transition
User Adoption and Training:	**Related Quotes:**
Geo-fencing and Data Sovereignty:	The layout of the deception solution has been strategically designed to mimic our actual network infrastructure.
Protection of Cloud APIs and Data Exfiltration Detection:	requirements, compliance considerations, and the overall strategic goals of our organization.
Related Quotes:	each environment.
The adoption was very quick; non-tech users take some more time to adopt but also faster than on-prem.	Yes, I would migrate immediately to hybrid mode.
We succeeded in benefiting from the efficiency and flexibility of cloud services while maintaining a strong security posture.	I think a hybrid model is the best in this case; it will reduce time for approval for such migration.
With the cloud, the responsibility for infrastructure maintenance, such as server updates, hardware management, and data center maintenance, largely shifts to the cloud service provider.	I will definitely recommend migrating in hybrid mode... the world is moving there, and we should not stay behind.
Cloud environments offer dynamic scalability. This means we no longer need to manually allocate and provision resources, optimizing resource utilization and potentially reducing costs.	
Many cloud providers offer automated backup and disaster recovery solutions. This simplifies the backup process and ensures data is protected and recoverable in case of a failure.	
Cloud providers typically handle security patching and updates, reducing the time and effort required to keep the deception solution secure and up to date.	
Cloud-based solutions often offer improved accessibility and remote management, enabling security teams to monitor and manage the deception solution from anywhere, improving overall efficiency and response times.	
Advanced threat attribution capabilities to help identify the origin and intent of attacks and attackers, providing valuable insights for incident response.	
Adding behavioral analysis to the deception solution to track and profile the behavior of attackers and provide insights into their motivations and methods.	
Leveraging machine learning and AI to continually improve the deception's ability to mimic real assets and adapt to evolving attacker techniques.	
Incorporating UEBA capabilities to detect anomalous user and entity behavior patterns within the cloud environment, enhancing threat detection and mitigation.	
The ability to dynamically scale deception assets based on cloud resource availability and demand, ensuring that the deception environment can adapt to varying workloads.	
Implementing deception assets in multiple geographic regions to diversify the deception environment and cover a broader range of potential attacker locations.	
All technical users adopted these cloud applications very easily, with other users, it took some more time but also less time than the on-prem application.	
If it's a hybrid cloud then sometimes it's more complicated because you need to use jump servers, use segmentation and isolation.	
The CoE team helps manage the organizational change associated with cloud adoption, ensuring a smooth transition for our staff and teams	
We succeeded in benefiting from the efficiency and flexibility of cloud services while maintaining a strong security posture.	
Training and user awareness are critical for successful adoption.	
Implementing deception elements to protect cloud APIs, as they are often targeted by attackers seeking to exploit vulnerabilities.	
Enhancing the solution's ability to monitor and detect data exfiltration attempts in the cloud environment.	
Implementing geo-fencing capabilities to control and limit the geographic locations where deception assets are active, addressing data sovereignty concerns and regulatory compliance.	

Fig. 2. Research Question 1: Themes 1&2- Selected Categories and Quotes

Research Question 2: How do organizations perceive the shift to the cloud when leveraging new cloud ecosystem integrations in the context of cyber-active defense technology/deception technology?
Theme3
Integrated Cloud Security: Orchestrating Cloud Security Ecosystem for Resilience
Related Categories:
Threat Intelligence Integration
Cloud-Native Integration
Unified Incident Response and Cloud Security Integration
Automation and Ecosystem
Incident Response Integration
Compliance Orchestration
Related Quotes:
Enhancing detection and response capabilities by integrating with threat intelligence feeds specific to cloud environments.
Improving threat detection and incident response within the cloud infrastructure through integration with cloud-native security tools and services.
Developing automated incident response capabilities to take predefined actions in response to specific threats within the cloud environment.
Seamless integration with our Security Information and Event Management (SIEM) system provides a comprehensive view of security events, enabling more efficient incident response.
Customizing security solutions according to organizational needs is crucial for a robust and tailored defense approach.
Advanced reporting and analytics provide comprehensive insights into threat activity, facilitating informed decisions and improved security strategies.
Integrating with cloud-native SIEM solutions centralizes event and log management for better visibility and correlation of security data.
Introducing third-party solutions creates a multi-layered defense approach that is often more effective in thwarting advanced threats.
Integration of compliance orchestration features automates compliance checks and reporting, ensuring continuous adherence to regulatory requirements.
Ecosystem integration, like isolating threats or placing decoys based on information received from NAC, helps remediate threats effectively.
Integrating third-party solutions into our cloud-based deception solution enhances security capabilities by keeping deception technology up to date with the latest threat intelligence and security innovations.

Fig. 3. Research Question2:Themes 3- Selected Categories and Quotes

Research Question 3: How do organizations perceive the shift to the cloud from a cost-saving perspective in the context of cyber-active defense technology/deception technology?
Theme 4
Optimized Cloud Operations: A Unified Approach to Economic Efficiency
Related Categories:
Cost Efficiency and Infrastructure Benefits
Reduced Infrastructure Costs
Scalability
Pay-as-You-Go Model
Reduced On-Site Presence
Resource Optimization
Operational Excellence in the Cloud
Saving Time
Accessibility
Automatic Updates
Disaster Recovery
Related Quotes:
By leveraging cloud-based services, we can eliminate the need for maintaining on-premises hardware.
Cloud services often operate on a pay-as-you-go model, meaning we only pay for the resources we actually use, optimizing cost efficiency.
Shifting our deception solution to the cloud offers advantages such as scalability, cost efficiency, global reach, redundancy, and automatic updates.
Scalability: Cloud-based solutions can easily scale to accommodate changing security needs, allowing us to quickly adapt to evolving threats.
Cloud-based deception solutions allow us to scale resources up or down as needed, reducing the cost of over-provisioning.
If our organization expands globally, cloud-based solutions can provide cost-effective coverage and accessibility across different geographic locations.
Cloud providers often offer advanced security features, including DDoS protection and encryption, which can augment the security of our deception solution.
Many repetitive security tasks can be automated in the cloud, reducing manual workload and the risk of human error.
We can eliminate the need for on-premises hardware and data center infrastructure, which can be a substantial cost-saving measure.
Shifting our deception solution to the cloud offers advantages such as scalability, cost efficiency, global reach, redundancy, and automatic updates.

Fig. 4. Research Question3:Themes 4- Selected Categories and Quotes

Research Question 4: How do organizations perceive the shift to the cloud according to their trust in cloud security in the context of cyber-active defense technology/deception technology?
Theme 5
Trust in Cloud Security: Navigating Risks and Challenges, Compliance and Buyer Dynamics When Shifting Cybersecurity Technologies From On-Premises to the Cloud or a Hybrid Cloud in the Context of Cyber-Active Defense
Related Categories:
Security, Compliance, and Operational Considerations:
Security Concerns:
Vendor Relationship and Trust:
Buyer Behavior Aspects:
Risk Mitigation and Cloud Adoption Challenges:
Data Privacy and Compliance:
Data Sovereignty and Compliance:
Security Risks
Integration Complexity
Vendor Dependency
Security Trust:
Internet Dependency
Data Transfer Costs
Latency
Related Quotes:
Private cloud is very secure; public cloud is less secure.
Choosing trusted and compliant solutions.
Managing data privacy and compliance in the cloud can be complex, especially if sensitive data is involved. It requires careful adherence to regulatory requirements.
Relying on a cloud provider requires a level of trust in their security practices, which may raise concerns about data protection and control.
Choosing reputable vendors is important.
Understanding increased with real events and threats.
It's a must today; people have to move to cloud environments.
The concept and future are cloud.
Cloud is the next thing everyone moves to. It brings great improvements for business organizations.
Storing and processing sensitive information in the cloud requires robust data security measures to prevent unauthorized access or data breaches.
Prioritize using authorized government data store marketplaces.
Responding to business demands for cloud services.
In the logistics industry, cloud solutions can benefit from scalability and accessibility.
In the financial sector, agility and flexibility are essential.
Cloud security solutions are essential for protecting data and applications.
Data encryption is a standard practice for data at rest and in transit.
Compliance monitoring is crucial for audits and regulatory reporting.
Implementing strong access controls for cloud resources.
Security policies need to be adapted to the cloud environment to ensure they align with security objectives.
When considering third-party solutions, careful vendor selection is vital.
Ensuring data sovereignty and compliance with healthcare regulations may be more complex in a cloud environment.
Cloud environments can introduce new security risks if not properly configured or if third-party integrations are not thoroughly vetted.
Relying on a cloud provider means that we may be dependent on their services and security measures, which can limit control over the environment.
Cloud solutions rely on internet connectivity, and any network disruptions can impact accessibility and security operations.
Moving data to and from the cloud can incur data transfer costs, which should be considered in the overall budget.
Latency issues can arise when certain security tasks require real-time responses, as cloud-based solutions might introduce delays compared to on-premises alternatives.
The potential for cost savings is evident in a cloud-based deception solution, it's essential to conduct a thorough cost-benefit analysis, factoring in migration costs, ongoing subscription expenses, and the specifics of our security needs.

Fig. 5. Research Question 4: Theme 5- Selected Categories and Quotes

4. Discussion

The qualitative content analysis undertaken in this study has revealed compelling themes that delve into organizations' viewpoints on the shift to the cloud within the domain of cyber-active defense technology and specifically deception technology. These emergent themes serve as the cornerstone for a nuanced discussion, offering immediate implications, acknowledging limitations, and paving the way for future research avenues.

The first theme, emphasizing the empowerment of AI-enhanced capabilities and advanced cloud functionalities (Theme 1), underscores a paradigm shift towards efficiency, security, and organizational evolution during cloud transitions. Concurrently, Theme 2 sheds light on the strategic importance of innovative cloud deception solutions for seamless

migrations. These findings prompt an exploration into the specific technologies and methodologies deployed by organizations in realizing these themes and the associated implications for evolving cybersecurity strategies.

In tandem, Theme 3 surfaces the critical need for integrated cloud security, advocating for the orchestration of the cloud security ecosystem to enhance resilience. This theme necessitates further examination of the challenges and opportunities inherent in integrating diverse elements within the cloud security landscape. Understanding the nuances of these integrations will contribute to a comprehensive grasp of the complexities involved in securing cloud environments effectively.

Furthermore, Theme 4 highlights the paramount importance of optimized cloud operations and a unified approach to economic efficiency. Delving into the operational practices and cost-saving strategies adopted by organizations becomes imperative for comprehending the broader economic implications of cloud migration within the context of cyber-active defense technology.

The exploration of Theme 5 brings to the forefront the intricacies surrounding trust in cloud security. It underscores the challenges, risks, compliance considerations, and buyer dynamics organizations grapple with during the transition. This theme invites deeper scrutiny into the factors influencing trust and the strategies employed by organizations to mitigate potential risks in the cybersecurity landscape.

As we consider the immediate implications of these findings, it is essential to acknowledge the limitations inherent in this qualitative analysis. The qualitative nature of the study provides depth but lacks the breadth that quantitative methodologies could offer. Future research endeavors should thus integrate quantitative approaches to validate and expand upon these qualitative insights, providing a more comprehensive understanding and the researcher plans to continue these research next stages.

Moreover, recognizing that this study represents the preliminary qualitative analysis of a broader mixed research initiative is crucial. The iterative nature of this research process ensures that subsequent stages will build upon these preliminary findings. Future research should aim to refine and expand the understanding of this critical intersection in the evolving landscape of cybersecurity, thus contributing to the ongoing discourse on cybersecurity buyer behaviour and developing a marketing startegic plan when shifting cybersecurity technologies from on-premises to the cloud or the hybrid cloud.

4.1. Disclosure and conflict of interest

The author of this article is a doctoral student researcher at “Alexandru Ioan Cuza” University of Iasi with more than 25 years of experience in high-tech, specializing in cybersecurity. Additionally, he works at Commvault (a global provider of cyber resilience solutions) as Field Security CTO. For this research paper, in order to avoid any conflicts of interest and remain as unbiased as possible, the author purposely selected participants who do not have any contractual, direct, or indirect obligations with his company. Furthermore, they did not have any work relations with him during the interviews.

Appendix A. The revised questionnaire following the pilot:

1. What are your general thoughts on cloud environments?
2. What do you think about cloud security solutions?
3. Do you currently have any applications or cybersecurity solutions deployed in the cloud within your organization? If yes, could you elaborate on the process of their adoption by end users?
4. What challenges and advantages have you encountered with your deception solution and what comments would you have about the layout and coverage?
5. How do you perceive the potential cost-saving for your organization if you were shifting your deception solution from on-premises to the cloud?
6. Are there any specific security concerns, that you believe are relevant to address when shifting your deception solution to the cloud? Do you see issues related to internal policy restrictions or external regulations, for example?
7. What additional features would you be interested in incorporating into your deception solution after shifting to the cloud?
8. Which security solutions are you currently utilizing?
9. How do you perceive the idea of integrating third-party solutions into your deception solution once shifted to the cloud?
10. What security, maintenance, or process activities do you think will become unnecessary or improved once you shift your deception solution to the cloud?
11. Would you consider migrating your deception solution from on-premises to the cloud or implementing a hybrid model where some components are on the cloud and some are on-premises?
12. What other advantages or disadvantages do you perceive when shifting your deception solution to the cloud?

Appendix B. Interviewees Participants Profile

Table 1. Interviewees Participants Profile

Participant Number	Age	Gender	Education	Role	Industry	Experience in IT & Cybersecurity
1	28	Female	Undergraduate degree andcertifications in the field of cybersecurity	SOC Manager	Defense Industry	8 years
2	47	Male	Undergraduate and graduate degrees and certifications in the field of cybersecurity	Chief Information Security Officer	Recycling	26 years
3	56	Male	Undergraduate degree and certifications in the field of cybersecurity	CEO	Managed Security Service Provider	33 years

4	51	Male	Undergraduate degree	Chief Information Officer	Real Estate	20 years
5	39	Male	IT and cybersecurity technical certifications	System Manager	Beverage	15 years
6	34	Male	IT and cybersecurity technical certifications	IT and Security Specialist	Government	7 years
7	42	Female	Undergraduate degree and certifications in the field of cybersecurity	Information Security Manager	Food producer/ Manufacturing	15 years
8	28	Male	IT and cybersecurity technical certifications	Security Analyst	High-Tech -Internet	4 years
9	32	Male	IT and cybersecurity technical certifications	IT& Security Specialist	Education	6 years
10	29	Female	Undergraduate degree and certifications in the field of cybersecurity	IT& Security System Administrator	Logistics	5 years
11	42	Male	Undergraduate degree and certifications in the field of IT & Cybersecurity	IT & Security infrastructure Manager	Financial-Private sector	15 years
12	28	Male	Certifications in the field of cybersecurity	Security Specialist	Financial-Public sector	4 years
13	36	Female	Undergraduate and certifications in the field of cybersecurity	Security Operations Control Manager	Healthcare	8 years

References

[1] I. D. C. FutureScape, "I.D.C. FutureScape: Worldwide I.T. industry 2022 predictions," 2022.

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

[3] N. Chowdhury, "Factors Influencing the Adoption of Cloud Computing Driven by Big Data Technology: A Quantitative Study," *Capella University*, 2018.

[4] M. Egbert, "Driving Public Cloud Adoption through Qualitative and Quantitative Modeling," *Doctoral dissertation, Pace University*, 2015.

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

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

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

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

[9] M. W. Meersman, "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*, 2019.

[10] K. E. Mulchahey, "Exploration of Complexities for Migration of Software-Licensing Models," *Capella University*, 2019.

[11] C. M. Taylor Sr, "Identifying and Overcoming the Barriers to Cloud Adoption within the Government Space," *Doctoral dissertation, The George Washington University*, 2018.

[12] L. N. Gumbi and E. Mnkandla, "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*, no. 7(4), p. 1, 2015.

[13] K. Gai, "A review of leveraging private cloud computing in financial service institutions: Value propositions and current performances," *Int. J. Comput. Appl*, no. 95(3), pp. 40-44, 2014.

[14] T. Boillat and C. Legner, "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*, no. 8(3), pp. 39-58, 2013.

[15] S. Bhayal, "A study of security in cloud computing," *California State University, Long Beach*, 2011.

[16] C. G. Sobragi, A. C. G. Maçada and M. Oliveira, "Cloud computing adoption: A multiple case study," *BASE: revista de administração e contabilidade da Unisinos= BASE: UNISINOS accounting and administration journal. São Leopoldo, RS*, vol. 11, no. 1, pp. 75-91, jan./mar. 2014.

[17] C. Liu, C. L. Sia and K. K. Wei, "Adopting organizational virtualization in B2B firms: An empirical study in Singapore," *Information & management*, vol. 45(7), pp. 429-437, 2008.

[18] E. M. Rogers, "Diffusion of Innovations: modifications of a model for telecommunications. In Die diffusion von innovationen in der telekommunikation," *Springer, Berlin, Heidelberg*, pp. 25-38, 1995.

[19] J. Pfeffer and G. R. Salancik, "The external control of organizations: A resource dependence perspective," *Stanford University Press*, 2003.

[20] C. Peake, "Accepting the Cloud: A Quantitative Predictive Analysis of Cloud Trust and Acceptance Among I.T. Security Professionals," *Doctoral dissertation, Capella University*, 2018.

[21] E. L. Slade, Y. K. Dwivedi, N. C. Piercy and M. D. Williams, "Modeling consumers' adoption intentions of remote mobile payments in the United Kingdom: extending UTAUT with innovativeness, risk, and trust," *Psychology & Marketing*, vol. 32(8), pp. 860-873, 2015.

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

[23] V. Venkatesh, M. G. Morris, G. B. Davis and F. D. Davis, "User acceptance of information technology: Toward a unified view," *MIS quarterly*, pp. 425-478, 2003.

[24] R. E. Freeman, "Strategic management: A stakeholder approach," *Boston: Pitman*, 1984.

[25] M. Fishbein and et al., "Belief, attitude, intention and behavior: An introduction to theory and research," *Reading, MA.: Addison-Wesley*, 1975.

[26] I. Ajzen, "From intentions to actions: a theory of planned behavior," *In: J*, 1985.

[27] J. A. Howard and et al., "The Theory of Buyer Behaviour," *London: John Wiley and Sons, Inc*, 1969.

[28] E. R. Teijlingen and V. Hundley, "The importance of pilot studies," *Social Research Update, 35*, 2001.

[29] B. L. Berg, "Qualitative research methods for the social sciences (4th Edition)," *Boston, MA: Allyn and Bacon*, 2001.