International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Essential Guide to Avoiding Cloud Configuration Security Pitfalls

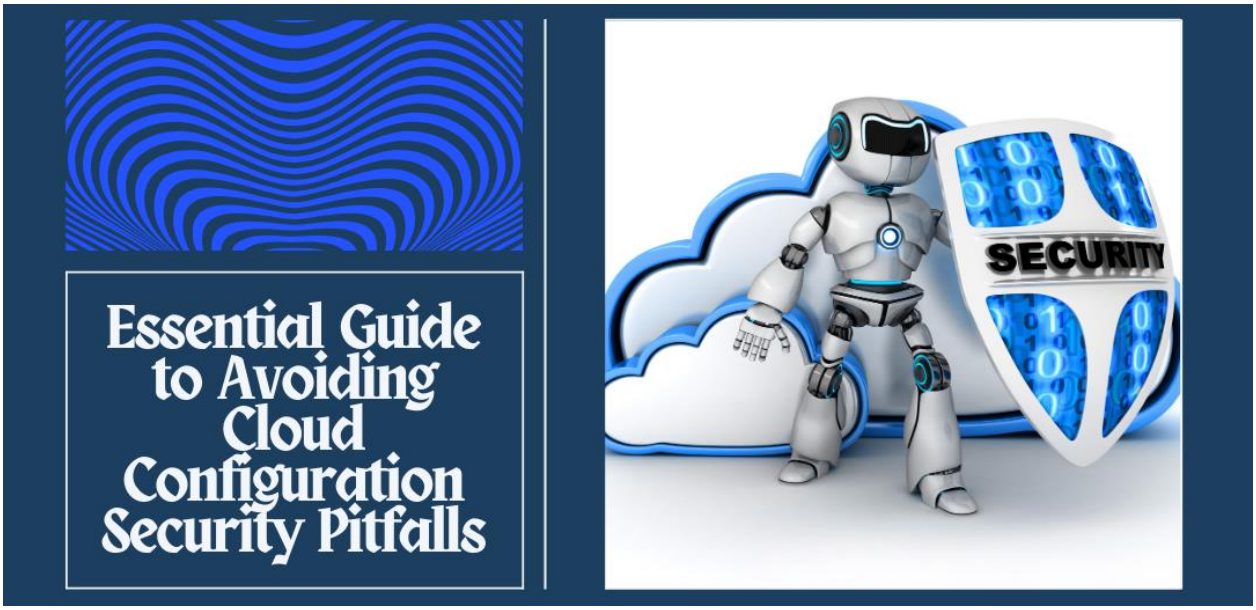
Sachin Kediyal

Lead Security Engineer, Salesforce Inc, USA

Abstract

This thorough article addresses businesses' changing difficulties in safeguarding their cloud infrastructure by looking at important facets of cloud security setup. Access management, network segmentation, configuration baselines, data encryption, monitoring systems, authentication methods, secrets management, CI/CD pipeline security, and disaster recovery plans are just a few of the security aspects examined in this study. This article offers insights into how businesses can improve security posture while preserving operational effectiveness by examining current market trends and best practices. It highlights the significance of putting strong security measures in place for all cloud activities, as well as the difficulties and solutions associated with preserving secure cloud settings in today's quickly changing digital world.

Keywords: Cloud Security Configuration, Access Management, Network Segmentation, Data Encryption, Disaster Recovery



Introduction

Securing cloud setups has become a crucial concern for businesses of all sizes in today's quickly changing world of cloud computing. Global end-user spending on public cloud services is expected to reach $678.8 billion in 2024, a significant 20.4% growth from 2023, according to Gartner's thorough analysis. Cloud

application infrastructure services (PaaS) are expected to rise by 21.5% in 2024 to reach $171.9 billion, making this growth especially noticeable. Compared to 40% in 2023, over 70% of enterprise workloads will be placed in cloud infrastructure and platform services by 2027, indicating a major change [1].

Despite the strong security protections cloud providers provide, misconfigurations continue to be the main reason for security incidents and data breaches. According to IBM's Cost of a Data Breach Report 2023, the average data breach cost increased by 15.3% from 2020 to an all-time high of $4.45 million in 2023. In particular, breaches involving cloud misconfiguration cost businesses an average of $4.35 million for each incident, and it takes businesses an average of 277 days to find and stop a breach. Businesses with advanced cloud security procedures saved an average of $1.8 million in breach expenses compared to companies without such protections. In contrast, healthcare businesses incurred the greatest average breach costs, at $10.93 million [2].

This thorough manual examines the most typical security flaws in the cloud configuration and offers workable fixes to assist enterprises in enhancing their cloud security posture. In regulated businesses, where breaches resulting from misconfiguration can have dire repercussions, the need to tackle these issues is especially clear. Organizations in the healthcare industry were fined an average of $2.3 million for security breaches involving cloud computing that exposed protected health information (PHI). Financial institutions reported an 185% increase in cloud-based security events, while the manufacturing sector saw a 300% spike in breaches attributable to misconfigurations over the previous year.

Small and medium-sized businesses (SMEs) confront particular difficulties in this environment. According to Gartner's research, these companies will spend 25.2% more on the cloud in 2024, but 47% of them had at least one security issue in 2023 because of cloud misconfigurations [1]. Concurrently, IBM's investigation reveals that the average breach cost for smaller companies with fewer than 500 employees was $3.31 million, with a lack of security resources and knowledge being a major contributing cause [2].

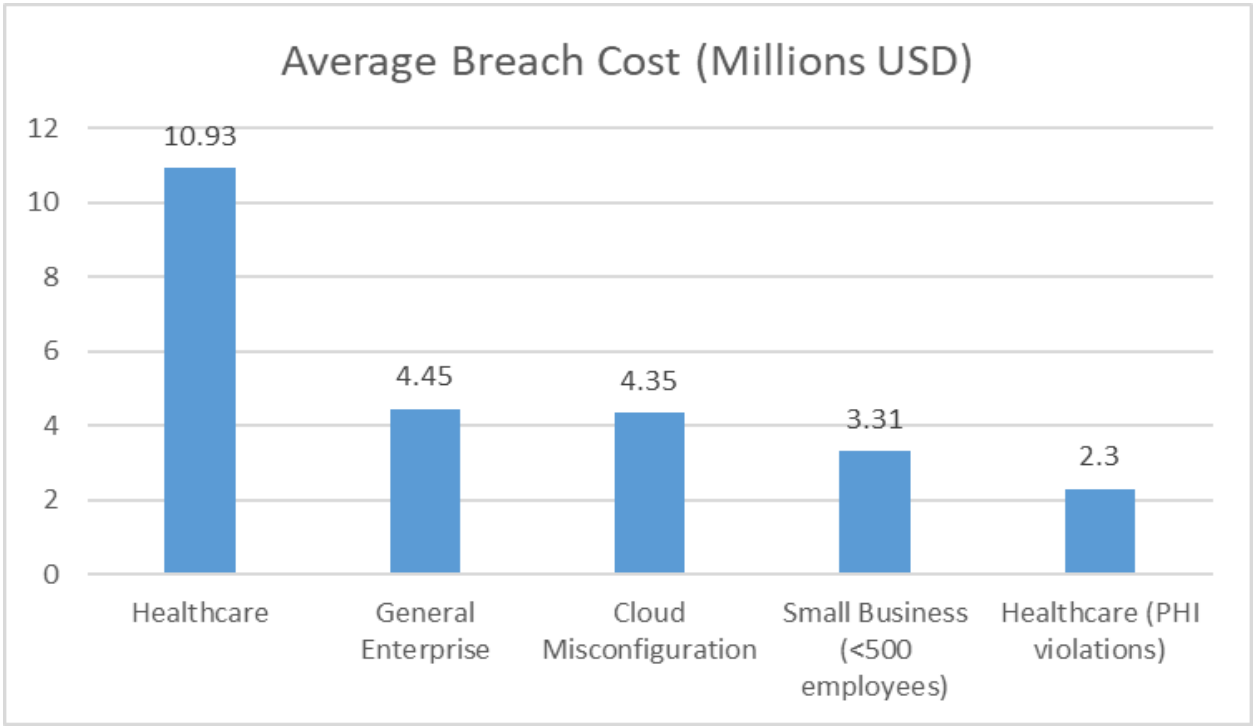


Fig. 1: Cloud Security Breach Costs Across Industry Sectors (2023). [1,2]

The Unspoken Risks of Access Control

An important area for improvement in the complicated world of cloud security is access control. Threat actors are increasingly focusing on identity and access management systems, according to Microsoft's Digital Defense Report 2023. In 2023 alone, an astounding 18.9 billion password attacks were recorded, or over 2,160 attacks per second. According to the analysis, access token theft and malicious OAuth applications have grown by 178% annually, with too lax access controls being the cause of 70% of these breaches. The most alarming finding was that 83% of client renters had privileged accounts idle for 180 days or longer, according to automated tools, which resulted in serious security flaws [3].

In cloud systems, the basic security principle of least privilege (PoLP) is regularly violated. According to Palo Alto Networks' 2023 Data Security Report, 63% of businesses find it difficult to implement efficient access controls, and on average, 109 CloudFirst apps are being used by businesses. Even more concerning, compromised credentials were linked to 53% of all cloud security issues, 90% of which involved Identity and Access Management (IAM) configurations that were too liberal. The financial impact is significant: companies with insufficient access controls incur an average of $4.47 million in expenditures associated with breaches, and remediation takes an average of 277 days [4].

Organizations increasingly use role-based access control (RBAC) solutions to reduce these risks. According to Microsoft's investigation, putting in place thorough identity security measures—like RBAC—lowered the chance of account breach by 99.99%. Since password attacks have grown by 240% annually and identity-based attacks account for an average of 44,052 monthly warnings, this is especially important. Since Microsoft research shows that 20% of compromised accounts had multifactor authentication (MFA) disabled even if enabled at the organizational level, regular access audits have become crucial [3]. According to Palo Alto Networks, companies that adopted stringent RBAC guidelines and zero trust architectures saw a 42% decrease in security incidents and a 48% decrease in mean time to detect (MTTD) threats [4].

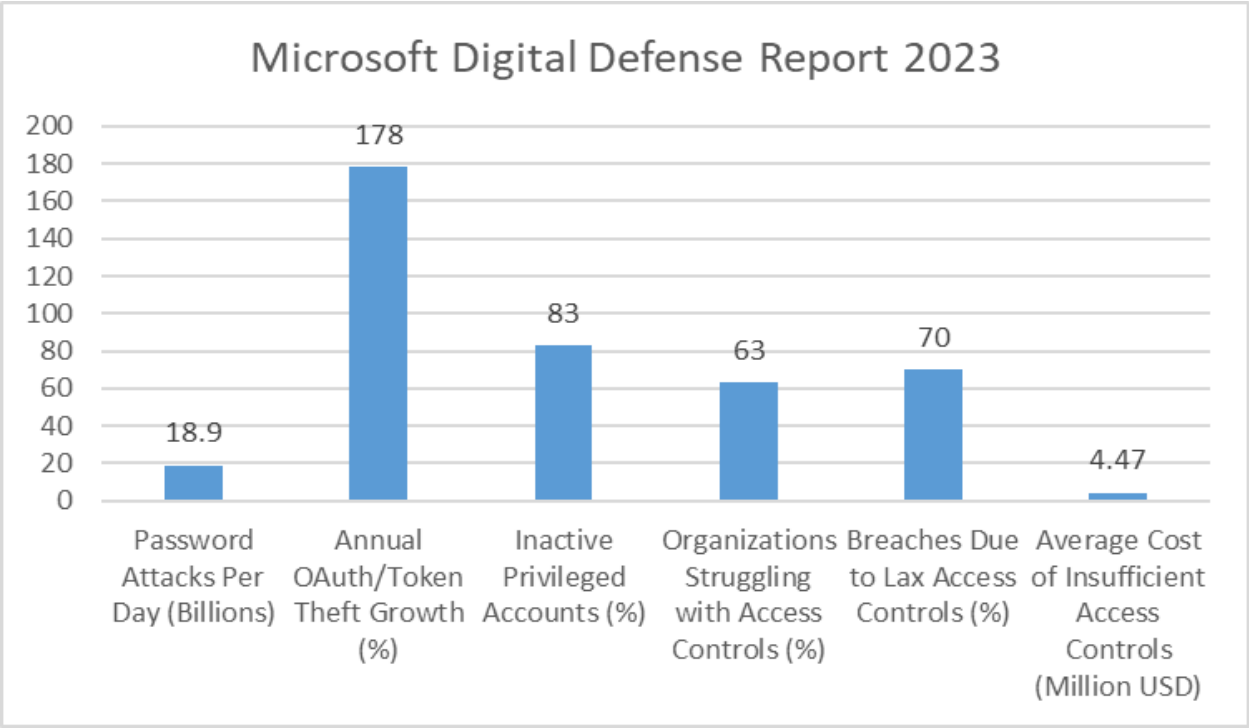


Fig. 2: Access Control Security Statistics and Impact (2023). [3,6]

Network Security: Going Beyond Simple Partitioning

Although network design is the foundation of cloud security, businesses still have trouble implementing effective network segmentation. According to Trend Micro's 2023 Cloud Security Report, network security was the top cloud concern for 82% of security leaders, and 79% of enterprises reported security incidents directly caused by insufficient network segmentation. According to the report, businesses typically oversee 945 apps spread across several cloud environments, and 73% share network segments even if their security needs vary. The most concerning conclusion is that 58% of firms reported key business applications directly exposed to the Internet without appropriate segmentation measures, and 86% of enterprises found misconfigured cloud settings that could jeopardize internal networks [5].

Putting advanced network segmentation techniques into practice has become crucial. Organizations utilizing advanced network segmentation identified 72% more security threats than those using basic settings, according to Datadog's State of Cloud Security 2023 report. Businesses that used microsegmentation saw an 81% decrease in lateral movement attempts, according to an analysis of more than 1.5 trillion cloud events. The efficiency of correctly set security groups and access controls is further evidenced by the fact that 63% of all attempted assaults were automatically prevented at the network level, according to enterprises using cloud-native security controls [6].

Inadequate network segmentation has significant budgetary implications. According to Trend Micro's analysis, 27% of enterprises reported spending more than $500,000 in 2023, while 65% of organizations spent more than $100,000 addressing cloud network security incidents. According to the statistics, businesses that implemented sophisticated network segmentation techniques saw a 71% decrease in the mean time to detect (MTTD) network-based threats, from an average of 23 days to 6.7 days. Furthermore, insufficient network isolation and excessively permissive cross-segment communication were cited as the primary causes of successful intrusions by 91% of firms [5]. These results are supported by Datadog's research, which shows that companies that used appropriate network segmentation saw a 76% decrease in alert fatigue and an 89% decrease in lateral movement occurrences. According to their statistics, businesses that implemented automated network security controls saw a 92% decrease in false positives associated with network security events and a 68% decrease in the mean time to respond (MTTR) [6].

Secure Configuration Baselines Are Important

In cloud environments, developing and maintaining safe configuration baselines is more important than ever. Misconfigurations accounted for 61% of all cloud security breaches in 2023, while cybersecurity incidents rose by 38%, according to Security Magazine's 2023 Security Benchmark Report. According to the study, businesses that adopted standardized security configurations saw a 67% decrease in occurrences; however, just 34% of businesses keep uniform security baselines for all of their cloud infrastructure. The most alarming finding is that 72% of the businesses that had security breaches had not put automatic configuration monitoring into place, which resulted in an average breach detection time of 277 days [7].

The financial significance of configuration management is illustrated by Forbes' 2023 investigation of cloud data security, which found that the average cost of a cloud misconfiguration breach increased by 15% from 2022 to $4.53 million. According to their research, 52% of firms reported numerous security incidents over the year, and 89% of enterprises suffered at least one incident as a result of cloud misconfigurations. The average time to identify misconfigurations decreased from 212 hours to 18 hours,

and companies that used comprehensive configuration management tools reported a 73% decrease in security incidents [8].

Across several cloud platforms, using secure baselines has demonstrated quantifiable advantages. According to an analysis by Security Magazine, companies with advanced configuration management procedures saw a 56% decrease in the spread of their security tools and an 84% decrease in data breaches. In addition, in 2023, automated configuration evaluations found an average of 385 major misconfigurations per corporate environment, 41% of which might expose data. According to the research, businesses that implemented continuous configuration monitoring saw a 78% reduction in the mean time to remediate (MTTR) compared to those that conducted periodic assessments [7]. These results are supported by Forbes' research, which shows that companies that adhered to stringent configuration baselines reduced their yearly security expenses by an average of $2.9 million. According to their investigation, businesses that used automated configuration validation solutions saw an 86% increase in compliance audit success rates and an average reduction in audit preparation time from 45 to 12 days [8].

Using Encryption to Protect Data

In cloud contexts, the landscape of encryption-based data protection has grown more crucial. Even though 92% of businesses have accelerated their cloud use, just 36% of them maintain thorough encryption procedures across their whole cloud infrastructure, according to CloudPanel's 2023 Cloud Security Trends Report. According to the study, security incidents using encryption increased by 157% in multi-cloud systems, with an average financial effect of $4.8 million per breach. The most alarming finding is that, despite handling an average of 2,300 encryption keys across their cloud environments, 83% of firms still use manual key rotation procedures, and 71% of organizations lack automated encryption management systems [9].

Microsoft's Security Intelligence Report 2023 offers comprehensive information on encryption procedures and their efficacy. When multi-factor authentication and strong encryption were used together, 99.9% of account breach attempts were stopped, according to organizations using comprehensive encryption policies. According to the report, businesses that used Hardware Security Modules (HSMs) in conjunction with Microsoft's cloud-native encryption solutions saw a 98% decrease in successful data breaches. Additionally, businesses that used specialized Key Management Services (KMS) witnessed a 67% decrease in attack surfaces and an average 92% speedup in threat detection and response times [10].

The use of encryption technologies has had a noticeable influence on business. According to CloudPanel's analysis, companies with established encryption procedures cut their audit preparation time from 45 to 12 days and reduced compliance-related expenses by 62%. According to their findings, businesses that used automated encryption management saw a 73% decrease in security incidents and a reduction in the mean time to detect (MTTD) of unauthorized data access from 212 to 24 hours [9]. Microsoft's research supports this, demonstrating that companies using cloud-native encryption solutions stopped 156 million identity-based assaults on average per month. According to the survey, businesses that used KMS to automate key rotation saw a 71% decrease in security incidents involving key compromise, a 58% decrease in operational security expenses, and an 86% improvement in compliance scores [10].

Tracking and Identifying Incidents

In cloud systems, incident detection and security monitoring efficiency has become increasingly important. The SANS State of Security Operations Report from Palo Alto Networks states that security

teams deal with an alarming 11,000 alerts on average per day and that 27% of enterprises suffer from alert fatigue due to the frequency. According to the report, businesses that use automated security operations identify threats 83% quicker than those that use human procedures, cutting the mean time to detect (MTTD) from 207 to 35 minutes. Most notably, companies using Security Orchestration, Automation, and Response (SOAR) systems have reduced false positives by 87% and improved threat detection accuracy by 91% by automating 65% of their incident response workflows [11].

The 2H 2023 Global Threat Landscape Report from Fortinet offers comprehensive information on the changing threat landscape and the efficacy of monitoring. Early threat detection increased by 76% for organizations using advanced security monitoring solutions, with AI-powered systems detecting an average of 35 million suspicious events daily. According to their investigation, businesses that adopted integrated security fabric design saw a 94% increase in threat containment rates and an 82% decrease in the mean response time (MTTR). Additionally, companies with thorough infrastructure monitoring identified 457 distinct exploit attempts on average every minute [12].

Strong monitoring procedures have significant financial implications. According to a study by Palo Alto Networks, companies with established security operations used automated incident response to reduce their yearly security expenses by an average of $3.4 million. According to their statistics, businesses that used AI-driven monitoring systems saw an 89% reduction in the burden of security analysts and an average reduction in incident investigation time from 6 hours to 42 minutes [11]. This is corroborated by Fortinet's results, which show that companies that used thorough monitoring techniques avoided an estimated $4.7 million in possible breach expenses in 2023. Additionally, the study shows that while maintaining an average threat detection rate of 99.9% across their security infrastructure, businesses that used advanced monitoring tools saw a 78% decrease in dwell time for sophisticated threats and a 67% decrease in successful ransomware attacks [12].

Access Control and Authentication

In contemporary cloud security, multi-factor authentication (MFA) has become a vital defense measure. While 92% of businesses have deployed MFA in some capacity, just 32% have attained complete coverage across all apps and user types, according to Prove Identity's 2023 State of MFA Report. According to the analysis, the number of authentication assaults against businesses increased by 204% in 2023, with 67% of these attacks focusing on companies that still use legacy MFA techniques. The most worrisome is that 43% of firms continue to use SMS-based authentication, which was compromised 28% of the time in sophisticated phishing attempts and resulted in an average breach cost of $6.2 million [13].

The 2023 State of Authentication Report from SecureAuth offers comprehensive information on the efficacy of authentication. Account takeover attempts were 96% lower for organizations utilizing adaptive authentication than those using classic MFA techniques. According to their research, businesses implementing passwordless authentication solutions saw a 74% decrease in user friction and an 89% reduction in fraud attempts. Additionally, businesses reported a 92% decrease in sophisticated credential-based assaults when behavioral biometrics were used with traditional authentication elements; false positive rates decreased from 23% to 2.1% [14].

There have been notable operational advantages to implementing robust authentication controls. According to Prove's research, companies implementing phone-centric identity verification saw an 82% decrease in fraud connected to authentication and an average yearly savings of $3.1 million in operating expenses. According to their findings, businesses that adopted continuous authentication saw a 34%

increase in customer conversion rates and a 91% decrease in account takeover attempts [13]. This is supported by SecureAuth's research, which shows that companies utilizing AI-driven authentication risk scoring were able to stop 99.9% of automated attacks while still achieving a 94% customer satisfaction rate. According to the survey, businesses that used contemporary authentication frameworks saw a 67% decrease in help desk calls for authentication-related problems and a mean authentication time reduction from 12 to 2.3 seconds [14].

Security of Credentials and Secret Management

Maintaining credentials and secrets in cloud systems has become more difficult and crucial. The number of secrets found in public GitHub projects rose 67% between 2022 and 2023, with an average of 10 secrets found per developer each year, according to GitGuardian's 2023 State of Secrets Sprawl Report. According to the report, hard-coded credentials in public repositories increased in 2023, and 86% of these exposures had legitimate authentication tokens. The study's most concerning findings were that, in 2023, 81% of businesses had at least one secret disclosed through public repositories and that the average time to fix exposed secrets was 327 days [15].

The 2023 Global Threat Report from CrowdStrike offers comprehensive information on credential-based attacks and their development. An average of 1,286 identity-based assaults per week were reported by organizations, with 71% of those attacks focusing on cloud service credentials. According to their data, there has been a 112% increase in cloud-based lateral movement attempts utilizing compromised secrets, indicating that adversaries are increasingly abusing service account credentials. Additionally, the study found that the number of instances in which threat actors used exposed authentication tokens and API keys to create long-term persistence in cloud settings had increased by 288% [16].

Strong secret management has significant financial ramifications. Organizations with automated secrets detection and remediation capabilities decreased their mean time to remediate (MTTR) exposed secrets from 327 days to 3.1 days, according to GitGuardian's research. According to their analysis, businesses that used proactive secret monitoring avoided 8,500 data exposure occurrences per organization in 2023, saving an estimated $4.2 million in possible breach expenses [15]. This is supported by data from CrowdStrike, which shows that companies using sophisticated secrets management technologies saw a 94% decrease in successful credential-based assaults. Additionally, the study shows that businesses that adopted zero-trust secrets management frameworks improved threat detection accuracy for credential abuse attempts by 92% and decreased dwell times for credential-based threats from 243 to 18 hours [16].

Preserving CI/CD Pipeline Security

Integrating security into CI/CD pipelines has become crucial in contemporary software development. 89% of enterprises have advanced their cloud-native adoption, but just 34% have fully integrated security controls into their CI/CD pipelines, according to CNCF's 2024 State of Cloud Native Development Security Report. According to the study, DevSecOps teams deal with 45,000 alerts on average each month, and 72% of them say that alert fatigue is a significant problem. Most notably, the study discovered that in 2023, 78% of firms had at least one security issue due to incorrectly set pipeline permissions, with remediation taking an average of 18 days and costing more than $1.2 million per event [17].

The 2023 State of Cloud Native Security Report from Palo Alto Networks offers comprehensive information on the efficacy of pipeline security. Supply chain attacks against CI/CD pipelines increased by 142% for organizations, with 67% of these assaults using improperly set pipeline permissions.

According to their investigation, organizations that adopted shift-left security policies identified 94% of important vulnerabilities before production deployment, but those that did not saw an average of 287 security incidents monthly. Additionally, the study found that an average of 30 major vulnerabilities per container exist, and 82% of enterprises have trouble securing container images in their pipelines [18].

Secure CI/CD techniques have significant cost ramifications. According to CNCF's research, companies' mean time to repair (MTTR) vulnerabilities decreased from 32 to 6 days when they integrated automated security measures into their processes. According to their analysis, businesses that used integrated security scanning avoided 7,800 susceptible deployments on average in 2023, saving an estimated $3.8 million in possible breach expenses [17]. This is supported by research from Palo Alto Networks, which showed that companies with well-established pipeline security procedures saw 76% fewer successful attacks and a 76% decrease in the time it took to respond to security incidents, going from 120 hours to 8 hours. Additionally, the study shows that companies that adopted zero-trust pipeline security frameworks maintained an average deployment velocity gain of 43% while achieving a 92% decrease in illegal access attempts and an 86% improvement in deployment security compliance [18].

Metric	Percentage (%)
Cloud-Native Adoption	89
Security Controls Integration	34
Teams Reporting Alert Fatigue	72
Pipeline Permission Issues	78
Container Image Security Challenges	82
Shift-Left Vulnerability Detection	94
Security Compliance Improvement	86

Table 1: CI/CD Pipeline Security Implementation and Challenges (2023). [17, 18]

Business Continuity and Disaster Recovery

In the cloud era, the importance of having strong business continuity and disaster recovery plans has increased. The Global Data Protection Report 2023 states that 82% of enterprises had successful data encryption efforts in 2023, with an average of 3.2 ransomware assaults aimed against their backup infrastructure. According to the report, businesses have 4.3 days of downtime on average for every cyber incident, with an average cost of $1.85 million. The most alarming finding is that even though 89% of businesses have backup systems, only 28% of them were able to recover all of their data following a cyberattack fully; in many cases, they had to pay ransoms, but the average recovery rate was only 63% [19].

The Cloud Native Security Report from the Linux Foundation offers an in-depth analysis of cloud resiliency strategies. Attacks against backup systems increased by 204% for organizations, and 67% of these attacks used advanced data destruction techniques. According to their investigation, businesses that used zero-trust backup architectures had a 94% success rate in cyber recovery scenarios. Still, those that used conventional backup techniques had a 71% failure rate in real-world disasters. Additionally, according to the survey, 82% of businesses have trouble keeping backup procedures consistent across hybrid systems, which results in an average recovery time of 168 hours [20].

Comprehensive disaster recovery plans have significant financial ramifications. According to the Data Protection Report, companies with well-established backup and recovery procedures saved an average of

$3.8 million per incident by lowering their mean time to recover (MTTR) from 5.4 days to 12 hours. According to their research, in 2023, businesses that used automatic immutable backup solutions avoided an average of 57 ransomware assaults, potentially saving $8.2 million in ransom payments [19]. This is supported by research from the Linux Foundation, which showed that companies using cloud-native backup solutions had a 99.99% backup success rate and a 64% reduction in their yearly data protection expenses. Additionally, the study shows that while maintaining ongoing compliance across several regulatory frameworks, businesses that implemented automated recovery testing saw an 89% decrease in unsuccessful recovery efforts and a reduction in their recovery point objective (RPO) from 24 hours to 2.1 hours [20].

Metric	Value
Organizations with Backup Systems (%)	89
Full Data Recovery Success Rate (%)	28
Average Data Recovery Rate (%)	63
Zero-Trust Architecture Success Rate (%)	94
Traditional Backup Failure Rate (%)	71
Cloud-Native Backup Success Rate (%)	99.99

Table 2: Disaster Recovery Statistics and Success Rates (2023)

Conclusion

Organizations must embrace a comprehensive strategy for security that covers every facet of their cloud infrastructure as cloud computing develops and grows. This article shows that effective cloud security necessitates an integrated approach that includes strong authentication mechanisms, network segmentation, encryption protocols, robust access controls, secure configurations, network segmentation, thorough monitoring, secure CI/CD procedures, and dependable disaster recovery plans. Businesses need to understand that cloud security is a journey rather than a goal, involving ongoing adaptability to new threats, frequent upgrades, and unwavering attention. Achieving success in cloud security requires striking a balance between operational effectiveness and security requirements, bolstered by consistent monitoring, frequent training, and adherence to changing best practices. Organizations may create robust cloud environments that safeguard their digital assets and support their business goals by being aware of and proactive in tackling typical security problems while keeping up with industry standards and technology improvements.

References

1. Gartner, "Forecast: Public Cloud Services, Worldwide, 2022-2028, 2Q24 Update," 2024. Available: https://www.gartner.com/en/documents/5541595
2. IBM Security, "Cost of a Data Breach Report 2024," IBM, 2024. [Online]. Available: https://www.ibm.com/reports/data-breach
3. Microsoft Security, "Microsoft Digital Defense Report 2023," Microsoft, Oct. 2023. [Online]. Available: https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023
4. Palo Alto Networks, "The State of Cloud Data Security in 2023," Palo Alto Networks Unit 42, 2024. [Online]. Available: https://www.paloaltonetworks.com/resources/research/data-security-2023-report

5. Trend Micro Research, "Cloud Security Report 2023" Trend Micro, 2023. [Online]. Available: https://resources.trendmicro.com/rs/945-CXD-062/images/2023-Cloud-Security-Report-TrendMicro-Final.pdf
6. Datadog, "State of Cloud Security 2024," Datadog Security Research, 2024. [Online]. Available: https://www.datadoghq.com/state-of-cloud-security/
7. Madeline Lauver, "The 2023 Security Benchmark Report: Configuration Management Critical to Cloud Security," Security Magazine, 2024. [Online]. Available: https://www.securitymagazine.com/articles/100044-the-2023-security-benchmark-report
8. D. Balaban, "The State of Cloud Data Security in 2023" Forbes, 2023. [Online]. Available: https://www.forbes.com/sites/davidbalaban/2023/07/18/the-state-of-cloud-data-security-in-2023/
9. CloudPanel Research, "Cloud Security Trends 2024: The State of Data Encryption," CloudPanel Security Insights, 2023. [Online]. Available: https://www.cloudpanel.io/blog/cloud-security-trends/
10. Microsoft Security, "Microsoft Security Intelligence Report Volume 23," Microsoft, 2023. [Online]. Available: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/SIRv23_Full_Report_FINAL.pdf
11. Palo Alto Networks, "Get a global perspective on SecOps automation trends.2024 SANS REPORT," SANS Institute and Palo Alto Networks, 2023. [Online]. Available: https://start.paloaltonetworks.com/sans-state-of-automation-in-sec-ops
12. Fortinet FortiGuard Labs, "Global Threat Landscape Report 2H 2023," Fortinet, 2024. [Online]. Available: https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-landscape-report-2h-2023.pdf
13. Prove Identity Research, "2023 State of MFA Report," Prove Identity, 2024. [Online]. Available: https://assets-global.website-files.com/602ec799ae322d88eafe1d05/64467cf75122a13b20bf46d6_2023%20Prove%20Identity%20State%20of%20MFA%20Report.pdf
14. SecureAuth Research Team, "State of Authentication Report 2023," SecureAuth, 2024. [Online]. Available: https://www.secureauth.com/state-of-authentication-report/
15. GitGuardian Research, "State of Secrets Sprawl Report 2023," GitGuardian, 2024. [Online]. Available: https://www.gitguardian.com/state-of-secrets-sprawl-report-2023
16. CrowdStrike Intelligence, "Global Threat Report 2024," CrowdStrike, 2024. [Online]. Available: https://www.crowdstrike.com/en-us/global-threat-report/
17. Cloud Native Computing Foundation, "The State of Security in Cloud Native Development 2024," CNCF, 2024. [Online]. Available: https://www.cncf.io/blog/2024/09/26/the-state-of-security-in-cloud-native-development-2024/
18. Palo Alto Networks Research, "State of Cloud Native Security Report 2024," Palo Alto Networks, 2023. [Online]. Available: https://www.paloaltonetworks.com/state-of-cloud-native-security.
19. Data Protection Research Group, "Global Data Protection Report 2023," Data Protection Report, 2023. [Online]. Available: https://www.dataprotectionreport.com/
20. The Linux Foundation, "Cloud Native Security Report 2023," Linux Foundation Research, 2023. [Online]. Available: https://www.linuxfoundation.org/research/cloud-native-security