Shifting Control Points: How AI Capabilities are Reshaping the SaaS Industry

Rui Gonçalves

Dissertation written under the supervision of Professors René Bohnsack and

Mickie De Wet

Dissertation submitted in partial fulfilment of requirements for the MSc in Management - Strategy, Entrepreneurship & Impact, at the Universidade Católica Portuguesa, January 4th, 2026.

[Page intentionally left blank]

Shifting control points: How AI Capabilities are Reshaping the SaaS Industry

Rui Gonçalves

Abstract

Artificial intelligence (AI) is widely regarded as a disruptive force in the Software-as-a-Service (SaaS) industry, raising questions about the sustainability of the control points that have historically supported SaaS incumbents. This dissertation examines how enterprise adoption of AI capabilities challenges traditional SaaS control points, how incumbents respond strategically, and whether AI-as-a-Service (AIaaS) and AI+SaaS strategies can serve as effective defensive mechanisms. Building on Control Points Theory, the study adopts a qualitative, inductive research design based on semi-structured interviews with consultants working closely with SaaS providers and enterprise clients, as well as professionals from SaaS incumbents and firms developing internal AI solutions. The findings show that AI does not lead to a uniform shift in control. First, application-layer technical control points become contestable in a capability-contingent manner, benefitting only firms with sufficient organizational capabilities. Second, strategic control points such as contractual relationships, compliance certifications, and customer relationships persist and may even strengthen as AI intensifies data governance and security concerns. Third, new technical control points emerge at the infrastructure layer, where access to compute resources, foundational models, and orchestration platforms becomes increasingly critical. Overall, the study concludes that AI reconfigures rather than erodes control in the SaaS industry, creating multi-layered, conditional, and contested control structures.

Keywords: Artificial Intelligence; Software-as-a-Service (SaaS); Control Points Theory; Value Capture; Enterprise Software

Shifting Control Points: How AI Capabilities are Reshaping the SaaS Industry

Rui Gonçalves

Resumo

A inteligência artificial (IA) é amplamente reconhecida como uma força disruptiva na indústria de Software-as-a-Service (SaaS), levantando questões sobre a sustentabilidade dos pontos de controlo que historicamente sustentaram os incumbentes. Esta dissertação analisa de que forma a adoção de capacidades de IA pelas empresas desafia os pontos de controlo tradicionais do SaaS, como os incumbentes respondem estrategicamente a estas mudanças e em que medida as estratégias de AI-as-a-Service (AIaaS) e AI+SaaS podem funcionar como mecanismos defensivos. Com base na Teoria dos Pontos de Controlo, o estudo segue uma abordagem qualitativa e indutiva, assente em entrevistas semiestruturadas realizadas a consultores que trabalham com fornecedores SaaS e clientes empresariais, bem como a profissionais de empresas SaaS incumbentes e de organizações que desenvolvem soluções internas de IA. Os resultados mostram que a IA não conduz a uma alteração uniforme das estruturas de controlo. Em primeiro lugar, os pontos de controlo técnicos ao nível da aplicação tornam-se contestáveis de forma contingente às capacidades organizacionais. Em segundo lugar, pontos de controlo estratégicos, como relações contratuais, certificações de conformidade e relações com clientes, persistem e podem até se fortalecer à medida que a IA intensifica as preocupações com a governança e a segurança dos dados. Por fim, emergem novos pontos de controlo técnicos ao nível da infraestrutura, associados ao acesso a recursos computacionais, modelos fundacionais e capacidades de orquestração. Conclui-se que a IA reconfigura, em vez de eliminar, os pontos de controlo na indústria SaaS, originando estruturas de controlo multinível, condicionais e disputadas.

Palavras-chave: Inteligência Artificial; Software-as-a-Service (SaaS); Teoria dos Pontos de Controlo; Captura de Valor; Software Empresarial

[Page intentionally left blank]

Acknowledgements

This thesis marks the end of my long, challenging, yet incredibly rewarding academic journey, which would not have been possible without the support and belief of those around me.

First and foremost, I would like to express my sincere gratitude to my advisor, Professor Mickie De Wet, for her guidance, critical feedback, and continued support, as well as for her availability and openness throughout the development of this dissertation.

I would also like to thank all the professors at Católica Lisbon who were part of my academic journey. Their teaching, mentorship, and intellectual challenge played a fundamental role in shaping my thinking and provided the foundation upon which this work was built.

To my parents, thank you for your unconditional support and for believing in me and my academic journey. You gave me the strength and encouragement needed to finish this journey.

To the rest of my family and my friends, thank you for your support, motivation, and companionship, which made this journey both more manageable and more meaningful.

To my girlfriend, thank you for being my daily support. Your care, patience, constant motivation, and belief in my potential gave me the capacity to push through the more challenging moments. Thank you for being there for me.

Lastly, I would like to acknowledge my own perseverance and continued belief in my potential throughout this journey.

I conclude with a quote that has consistently motivated my approach to work and discipline: "*Great things come from hard work and perseverance. No excuses*."

- Kobe Bryant

[Page intentionally left blank]

Table of Contents

Table of Figures

1. Introduction

Since the beginning of the century, the Software-as-a-Service (SaaS) sector has been the prevailing method of enterprise software delivery. SaaS incumbents have historically preserved their competitive edge via proprietary technology, data, platforms, and customer lock-in mechanisms that establish significant barriers for competitors (Opara-Martins et al., 2017). These firms were able to achieve more predictable revenue streams and scalability advantages by replacing traditional perpetual licensing models for software with cloud-based subscriptions (Guo & Ma, 2018). Over the years, SaaS has become central to enterprise digital transformation, with firms like Salesforce, Adobe, and ServiceNow being some of the biggest players in the market.

However, this sector is going through a significant transformation, with some industry observers arguing that Artificial Intelligence (AI) is emerging as the biggest disruptive force in the sector since its inception (Khanna et al., 2025). Generative AI, AI Agents, and easy-to-use toolkits (eg., LangChain, AutoML platforms, and others) are reducing the cost of firms developing their own AI solutions rather than relying on SaaS vendors. Additionally, Crawford et al. (2025) claim that the trend of moving to in-house application development is being accelerated by agentic AI (World Economic Forum, 2024) - autonomous AI systems capable of perceiving their environment, making decisions, and taking actions with minimal human intervention - and low-code AI development systems, which enable enterprises to automate processes that were previously handed off to SaaS platforms. Equally, Khanna et al. (2025) point out that companies are also moving AI models directly into their digital frameworks, skipping the SaaS middlemen as they create their own AI-led tools to analyze, manage their operations, and for customer relationship management.

These competitive dynamics can be understood through Control Points Theory, which examines the positions (i.e., control points) where firms create and capture value and exert power in the market (Pagani, 2013). In the SaaS market, such control points exist at multiple layers of the technology stack, which includes application platforms, data infrastructure, and cloud computing resources. For the purposes of this research, the application layer refers to end-user SaaS applications and domain-specific functionality, while the infrastructure layer refers to AI-enabling resources such as compute capacity, foundation models, and orchestration platforms. Competitive advantage depends on which actors hold technical and strategic positions that create dependencies, rather than on internal capabilities alone (Bohnsack et al., 2024).

Building on Pagani's (2013) foundational work on control points, Bohnsack et al. (2024) therefore distinguish between technical control points and strategic control points, both of which are shaped by institutional boundary conditions such as regulatory frameworks and industry norms. Technical control points can be defined as the technological aspects or infrastructure that allow firms to access and shape markets, including the ownership of data, platform interfaces, or other standards that define participation in digital markets. Strategic control points on the other hand, are about the relational and organizational aspects of value capture by firms, that is, how firms govern themselves, interact with customers or other market actors, and establish their position of power. Institutional factors, such as regulatory frameworks and industry norms, further limit and organize these control points by constraining which strategic and technical options firms can pursue, thereby shaping how power and value are distributed across ecosystems (Elaluf-Calderwood et al., 2011; Pagani, 2013; van Dyck et al., 2021; Hannah & Eisenhardt, 2018; Bohnsack et al., 2024). Also, according to Pagani (2013), control points are not static but evolve in response to technological and competitive triggers. Due to its novelty and rapid evolution, AI could therefore be a significant market disruptor for the SaaS sector from a control points perspective.

The SaaS sector provides a relevant case study to analyze the aforementioned competitive dynamics, since incumbents' dominance has been based on control points that AI challenges directly. In contrast to other sectors where AI improves existing workflows, in SaaS, AI could potentially challenge the need for the intermediary platform layer itself (Jacobides et al., 2021). It is evident that SaaS vendors have succeeded in capturing value by strategically positioning themselves as essential integrators. Nonetheless, by developing their own AI solutions (bypassing the traditional SaaS layer), enterprises attack the fundamental premise of dependency on vendors (Crawford et al., 2025; Khanna et al., 2025; McCord, 2025). According to a recent study in the industry, companies like Klarna are reasserting their domination by building custom stacks to substitute licensed SaaS services (McCord, 2025).

This prompts critical questions regarding the alignment structure of the multilateral partnerships that constitute SaaS ecosystems (Adner, 2017): which actors remain essential, which positions become vulnerable, and how relationships must be reconfigured.

Furthermore, SaaS incumbents face a strategic dilemma in their response. Some firms are starting to pursue different strategies to defend their position in the sector, such as AI-as-a-Service

(AIaaS), delivering AI capabilities as an independent service (e.g., Salesforce's Einstein APIs), and AI+SaaS (Khanna et al., 2025), where AI is integrated into their existing products (e.g., Salesforce's Einstein Copilot). For both theoretical and practical reasons, it is critical to understand if the sector's traditional control points remain defensible, how incumbents are responding with new approaches, and if these strategies are effective.

Despite the growing recognition of AI's transformative potential, empirical research about whether AI's development capabilities compromise the control points that have traditionally sustained SaaS incumbents' dominance, or whether new control points are emerging within AI-enabled enterprise environments that simply reconfigure vendor power, is still scarce.

As a result, this thesis seeks to answer the following:

a) How does enterprise adoption of AI capabilities challenge traditional SaaS control points?
b) What strategies are SaaS incumbents pursuing to maintain or reconfigure their market positions in response to enterprise AI adoption?
c) Can incumbents defend control points by offering AIaaS or AI+SaaS, and how effective are those strategies as a defence?

By answering these questions, this research contributes to Control Points Theory literature, while providing practical insights for SaaS firms navigating AI-driven disruption and for enterprises evaluating build-versus-buy decisions around AI capabilities. This research adopts a qualitative approach based on semi-structured interviews with two groups of informants holding complementary perspectives: consultants working closely with SaaS providers and enterprise clients, and professionals working in firms, including SaaS incumbents and organizations developing internal AI-enabled solutions. Following a snowball sampling approach, this study analyzes both sides of the disruption - those defending traditional control points and those challenging them. This contrast enables a comprehensive understanding of how AI is reshaping competitive dynamics within the SaaS ecosystem. The thesis is structured as follows: following this introduction, the literature review examines the SaaS industry, Control Points Theory, traditional control points, AI as a disruptive force, and incumbent responses. The methodology section then details the research design and data collection process. Subsequently, the analysis and

results section presents findings from the interviews. Finally, the general discussion offers main conclusions, implications for future research, and the limitations of the study.

2. Literature Review

The Software-as-a-Service (SaaS) business has established itself as a dominant business model in enterprise software delivery, and yet the swift progress of artificial intelligence (AI) is poised to disturb its traditional bases of value creation and value capture. This literature review analyzes how AI puts a strain on the traditional control points that have long served to sustain SaaS players, considers the appearance of new ones, and assesses how companies can protect themselves or reshape their positions. The review is divided into six thematic groups: an overview of the SaaS industry, Control Points Theory, conventional control mechanisms, AI-driven disruption, and incumbent strategic responses.

2.1. SaaS Industry and Competitive Dynamics

The Software-as-a-Service (SaaS) model has changed the way in which companies provide and consume software. Clients no longer need to buy software licenses, but subscribe to cloud-based services that can be accessed anywhere and updated automatically. This model decreased installation expenses and gave businesses the opportunity to allocate resources in a more effective manner (Guo & Ma, 2018). According to Guo & Ma (2018), SaaS improved scalability, access to customers, and control of costs, providing firms with stable and foreseeable revenues. This model was adopted by major providers like Salesforce and Adobe to create massive global user bases and provide ongoing innovation. Managing continuous updates, leveraging data, and maintaining active interactions with customers made these firms stable and formed long-term client relationships, which have made SaaS a pillar of digital transformation (Rrucaj, 2023).

SaaS companies secured their competitive edge by concentrating on innovation, ecosystem partnerships, and customer retention. As Chen (2022) notes, SaaS vendors aligning their business development around internal capabilities and customer needs tend to achieve stronger performance outcomes. Rrucaj (2023) also mentions that the rapid development of the software market does not allow for maintaining an advantage without strategic management and constant adaptation. Thus,

ecosystems of developers and partners are developed by many SaaS providers to generate value and dependency. According to Opara-Martins et al. (2017), this interdependence results in customer lock-in and high switching costs, which are conventional mechanisms of control through which incumbents defend themselves. In addition, the industry makes use of effective pricing and operating strategies. According to Li and Kumar (2022), flexible pricing models and effective service delivery enhance their profitability and retain their customer base.

The SaaS industry is, however, experiencing significant disruption due to the centrality of artificial intelligence in enterprise solutions (Khanna et al., 2025). Traditional control points, like ownership of the platform, customer data, and integration, are being put to the test. The current use of AI tools can enable businesses to build their own internal systems in some cases, thus eliminating the necessity to rely on external SaaS vendors (Khanna et al., 2025; Crawford et al., 2025). The emergence of AI is therefore shifting the power of data ownership and integration, and some of the classic systems with which SaaS incumbents retained their markets (Jacobides, 2022; Bohnsack et al., 2024) are being challenged.

Understanding how AI reshapes the competitive dynamics in the SaaS sector is crucial for identifying new control points and for explaining how incumbents can defend their market positions.

Firms in this industry operate in a complex digital ecosystem involving several actors that work together and compete to create value. Adner (2017) termed this interdependent market structure as "ecosystem-as-structure," emphasizing how firms organize interdependencies to achieve collective results. In the SaaS context, firms operate within networks of cloud service providers, application developers, integrators, and enterprise users, whose interactions shape competitive positioning and value creation. Rather than relying solely on internal resources, firms' performance increasingly depends on how they position themselves relative to other actors and manage dependencies across these relationships (Jacobides, 2022). From a control points perspective, these interdependencies are relevant because they influence which actors hold control over resource flows and value distribution. The adoption of AI increases the complexity of these relationships even further. Jacobides et al. (2021) describe how AI has introduced additional actors, including data platform owners, AI model developers, and infrastructure providers, whose control over critical technological inputs (e.g., data, models, and computing capacity) has become

increasingly important, reshaping competitive dynamics and redistributing influence among firms. Consistent with this view, Elaluf-Calderwood et al. (2011) highlight that control in digital settings frequently arises through the design and governance of technical standards and interfaces. These technical and institutional mechanisms increasingly shape companies' ability to maintain or contest control points, influencing which firms strengthen their position and which ones lose their authority in the SaaS industry as AI adoption grows.

Although research into the impact of AI on changes in power relationships within the SaaS industry is limited, existing academic literature increasingly examines how firms interact in complex and interdependent digital ecosystems. Most studies emphasize coordinated relationships between firms, yet pay less attention to competition for control and the mechanisms through which power and value capture are structured (Jacobides, 2022). The emergence of AI as a focal point in software delivery has made the distribution of control and value capture among firms a key issue for explaining the future competitive dynamics of the SaaS industry.

2.2. Control Points Theory and Their Application in SaaS Ecosystems

Control Points Theory explains how companies create and capture value by establishing power and competitive advantage within digital business ecosystems (DBEs). A control point is a position that can be defined as technical or strategic (Bohnsack et al., 2024), and which enables a firm to direct the flow of resources, standards, and interactions between actors within an ecosystem (Pagani, 2013). Technical control points are associated with the capability of a firm to facilitate value creation through the use of digital infrastructure, information control, or modular technological solutions. Conversely, strategic control points are associated with the ability of a firm to generate value by using institutional, relational, and organizational processes, including access to customers, brand reputation, or ecosystem orchestration (van Dyck et al., 2021; Bohnsack et al., 2024).

These control points in DBEs dictate the positioning of companies and the extent to which other actors are dependent on a company. Technical control points are frequently the result of digital infrastructure or other unique data assets, or scalable platforms that lead to lower costs of distribution and transaction between network participants (Pagani, 2013). Companies controlling

the technological infrastructure, including APIs, cloud systems, or other interoperability standards, enjoy a pivotal position since other stakeholders have to interact with their systems to be productive (Bohnsack et al., 2024). Meanwhile, strategic control points emerge when firms leverage capabilities such as networking and orchestration to coordinate various modules or value chains across the ecosystem. These control points enable firms to gain favorable positioning through relational power and coordination capabilities (Pagani, 2013). Additional sources of strategic control include brand strength, R&D expertise, and access to financial resources, all of which enhance a firm's long-term competitive influence (Bohnsack et al., 2024; van Dyck et al., 2021).

These control points have historically formed the basis for dominance by the incumbents in the SaaS industry. SaaS vendors like Salesforce, Adobe, and ServiceNow used technical control points in the form of proprietary platforms, integration frameworks, and a monopoly of access to customer data in the past. These systems developed lock-in effects that ensured that clients were unable to switch to competitors, and this strengthened their vendor power (Opara-Martins et al., 2017). The subscription-based model also acted as a strategic control point, creating recurring revenue streams and building strong customer relationships on a long-term basis. Pricing mechanisms (such as tiered or usage-based pricing) have also functioned as mechanisms of control, allowing firms to strike a balance between profitability and customer retention (Li & Kumar, 2022).

In addition, coordination and innovation have also been used by SaaS incumbents as strategic tools. By establishing interdependencies with developers, integrators, and enterprise clients, firms increased their centrality within these arrangements. This orchestration was the role that enabled them to control the course of innovation and compatibility of the complementary technologies within the ecosystem (Adner, 2017). Control points, therefore, played the role of not only supporting the expansion of these arrangements but also acted as deterrents to potential entrants (Bohnsack et al., 2024).

Nevertheless, as artificial intelligence and other sophisticated digital capabilities reshape the industry, these traditional control mechanisms are being reconfigured. The availability of power is no longer in the hands of application-layer providers but in the hands of the individuals controlling the data, algorithms, and the computational infrastructure that AI systems are built on (Jacobides et al., 2021). As such, the historical SaaS control points of platform ownership, integration, and customer data control are becoming less viable as companies engage more in open

and AI-driven digital environments. To comprehend this change, it is necessary to look at how the new AI technologies are redistributing technical and strategic control, which sets the stage for the next section's analysis of AI as a disruptive technology in the SaaS ecosystem.

2.3. AI as a Disruptor Shaping Control Points in SaaS

The competitive and structural bases of the SaaS industry are being redefined by AI (Khanna et al., 2025). The integration of AI into SaaS solutions enables automation, predictive analytics, and data-driven decision-making, allowing more accurate and informed value creation and capture. Khanna et al. (2025) argue that AI compels software vendors to change the structure of their businesses to stay competitive during the AI era. AI-driven applications now enable businesses to tailor services, streamline processes, and even develop their own intelligent applications within the company. This development threatens to weaken the control points (e.g., proprietary technology, data, etc.) through which SaaS incumbents previously dominated their markets. Ebert et al. (2025) show that the introduction of AI into cloud and SaaS architectures lowers the barriers between service providers and customers, and enables broader access to data-driven intelligence. As a result, users are increasingly shifting from consuming solutions to becoming active creators of digital solutions, which decreases the influence of vendors and intensifies competition in the market. This shift in user roles changes where control is exercised in the market, since value creation becomes less centralized around vendors and more distributed across digital platforms and user-driven activities.

The integration of AI into digital platforms has created new control points and weakened some conventional ones. Pagani (2013) defined control points as strategic spots where the companies create and capture value. In the AI era, control is increasingly breaking out of the application layer and is getting more and more distributed to those handling data, models, and computing infrastructure (Jacobides et al., 2021; Khanna et al., 2025; Crawford et al., 2025). Jacobides et al. (2021) note that the emergence of ecosystems in which AI is widely implemented has been accompanied by new complementors like data owners, developers of AI models, and cloud infrastructure providers. Ramamoorthi (2023) also emphasized that AI within cloud computing concentrates power in the hands of infrastructure providers that possess the computing power required to train and deploy the AI models. These providers now exert significant influence

over SaaS firms, which depend on their platforms to deliver services. Similarly, Lins et al. (2021) explain that the emergence of Artificial-Intelligence-as-a-Service (AIaaS) as an accessible cloud-based model allows organizations - including small firms - to access and deploy AI capabilities, although at the cost of increased dependence on the infrastructures of major technology vendors like Amazon, Microsoft, and Google.

Value creation processes in SaaS ecosystems are also changing with AI. Lee et al. (2022) have discovered that effective adoption of AI requires investments in research, talent, and data information that are complementary to each other. Companies that do not invest in these measures will lose ground to their rivals, who will utilize data more efficiently. Sullivan and Fosso Wamba (2024) concur, positing that AI reinforces flexibility and innovation and assists companies in adapting rapidly to changes in the market. Nevertheless, with the increased prevalence of AI-based automation, the differentiation, founded only on service delivery, may be harder to sustain. According to Crawford et al. (2025), AI leaders are increasing their competitive advantage through integrating smart agents (autonomous AI systems that perceive the surrounding world, learn through interactions, and proactively act without clear human instructions at varying levels of software), to grant them the ability to act adaptively and learn independently. Crawford et al. (2025) also warn that agentic AI may transform the experience of users within SaaS platforms by mediating access via such smart agents. Instead of entirely bypassing SaaS systems, these agents, such as the OpenAI GPT-5 Actions agent or Microsoft Copilot, can log into an application such as Salesforce or Notion and access data and perform actions on behalf of users, effectively serving as an intermediary that changes, but does not replace, the traditional SaaS interface model. Such a view is furthermore endorsed by research in the industry: Deloitte (2025) notes that the use of AI cases that support the core value proposition of a firm is a critical step in protecting competitive advantage in the SaaS market. The appropriate AI applications used by incumbents can help them remain profitable even in the face of increasing AI-driven competition by choosing AI applications that help achieve differentiation, efficiency, or customer engagement. According to the World Economic Forum and Capgemini (2024), the alteration of value distribution in industries through the creation of autonomous AI agents is shifting towards the decentralization of systems that are no longer connected to centralized SaaS providers. Wiesinger et al. (2024) highlight how intelligent agents can perform tasks and interact with external systems independently, expanding the reach of AI models beyond static uses. This increasing autonomy suggests that a competitive edge may

depend more on managing data, models, and algorithms than on traditional application-layer functions. These considerations do not only apply to large, established companies either. Clements (2025) argues that AI provides both opportunity and disruption for startups and SMEs as well, since smaller companies can use AI to disrupt incumbents by providing quicker innovation and reduced barriers to entry.

2.4. Incumbent Responses: AIaaS and AI + SaaS Integration

With the SaaS industry changing under the influence of AI, market leaders find themselves implementing new measures to safeguard their market status. One of the key strategies is the adoption of the Artificial-Intelligence-as-a-Service (AIaaS) model. Lins et al. (2021) define AIaaS as the provision of AI-related capabilities (automation, data analytics, and machine learning) through cloud-based infrastructures. This model enables organizations, including SaaS providers, to integrate these functionalities into their services without developing in-house AI systems. Ebert et al. (2025) note that AIaaS enables incumbents to retain strategic control by integrating AI functions into their ecosystems and introducing new revenue streams. By owning APIs, training models, and data pipelines, companies such as Amazon and Microsoft establish new control points that help them avoid erosion by their competitors (Ramamoorthi, 2023).

The other strategy employed by incumbents is to incorporate AI directly into existing SaaS applications, creating AI + SaaS models. According to Khanna et al. (2025), this hybrid model will transform conventional software into adaptable tools that can learn from their interaction with users and gain new insights. This, in turn, brings about personalization and improved performance, which enables firms to retain customers and continue with long-term contracts. Sullivan and Fosso Wamba (2024) add to this by showing that embedded AI promotes agility and innovation, which makes companies more receptive to market changes. Another finding, underlined by Crawford (2025), is that the introduction of AI in all layers of software allows incumbents to increase their competitive edge by automating decision-making and enhancing customer deliverables.

In order to maintain such changes, incumbents are therefore deepening their collaboration with AI developers and infrastructure providers. According to Deloitte (2025) and the World Economic Forum and Capgemini (2024), collaborative efforts such as these will enable firms to scale AI solutions quickly and to regulate autonomous systems. However, this also increases reliance on the major AI platforms (Clements, 2025). Thus, whereas AIaaS and AI + SaaS

approaches can assist incumbents to be more competitive, it is also an indicator of a change in the direction of a more distributed pattern of control in AI-enabled SaaS ecosystems. The creation of value and power is shifting towards infrastructure providers, data owners, and developers of AI models, making the centralized control of power formerly enjoyed by traditional SaaS vendors less significant (Lins et al., 2021).

3. Methodology

To examine how artificial intelligence (AI) is reshaping control points in the Software-as-a-Service (SaaS) industry, this study follows a qualitative, inductive, interpretive approach based on the Gioia methodology (Gioia et al., 2012; 2020). Since the phenomenon under study is relatively recent and still emerging, its strategic implications for SaaS remain theoretically underdeveloped. It is therefore necessary to adopt an inductive approach to get new insights based on the lived experiences and perceptions of industry professionals. Rather than seeking to generate an entirely new theory, this research aims to elaborate and refine Control Points Theory by examining how AI capabilities are interpreted, implemented, and governed by SaaS industry actors. The Gioia methodology offers a systematic approach to building theory inductively by starting with participants' own words and perspectives, which are coded as first-order concepts. These are then iteratively grouped into broader second-order themes and overall dimensions, allowing theoretical insights to emerge directly from the data with increased transparency and rigor. This leads to the identification of recurring patterns. This study adopts an approach based on Gioia principles to illustrate how established control points are being challenged, and which ones could be emerging under these new AI-driven conditions. Moreover, this methodology defines actors in organizations as "knowledgeable agents" (Gioia et al., 2012) capable of articulating complicated strategic dynamics, thereby emphasizing the suitability of this methodology for the research context.

3.1. Research Design

This study consists of ten semi-structured interviews with professionals working in the enterprise software ecosystem. The chosen sample size reflects the exploratory nature of the study and the emerging, highly dynamic character of the phenomenon under investigation. Given that

AI's impact on control points in the SaaS industry is driven by recent technology that is rapidly evolving, this research prioritizes depth of insight over breadth. This approach is consistent with inductive-theory building, which favors rich and detailed perspectives from expert informants rather than large samples (Gioia et al., 2020; Eisenhardt, 1989).

The study combines two distinct groups of informants with complementary perspectives.

First, five interviews were conducted with consultants working closely with SaaS providers and enterprise clients. The informants were selected deliberately, given their exposure to AI adoption across different organizations and industries. They are particularly valuable for this research, since they can compare strategic responses and challenges across firms rather than in a single organizational context.

Second, five interviews were conducted with professionals working in firms, including SaaS incumbents and firms developing internal AI-enabled solutions. These interviews offer a deeper understanding of organizational decision-making, dependency relationships, and practical responses to AI adoption from the company's viewpoint.

These perspectives are crucial for the study, since they capture both those being challenged and those challenging them, from a Control Points Theory perspective.

Semi-structured interviews align with the Gioia methodology because they guarantee comparability while keeping enough openness to allow for the emergence of unforeseen themes, which is essential for inductive theory building (Gioia et al., 2020; Eisenhardt, 1989). The interview questions focus on the following topics: context of the informant's firm, the traditional SaaS model, the firm's AI adoption and integration, changing control points and power shifts in the industry, strategic responses, and the future outlook of the sector. This structure ensures that it captures the informant's perspective at multiple levels - firm, industry, and strategic – helping build a clear understanding of how AI may be reshaping control points in the SaaS sector. Each interview lasted approximately 45 minutes. This extended duration allowed for in-depth discussion of these complex topics.

3.2. Sampling Strategy

I adopted a snowball sampling approach in this study due to the specialized nature of the topic and the difficulty in finding informants with direct and in-depth experience of the SaaS landscape in the AI context. Starting with initial contacts derived from the author's professional

network as well as LinkedIn searches, each participant was asked to recommend additional informants who would fit the purpose of the study.

Since the study is exploratory in nature, the objective was to collect varied, informed viewpoints on this emerging phenomenon from players occupying different positions within the ecosystem rather than to achieve numerical saturation.

Snowball sampling is an advantageous approach for the study, since it provides access to professionals across different organizational settings - from established incumbents to smaller firms, that could be building internal solutions or not – which increases sample diversity. Also, it leverages participants' knowledge and professional networks to identify other possible informants who could have relevant experience for the study, thus increasing its relevance.

3.3. Data Analysis

The analysis of the data from the interviews proceeded in three stages that followed Gioia-inspired (Gioia et al., 2012, 2020) principles. Throughout the analytical process, the large language model (LLM) ChatGPT 5.2 was used as a computational aid to support pattern recognition and thematic organization, while all interpretive decisions and final analytical judgements remained with the author.

First, the interview transcripts were read by the author, and then coded using informant-centric first-order codes, preserving informants' own language and interpretations. An AI-assisted coding approach was adopted to generate initial code suggestions using ChatGPT, which functioned as a computational aid comparable to traditional qualitative data analysis software. These codes were then manually cross-checked against the transcripts, refined, and consolidated. Codes were retained, modified, or rejected based on whether they (a) accurately reflected informant statements, (b) preserved informant-centric language, and (c) avoided semantic overlap with other codes. This resulted in thirty first-order codes that matched the language and perspectives of the interviewees verbatum.

Second, the first-order codes were examined in order to find how they related to each other and look for recurring patterns. Following this, potential groupings were identified with the computational assistance of ChatGPT, and codes that were conceptually identical were grouped into seven second-order themes informed by Control Points Theory. This analysis prioritized coherence and relevance, rather than maximizing the number of themes.

Lastly, the second-order themes were consolidated into three aggregate dimensions: (1) Contestation of Application-Layer Control, (2) Institutional and Economic Reinforcement, and (3) Infrastructure Reconfiguration and Strategic Adaptation. These dimensions represent the main patterns through which AI is reshaping control points in the SaaS industry. This was done with LLM assistance by considering the data and the emergent themes identified in the analysis, and evaluating potential theoretical aggregations.

It is essential to acknowledge that the author thoroughly reviewed the themes and dimensions manually against the research questions, theoretical framework, and supporting evidence across informants, guaranteeing control and accuracy at every stage of the process.

This three-stage analytical process ensured a systematic approach to the analysis of the data, allowing empirical patterns to emerge while preserving the informants' perspectives. This was crucial to obtain reliable insights about the research topic.

In line with the Gioia methodology, the complete data structure is presented in Figure 1 below.

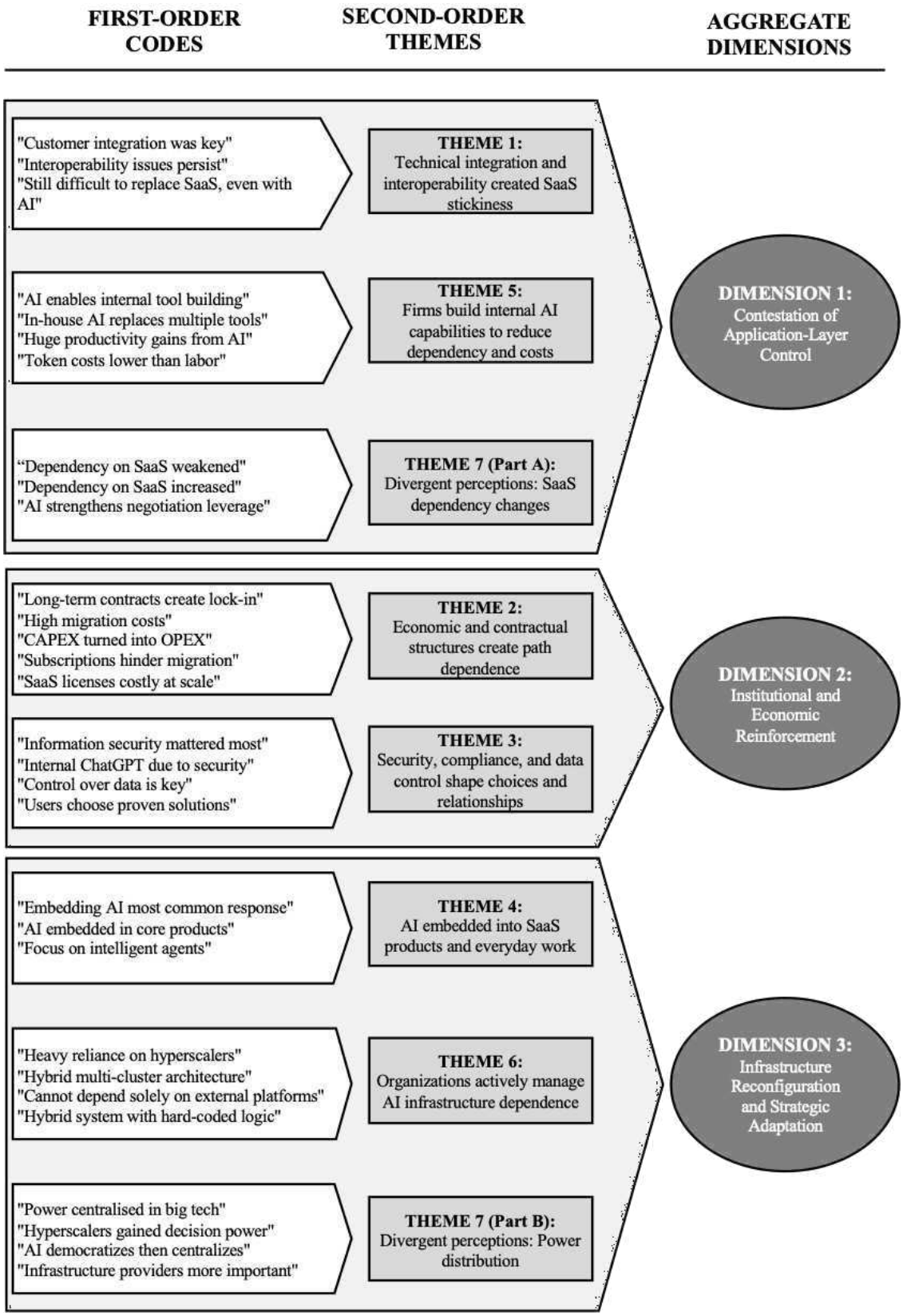

Figure 1 - Data Structure Following the Gioia Methodology

4. Findings

4.1. Contestation of Application-Layer Control

The first dimension reveals a core tension in how AI affects traditional SaaS dependencies. While technical integration and interoperability created strong vendor lock-in mechanisms in the past, AI now provides organizations with the tools to build internal alternatives. This idea emerged from three themes: how technical integration and interoperability created SaaS stickiness (Theme 1), how firms are building internal AI capabilities to reduce dependency and costs (Theme 5), and divergent perceptions about changing SaaS dependency (Theme 7A).

Informants consistently described the historical strength of application-layer control. One of them said that "customer integration was key", highlighting its importance. The barriers were both technical and organizational, with informants reporting that they can't just pull out one system and drop in another, because there are dependencies, data formats, and APIs that all need to work together. These integration challenges, combined with proprietary data models and standardized industry solutions, created significant switching costs that reinforced vendor power.

AI's potential to challenge this dynamic is what makes it important. Multiple informants described how organizations are now building internal tools that are able to substitute functionalities that were previously provided as SaaS. Many informants reported that they are seeing companies build their own AI agents to automate tasks they used to pay SaaS vendors for. Additionally, AI-enabled solutions lead to "huge productivity gains", as mentioned by some informants.

From a cost-benefit perspective, there is a strong incentive for firms to develop their own solutions instead of relying on these vendors. Two informants from SaaS incumbents also mentioned that, in their companies, they built their own AI mostly to automate analysis, while emphasizing that "token costs are lower than labor costs".

Beyond cost savings, internal development also offers customization advantages that challenge SaaS vendors' technical control points. Traditionally, vendors maintained control through proprietary platforms and data models that required customers to adapt their processes to standardized solutions. By building internally, companies can tailor the solution exactly to their processes. Several informants pointed to their domain knowledge as enabling them to create tools that fit their specific workflows and business logic more precisely than standardized external

solutions. By doing this, it weakens the technical control point based on platform architecture and proprietary integration, reducing firms' dependency on vendor-controlled technical infrastructure.

However, this contestation of application-layer control points is far from universal because digital maturity varies a lot across organizations, and so, many of them still lack the technical resources that are needed for the internal development of solutions. A Head of Operations of a SaaS firm explained that digital maturity is uneven across teams and organizations, so for smaller or less technical firms, SaaS is still unavoidable. For these organizations, vendors' technical control points remain effective because they cannot leverage AI to reduce dependency since they lack resources. Even organizations with stronger technical capabilities tend to remain selective about building internally. An informant from a SaaS firm also said: "Companies buy what adds no value building internally." This strategic selectivity means SaaS vendors can maintain technical control points in non-core domains even when technical contestation is possible. The vulnerability of the technical control points is therefore capability-contingent and domain-specific rather than universal.

4.2. Institutional and Economic Reinforcement

Although AI allows firms to technically challenge application-layer control, non-technical forms of control continue to persist and may even be reinforced. This is the key insight provided by this dimension, which arose from the following two themes: how economic and contractual structures create path dependencies (Theme 2) and how security, compliance, and data control shape choices and relationships (Theme 3).

The subscription model that was adopted by SaaS vendors in the first place became a form of lock-in. This model made SaaS accessible and, as more than one informant, including a Ceo of a SaaS company and a consultant with multi-industry knowledge said, "CapEx turned into OpEx" – meaning companies no longer needed to make large upfront capital investments in software and infrastructure but could instead pay ongoing operational costs - allowing companies to predict their costs. This predictability is valuable and makes it less attractive for firms to switch solutions, even when alternatives exist. This idea was supported by many informants. As one said: "subscriptions hinder migration".

Many SaaS solutions are provided through contracts, which further establish these relationships by, in many cases, contractually binding both entities. The head of the consulting business unit from a multinational company mentioned: "long-term contracts create lock-in".

Institutional boundaries are also important to consider. Security and compliance act as institutional constraints that shape technology choices and vendor relationships in the SaaS ecosystem. Some informants mentioned that “information security mattered most” when choosing a service provider. This is even more important for companies that have access to clients’ sensitive data, so “users choose proven solutions”, as one informant said. These institutional boundaries moderate value creation and capture potential by limiting vendor choice and creating dependencies on trusted providers.

With AI adoption, data governance concerns have intensified rather than diminished. “Control over data is key”, one informant emphasized. When companies use AI services, they are giving external platforms access to sensitive data, which is raising concerns about data ownership and protection. Two informants from SaaS firms mentioned that they use an “internal ChatGPT due to security”, meaning that they use an adapted version of OpenAI’s LLM to protect their internal data and their clients’ data. This is done by using a “wrapper” between the model and the data. Similar to how Bohnsack et al. (2024) identify institutional boundaries such as market design and state intervention as external conditions shaping control point dynamics, security and compliance requirements function as institutional boundaries that influence strategic positioning in the SaaS ecosystem in the AI era. This means that organizations are even more cautious about vendor relationships when AI is involved, usually favoring trusted providers with strong data protection practices.

These economic and institutional constraints explain why many informants reported that AI has not fundamentally altered their SaaS dependency. If anything, it may strengthen rather than weaken these strategic control points.

4.3. Infrastructure Reconfiguration and Strategic Adaptation

The third dimension reveals a reconfiguration of where control resides within the technology stack. In this AI era, power is being redistributed across different actors: control is shifting upwards toward infrastructure providers who supply foundational capabilities, while SaaS vendors are responding by embedding AI into their offerings to sustain their position in the market, and organizations are actively managing their dependencies through architectural choices. This dimension emerged from the following three themes: how AI is embedded into SaaS products and

everyday work (Theme 4), how organizations actively manage AI infrastructure dependence (Theme 6), and divergent perceptions about power distribution (Theme 7B).

The most common pattern found in the data is acknowledged dependence on infrastructure providers, particularly hyperscalers like AWS, Azure, and Google Cloud, as well as major large language model (LLM) providers like OpenAI and Microsoft. “There is a heavy reliance on hyperscalers”, as one consultant stated.

This dependency is not only operational but also strategic. Infrastructure providers influence architectural decisions, technology choices, and product roadmaps in ways that were less evident in the pre-AI era. One consultant with cross-industry experience mentioned that “hyperscalers have gained decision power”. The concentration of compute resources, model access, and orchestration capabilities at the infrastructure layer creates new control points that did not exist when software was primarily about application logic. Specifically, informants identified three key infrastructure-layer technical control points. First, control over foundational models emerged as critical, with multiple informants noting their dependency on accessing LLMs that they cannot feasibly develop internally. The main reasons mentioned were the lack of resources and not having enough capital for such a big investment. Second, compute infrastructure became a technical control point, since AI workloads require significant processing power that only hyperscalers can provide at scale. As mentioned before, one informant noted that “hyperscalers have gained decision power”, mentioning also that “there is a heavy reliance on hyperscalers”. Third, orchestration capabilities – the platforms and APIs that enable organizations to integrate LLMs with their data and applications – emerged as technical control points. Informants often described their dependency on APIs provided by firms such as OpenAI and AWS to connect LLMs to their systems and coordinate AI services.

SaaS incumbents are responding to this shift by embedding AI capabilities directly into their products. Many informants described this as the dominant strategy adopted by SaaS vendors. Some examples are chatbots for customer service, agents for automation, and AI-powered analytics. By embedding AI, SaaS vendors act as intermediaries between their customers and the underlying infrastructure providers, maintaining their position in the value chain.

To manage these new dependencies, many organizations are adopting hybrid architectures designed to manage infrastructure exposure. A CEO of a SaaS firm stated: “We use hybrid multi-cluster architecture to avoid dependence on a single provider.” Others use technical approaches to

limit their reliance on models: “We use hybrid systems with hard-coded logic for critical business rules. We avoid reliance on LLM accuracy”. These strategies reflect an awareness that infrastructure dependencies create new vulnerabilities.

Informants tended to diverge a lot on the broader implications of these shifts for power distribution. Some believe that AI democratizes software creation by lowering barriers, while others state that it is centralizing the power in the big tech companies controlling infrastructure and models. Some informants had a mix of both perspectives, explaining that “AI democratizes then centralizes”, meaning that initially barriers drop, but eventually power becomes centralized in the companies mentioned before (hyperscalers).

This dimension reveals a reconfiguration of how control is being distributed and contested.

5. Discussion

This research aims to understand how enterprise adoption of AI capabilities challenges traditional SaaS control points, what strategies SaaS incumbents pursue in response, and whether AIaaS and AI+SaaS offerings can effectively defend incumbent positions.

The analysis revealed three aggregate dimensions that demonstrated that AI is neither eliminating traditional control points nor leaving the competitive landscape unchanged. Instead, AI is redistributing control across multiple layers, weakening some technical control points, reinforcing some strategic ones, and creating new technical control points at the infrastructure layer. The first dimension shows that AI enables capability-contingent contestation of application-layer technical control points. The second one indicates that strategic control points rooted in economic and institutional mechanisms (e.g., subscription model, security requirements) tend to persist independently of technical disruption. The third dimension demonstrates that control is migrating toward infrastructure providers while SaaS vendors adapt through embedding strategies. Together, these findings extend Control Points Theory by demonstrating that AI does not lead to an inevitable power shift but creates conditional, multi-layered control that different actors can contest.

5.1. Theoretical Contributions to Control Points Theory

This research makes three primary theoretical contributions to Control Points Theory and the broader literature on SaaS ecosystems. First, it demonstrates that different types of control points respond differently to AI disruption, showing that technical control points can be contested by capable organizations, while strategic control points tend to persist and may even strengthen. Second, this study shows how control migrates across layers of the AI-enabled SaaS ecosystem. Third, it demonstrates how security and compliance requirements reinforce strategic control points, enabling incumbents to defend their positions.

The first contribution addresses the first research question ("How does enterprise adoption of AI capabilities challenge traditional SaaS control points?") by showing that AI's challenge to traditional SaaS control points is fundamentally heterogeneous between different types of control points. While Pagani (2013) defined control points as positions of influence where firms can shape interactions and capture value within digital ecosystems, and Bohnsack et al. (2024) distinguished between technical and strategic control points, this study extends this framework by demonstrating that these two types exhibit different vulnerability profiles when confronted with AI disruption. The first dimension ("Contestation of Application-Layer Control") reveals that technical control points at the application layer (proprietary platforms, integration frameworks, and data models) face contestation from firms developing internal solutions powered by AI. However, as mentioned before, this contestation is capability-contingent, since only organizations with sufficient digital maturity, technical resources, and domain knowledge can leverage AI to reduce their dependency on SaaS vendors. This finding refines Control Points Theory by showing that the contestability of technical control points depends on firm-level capabilities rather than occurring uniformly across firms. Rather than reflecting a general effect, this pattern highlights a heterogeneity mechanism in how AI reshapes control. Identical AI capabilities can lead to different outcomes in terms of dependency and bargaining power because they are embedded within distinct organizational contexts. Prior research has shown that the value generated by AI depends on how it is configured, integrated, and operationalized within firms, rather than on access to the technology alone (Kemp, 2023). Extending this insight to a control points perspective, the findings show that AI-driven capabilities interact with existing technical and institutional control points in different ways, producing uneven effects on value capture and control across firms.

The second dimension ("Institutional and Economic Reinforcement") demonstrates that strategic control points – contracts, compliance certifications, customer relationships, and brand reputation – persist independently of technical disruption. Informants consistently reported that, even though AI enabled firms to develop alternative solutions, economic lock-in through subscription models, contractual obligations, and switching costs remained effective. Moreover, institutional boundaries such as security requirements, compliance frameworks, and data governance concerns intensified with AI adoption. These findings address the first research question by showing how AI challenges both technical and strategic control points differently. While Bohnsack et al. (2024) distinguish between technical and strategic control points, they offer limited insight into how these types of control points respond in distinct ways to rapid technological change, such as that resulting from AI adoption. This research demonstrates that SaaS strategic control points tend to be less directly affected by technological disruption, since they function through institutional and economic mechanisms that AI capabilities cannot directly undermine, at least at the present time and in the near future. As mentioned before, strategic control points may strengthen as AI adoption intensifies data governance concerns and security requirements, creating higher barriers for new entrants who lack established compliance certifications and institutional trust. This implies that Control Points Theory must account for multi-dimensional control structures in which technical and strategic control points respond differently to disruption.

The second contribution reveals how new control points are emerging at different layers of the technology stack. The third dimension ("Infrastructure Reconfiguration and Strategic Adaptation") demonstrates that AI drives migration of control from the application layer to the infrastructure layer through three new technical control points: access to foundational models, compute infrastructure, and orchestration capabilities (e.g., APIs and platforms enabling integration). This is illustrated in Figure 2 below.

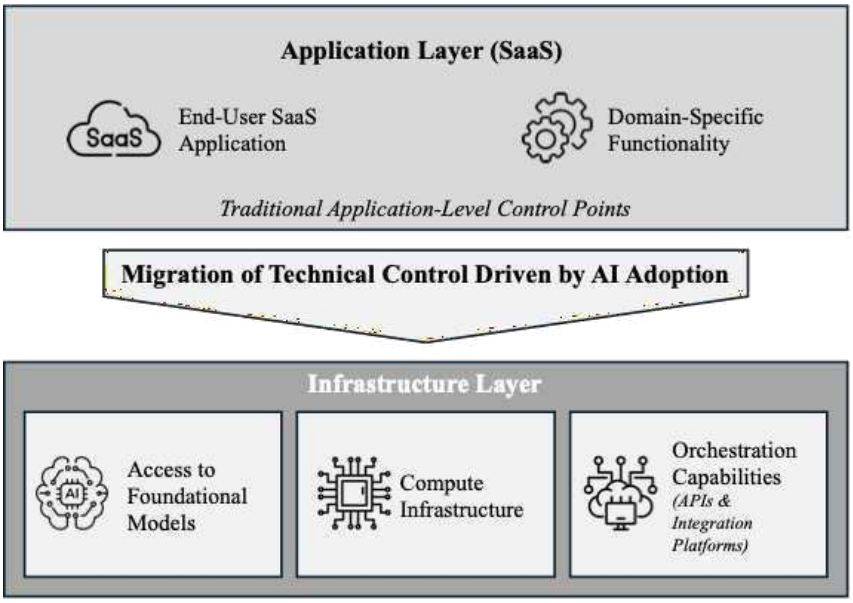

Figure 2 - Technical Control Migration

This builds on Jacobides et al. (2021), who described how AI-driven ecosystems consist of multiple, interdependent, and specialized actors, by showing how infrastructure providers such as AWS, Azure, Google Cloud, and OpenAI establish technical control points within these ecosystems. These control points arise from their governance of critical AI-enabling resources that are essential for delivering AI-enabled services and difficult for application-layer providers, including SaaS vendors, to reproduce independently.

This research demonstrates that as these technologies evolve, control becomes concentrated at the infrastructure layer, where resources are limited and hard to replicate. Consequently, application-layer providers, including SaaS vendors, function as intermediaries that depend on infrastructure providers for critical resources while preserving customer relationships. This directly answers the second research question ("What strategies are SaaS incumbents pursuing to maintain or reconfigure their market positions in response to enterprise AI adoption?"). SaaS vendors respond to the increasing control concentration at the infrastructure-layer by embedding AI capabilities into their products (AI+SaaS strategy), positioning themselves as intermediaries that simplify infrastructure access, tailor their solutions to specific domains, and maintain customer relationships.

The findings of this study suggest that SaaS providers must combine embedded AI capabilities with strategic control points such as compliance and customer trust to defend their position in the market. This reveals a pattern of control point reconfiguration.

The third contribution addresses how institutional boundaries shape control point effectiveness. Bohnsack et al. (2024) conceptualize institutional boundaries as external conditions that condition control point dynamics, and this research extends this by demonstrating how they operate in practice, and particularly within an AI-driven environment. The second dimension ("Institutional and Economic Reinforcement") demonstrates that security requirements, compliance, and data governance concerns function as institutional boundaries that reinforce strategic control points. Firms cannot focus on simply choosing the most cost-effective or technically superior solution— they need to keep these constraints in consideration, limiting their vendor options. Regulations such as the GDPR (General Data Protection Regulation), alongside newer initiatives like the EU AI Act, introduce obligations related to risk management, transparency, and auditability, which increase the importance of established compliance capabilities in vendor selection (IAPP, 2024; Centre for Information Policy Leadership [CIPL], 2024). According to this, SaaS firms that possess relevant compliance certifications (e.g., GDPR-aligned data protection frameworks, or sector-specific certifications in regulated industries) or established security track records hold strategic control points that are not easily replicated by new entrants or by companies that try to develop their own internal solutions, as these capabilities depend on long-term investments, audit processes, and accumulated organizational trust rather than purely technical capabilities (Lansing et al., 2019; Lansing & Sunyaev, 2016). These institutional boundaries intensify with AI adoption due to the increasing data governance concerns related to the access that AI systems have to sensitive data (European Commission, 2024 - AI Act).

This addresses the third research question ("Can incumbents defend control points by offering AIaaS or AI+SaaS, and how effective are those strategies as a defence?") by showing why AIaaS and AI+SaaS strategies can be effective defence mechanisms. Incumbents that leverage established compliance infrastructure, relevant security certifications, and trust relationships can defend their positions against other alternatives, because institutional boundaries sustain strategic control points that remain effective regardless of technical disruption. Theoretically, this emphasizes that control in digital ecosystems is also institutionally embedded. Elaluf-Calderwood et al. (2011) show how technical standards shape ecosystem control, and this research demonstrates

that regulatory and compliance frameworks can operate as comparably powerful control mechanisms.

These three contributions collectively answer the three research questions.

5.2. Implications for Practice

The theoretical contributions made by this research translate into concrete implications for the different actors within the SaaS ecosystem that are facing AI-driven transformation.

SaaS incumbents face a dual challenge in which technical control points become increasingly contestable as dependency on infrastructure providers grows. The findings highlight their need to reinforce strategic control points while adapting technical offerings. More specifically, incumbents should prioritize three actions in order to stay relevant in the market. First, firms should reinforce contractual relationships and increase switching costs through economic mechanisms, since subscription-based lock-in shows that pricing models and long-term contracts can sustain defensible positions even when technical control points are contestable. Second, SaaS firms should strongly invest in compliance infrastructure and security certifications. Compared to traditional SaaS, AI-enabled services introduce new requirements related to data governance and security, model transparency, and accountability, turning compliance from a necessity into a strategic control point that favors firms with mature capabilities in these subjects. Third, SaaS vendors should adopt an AI+SaaS embedding strategy, allowing them to maintain a position as an intermediary while adapting to technical disruption. The findings show that firms still value domain-specific customization and easy access to infrastructure, so incumbents can remain relevant in the market and defend their positions by embedding AI capabilities into their solutions. A critical insight is that defensive strategies must combine technical and strategic dimensions, because embedding AI alone is insufficient if strategic control weakens, and maintaining contracts alone is also insufficient if products lack technical relevance, because eventually they will lose them. The most defensible positions arise from hybrid strategies that reinforce strategic control while adapting technical offerings. This has also been the prevalent strategy adopted by incumbents, according to the majority of the informants in this study.

In contrast to what is happening to SaaS incumbents, enterprise customers now face complex build-versus-buy decisions due to AI disruption (Korst et al., 2025). The findings of this study show that organizations should build internally when they present a sufficient level of digital

maturity, enough technical resources, and when the domain knowledge is critical to competitive advantage. This depends on the assumption that the switching costs in these cases are manageable. In contrast, they should buy when they lack capabilities, when the domain is not core to their competitive advantage and do not have enough resources to develop these tools, and when security or compliance requirements make established vendors safer. The key insight is that organizations should manage vendor dependencies deliberately rather than trying to eliminate them by default. The objective is to preserve negotiating leverage and ensure that dependencies support, rather than constrain, strategic priorities.

In addition, infrastructure providers are emerging as dominant actors within the ecosystem with control over compute power, models, and orchestration platforms. They should recognize that their position is conditional on the absence of regulatory intervention and, also, should anticipate scrutiny regarding market concentration, data governance, and competitive fairness. Because of this, policymakers face a tension between supporting AI innovation and preventing excessive concentration at the infrastructure layer (Meyers & Bourreau, 2025; OECD, 2025). The study's findings show that institutional boundaries strongly shape competitive dynamics, so regulators should therefore implement rules that promote competition without slowing innovation. This logic is reflected in the EU Artificial Intelligence Act, which explicitly seeks to balance innovation with safeguards related to market concentration, data governance, and risk management in AI-enabled markets (European Commission, 2024 – AI Act)

The primary practical implication, however, is that control in AI-enabled ecosystems is multi-layered, distributed, and actively contested. For companies to succeed, it requires understanding which control points are vulnerable, which are durable, and which are emerging. This study provides relevant insights that allow actors to make such distinctions, for example, by helping SaaS firms identify when technical control points can be adapted or contested through AI integration, and evaluate if strategic control points should be reinforced. Firms that use this understanding to selectively invest in, defend, or reposition control points will be better positioned as AI continues to reshape digital ecosystems. The findings of this research challenge simplistic narratives that AI will either destroy SaaS incumbents or leave the competitive dynamics unchanged, demonstrating instead how control is being reconfigured in ways that create both threats and opportunities for all actors within SaaS ecosystems.

6. Conclusion

This thesis examined how enterprise adoption of AI capabilities challenges traditional SaaS control points, what strategies incumbents pursue in response, and whether AIaaS and AI+SaaS offerings can effectively defend their positions. Through qualitative analysis of ten semi-structured interviews with industry professionals, this research reveals that AI is neither eliminating traditional control points nor leaving the competitive dynamics unchanged. Instead, AI weakens application-layer technical control points for capable firms, reinforces strategic control points through contracts and compliance, and creates new technical control points at the infrastructure layer where foundational models, compute resources, and orchestration platforms reside.

The study makes three main theoretical contributions to Control Points Theory. First, it demonstrates that technical and strategic control points respond differently to AI disruption. Technical control points at the application layer face capability-contingent contestation, since only organizations with sufficient digital maturity and technical resources can leverage AI to reduce their dependency on SaaS vendors. In contrast, strategic control points that are shaped by contracts, compliance certifications, and institutional trust tend to persist, since these tend to be less directly affected by technological disruption and may even strengthen as AI increases data governance concerns. This extends existing theory by specifying that control points are multi-dimensional and that different types exhibit different vulnerability profiles in response to rapid technological disruption.

In addition, this research reveals how control migrates from the application layer to the infrastructure layer as AI matures. Access to foundational models, compute infrastructure, and orchestration capabilities emerge as three new technical control points at the infrastructure layer. Infrastructure providers possess critical AI-enabling resources that are essential for AI-enabled services. This control reconfiguration transforms SaaS vendors into intermediaries who depend on infrastructure providers while maintaining customer relationships. Notably, this creates a dependency paradox, since both SaaS vendors and companies building internal AI solutions become dependent on the same infrastructure providers, yet SaaS vendors maintain value through their intermediary position by offering domain expertise, simplified access, and established customer relationships. To adapt to this change, incumbents adopt the AI+SaaS strategy as their main strategic response, embedding AI capabilities into their offerings to defend their position in the market. However, this strategy proves effective as a defensive mechanism only when combined

with strategic control points, since technical embedding alone is insufficient without contractual lock-in, compliance infrastructure, and institutional trust.

Finally, the study demonstrates how institutional boundaries, such as security requirements and compliance frameworks, reinforce strategic control points (e.g., compliance certifications, institutional trust), allowing incumbents to defend their positions even when technical alternatives become available.

For practitioners, these findings offer concrete guidance. SaaS incumbents should strengthen strategic control through contractual relationships and compliance infrastructure while embedding AI capabilities into their solutions to maintain technical relevance. Enterprise customers face complex build-versus-buy decisions that depend on organizational capability, domain complexity, and strategic importance. Organizations should manage their vendor dependencies strategically to preserve negotiating leverage, rather than eliminating them. Lastly, infrastructure providers must recognize that their control depends on regulatory tolerance, while policymakers face tensions between enabling innovation and preventing excessive control concentration at the infrastructure layer.

This study has limitations that point to opportunities for future research. The sample size of ten interviews prioritized depth of insight over breadth of coverage. Also, the study captures only a single point in time within a fast-evolving phenomenon. Research tracking control point evolution in the SaaS sector over time would provide valuable insights into how the three dimensions develop as AI capabilities mature. Comparative studies across different SaaS market segments, organizational sizes, and regulatory contexts would test the generalizability of these findings. Furthermore, testing whether these control point dynamics emerge in other AI-disrupted industries (eg., fintech intermediaries, logistics platforms, and healthcare information systems) would determine the generalizability of these findings beyond enterprise software. Additionally, future research could examine how institutional boundaries evolve as AI regulation matures, particularly investigating whether emerging frameworks such as the EU AI Act reshape the effectiveness of compliance-reinforced strategic control points or create new regulatory barriers to entry.

Despite these limitations, this thesis contributes to both theory and practice by demonstrating that AI creates conditional, multi-layered, and contested control structures. By revealing how different types of control points respond differently to disruption, how control migrates across layers, and how institutional boundaries moderate these dynamics, this research

offers empirically grounded insights into how AI-enabled disruption affects the SaaS ecosystem. As AI continues to transform enterprise software, these insights offer guidance for actors navigating this evolving landscape.

References

Adner, R. (2017). Ecosystem as structure: An actionable construct for strategy. Journal of Management, 43(1), 39–58. https://doi.org/10.1177/0149206316678451

Bohnsack, R., Rennings, M., Block, C., & Bröring, S. (2024). Profiting from innovation when digital business ecosystems emerge: A control point perspective. Research Policy, 53, 104961. https://doi.org/10.1016/j.respol.2023.104961

Centre for Information Policy Leadership. (2024). From barriers to bridges: Cloud computing in support of privacy and security. Centre for Information Policy Leadership, Hunton Andrews Kurth LLP.

Chen, H. (2022). An empirical analysis of Software-as-a-Service (SaaS) development mode and firm performance. Technological Forecasting and Social Change, 180, 121700. https://doi.org/10.1016/j.techfore.2022.121700

Clements, H. (2025, February). How AI is affecting SaaS founders. HSBC Innovation Banking. https://www.hsbcinnovationbanking.com/gb/en/resources/how-ai-is-affecting-saas-founders

Crawford, D., McLaughlin, C., Doddapaneni, P., & Fiore, G. (2025). Will agentic AI disrupt SaaS? In Bain Technology Report 2025. Bain & Company. https://www.bain.com/insights/will-agentic-ai-disrupt-saas-technology-report-2025/

Deloitte. (2025). Unlocking the right agentic AI use cases: The business imperative for agentic AI. Deloitte Insights. https://www.deloitte.com/

Ebert, C., Duarte, C., Zeng, X., & Zhao, L. (2025). AI for cloud and SaaS: Technologies and business models. IEEE Software, 42(1), 48–56. https://doi.org/10.1109/MS.2024.3456789

Eisenhardt, K. M. (1989). Building theories from case study research. Academy of Management Review, 14(4), 532–550.

Elaluf-Calderwood, S. M., Sørensen, C., & Maitland, C. (2011). Mobile platforms: The role of boundary objects in control and coordination of an ecosystem. Information Systems Journal, 21(4), 355–380. https://doi.org/10.1111/j.1365-2575.2011.00362.x

European Commission. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union.

Gioia, D. A. (2021). A systematic methodology for doing qualitative research. *The Journal of Applied Behavioral Science, 57*(1), 20–29. https://doi.org/10.1177/0021886320982715

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2012). Seeking qualitative rigor in inductive research: Notes on the Gioia methodology. Organizational Research Methods, 16(1), 15–31. https://doi.org/10.1177/1094428112452151

Guo, X., & Ma, J. (2018). A model of competition between perpetual software and Software-as-a-Service. MIS Quarterly, 42(1), 101–120. https://doi.org/10.25300/MISQ/2018/14071

Hannah, D. P., & Eisenhardt, K. M. (2018). How firms navigate cooperation and competition in nascent ecosystems. Strategic Management Journal, 39(12), 3163–3192. https://doi.org/10.1002/smj.2750

International Association of Privacy Professionals. (2024). EU Data Act: Operational impacts, compliance, and technical considerations of cloud switching. https://iapp.org/news/a/eu-data-act-operational-impacts-compliance-and-technical-considerations-of-cloud-switching

Jacobides, M. G. (2022). How to compete when industries digitize and collide: An ecosystem development framework. California Management Review, 64(3), 99–123. https://doi.org/10.1177/00081256221085023

Jacobides, M. G., Brusoni, S., & Candelon, F. (2021). The evolutionary dynamics of the artificial intelligence ecosystem. Strategy Science, 6(4), 412–435. https://doi.org/10.1287/stsc.2021.0153

Kemp, A. (2023). Competitive advantages through artificial intelligence: Toward a theory of situated AI. Academy of Management Review, 48(2), 302–325. https://doi.org/10.5465/amr.2020.0205

Khanna, M., Mittal, N., Wu, A., & Castillo, M. (2025, September). Upgrading software business models to thrive in the AI era. McKinsey & Company, Technology, Media & Telecommunications Practice. https://www.mckinsey.com/

Korst, J., Puntoni, S., & Tambe, P. (2025). AI adoption in enterprises: Evidence from large-scale survey data. Wharton Human–AI Research Initiative & GBK Collective.

Lee, S., Kim, J., Choi, D., & Kim, Y. (2022). When does AI pay off? AI-adoption intensity, complementary investments, and R&D strategy. Technovation, 118, 102534. https://doi.org/10.1016/j.technovation.2022.102534

Li, X., & Kumar, S. (2022). Managing Software-as-a-Service: Pricing and operations. Production and Operations Management, 31(12), 4663–4681. https://doi.org/10.1111/poms.13800

Lins, S., Schneider, J., Sunyaev, A., & Buxmann, P. (2021). Artificial intelligence as a service: Classification and research directions. Electronic Markets, 31(1), 171–195. https://doi.org/10.1007/s12599-021-00708-w

Lansing, J., & Sunyaev, A. (2016). Trust in cloud computing: Conceptual typology and trust-building antecedents. Journal of Management Information Systems, 33(3), 820–856. https://doi.org/10.1080/07421222.2016.1243943

Lansing, J., Siegfried, N., Sunyaev, A., & Benlian, A. (2019). Strategic signaling through cloud service certifications: Comparing the relative importance of certifications' assurances to companies and consumers. Journal of Strategic Information Systems, 28(4), 101579. https://doi.org/10.1016/j.jsis.2019.101579

McCord, D. (2025, April 8). Build it or buy it: The AI agent SaaS impact. Peterson Technology Partners. https://www.ptechpartners.com/2025/04/08/build-it-or-buy-it-the-ai-agent-saas-impact/

Meyers, Z., & Bourreau, M. (2025). A competition policy for cloud and AI. Centre on Regulation in Europe (CERRE). https://www.cerre.eu

Opara-Martins, J., Sahandi, R., & Tian, F. (2017). A holistic decision framework to avoid vendor lock-in for cloud SaaS migration. Computer and Information Science, 10(3), 29–48. https://doi.org/10.5539/cis.v10n3p29

Organisation for Economic Co-operation and Development. (2025). Competition in artificial intelligence infrastructure (OECD Roundtables on Competition Policy Papers No. 330). OECD Publishing. https://doi.org/10.1787/20758677

Pagani, M. (2013). Digital business strategy and value creation: Framing the dynamic cycle of control points. MIS Quarterly, 37(2), 617–632. https://doi.org/10.25300/MISQ/2013/37.2.13

Ramamoorthi, V. (2023). Applications of AI in cloud computing: Transforming industries and future opportunities. International Journal of Scientific Research in Computer Science,

Engineering and Information Technology, 9(4), 472–483.* https://doi.org/10.32628/CSEIT2394103

Rrucaj, A. (2023). Creating and sustaining competitive advantage in the Software-as-a-Service (SaaS) industry: Best practices for strategic management. University of Ljubljana. https://repozitorij.uni-lj.si/

Sullivan, S., & Fosso Wamba, S. (2024). Artificial intelligence and adaptive response to market changes: A strategy to enhance firm performance and innovation. Journal of Business Research, 174, 114265. https://doi.org/10.1016/j.jbusres.2024.114265

Van Dyck, M., Lüttgens, D., Piller, F., & Diener, K. (2021). Positioning strategies in emerging industrial ecosystems for Industry 4.0: A longitudinal study of platform emergence in the agricultural industry. In Proceedings of the 54th Hawaii International Conference on System Sciences (HICSS) (pp. 6153–6163). University of Hawaii at Manoa. https://hdl.handle.net/10125/71363

Wiesinger, J., Marlow, P., & Vuskovic, V. (2024, September). Agents. Google Cloud White Paper. https://cloud.google.com

World Economic Forum, & Capgemini. (2024). Navigating the AI frontier: A primer on the evolution and impact of AI agents. World Economic Forum. https://www.weforum.org/publications/navigating-the-ai-frontier/