Shadow IT risk analysis in public cloud infrastructure

Yevhenii Martseniuk[1,*,†], Andrii Partyka[1,†], Oleh Harasymchuk[1,†], Elena Nyemkova[1,†] and Mikolaj Karpinski[2,†]

[1] Lviv Polytechnic National University, 12 Stepana Bandery str., 79000 Lviv, Ukraine
[2] University of the National Education Commission, 2 Podchorazych str., 30-084 Krakow, Polska

Abstract

Shadow IT, where IT systems and services are used without explicit approval from an organizational IT department, has risen to be an important issue for cloud computing. Its growth emanates from the growing capabilities and accessibility of cloud services that often circumvent the IT pre-established policies and governance mechanisms. This paper aims to research and investigate the complex nature of Shadow IT within public cloud environments, focusing on the risks it poses, its effects, and the strategies to manage it effectively. These risks are varied and significant, with great concern over data protection and security. Thus, unauthorized use of cloud services exposes organizational data to vulnerabilities. Furthermore, cloud environments could face a situation of policy shadowing in which higher-level policies shadow more granular but potentially conflicting policies, therefore leading to unnoticed security gaps. There are also great threats associated with legal and compliance risks, through which companies might have to incur huge penalties because of unauthorized cloud service usage. This research explains the various types of Shadow IT: from unauthorized software and hardware to unapproved cloud computing services and unsanctioned development activities. Additionally, the paper will detail the major Shadow IT risks related to security, compliance, cost, and interoperability problems. It further deals with strategic management towards the mitigation of risks involved in Shadow IT. More so, it focuses on IT governance models that can cope with the increasing need for control against the pressures for more flexibility and swifter innovation. Such effective strategies include implementing Cloud Access Security Broker (CASB) solutions, adopting secure information-sharing models in public clouds, and the proactive management of usage in clouds. Moreover, the paper shows the potential advantages of Shadow IT in terms of innovation and exploration of real user needs and preferences. By recognizing and exploiting the good sides of Shadow IT, organizations can turn the challenges into opportunities for growing and improving their IT strategies. By doing so, all of these challenges help concretely frame Shadow IT in a way that enables it to be handled with a structured and proactive management strategy to achieve a comprehensive approach to maintaining security, compliance, and operational efficiency. The paper underlines the need for changing IT management practices as per the emerging changes brought in by rapid developments in cloud technology and the ever-changing needs of enterprise IT.

Keywords

shadow IT, public clouds, AWS, cyber security risks, compliance, cloud operations, automation, risk analysis, cloud infrastructure

1. Introduction

Shadow IT, defined as the use of information technology systems, solutions, and services without explicit organizational approval, has become an increasingly critical issue with the advent and widespread adoption of cloud computing. Recent studies have extensively examined the multifaceted risks and challenges associated with Shadow IT, particularly within public cloud environments.

For example, Edwards et al. (2019) [1] highlighted that Shadow IT introduces significant security vulnerabilities due to the lack of oversight and proper security measures. Their study illustrated how unauthorized cloud services could lead to severe data breaches and unauthorized access to sensitive information, posing substantial risks to organizational data integrity and security. Similarly, Akello (2021) [2] explored the volitional non-malicious insider threats associated with Shadow IT, especially in the context of Work-From-Home (WFH) arrangements during the COVID-19 pandemic. This research emphasized the heightened risk of data exposure and security breaches due to the uncontrolled use of cloud-based applications by employees working remotely.

Furthermore, Selvam (2022) [3] discussed the efficacy of Cloud Access Security Broker (CASB) solutions in mitigating Shadow IT risks. The study demonstrated how CASBs could help organizations monitor and control cloud traffic, thereby reducing the unauthorized use of SaaS

CSDP-2024: Cyber Security and Data Protection, June 30, 2024, Lviv, Ukraine
*Corresponding author.
†These authors contributed equally.
yevhenii.v.martseniuk@lpnu.ua (Y. Martseniuk); andrii.i.partyka@lpnu.ua (A. Partyka); garasymchuk@ukr.net (O. Harasymchuk); garasymchuk@ukr.net (E. Nyemkova); garasymchuk@ukr.net (M. Karpinski)

0009-0009-2289-0968 (Y. Martseniuk); 0000-0003-3037-8373 (A. Partyka); 0000-0002-8742-8872 (O. Harasymchuk); 0000-0003-0690-2657 (E. Nyemkova); 0000-0002-8846-332X (M. Karpinski)

applications and managing third-party app permissions. This underscores the need for advanced security solutions to address the unique challenges posed by Shadow IT in cloud environments.

Moreover, Khan, H., Zahoor, E., Akhtar, S., & Perrin, O. (2022) [4] examined the challenges of secure information sharing in public clouds, focusing on community-based secure information sharing models. They argued that while these models could facilitate controlled collaboration and data sharing, they also highlighted the inherent risks of Shadow IT, such as the potential for data leaks and policy conflicts between different cloud services.

Finally, a study by Vakhula, Kurii, and Opirskyy (2024) [5] on security challenges in cloud environments emphasized the importance of adopting a Security-As-Code approach. This research indicated that automated security measures and continuous monitoring could significantly mitigate the risks associated with unauthorized cloud services, thereby enhancing overall cloud security and compliance.

This work aims to explore the complex nature of Shadow IT within public cloud environments, focusing on the risks it poses, the impacts it incurs, and the strategies that can be employed for its effective management. By synthesizing recent literature and proposing comprehensive risk mitigation strategies, this study seeks to provide a robust framework for organizations to manage Shadow IT more effectively, ensuring data protection, security, and compliance in cloud computing.

2. The risks and impacts of shadow IT

2.1. Security risks

Shadow IT, by its very nature, introduces significant security challenges for organizations, as it encompasses the use of IT resources that have not been vetted or approved by the official IT department. These rogue applications and devices may be inherently insecure, potentially packed with malware, or present exploitable vulnerabilities that hackers can leverage to gain unauthorized access. The lack of formal oversight means such devices and software are seldom updated or patched promptly, if at all, leaving them perpetually vulnerable to emerging threats. Furthermore, the improper configuration of shadow IT resources can inadvertently open up additional security loopholes. The ad hoc management of sensitive data within the shadow IT ecosystem also raises serious concerns, as it may not be backed up or stored with the necessary security measures, increasing the risk of data loss or exposure. Lastly, the unchecked use of shadow IT can lead to unmonitored access to critical and confidential company information, significantly elevating the risk profile for data breaches and information theft.

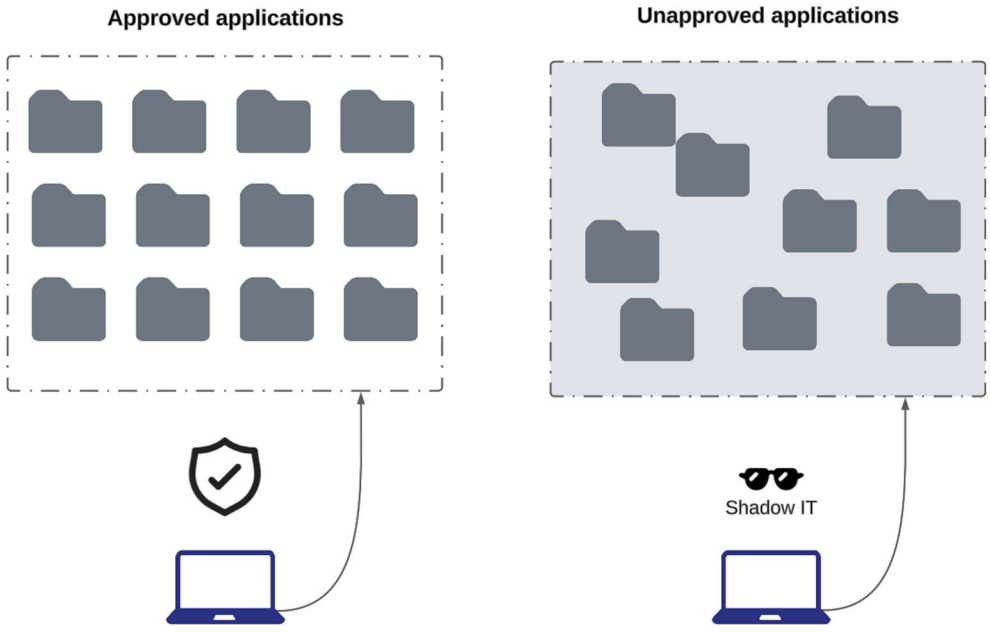

Figure 1: Applications from Shadow IT perspective

Data Protection and Security Risks. The unauthorized adoption of cloud services, a hallmark of Shadow IT, significantly jeopardizes data protection and security. In the realm of cloud computing, where data is often stored off-premises, the lack of oversight on these services can lead to breaches and unauthorized access [6] highlighting how the allure of convenient cloud solutions tempts users to sidestep established IT protocols, thus exposing sensitive data to potential cyber threats. For instance, a multinational corporation recently faced a severe data breach when confidential customer information was leaked through an unapproved cloud storage service. This incident underscores the tangible risks of Shadow IT in compromising data integrity and security.

Policy Shadowing in Cloud Authorization. Another critical risk associated with Shadow IT in cloud environments is policy shadowing. As detailed by Šedivcová, Lada & Potančok, Martin. [7], higher-level cloud

policies may inadvertently obscure or conflict with lower-level security policies, leading to overlooked vulnerabilities. An example of this can be seen in organizations where overarching cloud access policies do not account for the granular permissions required by different user groups, thereby creating security loopholes that can be exploited.

2.2. Compliance risks

The presence of shadow IT in organizations, particularly those operating within tightly regulated fields, poses a significant risk from a compliance standpoint. Auditors tasked with ensuring that organizations adhere to specific regulatory standards may respond unfavorably upon identifying the use of unauthorized IT resources. This adverse reaction is due to the potential for such resources to circumvent established data protection and security protocols, thereby violating compliance requirements.

The financial repercussions for organizations can be severe, with hefty fines imposed as a penalty for the lack of adequate data controls. These fines serve as a tangible reflection of the compliance risks associated with shadow IT, underscoring the necessity for organizations to establish robust governance frameworks to mitigate the risks associated with unauthorized IT assets and ensure regulatory compliance.

Legal Ramifications of Unauthorized Cloud Service Usage. The use of unapproved cloud services in Shadow IT scenarios can lead to serious legal consequences for organizations. As Walterbusch, Fietz, and Teuteberg [8] discuss, many employees engaging in Shadow IT activities are often unaware of the legal implications of using unauthorized cloud services. These can range from breaches of data privacy laws to violations of regulatory compliance standards. For instance, a healthcare provider might unknowingly violate the Health Insurance Portability and Accountability Act (HIPAA) if sensitive patient data is stored or transmitted via an unauthorized cloud service. Such violations can result in substantial fines and damage to the organization's reputation.

Compliance Risks in Shadow IT. Compliance risks in Shadow IT are predominantly related to the failure to meet industry-specific regulations and standards. In sectors like finance or healthcare, where data security and privacy are paramount, the uncontrolled use of cloud services can lead to non-compliance with standards like Sarbanes-Oxley or GDPR. This non-compliance is not merely about facing penalties but also concerns the broader aspect of trust and reliability in the eyes of customers and stakeholders. A notable example includes a financial institution that faced regulatory scrutiny and hefty fines due to its failure to monitor and control Shadow IT practices, leading to non-compliance with financial reporting standards.

Impact on IT Governance. Erosion of Traditional IT Governance Structures. Shadow IT represents a significant challenge to traditional IT governance structures. In an environment where decisions about IT resources and services are increasingly made outside the purview of the IT department, the centralized control and strategic planning of IT resources are undermined. This decentralization not only disrupts the established IT governance framework but also leads to inconsistencies in IT standards and policies across the organization. For instance, different departments might adopt varying cloud services for similar tasks, leading to inefficiencies and difficulties in data integration and management.

Balancing Flexibility and Control. The rise of Shadow IT also highlights the need for IT governance models to evolve, balancing the need for control with the demand for flexibility and rapid innovation. Traditional governance models, often seen as rigid and slow to respond to new technology trends, can drive employees towards Shadow IT as a means to circumvent these limitations. Therefore, IT governance must adapt to provide guidelines that accommodate the rapid adoption of new technologies while maintaining control over security and compliance standards. For example, some organizations are now implementing hybrid governance models that allow for the controlled use of certain cloud services, providing the flexibility that employees need while maintaining oversight [9].

IT Governance as a Strategic Partner. To effectively manage Shadow IT, IT governance needs to transition from being a gatekeeper to a strategic partner. This involves understanding the business needs that drive employees towards Shadow IT and providing solutions that meet these needs within the governance framework. By adopting a more collaborative approach, IT departments can better align their strategies with business objectives, ensuring that technology adoption is both effective and secure. Successful cases have shown that when IT governance is closely integrated with business strategy, it can lead to innovative solutions that enhance productivity without compromising security and compliance.

2.3. Cost risks

The allure of public cloud platforms lies in their ease of access, scalability, and the perception of cost-effectiveness. However, when employees or departments bypass official channels to leverage these services without proper oversight, the organization faces multifaceted financial risks.

Economic Redundancy in Public Cloud Usage. The use of unauthorized public cloud services for functionalities already provided by sanctioned organizational resources epitomizes economic redundancy. Organizations find themselves paying for duplicate services, as official and shadow public cloud instances run in parallel to fulfill the same operational needs. This redundancy not only inflates IT expenditures unnecessarily but also complicates data management and integration processes, leading to inefficiencies that further strain organizational resources.

Hidden Costs and Security Implications. Even free or seemingly low-cost public cloud applications can entail significant hidden costs. Unauthorized use of public cloud services elevates the risk of data breaches, as these platforms might not conform to the organization's security and compliance standards. The consequences of such breaches include not just the direct costs of incident response and data recovery but also longer-term financial liabilities stemming from regulatory fines, legal actions, and reputational damage. The indirect costs associated with the loss of customer trust and potential business disruptions can far exceed any perceived savings from using unsanctioned cloud services.

Duplicitous Spending and Operational Risks. Choosing unauthorized public cloud solutions over approved organizational options leads to duplicative spending on cloud services. This practice not only represents an unnecessary financial outlay but also introduces operational risks. The lack of coordination between shadow and sanctioned IT resources can result in data silos, inconsistent data management practices, and inefficiencies in resource utilization. Additionally, the unmonitored use of public cloud services can lead to compliance gaps, exposing the organization to regulatory scrutiny and potential penalties and expenses arising from their risks, illustrating the financial pitfalls of shadow IT beyond mere duplication of costs [10].

2.4. Interoperability

Interoperability Challenges in Public Cloud Infrastructure: Bridging Shadow IT and Official IT Department Activities. The emergence of shadow IT within an organization, particularly when it involves public cloud services, significantly complicates interoperability between different departments and the official IT department. This complexity arises due to the adoption of various programs and cloud services without a coordinated strategy, leading to a fragmented IT landscape that hampers data cohesion and operational efficiency.

Data Harmonization Challenges. The use of disparate software solutions across departments necessitates additional processes to ensure data harmonization. This involves converting and formatting data into a universally recognized format that can be seamlessly integrated and utilized across the organization. Such efforts require not only technical resources but also time and financial investment, often necessitating the use of specialized data integration tools or platforms.

Cloud Service Fragmentation and Associated Costs. When departments independently select different public cloud services, the organization faces a multi-cloud environment where data resides in siloed ecosystems. Each cloud provider may have its own set of protocols, standards, and services, complicating data interoperability. Moreover, transferring data between these services can incur additional fees, especially if large volumes of data are involved or if frequent data sharing across platforms is necessary. Cloud service providers often charge for egress or API calls, which can accumulate significant costs unbeknownst to the central IT department.

2.5. The silver lining of shadow IT

Embracing Innovation and User-Driven Solutions. Shadow IT is often viewed through a lens of caution due to the potential risks it poses to data security, compliance, and financial management. However, this perspective overlooks the valuable insights and innovative potential that shadow IT activities can bring to an organization. Recognizing and harnessing the positive aspects of shadow IT can transform perceived challenges into opportunities for growth and improvement in IT strategies.

Insight into User Needs and Preferences. One of the most significant benefits of shadow IT is its ability to reveal the genuine needs and preferences of users within an organization. When employees turn to unauthorized tools and services, it often indicates that existing IT solutions do not fully meet their requirements or that there are gaps in the available technology offerings. This direct feedback from the user base provides the IT department with critical insights into where improvements are needed, allowing for more user-centric IT planning and development.

Key Advantage 1: Shadow IT acts as a grassroots feedback mechanism, highlighting the specific needs and workflow preferences of different departments. By analyzing the types of solutions employees seek out on their own, the IT department can better understand the evolving technology needs of the organization and adapt its strategy accordingly.

Collective Problem-Solving and Innovation. Shadow IT represents collective problem-solving in action. Employees engaging in shadow IT are not just bypassing official channels but are actively seeking solutions to their challenges. This proactive approach to problem-solving can lead to the discovery of innovative tools and workflows that the IT department may not have considered. Many successful IT programs and tools used today originated from such grassroots initiatives and were later formally adopted and integrated into the organization's official IT infrastructure.

Key Advantage 2: Embracing shadow IT as a form of collective innovation encourages a culture of creativity and problem-solving within the organization. It acknowledges the valuable contributions employees can make to the IT landscape and leverages their firsthand experience to improve and innovate IT services and solutions [11].

2.6. Strategic approaches to leveraging shadow IT

Formalize a Process for Innovation Submission: Create channels through which employees can propose the tools and solutions they have found useful, allowing the IT department to evaluate and potentially adopt these innovations officially.

Conduct Regular Needs Assessments: Engage with users across the organization to understand their technology needs and frustrations, aiming to reduce the necessity of seeking shadow IT solutions.

Foster a Collaborative IT Culture: Develop an IT department ethos that is seen as approachable and responsive to user needs, encouraging open dialogue about new tools and technologies.

By shifting the narrative around shadow IT from a risk to be mitigated to an opportunity for user-driven innovation, organizations can harness the creativity and ingenuity of their workforce to enhance their IT strategies and solutions.

In conclusion, the pervasive use of Shadow IT within organizations represents a considerable threat to data security, compliance, and overall IT governance. The unauthorized adoption of cloud services, policy shadowing, and inadequate oversight collectively contribute to a heightened risk environment. Traditional IT governance structures must evolve to address the complexities introduced by Shadow IT. As organizations increasingly rely on cloud computing, the need for robust strategies to mitigate these risks becomes imperative.

3. Risk mitigation strategies and reducing shadow IT

Understanding the scope and impact of shadow IT within an organization, particularly in the context of public cloud environments, is crucial for developing effective management strategies. The ease of access and widespread adoption of public cloud services has significantly increased the prevalence of shadow IT, as departments and individuals can readily procure cloud services without IT department approval. Both technology solutions and proactive engagement are essential in gaining insights into these unauthorized IT activities. By focusing on public cloud environments, organizations can tailor their management strategies to address the unique challenges and risks associated with the unauthorized use of cloud services, ensuring a comprehensive approach to maintaining security, compliance, and operational efficiency.

3.1. Automated approach for risk mitigation strategy

In addressing the risks associated with shadow IT, especially within public cloud environments, it's crucial to identify and prioritize key risk areas. By focusing on these domains, organizations can develop a more effective strategy for mitigating the potential threats shadow IT poses. The main areas of risk include:

Implementing Cloud Access Security Broker (CASB) Solutions. One of the primary strategies for mitigating the risks of Shadow IT involves the adoption of Cloud Access Security Broker (CASB) solutions. CASBs serve as a security policy enforcement point, placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as cloud-based resources are accessed. CASBs can provide visibility into unauthorized cloud applications, helping organizations to control and monitor cloud traffic. Selvam [12] emphasizes the effectiveness of CASBs in addressing unauthorized SaaS applications and managing third-party app permissions, thereby reducing the risks posed by Shadow IT.

Developing Secure Information Sharing Models in Public Clouds. The creation of secure information-sharing models within public clouds is another crucial strategy. As noted by Pandita, U., Katy, H., Kalpana, & Sonawane, D. [13], these models are essential for mitigating the risks associated with Shadow IT in public clouds. By enabling secure and controlled collaboration, these models ensure that even when employees use cloud services outside the formal IT infrastructure, the data remains protected. This approach promotes a balance between the flexibility of cloud services and the security requirements of the organization.

Active Management and Control of Cloud Usage. Proactively managing and controlling cloud usage within an organization is key to preventing the spread of Shadow IT. This involves not just the implementation of technological solutions but also the fostering of a culture where employees understand the risks associated with unauthorized cloud services. [14] suggests that IT departments should work closely with other departments to identify and approve cloud services that meet both the business and security needs of the organization. This collaborative approach can significantly reduce the proliferation of Shadow IT and ensure that cloud services are used safely and effectively [15].

3.2. Optimizing IT operations for strategic business alignment

In the dynamic landscape of organizational technology management, the balance between meeting user demands and adhering to security, compliance, and budget constraints presents a significant challenge. Addressing this challenge requires not just managing IT resources but transforming the IT department into a strategic partner that is closely aligned with the business's needs and goals.

Streamlining IT Processes. Efficiency in IT operations is crucial for meeting the fast-paced demands of today's business environment. Streamlining IT processes involves critically evaluating existing procedures to identify bottlenecks and redundancies. This process includes:

- Automation: Implementing automation for routine tasks, such as software updates, user account management, and data backups, can significantly reduce the time and resources required for these activities, allowing IT staff to focus on more strategic initiatives.
- Simplifying Approval Processes: Revising approval workflows to eliminate unnecessary steps without compromising security or compliance can expedite the provisioning of IT resources and services, thereby enhancing user satisfaction and reducing the temptation to seek shadow IT solutions.
- Frequent Review and Adaptation: Continuously monitoring and adapting IT processes to address evolving business needs ensures that the IT department remains agile and responsive [16].

Becoming a Business Partner. Transitioning from a traditional service-oriented role to that of a strategic business partner involves a proactive approach to understanding and addressing the technology needs of the organization:

- Engagement and Communication: Regularly engaging with users and stakeholders to discuss their challenges and requirements helps build trust and ensures that IT solutions are closely aligned with business objectives.
- Education and Awareness: Actively educating users about available IT resources and solutions can demystify technology and empower users to leverage official channels for their IT needs. This includes workshops, newsletters, and one-on-one consultations to discuss potential IT solutions.
- Collaborative Solution Development: Involving users in evaluating and selecting new technologies fosters a sense of ownership and partnership. Collaborative decision-making ensures that IT investments are directly linked to enhancing productivity and achieving business goals.

- Policy Development: Employees need to be made aware of the potential security threats and legal implications of using unauthorized cloud services. Alongside education, organizations should develop IT policies that clearly define acceptable and unacceptable uses of cloud services, thus providing a framework that guides employee behavior in a secure and compliant manner [17].

Impact of an IT-Business Partnership. When the IT department operates as an integrated business partner, it achieves a deeper understanding of the organization's needs and is better positioned to develop solutions that are both effective and strategically aligned. This partnership:

- Reduces the prevalence of shadow IT by providing timely and relevant solutions that meet users' needs.
- Enhances organizational agility by enabling quicker adaptation to market changes and technology advancements.
- Improves risk management by ensuring that security and compliance are integral to all IT solutions and practices [18].

Transforming IT into a strategic business partner is a journey that requires commitment, communication, and continuous improvement. By focusing on streamlining processes and fostering a collaborative relationship with the rest of the business, IT can significantly contribute to the organization's success and innovation capacity.

As organizations continue to confront the complexities of Shadow IT, the implementation of automated solutions becomes increasingly vital. Automation can provide the necessary tools to manage and monitor cloud environments more efficiently, reducing manual oversight and minimizing human error.

4. Automation approach for public cloud provisioning which helps exclude shadow IT

The adoption of an automation approach for public cloud provisioning plays a pivotal role in mitigating the risks associated with Shadow IT, primarily by streamlining the deployment of cloud resources and ensuring compliance with organizational policies. Automating the provisioning process [19] can significantly enhance efficiency, security, and governance across public cloud environments, directly addressing the factors that often lead to the emergence of Shadow IT. Here are key aspects illustrating the importance of automation in this context.

4.1. Enhancing cloud security and efficiency with self-service automated configuration scanning

Automated configuration scanning emerges as a pivotal strategy for maintaining cloud security and operational efficiency, leveraging a self-service model. This approach utilizes a central orchestrator, specifically the Rundeck platform, complemented by a robust toolkit including Ansible for IT automation and Python for scripting [20]. These tools are integral to a continuous integration development process, characterized by rigorous code control and testing. The orchestrator and its scenario scripts are meticulously designed to avoid storing any cloud environment data directly, instead relying on REST API communications with Rundeck for job execution and status updates. This architecture is pivotal for scalability, system availability, and enhanced security [21].

To bolster the security framework of the orchestrator, particularly in the context of cloud environment assessments, integration with HashiCorp Vault is recommended for secure information storage.

The core of configuration scanning lies in its ability to identify discrepancies within cloud configurations by analyzing environment logs (Audit logs, Flow logs). This analysis is juxtaposed against established cybersecurity standards such as NIST 800-53, HIPAA, PCI-DSS, SOC, and ISO, ensuring configurations adhere to the highest security protocols [22]. The implementation of continuous integration, facilitated by audit and flow logs between cloud environments and platforms like Prisma Cloud, ensures ongoing monitoring and compliance. This setup offers an instantaneous overview of the cloud infrastructure, enabling swift identification and correction of deviations from security standards or operational benchmarks. The adoption of continuous integration not only bolsters security measures but also enhances the reliability and efficiency of operations [23].

Advanced analytics play a crucial role in interpreting log data, shedding light on usage trends and potential security vulnerabilities. This proactive stance towards security is further enriched by the application of machine learning algorithms, which predict possible issues based on historical data, allowing for anticipatory risk mitigation strategies.

Operational flexibility and adaptability are also central to this system's design. The modular nature of the scenario architecture affords quick adaptability and customization, catering to the dynamic needs of businesses and evolving technological landscapes. The choice of Ansible and Python for automation and scripting places the system at the cutting edge of technology, backed by extensive community support and regular updates [24].

In essence, this self-service automated configuration scanning model achieves continuous control over cloud configurations, external security perimeters, costs, and compliance with security standards, underscoring a commitment to security, operational efficiency, and adaptability (Fig 2).

4.2. Financial advantages of implementing automated configuration scanning

Operational Efficiency and Cost Savings: The transition to automated configuration scanning significantly lowers operational expenses. By streamlining routine checks and maintenance through automation, the need for manual oversight is drastically reduced. This efficiency not only cuts down on the labor and time involved but also redirects staff efforts towards higher-value activities, resulting in direct financial benefits [25].

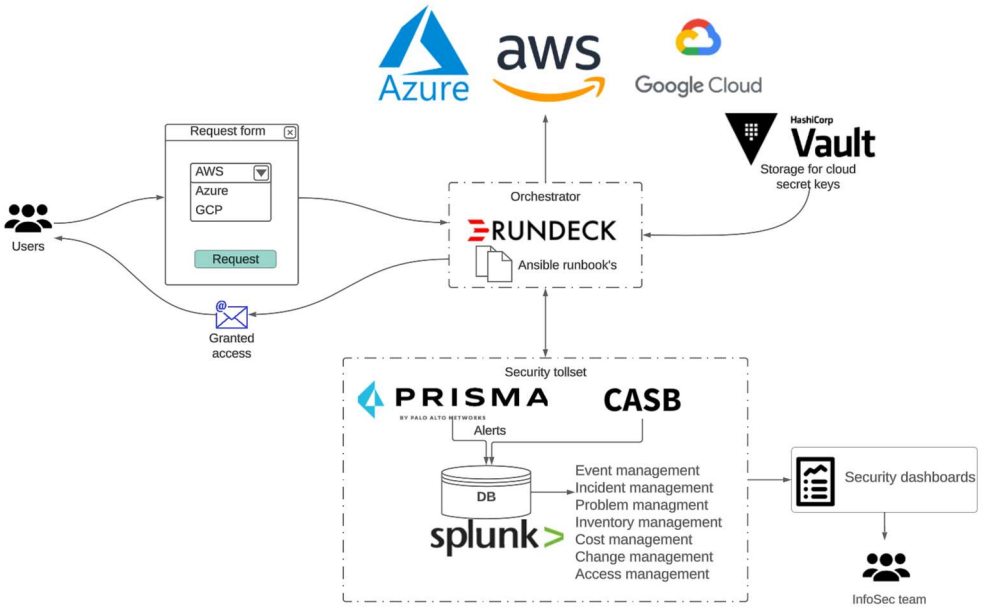

Figure 2: Automation cloud provisioning process

Mitigation of Security-Related Financial Risks: Early identification of vulnerabilities through automated scanning is crucial in averting security breaches, which can be financially draining and damaging to reputation. By proactively addressing these vulnerabilities, organizations can sidestep the extensive costs associated with data breaches, making automated scanning a wise investment for safeguarding assets.

Cloud Resource Optimization: Automated scanning provides insights into the usage of cloud resources, pinpointing areas of waste or underutilization. Adjusting these resources accordingly can lead to considerable savings on cloud spending, while also boosting the efficiency and performance of cloud-based operations [26].

Avoidance of Compliance-Related Fines: Keeping up with compliance requirements is essential to avoid financial penalties and legal issues. Automated configuration scanning facilitates ongoing adherence to regulatory standards, helping organizations avoid the financial pitfalls of non-compliance and reinforcing their standing in regulated sectors.

Enhancement of System Reliability: Proper configuration management through automated scanning contributes to the reliability and uptime of systems. The cost implications of downtime—lost revenue and recovery efforts—are significant, making the stability ensured by regular scanning a valuable asset in maintaining continuous business operations [27].

Strategic Organizational Growth: Beyond immediate financial gains, automated configuration scanning aligns with broader strategic objectives, nurturing an organizational ethos of efficiency, security, and regulatory compliance. While these advantages may not be immediately quantifiable, they play a critical role in sustaining the long-term vitality and competitive edge of the business.

The financial analysis of automated configuration scanning underscores its substantial value proposition. The initial investment in automation technology is quickly offset by savings in operational expenditures, enhanced security measures, efficient resource management, reduced compliance costs, improved system uptime, and strategic organizational benefits. This analysis highlights automated configuration scanning as an indispensable tool in contemporary cloud management frameworks.

4.3. Engagement and communication

Automated Feedback and Communication Systems: Utilizing automation for regular feedback collection, such as through automated surveys and quick polls, facilitates constant dialogue between IT and users. Automated ticketing systems for IT requests can update users on the status of their queries or problems in real time, improving transparency and trust.

Automated Reporting: Dashboards and automated reports on service usage, incident resolutions, and project statuses can be shared with stakeholders, keeping everyone informed and aligned with organizational goals and IT capabilities [28].

4.4. Education and awareness

E-Learning Platforms: Automated deployment of e-learning modules tailored to different roles within the organization helps in systematically educating employees about the safe and effective use of IT resources, including cloud services. These platforms can track progress and adapt learning paths based on user performance and feedback.

Automated Notifications: Regular, automated communications such as newsletters, security alerts, updates on new tools, and best practices help keep all users informed and aware of the resources available to them and the importance of following security and compliance guidelines [29].

4.5. Collaborative solution development

Self-Service Portals: Automation can power self-service portals where users can request new tools, access trial software, and provide feedback on their needs and experiences. Such platforms can aggregate user requests and feedback, facilitating data-driven decision-making in technology selection and implementation.

Automated Prototyping Tools: For development teams, automated environments for testing and prototyping new solutions can accelerate the innovation process. These tools allow for the quick setup and teardown of test environments, encouraging experimentation and iterative development with direct user involvement [30].

4.6. Policy development

Automated Policy Enforcement: Automation tools can monitor the IT environment to ensure compliance with established policies, automatically flagging or restricting the use of unauthorized services. This includes the deployment of security configurations and compliance standards across cloud services.

Dynamic Policy Updates: As policies evolve, automated systems can update users on changes and ensure that all employees complete acknowledgment or training sessions related to new policies. This ensures that policy awareness is consistent and up-to-date [31].

By leveraging automation in these critical areas, organizations can foster a more engaged, informed, and collaborative culture regarding IT resource use. This not only reduces the reliance on Shadow IT by making authorized channels more accessible and responsive to user needs but also strengthens compliance and security postures. Automating engagement, education, solution development, and policy management processes thus becomes a cornerstone strategy in aligning IT practices with business objectives and user requirements [32].

5. Analysis of results after implementation of the proposed approach

This comprehensive case study showcases a strategic and structured approach to managing a multi-cloud infrastructure (AWS, Azure, and GCP) that began in late 2020 and continued through 2023. Here is an overarching summary of the project's progression, achievements, and significant milestones:

End of 2020: The infrastructure comprised 230 known accounts, setting the baseline for the forthcoming enhancements.

2021 Timeline and Strategic Initiatives:

1. **Audit and Monitoring:** Initiation of active audit processes and implementation of monitoring systems on all discovered accounts to ensure full visibility and control.
2. **Compliance Enhancement:** Rigorous correction of compliance issues according to NIST 800-53 rev.4 standards, raising the security and regulatory standards across the board (Fig. 3).
3. **Discovery and Management:** Identification of over 120 previously unknown cloud accounts, integrating them into the organization's formal management system.
4. **Account Optimization:** Closure of more than 30 obsolete accounts, streamlining operations and eliminating unnecessary security risks.

2022–2023: Expansion and Stabilization:

1. Growth in Infrastructure: Systematic increase in the number of cloud accounts to 447, reflecting an expanded and more robust infrastructure.
2. Security and Compliance: Continued improvements in security measures leading to an advanced and stable infrastructure adept at risk analysis and incident response.

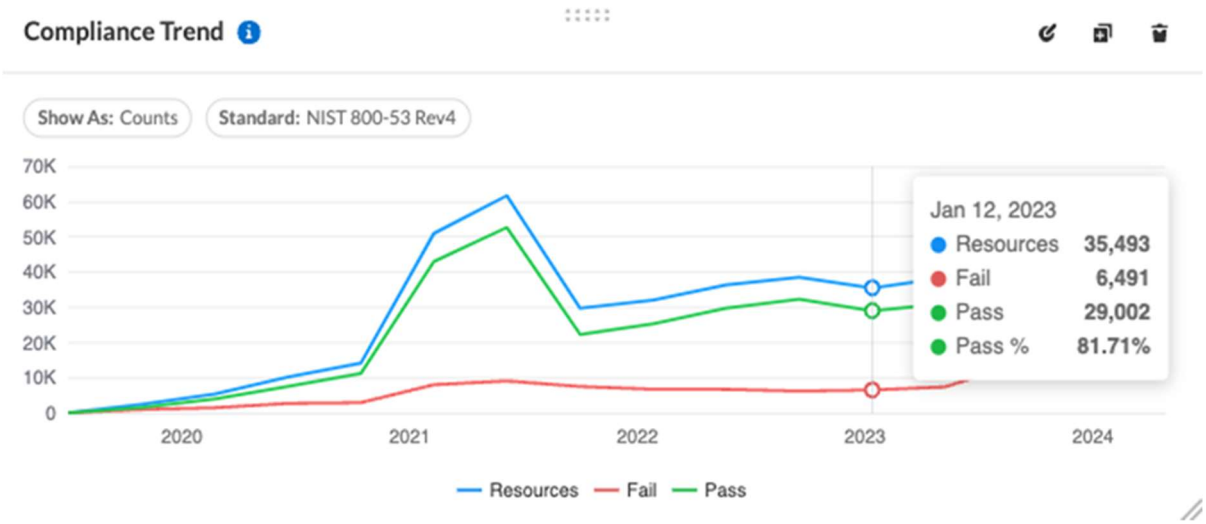

Figure 3: Compliance trend analysis

End of 2023. Key Insights and Achievements:

1. **Total resources managed:** 35,493.
2. **Vulnerability levels:** Zero critical and high vulnerabilities; 954 medium; 1,870 low; 3,667 informal (Fig. 4).
3. **Compliance level:** An increase from 67% to 82%, indicating enhanced governance and adherence to high standards.
4. **Security Improvement:** The elimination of critical and high-level vulnerabilities by the end of 2023 is a testament to the effective security management and mitigation strategies employed, ensuring a highly secure cloud environment.
5. **Compliance Increase:** The significant rise in the compliance level from 67% to 82% within three years underscores the successful enhancement in governance and adherence to stringent security standards.
6. **Account Management:** The proactive management of both known and previously unknown accounts illustrates a decisive action against shadow IT practices, improving control and visibility across the cloud environment.

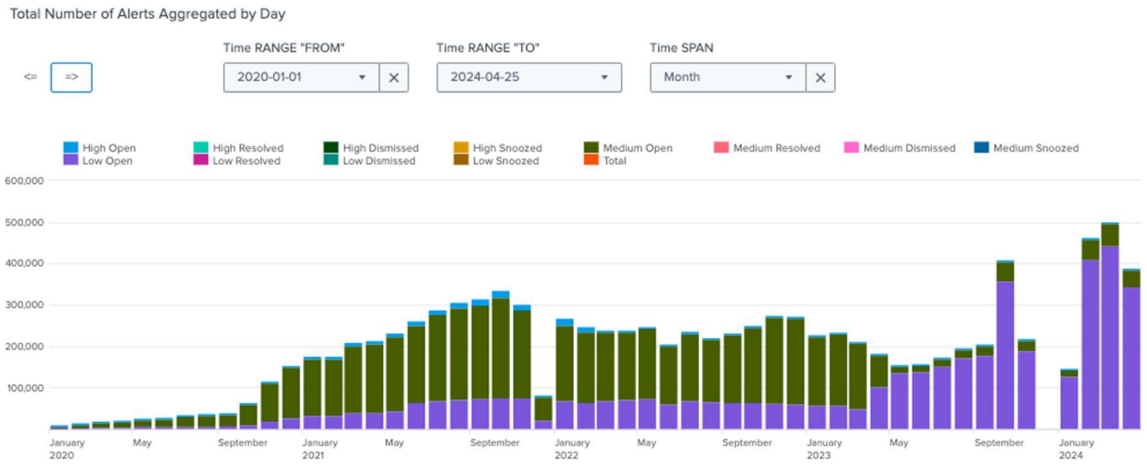

Figure 4: Compliance trend analysis per alert priority

This case study exemplifies the importance of a structured and proactive approach to cloud infrastructure management. Through regular audits, continuous monitoring, and a strong focus on compliance and security, the organization not only improved its operational security but also aligned its cloud resources more closely with organizational goals. The strategic management of cloud accounts, including the identification and elimination of unnecessary or redundant accounts, played a crucial role in enhancing cost efficiency and resource management. Overall, this journey reflects a model for effective cloud governance that can serve as a benchmark for similar enterprises aiming to secure and optimize their cloud environments.

6. Conclusions

In conclusion, the strategic application of automation across various facets of IT management—ranging from user engagement and education to collaborative solution development and policy enforcement—emerges as a pivotal solution to the pervasive challenge of Shadow IT, particularly within public cloud environments. By harnessing automation, organizations can significantly enhance their IT governance, ensuring that IT practices are not only aligned with business objectives but also responsive to user needs, thereby reducing the inclination towards unauthorized IT solutions.

The deployment of automated tools and processes fosters a culture of transparency, efficiency, and security, which is essential for mitigating the risks associated with Shadow IT. These risks, including security vulnerabilities, legal ramifications, and compliance breaches, pose significant threats to the integrity and operational efficacy of cloud computing frameworks.

Furthermore, proactive engagement strategies facilitated by automation—such as continuous feedback mechanisms, personalized educational programs, and inclusive technology evaluation platforms—encourage a more informed and collaborative approach to IT resource utilization. This not only enhances the user experience by making approved IT channels more accessible but also aligns IT initiatives with the dynamic requirements of the modern enterprise.

Ultimately, addressing the challenges of Shadow IT through automation underscores a commitment to maintaining a secure, efficient, and adaptable cloud environment. It highlights the necessity of evolving IT management strategies to keep pace with the rapid advancements in cloud technology and the changing landscape of enterprise IT needs. Adopting these automated approaches signifies a decisive step towards empowering organizations to leverage the full potential of cloud computing, ensuring that it serves as a catalyst for innovation and growth rather than a source of risk and inefficiency.

References

[1] K. Edwards, Expected and Realized Costs and Benefits when Implementing Product Configuration Systems, Mass Customization for Personalized Communication Environments: Integrating Human Factors (2010) 216–231. doi: 10.4018/978-1-60566-260-2.ch012.

[2] P. Akello, Volitional Non-Malicious Insider Threats: At The Intersection of COVID-19, WFH and Cloud-Facilitated Shadow-Apps, 27th Annual Americas Conference on Information Systems, AMCIS 2021 (2021).

[3] P. Selvam, (2022). Secure Cloud Services by Integrating CASB based Approach, Int. J. Sci. Res. Eng. Manag. 6(7) (2022) 1–5. doi: 10.55041/IJSREM15210.

[4] H. Khan, et al., A Blockchain-Based Approach for Secure Data Migration from the Cloud to the Decentralized Storage Systems, Int. J. Web Services Res. 19(1) (2022) 1–20. doi: 10.4018/ijwsr. 296688.

[5] O. Vakhula, I. Opirskyy, O. Mykhaylova, Research on Security Challenges in Cloud Environments and Solutions based on the "Security-as-Code" Approach, in: Cybersecurity Providing in Information and Telecommunication Systems-II, vol. 3550 (2023) 55–69.

[6] I. Kirin, Shadow IT: Data Protection and Cloud Security (2017). doi: 10.2139/ssrn.3020880.

[7] L. Šedivcová, M. Potančok, Shadow IT Management Concept for Public Sector (2019) 65–73. doi: 10.1007/978-3-030-37632-1_6.

[8] M. Walterbusch, A. Fietz, F. Teuteberg, Missing Cloud Security Awareness: Investigating Risk Exposure in Shadow IT, J. Enterprise Inf. Manag. 30 (2017) doi: 10.1108/JEIM-07-2015-0066.

[9] R. Taylor, Everything You Need to Know About Shadow IT, Bluecat Networks (2021). URL: https://bluecatnetworks. com/blog/everything-you-need-to-know-about-shadow-it/

[10] M. Silic, A. Back, Shadow it—A View from Behind the Curtain, Inf. Syst. Econom. eJ. (2014).

[11] R. Walters, Bringing IT Out of the Shadows, Netw. Secur. 2013(4) (2013) 5–11. doi: 10.1016/S1353-4858(13)700 49-7.

[12] X. Zeng, et al., Flow Context and Host Behavior Based Shadowsocks's Traffic Identification, IEEE Access (2019).

[13] U. Pandita, et al., Effective Management of Proofs Of Log, Int. J. Adv. Res. Innov. Ideas Educ. 3(3) (2017).

[14] D. Shevchuk, et al., Designing Secured Services for Authentication, Authorization, and Accounting of Users, in: Cybersecurity Providing in Information and Telecommunication Systems–II, vol. 3550 (2023) 217–225.

[15] M. Silic, D. Silic, G. Oblakovic, Influence of Shadow IT on Innovation in Organizations, Complex Systems Informatics and Modeling Quarterly (2016) 68–80. doi: 10.7250/csimq. 2016-8.06.

[16] H. Fujinoki, S. Dehkordi, Split Clouds: New Security Architecture for Protecting User Information from Cloud Insiders—Designs, Implementation, and Performance Evaluations (2012) 824–829.

[17] H. Rajavaram, T. Balasubramanian, V. Rajula, Automation of Microservices Application Deployment Made Easy By Rundeck and Kubernetes. IEEE International Conference on Electronics, Computing and Communication Technologies (2019) 1–3. doi: 10.1109/CONECCT47791.2019.9012811.

[18] T. Kenaza, et al., A Secure and Interoperable Architecture for Blockchain/IPFS Assisted Electronic Health Record Access Control and Sharing (2023) doi: 10.21203/rs.3.rs-3209163/v1.

[19] K. Murakami, et al., A Cloud Architecture for Protecting Guest's Information from Malicious Operators with Memory Management (2014) 155–158. doi: 10.1145/2557547.2557585.

[20] Y. Martseniuk, et al., Automated Conformity Verification Concept for Cloud Security, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3654 (2024) 25–37.

[21] H. Wang, Proxy Provable Data Possession in Public Clouds. Services Computing, IEEE Transactions 6 (2013) 551–559. doi: 10.1109/TSC.2012.35.

[22] V. Susukailo, I. Opirsky, O. Yaremko, Methodology of ISMS Establishment Against Modern Cybersecurity Threats, Future Intent-Based Networking, LNEE 831 (2022). doi: 10.1007/978-3-030-92435-5_15.

[23] O. Deineka, et al., Designing Data Classification and Secure Store Policy According to SOC 2 Type II, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3654 (2024) 398–409.

[24] V. Rajaraman, Cloud Computing, Resonance 19 (2014) 242–258. doi: 10.1007/s12045-014-0030-1.

[25] An Assessment of the National Institute of Standards and Technology Center for Neutron Research, Technology, Panel & Programs, Committee & Board, Laboratory & Sciences, Division & Medicine, National (2016). doi: 10.17226/21878.

[26] R. Buyya, et al., Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility, Future Gener. Comput. Syst. 25 (2009) 599-616. doi: 10.1016/j.future.2008.12.001.

[27] S. Çevik, A. Ustundag, Smart and Connected Product Business Models (2018). doi: 10.1007/978-3-319-57870-5_2.

[28] R. Clark, R. Mayer, W. Thalheimer, E-Learning and the Science of Instruction: Proven Guidelines for Consumers and Designers of Multimedia Learning, Performance Improvement 42 (2003). doi: 10.1002/pfi.4930420510.

[29] A. Nordby, et al., System Thinking in Gamification, SN Comput. Sci. 5 (2024). doi: 10.1007/s42979-023-02579-2.

[30] F. Yaseen, Chapter 2 2. Literature Review 2.1. Information Security Policy Availability and Compliance Literature. (2024).

[31] V. Khoma, et al., Comprehensive Approach for Developing an Enterprise Cloud Infrastructure, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3654 (2024) 201–215.

[32] S. Yevseiev, et al., Models of Socio-Cyber-Physical Systems Security: monograph, PC Technology Center (2023). doi: 10.15587/978-617-7319-72-5.