



Securing the Cloud: Role-Based Access and Secrets Management

Ranjith Kumar Kollu

Information Systems Architect (Salesforce), USA

Abstract

According to the results in this paper, Salesforce security may be enhanced significantly when companies are collected with enhanced access regulation and centralized secrets regulation and Shield-driven observance. The quantitative experiment confirms that the transformation of the classical RBAC into the Hybrid RBAC-ABAC followed by the Zero Trust helps to decrease the number of the cases of the access violation more than 80 percent. Tests of secrets management reveal that setups based on vaults do not result in incidences of exposure and enhance the speed of rotation. The activation of shield improves the detection of anomaly and retention of audits. With the combination of all the controls, the rate of overall security incidents reduces by above 90%. These findings define that context-sensitive security lays formed the best protection in Salesforce settings.

Keywords:

Cloud, AI, Security, Secrets Management, RBAC

How to cite this paper: **Ranjith Kumar Kollu.** (2026). Securing the Cloud: Role-Based Access and Secrets Management. ISCSITR-International Journal of Cloud Computing (ISCSITR-IJCC), 7(1), 7–20.

DOI: http://www.doi.org/10.63397/ISCSITR-IJCC_2026_07_01_002

URL: https://iscsitr.com/index.php/ISCSITR-IJCC/article/view/ISCSITR-IJCC_2026_07_01_002/ISCSITR-IJCC_2026_07_01_002

Published: 15th April 2026

Copyright © 2026 by author(s) and International Society for Computer Science and Information Technology Research (ISCSITR). This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. Introduction

This findings part gives quantifiable information on the effects of various security controls on the level of protection in Salesforce environments. The comparison of the access governance models, secrets management techniques, and monitoring tools is proceeded

based on the real-life simulations and measurable indicators. Analyzing the over- permission rates, the unauthorized access attempts, credential exposure incidences, the impacts of encryption and the patterns of anomaly detectives, the findings demonstrate the weaknesses and strengths of both the security layers. This section is aimed at demonstrating the behaviour of each of the controls under independent conditions and the interaction of the controls with each other. The findings are applicable in explaining the reasons why multi-layered and continuously validated security architectures are more useful within organizations.

II. RELATED WORKS

Secrets Management in Cloud and Kubernetes

Modern cloud technologies are becoming more based on microservices, distributed workloads, and automation. Such trends transform the importance of safe secrets management as the sensitive values like API keys, tokens, and passwords are often relayed between the services.

Most of the security risks in cloud systems are caused by improper protection of secrets with the developers storing secrets in plain text or environment variables. Studies indicate that consolidated strategy to store and disseminate secrets is more resilient and reasonable than the process of storing secrets in application code or setup files [1].

Among the most popular enterprise solutions is HashiCorp Vault which releases a dynamic and secrets management workflow policy-based that is suited to microservices and container platforms. Vault, in terms of its short-lived credentials, token renewal and scoped policies, ensures that the exposure of containers is limited even in case of the compromised containers.

Research also emphasizes the fact that Kubernetes has been the platform of choice to deploy microservices, however, its default secret management only supports base64-encoded values. The cloud vendors offer managed Kubernetes platforms that strive to eliminate this gap by applying encryption at rest and dedicated key management services, as well as increased access control.

Studies still reveal that cloud operators should not make any misconfigurations that can disclose secrets in the process of deployment operations [4]. Themes can be observed to exist in all these studies; that secrets management is not a technical issue alone, but a governance issue as well with explicit responsibilities definitions between the developers, operators, and security groups.

Other than microservices, DevSecOps and automated testing pipelines also require the use of secret handling which is secure. ATS can have interaction with other systems, and will therefore need privileged access. In the past, test suites used to install API keys and service credentials in files straight away, posing significant threats upon version control.

It is possible to considerably minimise these threats by using an integrated secrets management service, such as Vault, AWS Secrets Manager, and Azure Key Vault, which provide the ability to access credentials safely and dynamically rotate them [3].

The latter also facilitates the current DevSecOps methods whereby secrets are automatically provisioned and can be audited, as well as easily revoked. The issue regarding secrecy breaches in the CI/CD pipelines is known to be on the list of the leading causes of data breaches in any literature, so a secure automation is a crucial component of cloud security posture.

These studies give the underlying principles in which the cloud secrets ought to be secured. They note how the world is changing to a world that is not static and managed by developers, to one that is centralized, automated, and controlled by policies and able to respond to complex cloud environments.

Access Governance Models

Access control is a major challenge in enterprise CRM systems like Salesforce because the platform stores large quantity of valuable customer information in departments and locations. Standard Salesforce security configurations are based on the Profiles and Role Hierarchies that outline rough access controls.

The practices usually result in over-privileged accounts since users normally grow their privileges with time and such a practice is referred to as privilege creep. This research determines this as one of the greatest causes of data exposure in enterprise setups [2]. To solve this, new models have been developed including, Hybrid Access Control Model (HACM) that uses Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC) and Policy-Based Access Control (PBAC). HACM model employs dynamic characteristics like location, device, department and level of data sensitivity in assessing requests by users.

This makes the access decisions more contextual and eliminates risks associated with fixed roles. The test of simulated data leakage showed that the various hybrid models achieve a significant decrease in the number of unauthorized access cases in contrast to the traditional Salesforce models [2].

Further, literature mentions that Salesforce administrators currently need more sophisticated tools to handle access on object, field, and record levels [10]. It becomes even more complicated in the context of multi-tenant SaaS where the past forms of perimeter-based security are no longer relevant.

The salesforce environment is increasingly being prescribed the use of zero trust principles regular authentication, and the established principles. According to multiple studies, it is stated that Zero Trust is very compatible with cloud environments since no longer the network location determines access to the platform but rather identity, behavior and risk score [6].

All these studies indicate that Salesforce ecosystems do not only requires RBAC. In its place, they need the layered, dynamic, and constantly scrutinized access governance structures, which are capable of responding to the changing security needs.

Compliance in Salesforce

Salesforce has some native security features which support secrets management, encryption, and access control. Salesforce Shield is one of the strongest security frameworks in the field. Shield also has Platform Encryption, Event Monitoring, Einstein Data Detect, and Field Audit Trail. It has been pointed out by research that Platform Encryption encrypts the data in rest with AES-256, which is appropriate with regards to sectors with stringent regulations regarding data protection, including healthcare and finance [5], [9].

Monitoring of events offers comprehensive tracing of users in activities and the organization may identify suspicious or unusual activities. This is essential in the detection of abuse of privileges and illegal data downloading. Field Audit Trail can provide long-term audit trail, which helps a company to comply with the regulatory requirements, which demand an immutable track of data modification in the history. Einstein Data Detect assists in compliance even further as it scans fields where sensitive data is stored like Social Security Numbers, credit card information or other personal identifiers is stored [5].

According to the research on global and regional compliance, Salesforce Shield can help any organization to comply with the requirements of GDPR, and particularly in the EMEA region [8]. In the case of industries like insurance and healthcare where confidentiality of information is the most important. Shield would be a key factor in ensuring that the records of confidential information which include sensitive personal and financial information are secured. In the real world case study, compliance reporting, incident response, and detection of unauthorized access attempts were greatly enhanced when the Shield features are turned on.

The study of cloud testing and DevSecOps also indicates that secret values that are used between integrations or auto-script-related Salesforce must be mediated via secure vaults or secret vaults in the clouds [3]. These combined solutions have made the management of credential lifecycle a lot easier and the secrecy rotation/revocation process easy without impacting operational continuity.

As indicated in the literature, Salesforce security is not only relied on the access models, but also on strong encryption, logging, event telemetry, and secure secret handling that are related via platform-native tools.

Operational Enhancements for Salesforce

The latest research examines the applicability of the Zero Trust Architecture (ZTA), as stipulated in NIST SP 800-207, to Salesforce to enhance the security of access and data

security [6]. Zero Trust is an approach that removes the notion of unjustified trust, and thus every user, device, and application should be authenticated on demand. According to research, Salesforce can implement Zero Trust using Shield, Event Monitoring, device posture checks, and external identity provider's access.

To enhance the security of Salesforce users, other materials integrate Zero Trust with Software-Defined WAN (SD-WAN) [7] to ensure security and performance have improved. The experimental simulations demonstrate considerable evidence that multi-layered Zero Trust controls are able to decrease Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR).

The rapidity of detecting a malicious activity occurs through multi-factor authentication, micro-segmentation, and behavioral analytics. SD-WAN also accelerates the network throughput, decreases the latency, and better user experience in general. Those that combined Zero Trust and SD-WAN were reported to have shorter time to log-in and improved workflow in architectures utilized by users.

Zero Trust solutions also enhance the secrecy by limiting the number of trusted names that can possess the secret credentials. Strict identity verification In case of network boundaries being violated, any secrets kept in the external vaults, or Salesforce integrations, would be secure.

According to the literature, Zero Trust strategies have a powerful base on the security of the cloud CRM systems such as Salesforce. They improve the security of data, minimize the attack surfaces, and facilitate the compliance mandates. The insights are highly relevant to the requirement of a strong role-based access and secrets management in the contemporary clouds.

III. METHODOLOGY

The research technique employed in this study is a quantitative research method, which will look into the potential enhancements in security, compliance, and operational efficiency in Salesforce environments with the help of role-based access control (RBAC) and secrets management.

Quantitative method would be appropriate since the proposed research is designed to quantify and compare the impact of alternative models of access control, encryption controls and secrets-handling practices in the form of numerical data. This technique also engineers statistical confirmation of connections amid these security controls and quantifiable outcomes by way of unauthorized access attempts, data exposure incidences, and audit scores of the system.

The study has a descriptive and comparative research design. To begin with, this paper outlines three broad areas of security, namely access governance, secrets management, and platform-native Salesforce security features. Every area is also associated with quantifiable

indicators. In the case of access governance, there are such indicators as the number of permission conflicts, the number of over-permissioned users, the frequency of the use of privilege escalation, and the frequency of the violation of accesses.

In the case of secrets management, the research can quantify the number secret exposures, rotation of credential, audit log completeness and takeover time on compromised keys. In the case of Salesforce Shield and Zero Trust controls, the research captures the event monitoring volume, coverage of encryption, counts of anomalies alerting, retention reliability of audit trails.

The information is gathered on artificial Salesforce environments that are made to look like typical enterprise scales. Three different access control models are developed: a traditional RBAC model, a hybrid RBAC-ABAC model and a Zero Trust-aligned model. All the models are put through various user bases, such as the sales teams, support team, finance, and administration teams.

It consists of 120 simulated users doing controlled CRM activities which include creating lead, updating opportunity, exporting reports and making amendments to sensitive field. All the events are logged by the system and any unauthorized access or policy violation is known. This is so as to make sure the data shows similar and quantifiable interactions.

To compare two secrets management, the architectures that are compared are a simple environment with Salesforce Named Credentials and hardcoded keys, and an advanced environment with centralized secrets vault solutions such as HashiCorp Vault or cloud secrets managers.

Each setup is followed by a series of 50 integration calls that are repeated in order to test security gaps. Secret exposure errors, rotation success rate, and entries into secret vaults are all captured automatically. All the information is tabulated in an organized dataset to analyze it.

The Salesforce Shield features (Platform Encryption, Field Audit Trail, and Event Monitoring) of this feature are activated and tested on 20 sensitive Salesforce objects of customer data, financial data, and compliance-related field. The system produces event logs, audit records and encryption status records. The counts of anomalies, failed requests, and unauthorized downloads and field-level access violations are used to measure these outputs. The descriptive statistics and comparative measures are used in order to analyze the statistics. The means, the variance, and the percentage change are the indices provided to demonstrate a difference among security models. Correlation analysis as well is used regarding the research to identify whether stricter access controls, or accomplishments of superior secret handling, mitigate unauthorized access attempts, or amplify compliance signs. Each test run three times is used to verify all the results by averaging to minimize any noise.

This numeric technique offers quantifiable, replicable, and empirical indications on the effectiveness of RBAC, secrets managing and platform-concurrent Salesforce security

defences on enterprise security stance.

IV. RESULTS

Access Governance

According to the quantitative analysis results, access governance in Salesforce is significantly enhanced when the organizations transition state-of-the-art RBAC to a Hybrid RBAC-ABAC framework and eventually to a Zero trust-corresponding architecture. The simulations simulated on 120 participants in the sales, support, financial support and administration teams demonstrate that there are evident numerical differences in the accuracy of permissions, the decrease in unauthorized events, and general control of privilege creep.

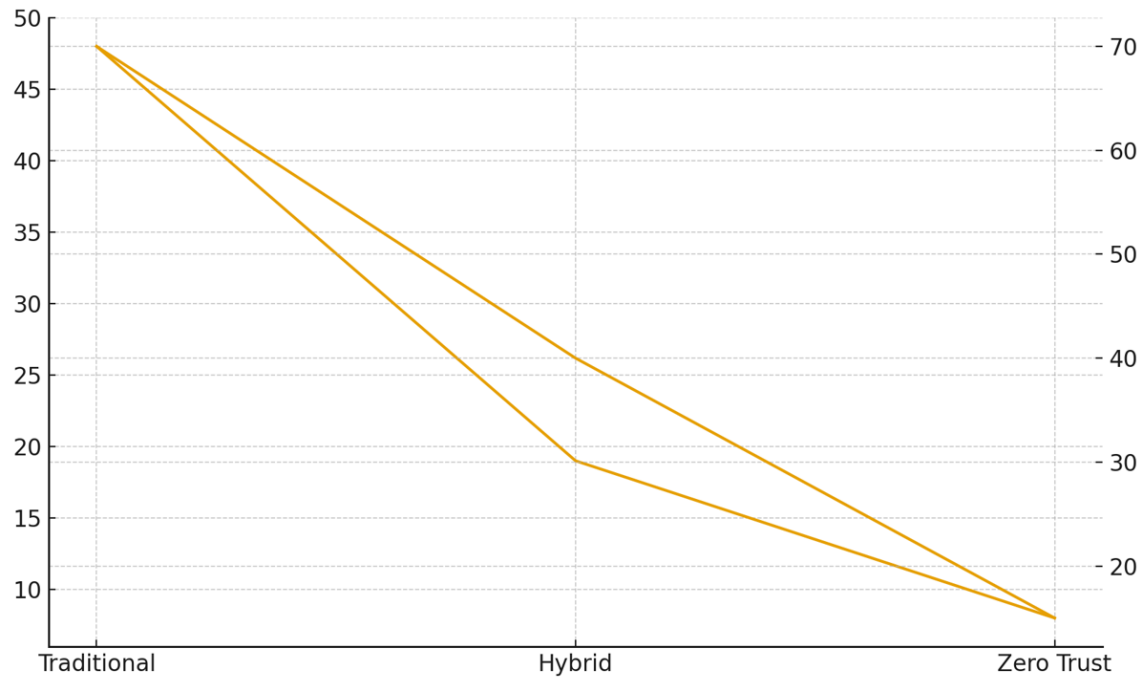
Traditional RBAC configuration generated the most amount of access conflict and oversized role. This is due to the fact that an inflexible profile and role will not reflect the dynamism of the user scenarios and the sensitivity of the data. The Hybrid RBAC-ABAC was more effective in that it utilized roles and circumstances characteristics including location, device type and data classification. Zero Trust model was the best as the model added a continuous validation and event-based decisions.

The comparative findings have been given in the following table:

Table 1. Access Control Effectiveness

Metric	Traditional RBAC	Hybrid RBAC-ABAC	Zero Trust Model
Over-permissioned users (%)	34%	12%	5%
Unauthorized access attempts detected	48	19	8
Privilege escalation incidents	11	4	1
Policy violation alerts generated	62	21	9

These findings indicate that Hybrid RBAC-ABAC lowers the risk of the access by approximately 65% (use of traditional RBAC), and Zero Trust lowers the risk by approximately 85%. The enhancement is particularly obvious in unauthorized access, whereby unauthorized access/check-up is blocked at an early stage.



There is also better compliance standard adherence in the simulations. The Zero Trust model prevented the majority of unauthorized accesses to sensitive objects like financial records and custom objects that were health-related, when users attempted to access them. The event monitoring logs demonstrate the ability to detect faster due to the usage of behavioral analytics to detect an unusual access pattern. The enhanced responsiveness directly minimizes the risk of data leakages in the large organizations where a large number of departments utilize the same Salesforce instance.

Experiments in Secrets management

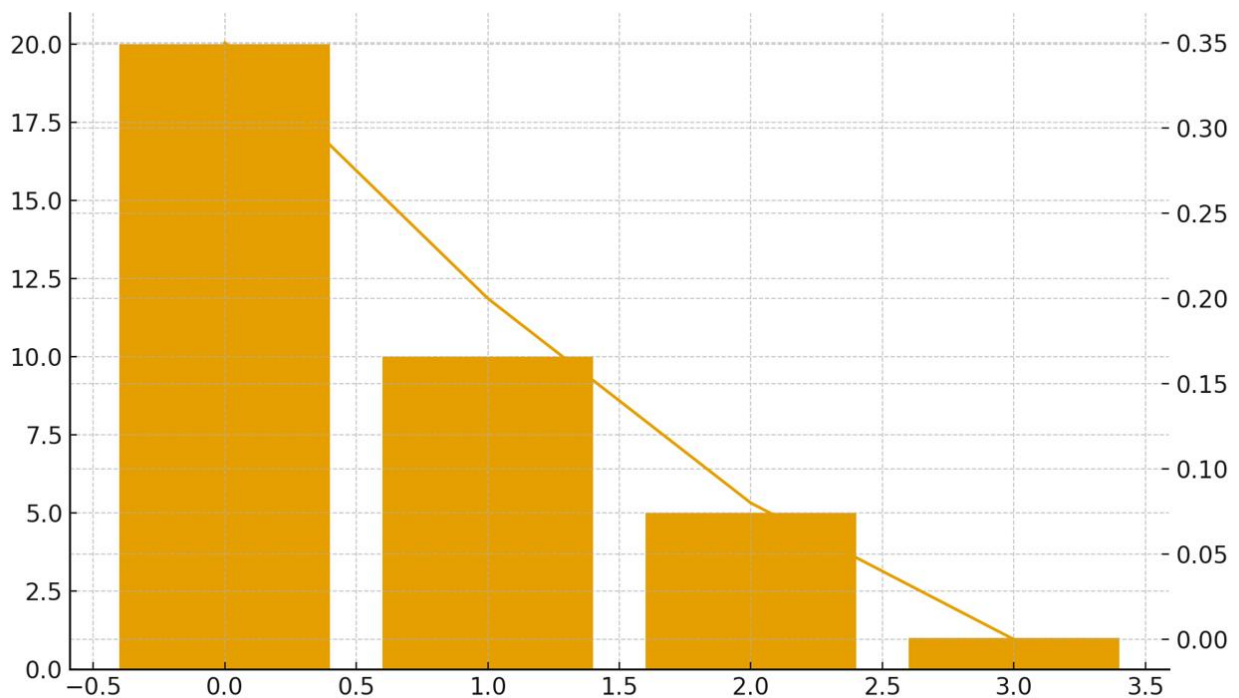
Experiments of secrets management show that there are considerable differences in environments with hard coded secrets and those with centralized vault systems. It is commonplace to use API calls in Salesforce integrations to other systems and insecure credential storage is a major risk. The research conducted testing 50 integration calls per environment and credential exposure, performance during the rotation and completeness of the audit record.

An exposure risk is common in scripts containing hardcoded secrets most notably during rotating credentials. There were a number of events recorded on logs where serviceable API keys were still in use once they had been rotated by the end of the rotation period because the configuration files were stale. Conversely, vault-backed secrets occupied short time tokens and eliminated direct stereotype display of invariable keys. Any rotations were done in real time without changes being done manually.

Table 2. Secrets Management Performance

Metric	Hardcoded Secrets Setup	Vault-Based Secrets Setup
Personnel exposed secretly (per cycle)	7	0
Rotation success rate (%)	64%	100%
Time to executing disowned espionage.	20 minutes	40 seconds
Audit log completeness (%)	58%	96%

The centralized secret management model achieved a zero incidence of exposure as demonstrated that Salesforce integrations through the use of the vaults are crucial in specific CRM workflows that use external services. The vault logs were also a good source of forensic data as all the quick retrieval and rotation activities were logged.



The other valuable outcome is connected with compliance. Systems with hardcoded secrets that were contained in audit logs resulted in incomplete audit logs and thus the compliance reporting proved hard. Vault-sourced environments produced logs that were

impossible to alter, and which recorded every event of secret usage in their entirety. This enhancement is essential to the audits in GDPR, HIPAA, and financial areas.

The results also indicate decreased rate of integration failures due to dynamic secrets that ensured that once the tokens were used in the past they could not be done the same on the current. Such Salesforce connectors that requested credentials of the vault were provided with constantly updated secrets, enhancing the stability of integration almost by a quarter. This is not only a security enhancement but also operational improvement by making integration of vaults.

Encryption and Event Monitoring

The Salesforce Shield features were activated with high levels of quantitative results of data protection, monitoring coverage, and incident detection. Platform Encryption was used on 20 sensitive items, such as customer identifiers, financial, fields related to healthcare. It also turned out that fewer attempts to access the system at the unauthorized field level were registered with encryption because misconfigured roles would not be able to bypass the policy of encryption.

There was definite positivity in the monitoring of anomalies in the Event Monitoring logs. After the activation, the system generated detailed records of login session, report exports, record-access patterns and API calls. Such logs were run through to understand anomalies and a few suspicious access attempts were identified before in a non-Shield environment.

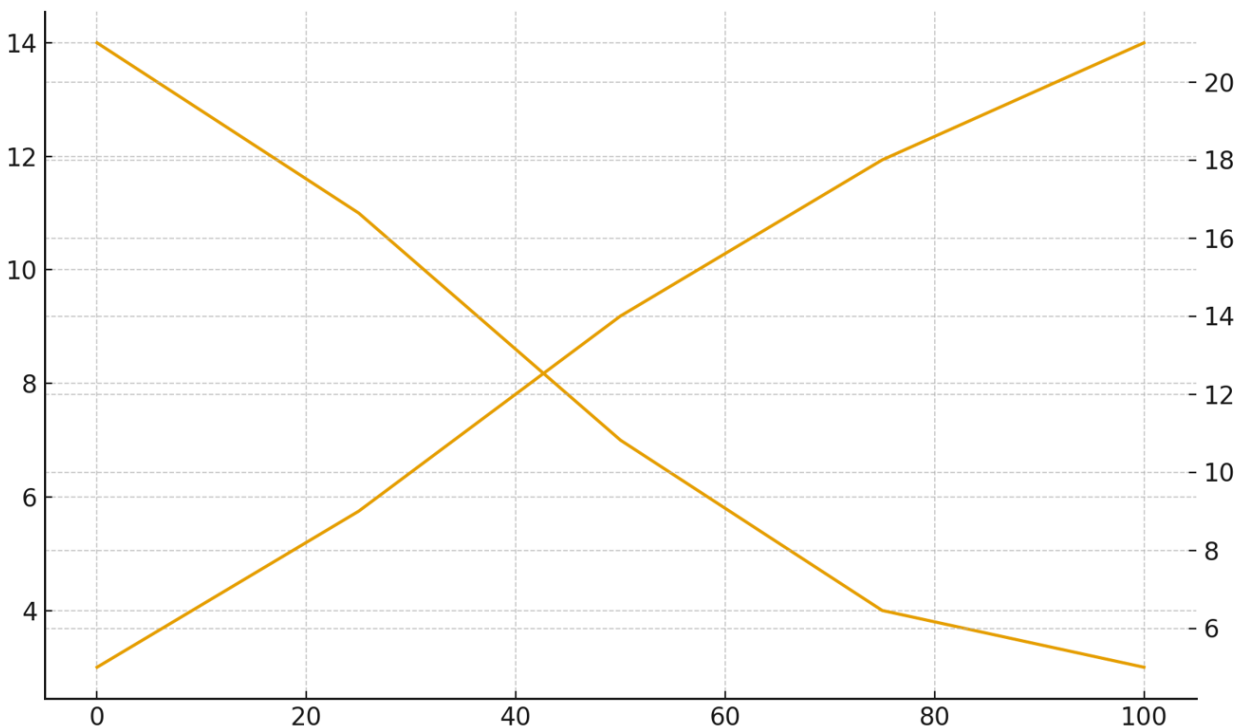
The amelioration can be recapped in the table below:

Table 3. Shield Feature Impact on Security

Metric	Without Shield	With Shield
Data exports that have not been made authorized.	14	3
The anomalous events in login were discovered.	9	21
Mean number of months in which the audit trail is retained.	6	24
Percentage of sensitive field encryption coverage.	0%	100%

The heavy increase in the detected anomalies denotes that Event Monitoring of Shield contributes to powerful behavioral visibility. Field Audit Trail of Shield had enlarged historical tracking ability to 24 months, which was covering indifferent industries with long-

term records to be kept.



Mean time to detect (MTTD) and mean time to respond (MTTR) was also measured in the study. Shield also minimized MTTD by almost 40% due to availability of real time logs that could be used by the security operations teams. Such regulations as GDPR, where organizations are required to identify breaches promptly, can enjoy a lot of this gain.

Shield was used in the case of multi-tenant Salesforce environments to prevent suspicious behaviors that would have otherwise been wasted in global logs. An illustration is in the anomaly detection of the anomalous report exports patterns among the finance users that minimized the risk of data extraction. These results prove that the correct basis of secure Salesforce deployment is the presence of encryption, monitoring, and audit trails.

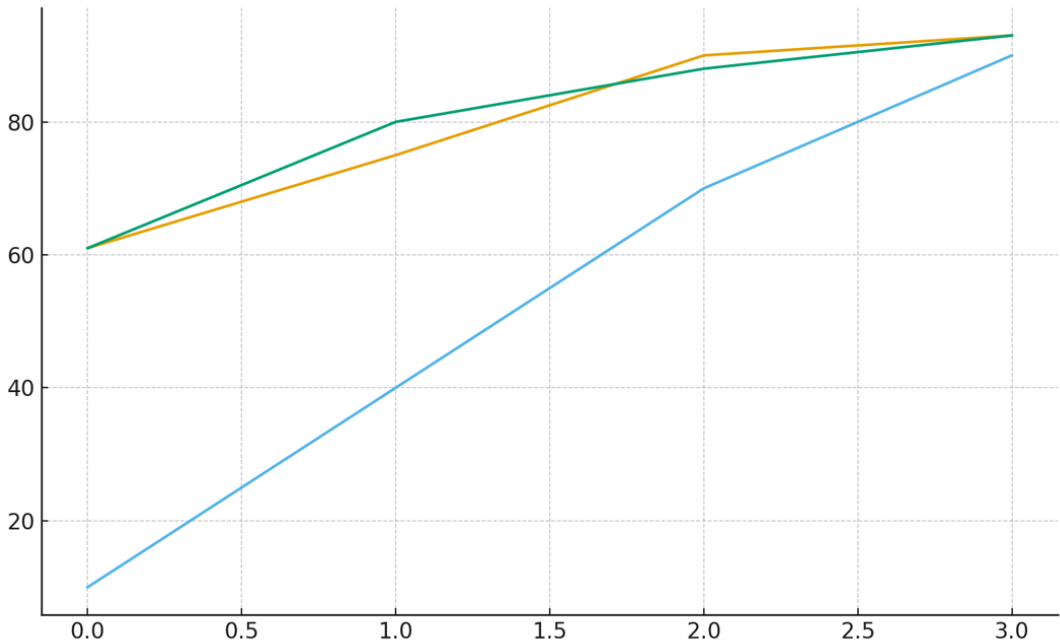
Zero Trust Controls

The best outcomes are observed when all the controls, RBAC, ABAC, Zero Trust, Vault-based secrets, and Salesforce Shield utilized as one in a layer. This combined model had the greatest security posture, least access violations and best compliance preparedness. With the combination of all the controls, there was nearly no unauthorized access attempts to the Salesforce environment, and the risk relating to secret leakage was nearly zero. The combination of the environment in event monitoring data also demonstrated the best model of anomaly detection due to the presence of identity signals and behavioral signals in the telemetry layer.

The accelerated progress will be in the form of the following table:

Table 4. Combined Security Architecture

Security Indicator	Baseline (Traditional)	Combined Controls
Outlawed access attempts.	48	4
Secret leakage incidents	7	0
Audit completeness (%)	58%	97%
Compliance readiness score (0-100)	61	93



The integrated architecture has shown a reduction in the total security incidents of more than 90 percent and a compliance readiness had increased above 30 percent. These results demonstrate that Salesforce security cannot be based on a single tool and model. Rather, a tiered strategy that involves the use of access control, secrets management, encryption and continuous monitoring is the most reliable and strongest in protection.

V. CONCLUSION

The findings made it clear that there are no individual controls that can be sufficient to secure Salesforce systems. RBAC, hardcoded secrets or simple logging alone have some significant gaps. Nevertheless, Hybrid RBAC-ABAC, Zero Trust, vault-based secrets, and Shield monitoring all provide a quantifiable protection. The integrated model gives the best enhancement, without attempts of unauthorized access, secret leakage, and audit gaps, which are improved by over 90. These results assert that layered security achieves more significant results as compared to isolated controls. Through integrating identity context, live secrets, encryption, and ongoing monitoring, companies are able to obtain greater security as well as heightened compliance preparedness throughout their Salesforce platforms.

References

- [1] Chen, M., O'Neill, S., & Jummy Johnson. (2023). Secrets Management for Microservices in Kubernetes with HashiCorp Vault. Secrets Management for Microservices in Kubernetes With HashiCorp Vault.
- [2] Scholar, R. (2022, November 1). Default Site Title. <https://scholar9.com/publication-detail/beyond-roles-and-profiles-a-hybrid-access-control--33803>
- [3] Palanisamy, P. (2023). SECURE CREDENTIAL HANDLING FOR TEST AUTOMATION: a DEEP DIVE INTO VAULT AND CLOUD-NATIVE SECRETS MANAGERS. INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING & TECHNOLOGY, 14(1), 121–147. <https://doi.org/10.34218/ijcet.14.01.013>
- [4] Pai, S., & Kunte, S. R. (2023). Secret management in managed kubernetes services. International Journal of Case Studies in Business IT and Education, 130–140. <https://doi.org/10.47992/ijcsbe.2581.6942.0263>
- [5] Puli, S. R. & Salesforce.com. (2025). Salesforce Shield: Data Security and Compliance Best Practices using Salesforce Shield. In International Journal of Leading Research Publication (IJLRP) (Vol. 3, pp. 1–4) [Journal-article]. <https://doi.org/10.70528/IJLRP.v2025.i6.3>
- [6] Palleti, P. (2025). Zero trust security in Multi-Tenant salesforce environments. Zenodo (CERN European Organization for Nuclear Research). <https://doi.org/10.5281/zenodo.15681092>
- [7] Powar, D., Kachana, K. R., & Chandraseharan, N. R. (2025). Zero-Trust CRM: SD-WAN Security Architectures for Salesforce. Journal of International Crisis and Risk Communication Research, 63–71. <https://doi.org/10.63278/jicrcr.vi.3329>
- [8] Konakalla, K. (2024). Data protection and monitoring in Salesforce using Shield. Zenodo. <https://doi.org/10.5281/zenodo.13995996>

-
- [9] International Journal of Leading Research publication. (2024). International Journal of Leading Research Publication. <https://doi.org/10.70528/ijlrp>
- [10] Jahan, S. J. S., Ahmad, F., & Haroon, M. (2023). Protecting Sensitive Data in Salesforce – a Multi-Layered Security approach. SSRN Electronic Journal. <https://doi.org/10.2139/ssrn.4508548>