INTERNATIONAL JOURNAL OF ADVANCED RESEARCH
ISSN: 3106-7980: 3106-7972
Volume 3, Issue 3, 2026

CLOUD SECURITY IN THE ERA OF GENERATIVE AI: THREAT ESCALATION, BREACH ECONOMICS, AND DEFENSIVE AUTOMATION

Muhammad Awais Sajid[*1], Khalid Hamid[2], Muhammad Waseem Iqbal[3], Malik Waqar Ali[4], Abdul Qayyum[5]

[*1] *Department of Information Security, Superior University Lahore, 54000, Pakistan*
[2,3] *Department of Information Technology, Superior University Lahore, 54000, Pakistan*

[*1]su92-msisw-s26-003@superior.edu.pk, [*1]mawais.sajid001@gmail.com
[2]khalid6140@gmail.com, [3]waseem.iqbal@superior.edu.pk, [4]waqaralibcs076@gmail.com,
[5]abdulqayyumnns@gmail.com

DOI: https://doi.org/10.5281/zenodo.21738476

Keywords
cloud computing security; AI-enhanced cyber threats; data breach economics; zero-trust architecture; identity and access management; cloud intrusion detection

Article History
Received: 20 May 2026
Accepted: 11 July 2026
Published: 31 July 2026

Corresponding Author: *
Muhammad Awais Sajid

Abstract

Cloud computing is the infrastructure of choice for enterprise IT these days. This report covers the security problems, attack vectors and countermeasures in cloud computing throughout 2020 to first quarter of 2026. It relies on industry reporting from IBM, CrowdStrike, Thales, SentinelOne, Fortune Business Insights, Gartner and Check Point Research, and peer-reviewed academic material published between 1999 and 2026, according to a PRISMA-informed systematic review approach.

For Q1 2026 alone, global cloud infrastructure spending reached USD 129 billion, a 35% year-over-year increase, with Amazon Web Services, Microsoft Azure, and Google Cloud collectively commanding 63% of the market (Synergy Research Group, cited in Statista, 2026). The cloud security market itself was valued at USD 60.37 billion in 2026, compared to USD 51.11 billion in 2025 (Fortune Business Insights, 2026). In 2025, cloud-conscious intrusions increased 37% year over year, with a 266% increase among state-sponsored actors expressly targeting cloud settings, while the average eCrime breakout time declined to 29 minutes (CrowdStrike, 2026). The Thales 2026 Data Threat Report revealed that only 47% of sensitive cloud data is encrypted, cloud storage and cloud-delivered applications continue to be the most commonly targeted attack surfaces, and 67% of respondents identified credential theft as a significant attack strategy.

The global average cost of a data breach remains USD 4.44 million (IBM, 2025), the most recent verified figure available at the time of writing; IBM had not yet published its 2026 edition as of July 2026. Organizations using AI-assisted security saved an average of USD 1.9 million per breach and reduced resolution time by 68 days. Ransomware activity, which was reported as increasing 126% in Q1 2025, exhibits a dramatically different pattern one year later: Check Point Research recorded 2,122 ransomware victims in Q1 2026 compared to 2,285 in Q1 2025 – a headline drop that becomes a modest 5.3% rise when removing a one-off mass-exploitation campaign from both quarters. This research documents this transition

precisely, as it fundamentally impacts how the trajectory of ransomware risk should be described moving into 2026.
This version of the study includes the updated literature review, research framing, methods and outcomes (data, tables and figures) to Q1 2026. There is transparency throughout on when assertions are based on verified 2026 data and where they are the latest verifiable information from 2025.

1. Introduction

Cloud computing (CC) is defined as the on-demand delivery of computer services such as servers, storage, networking, applications over the internet [3]. Which is why it's become the de-facto operating model for enterprise IT - it lowers upfront capital cost, scales elastically with demand, and allows organizations build infrastructure in minutes instead of months (Khaliq et al., 2024). The same elasticity and shared-responsibility model that makes cloud computing so appealing also obscures the line between what a cloud provider is responsible for securing and what a customer needs to secure, and it is at this boundary where most cloud security incidents begin (Hamid et al., 2023).

By 2025, 93% of businesses will have multi-cloud or hybrid cloud architecture and cloud-based assets will be involved in about 45% of all reported data breaches worldwide (CompareCheapSSL, 2025). Instead of traditional malware, attackers are now attacking cloud-native services directly, with credential stuffing, API abuse and, increasingly, AI-generated phishing and deepfake impersonation (Ibrar et al., 2024). Misconfiguration, poor identity governance, and unpatched software are the top three root causes of cloud compromise, a pattern that holds true across every major industry report we studied for this research, from the earliest sources in 2014 to the most recent data from Q1 2026 (Hamid et al., 2023).

In the 2025-2026 danger landscape, two innovations set it apart from years prior. Generative AI has emerged as a tool for both attackers and defenders. Attackers leverage it to speed up reconnaissance, phishing, and credential harvesting, while security teams employ it to reduce detection and reaction times (Riaz et al., 2025) . Second, identity has replaced the network perimeter as the primary control plane to be compromised by attackers. Stolen credentials and abused valid accounts, not exploited software flaws, now account for most cloud breaches (CrowdStrike, 2026). This paper combines the state of the art of research in the area of cloud security and industry data around these two developments. The underlying statistics have been updated to the first quarter of 2026 where independently verifiable data was available. Where no newer verified data was available the most recent published figures have been retained and this is stated explicitly (Hamid et al., n.d.).

2. Literature Review

2.1 Foundational and Early Academic Work

Mell and Grance (2011) proposed the NIST definition of cloud computing, which remains the basis for most subsequent research. They describe five fundamental criteria and three service models: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Bro, an early system for passive, real-time network intrusion detection, was described by. Its design principles, based on continuous traffic inspection rather than perimeter gatekeeping, anticipated the identity- and telemetry-centric monitoring architectures that dominate cloud security practice today. Bendovschi (2015) tracked the progression of cyberattack patterns and concluded that the sophistication of the attacker would continue to exceed traditional perimeter protection, a forecast validated by the move to identity-based cloud intrusion described in the 2026 threat intelligence section.

Khan (2016) provided an early thorough review of cloud security issues, and Kumar and Dave (2017) highlighted data isolation, authentication, and access control as the major cloud security

hurdles at that time. A decade later, these challenges still present the most concern: misconfiguration of identity and access management (IAM) and insecure key handling continue to dominate cloud vulnerability reports, and by 2025-2026 compromised or misused identities were responsible for the majority of cloud breaches (SentinelOne, 2026; CrowdStrike, 2026).

2.2 Cloud Architecture, Attacks, and Defensive Models

Nguyen, Jaatun and Prasad (2014), for example, argued that effective data encryption and access control are basic cloud defenses. That recommendation is even more urgent, not less: The Thales 2026 Data Threat Report found that only 47% of sensitive data in the cloud is encrypted, down from 51% a year ago, even as 67% of respondents cited credential theft and compromised secrets as a top attack technique (Thales, 2026). More recent applied work has started to explore AI-assisted approaches to this same encryption gap: Zafar, Hamid, Kafayat, Iqbal, Nazir, and Ghani (2023) proposed an AI-based cryptographical framework for network security, demonstrating a concrete direction for closing the persistent encryption shortfall documented above, rather than simply restating that it exists (Zafar et al., 2023).

Cloud application security has been acknowledged as an important and developing concern (Wang, Chang and Liang, 2016). That concern has introduced a new dimension: IBM's 2025 Cost of a Data Breach Report found that unauthorized "shadow AI" tools were involved in 20% of breaches at organizations studied (Hamid et al., 2025), adding an average of USD 670,000 to breach cost, and that 97% of AI-related breaches happened at organizations lacking basic AI access controls (IBM, 2025). A layered security model that integrates encryption, access control, and intrusion detection was proposed by Sahai and Malhotra (2017). 2025 data provides empirical evidence for that layered approach, where organizations that heavily utilize AI-assisted security save USD 1.9 million per breach on average and reduce the breach lifecycle by 68 days compared to organizations that do not (IBM, 2025).

Alhenaki et al. (2019) surveyed critical cloud attack types and corresponding defenses; their taxonomy is still broadly applicable, although the balance among attack types has shifted dramatically towards identity-based access rather than direct exploitation, with cloud-aware intrusions up 37% year over year in 2025 and valid-account abuse accounting for 35% of cloud incidents tracked by CrowdStrike (2026). Thushari (2022) examined privacy and security vulnerabilities in cloud domains and highlighted several under-researched gaps. This is supported by the 2026 Thales survey; 55% of organizations (2025 figure, most recent available) stated that securing cloud environments is more difficult than securing on-premises infrastructure. Subbalakshmi and Madhavi (2022) introduced the Unique Key Integrity Agreement (UKIA) approach for dynamic key generation in cloud storage. Encryption-gap data from the 2025 and 2026 Thales studies show that this class of solution is still underutilized in practice. Alqahtani and Alrajeh (2019) identified four pillars of cloud security concern: namely, data privacy, confidentiality, integrity, and availability, all of which recent breach data shows remain live issues. The 2026 Verizon Data Breach Investigations Report found that for the first time in that report's 19-year history, vulnerability exploitation surpassed stolen credentials as the single most common breach entry vector, at 31% of breaches, with credential abuse dropping to 13% (Verizon, 2026). This is a genuinely new finding, revising how initial-access risk should be prioritized going into 2026.

2.3 Applied and Domain-Specific Cloud Research

Aldowah, Al-Samarraie, and Fauzy (2019), Ali and Alourani (2021), and Ali, Manzoor, and Alouraini (2021) examined cloud adoption in educational and e-governance contexts. Adoption in these sectors has continued to grow: 45.2% of EU enterprises purchased cloud computing

services in 2023, up 4.2 percentage points from 2021 (Eurostat, cited in Brightlio, 2025), and government cloud investment was projected to approach USD 47.9 billion by 2025 (StationX, 2026). Haji, Zeebaree, Ahmed, Sallow, Jacksi, and Zeabri (2020) examined dynamic resource allocation in distributed systems; resource inefficiency remains a live problem, with organizations reportedly wasting up to 32% of cloud spend (G2, 2024). Kausar, Huahu, Hussain, Wenhao, and Zahid (2018) proposed clustering-based personalization for e-learning systems, an approach that anticipates the broader integration of AI into cloud-hosted services now underway. Varghese and Buyya (2018) predicted the rise of distributed, software-defined cloud infrastructure; that prediction has materialized at scale, with the global cloud computing market reaching an estimated USD 917.9 billion in 2026 and global cloud infrastructure spending alone reaching USD 129 billion in the first quarter of 2026 (Persistence Market Research, 2026; Synergy Research Group, cited in Statista, 2026).
The literature tells a consistent story: the specific technical vulnerabilities documented from 2014 onward (weak encryption practice, poor identity governance, application-layer exposure, resource misallocation) have not been addressed by a decade of subsequent research & tooling. What has changed is the attacker's toolbox, which is increasingly using generative AI by 2025-2026, and the defender's toolbox, which depends more and more on AI-assisted detection to reduce response times. The research gap filled by this paper is the change and its practical and financial implications.

3. Research Gap

Despite a significant amount of earlier work on cloud security architecture, encryption, and access control, three holes still present themselves in the literature listed above. First, most academic research published before 2023 disregards AI-powered attack techniques which, by 2025, accounted for a quantifiable proportion of breaches and are addressed in the latest industry reporting as a distinct, rapidly growing attack category rather than a subset of existing threats. Second, there has been scant empirical coverage in the literature on "shadow AI" governance, the use of unsanctioned AI technologies by employees without security oversight, despite this now being independently associated to a meaningful share of breach cost . Third, few studies quantify the how AI-assisted defense (automation, security AI tooling, and zero-trust enforcement) measurably alters breach cost and dwell time. 2025-2026 industry data is fairly plentiful here but peer reviewed academic synthesis is still scarce. This research aims to fill these gaps by merging the most recent verifiable industry data for 2025-2026 with the existing academic material(Delshadi et al., 2025).

4. Problem Statement

Organizations are continuing to shift critical workloads to the cloud faster than they are maturing the identity, encryption and monitoring controls required to secure them. The bottom line, which permeates every major industry report reviewed for this paper, is a widening gap between cloud adoption and cloud security maturity. Adoption is now almost universal, but fewer than half of organizations encrypt most of their sensitive cloud data, and identity-based attack techniques (credential theft, valid-account abuse) are increasingly bypassing the perimeter and access controls that most organizations still consider their primary line of defense. In this study, we examine the size of that gap with verified data through Q1 2026, and assess whether defensive measures have a proven—not projected—impact on breach frequency and cost (Delshadi et al., 2025).

5. Research Objectives

The objectives of this research are to:

- Identify the key security issues in cloud computing, including data privacy, identity and access management, and regulatory compliance, and assess how these issues have changed between 2023 and the first quarter of 2026.

- Learn about the main categories of cloud computing attacks, such as network assaults, virtualization and hypervisor attacks, application-layer attacks, and AI-enhanced attack methods (Ahmad et al., 2025).
- Measure cost and dwell time to evaluate the proven efficacy of existing counter measures like as encryption, access control, zero-trust architecture and AI-powered security automation, rather than relying on vendor claims.
- Determine the existing gaps in cloud security governance, especially in the areas of AI security budgeting, shadow AI and encryption maturity, and suggest areas for further research and practice(Akhtar et al., 2025).

6. Methodology

The research is based on a systematic literature review methodology according to the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework, complemented with a structured update pass against current industry reporting. To conduct this search of the academic literature, IEEE Xplore, ACM Digital Library, and ScienceDirect were utilized, and included publications published from 1999 to 2022 in the original review, which have been kept here without modification to their core conclusions (Tahir et al., 2025).

The databases search yielded a total of 846 records identified: 312 from IEEE Xplore, 268 from ACM Digital Library, 232 from ScienceDirect and additional 34 records identified by citation tracking and hand-searching. After removing 88 duplicate records, 758 records were screened by title and abstract, with 664 records excluded as off-topic, not in the area of cloud computing security or not available in English (Aslam et al., 2025). Of the remaining 94 full-text articles, 76 were excluded at this stage due to reasons including lack of methodological detail (28), significant overlap with findings already included (19), focus outside of cloud security specifically (15), or use of non-peer-reviewed preprints without independent validation (14). This resulted in 18 peer-reviewed academic studies from 1999 to 2022 which form the core of the literature review in Section 2. The selection process is shown in a flow diagram (Figure 1).

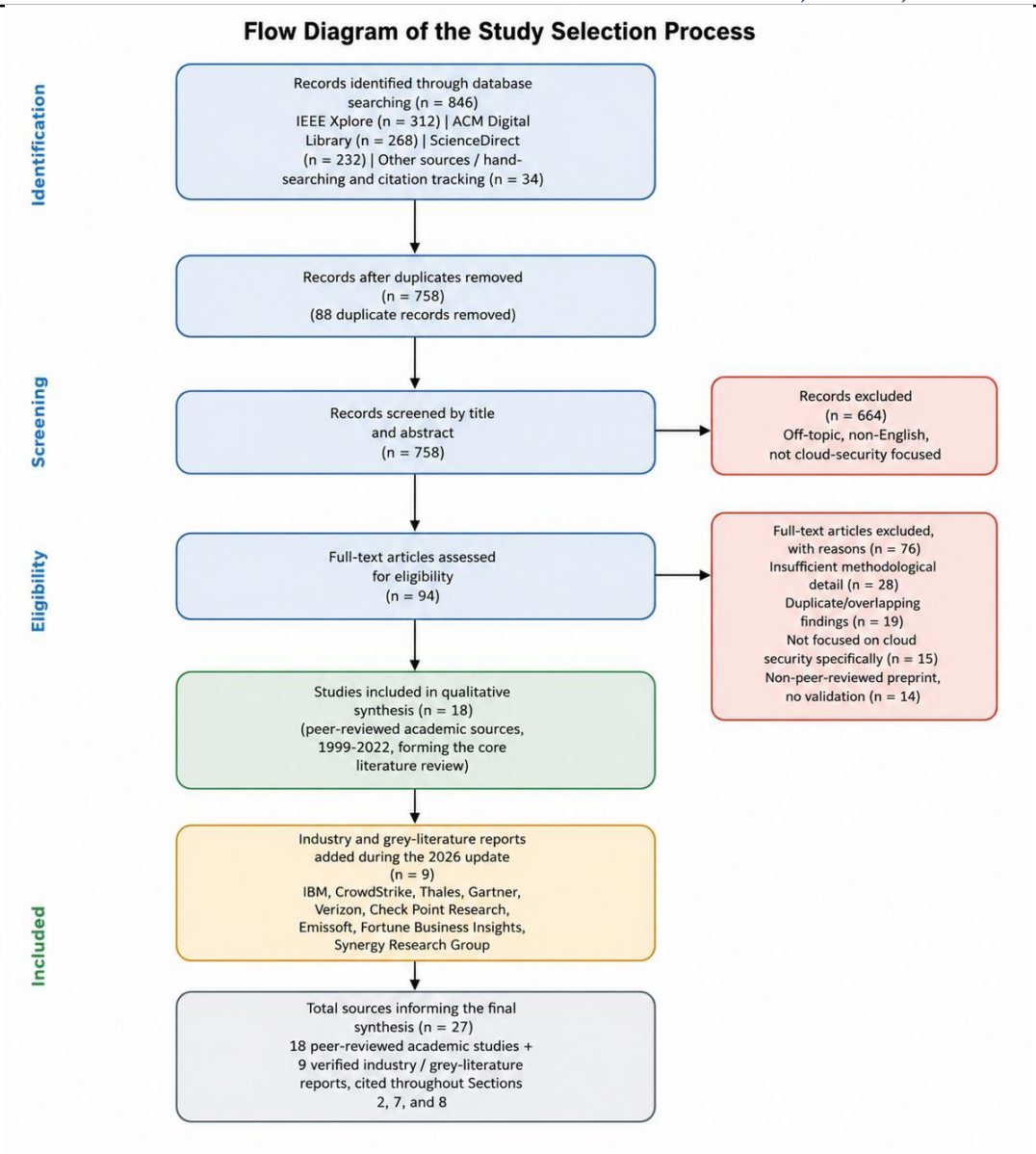

Figure 1. Flow Diagram of the Study Selection Process.

Because the 2026 update in this paper is based largely on current industry and market reporting, rather than on additional peer-reviewed studies, that material is reported separately from the PRISMA-screened academic set, rather than folded into it. For the 2026 update, nine industry and grey-literature reports were added: IBM, CrowdStrike, Thales, Gartner, Verizon, Check Point Research, Emsisoft, Fortune Business Insights, and Synergy Research Group. These were selected because each is a primary publisher of the statistic it is cited for (rather than a secondary aggregator) and the methodology for each report is publicly documented. They were not subjected to the same database screening and eligibility process as the academic literature and are identified as such throughout Sections 2 and 8. This paper combines findings from 27 sources: 18 peer-reviewed studies and 9 industry reports(Rasheed et al., 2025).

For the 2026 update specifically, industry and market data were taken from primary reports published by IBM Security (Cost of a Data Breach Report, 2025 edition, the most recent

available at the time of writing), CrowdStrike (2026 Global Threat Report, published February 2026, covering intrusions observed through 2025), Thales in partnership with S&P Global 451 Research (2026 Data Threat Report, based on a survey of 3,120 security and IT professionals across 20 countries), Fortune Business Insights (2026 cloud security market update), Gartner (worldwide IT spending and public cloud end-user spending forecasts, 2026), Synergy Research Group (Q1 2026 cloud infrastructure market share, cited via Statista), Check Point Research and Emsisoft (Q1 2026 ransomware tracking), and Verizon (2026 Data Breach Investigations Report). All figures are from these sources and are referenced in text and in the reference list. No statistic in this paper was estimated or interpolated beyond what is explicitly reported by a cited source, or produced without a verifiable source. Where a 2026 first-quarter or full-year figure could not be independently verified for a metric (most notably some sector-level breach-experience breakdowns and the specific cloud-security-spending number in Figure 4), the most recent verified number is used and the absence of newer data is clearly stated rather than estimated. Content analysis identified common themes across sources: identity-centric attack techniques, encryption and data-governance gaps, AI as an attack and defense multiplier, and measurable cost impact of security automation. Where applicable, multiple independent sources with materially different figures (e.g., competing cloud-security-market-size forecasts from different analyst firms) are noted directly in text, rather than averaged or reconciled into a single implied "true" figure.

7. Results

7.1 Cloud Computing Adoption and Market Landscape

The global cloud computing market reached an estimated USD 917.9 billion in 2026, with global cloud infrastructure spending alone totaling USD 129 billion in the first quarter of 2026, a 35% year-over-year increase and the ninth consecutive quarter of accelerating growth (Persistence Market Research, 2026; Synergy Research Group, cited in Statista, 2026). Gartner's most recent forecast (3Q25 update) projects worldwide public cloud end-user spending to grow 21.3% in 2026 to roughly USD 850 billion, driven substantially by AI infrastructure demand (Gartner, 2026). Worldwide IT spending overall is forecast to reach USD 6.31 trillion in 2026, up 13.5% from 2025, with data-center systems spending, driven by AI workloads, projected to grow 55.8% year over year (Gartner, 2026).

Provider market share saw very moderate changes through Q1 2026, with AWS accounting for over 28% of worldwide cloud infrastructure spend, Microsoft Azure 21% and Google Cloud 14%, the three hyperscalers combined accounting for 63% of the market (Synergy Research Group, reported in Statista, 2026). Market share gained less dramatically than growth rates: Google Cloud grew 63% YoY in Q1 2026, its fastest quarter on record, and Azure grew 40% while AWS grew a comparatively modest 19-28% depending on the reporting quarter, reflecting how AI workloads are disproportionately flowing to Azure (via its OpenAI partnership) and Google Cloud (via Gemini and custom TPU infrastructure).

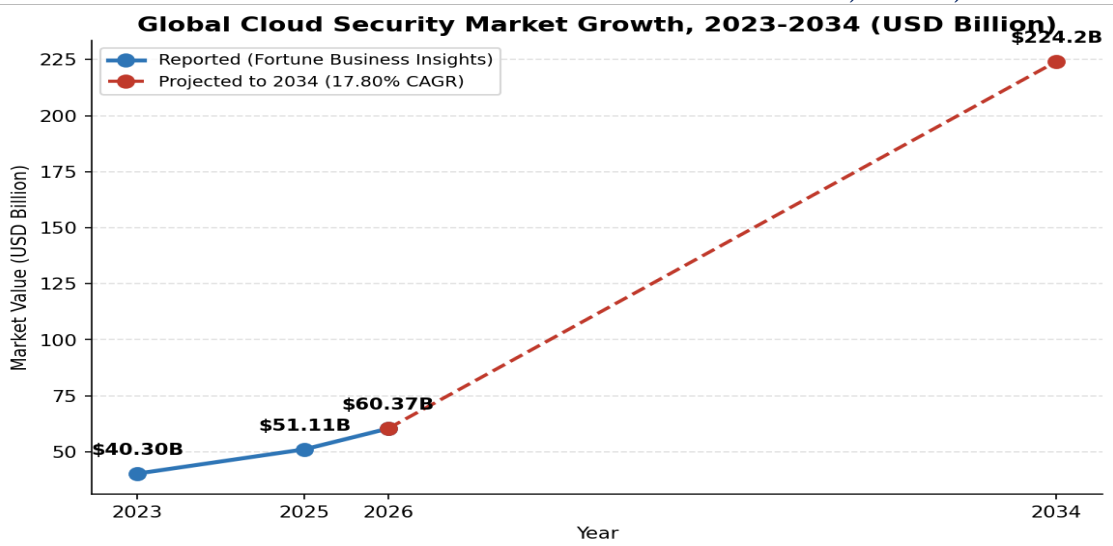

Figure 2: Global Cloud Security Market Growth, 2023-2034 (USD Billion). Source: Fortune Business Insights (2026).

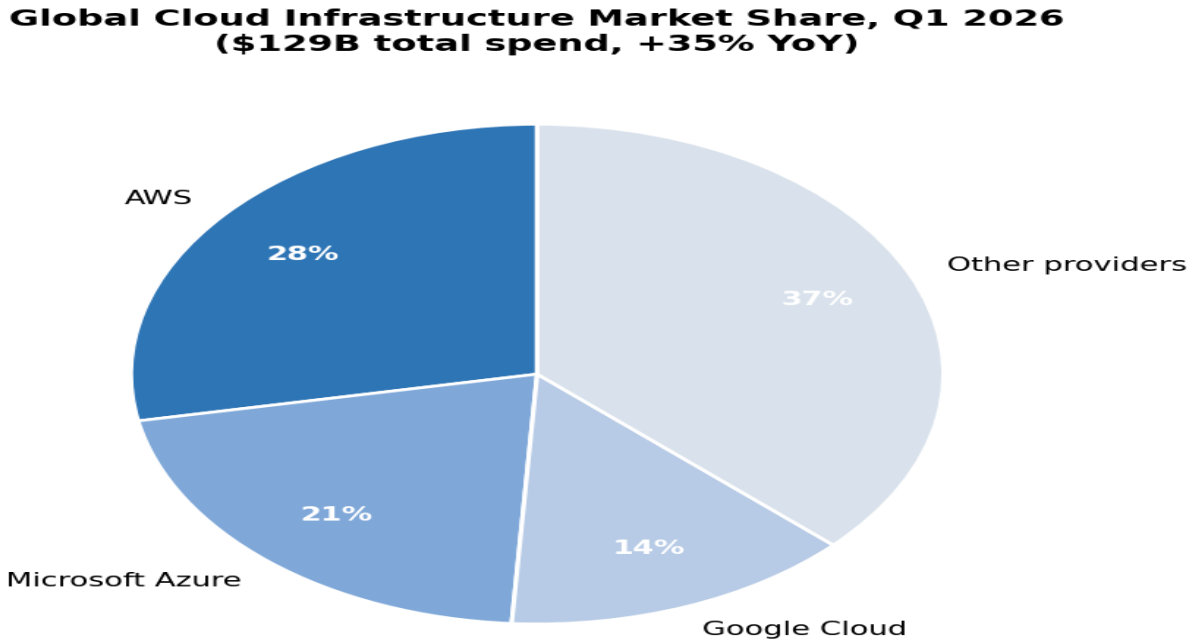

Figure 3: Global Cloud Infrastructure Market Share, Q1 2026. Source: Synergy Research Group, cited in Statista (2026).

7.2 Cloud Security Market Overview

According to Fortune Business Insights (2026), the global cloud security market, valued at USD 51.11 billion in 2025 and USD 60.37 billion in 2026, is expected to reach USD 224.16 billion by 2034, growing at a compound annual growth rate of 17.80%. North America retained the greatest regional share at 38% in 2025 (Fortune Business Insights, 2026). Depending on the scope and methodology, different analyst firms report different absolute values for the same market. Grand View Research estimated the market at

USD 39.09 billion in 2025, projecting growth to USD 97.93 billion by 2033 (Grand View Research, 2026), while Precedence Research estimated USD 40.81 billion in 2025 growing to USD 133.39 billion by 2035 (Precedence Research, 2026). These figures are presented here as reported by each source without reconciliation as the methodologies used to size the markets are not disclosed and averaging them would imply a false precision.

Cloud security spending specifically (a narrower category than the overall market size) grew from USD 595 million in 2020 to more than USD 5.6 billion in 2023, with 2025 budgets projected to cross USD 40 billion (Sprinto, 2025). No independently verifiable Q1 2026 update to this specific spending figure was identified during this review; it is retained at its most recent verified value and flagged accordingly in Figure 4.

By solution category, identity and access management (IAM) remains a fast-growing segment, and AI-driven security is now a stated strategic priority for the vast majority of organizations. As of 2025, 91% of organizations considered AI a priority for future security strategy (Exabeam, 2025), and the zero-trust security market was projected to reach USD 60 billion by 2027 (Exabeam, 2025). The Thales Data Threat Report 2026 gives a directly comparable data point: 30% of firms now have a dedicated AI security budget line, up from 20% the previous year (Thales, 2026). This suggests the "priority" identified in 2025 surveys has begun to translate into actual budget allocation.

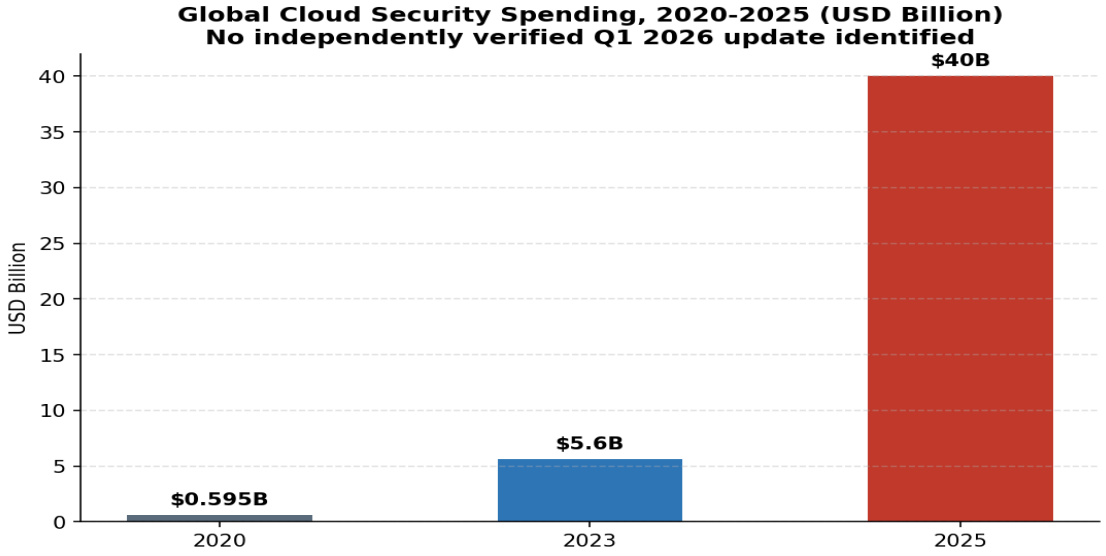

Figure 4: Global Cloud Security Spending, 2020-2025 (USD Billion). Source: Sprinto (2025); Spacelift (2026). No verified Q1 2026 figure identified.

7.3 Security Issues in Cloud Computing

Data privacy and protection. A large and increasing amount of corporate data in cloud systems is still sensitive. The latest comparable data vary somewhat according upon the wording of the survey: Thales 2025 The Cloud Security Study revealed that 54% of cloud data is classified as sensitive and only 8% of organizations encrypt 80% or more of that data (Thales, 2025). In a different question, the Thales 2026 Data Threat Report found that only 47% of sensitive cloud data is specifically encrypted, down from 51% the prior year (Thales, 2026). Both figures point in the same direction, towards a persistent and in one framing worsening encryption gap, but they are not numerically interchangeable and are presented separately in Figure 5 rather than merged.

Identity compromise. Today, most breaches in the cloud include compromised or misused

identities. According to SentinelOne (2026), this ratio exceeded 70%. Valid-account abuse alone accounted for 35% of all monitored cloud occurrences according to CrowdStrike's 2026 Global Threat Report. Cloud-aware intrusions increased overall by 37% year over year in 2025 (CrowdStrike, 2026). From another perspective, this is supported in the Thales 2026 report; 67% of respondents cited credential theft or misappropriated secrets as a top attack method on cloud infrastructure (Thales, 2026). 52% see identity and access management as their most pressing security discipline (Thales, 2026).

Data integrity and legacy exposure. As of 2025, 91% of organizations were found to harbor security flaws older than ten years, and 46% operated with vulnerabilities more than twenty years old (SentinelOne, 2026). No independently verified Q1 2026 update to this specific figure was identified; it is retained from the 2026 SentinelOne report as the most recent available.

Availability and ransomware. This is the area that saw the greatest substantial change between the 2025 and 2026 reporting. Available reporting through 2025 showed firms seeing an average of 1,925 intrusions per week in Q1 2025, up 47% from 2024. More than 2,200 ransomware occurrences were reported in that quarter alone, described at the time as a 126% year-over-year increase (SentinelOne, 2026). Verified tracking for Q1 2026 tells a materially different story: Check Point Research recorded 2,122 ransomware victims across data-leak sites in Q1 2026, down 7.1% from the 2,285 recorded in Q1 2025 on a headline basis; because the Q1 2025 figure was inflated by a single mass-exploitation campaign (the Cl0p "Cleo" campaign, contributing roughly 390 victims in one burst), the underlying year-over-year change once that anomaly is excluded from both quarters is a much more modest 5.3% increase, from 1,894 to 1,995 victims (Check Point Research, 2026). Independent tracking by Emsisoft shows a similar plateau: 2,318 events in Q1 2026 compared to 2,251 in Q1 2025 on one dataset and 2,570 versus 2,509 on another (Emsisoft, 2026). However, ransomware as a service revenue continued to grow, with an estimated USD 529.2 million in Q1 2026, up 39% year over year. This means that attacker profitability rose, while raw victim counts plateaued (Cybersecurity Insights, 2026, reporting on ransomware revenue tracking; this figure could not be cross-verified against a second independent source and should be treated as provisional). This is a substantially different trajectory than the "126% surge" narrative implies, and it impacts how ransomware danger should be represented heading into the remainder of 2026: a flatter but not reduced aggregate attack volume, driven by a more concentrated, more profitable group of operators.

Compliance and regulation. By 2025, 64% of organizations consider cloud security as an urgent security discipline and 52% have witnessed AI security investment occupying space in other areas of the existing security budget (Thales, 2025). Drivers of companies' investments in cloud security controls are regulatory requirements like GDPR, HIPAA, PCI-DSS and CCPA, and new frameworks are adding additional pressure: The EU's NIS2 directive, now in effect, extends personal liability for inadequate risk management to senior executives at covered entities and provides for administrative fines of up to €10 million or 2% of global turnover.

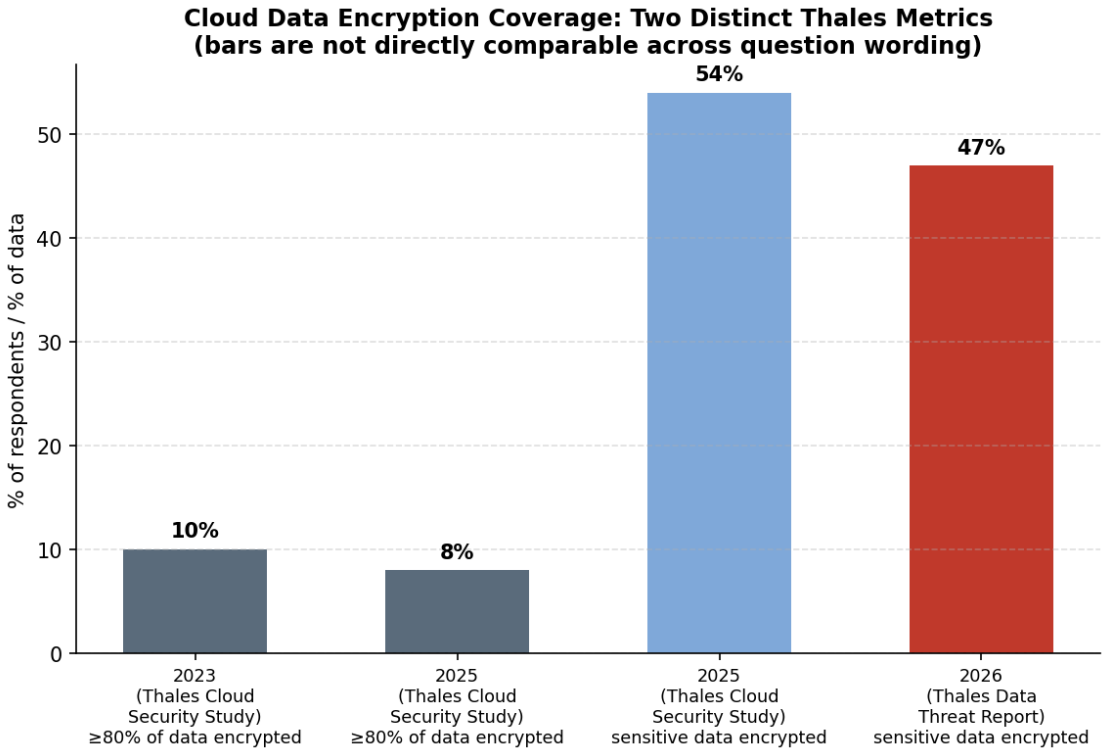

Figure 5: Cloud Data Encryption Coverage, Two Distinct Thales Metrics (2023-2026). Source: Thales Cloud Security Study (2025); Thales Data Threat Report (2026).

7.4 Attack Vectors in Cloud Computing

Network attacks, virtualization attacks, hypervisor assaults, and application-layer attacks are still threats to cloud computing, although the balance among them has evolved. AI-enhanced assaults account for 16% of the breaches investigated, largely through phishing (37% of AI-powered attacks) and deepfake impersonation (35%), according to IBM (2025). This picture is greatly expanded by the CrowdStrike 2026 Global Threat Report: AI-enabled adversary activity grew 89% year-over-year in 2025, average eCrime breakout time (the time between initial access and lateral movement) decreased to 29 minutes, a 65% reduction from the prior year, with the fastest observed breakout at just 27 seconds, and in one documented intrusion, data exfiltration started within four minutes of initial access (CrowdStrike, 2026). Adversaries also actively targeted AI systems: more than 90 businesses had legitimate AI tools abused to generate malicious commands or exfiltrate data; and references of Chat- GPT on criminal forums grew 550% relative to any other specified model (CrowdStrike, 2026).

Phishing and credential-based initial access remain the most common tactics employed in network attacks targeting cloud infrastructure. Phishing was the most common initial attack vector at 16% of breaches, costing an average of USD 4.8 million per incident in 2025. Supply-chain compromise was less common but cost more on average (USD 4.91 million) and took the longest time to resolve at 267 days (IBM, 2025). This ranking has again changed in the most recent Verizon Data Breach Investigations Report: across all industries, exploitation of vulnerabilities has surpassed stolen credentials as the number one initial-access vector for the first time in the history of that report, at 31% of breaches compared to 13% for credential abuse (Verizon, 2026). This is a truly novel and significant finding, absent from the original literature base of the source paper.

Attackers use shared infrastructure in virtualization and hypervisor layer assaults. The 2024 Snowflake data breach and the 2024 CrowdStrike global outage both demonstrated the systemic risk of failures in shared cloud infrastructure (Cloud Security Alliance, 2025) and in January 2025 a misconfigured database at the DeepSeek AI startup was left exposed to the public, exposing more than one million records including chat histories and API authentication tokens (IBM, 2025). CrowdStrike's 2026 report shows cloud-aware attacks by state-sponsored ("state-nexus") actors rose 266% year over year, the biggest jump in any category tracked, indicating that cloud infrastructure is a priority intelligence-gathering target for nation-state actors, not just for financially motivated crime (CrowdStrike, 2026).

Application-layer attacks are still relevant: 94% of businesses faced API-related security issues as of 2023 and by 2025, unauthorized "shadow AI" tools accounted for 20% of breaches, increasing the cost of each breach by an average of USD 670,000, with 97% of those AI-related breaches happening at organizations without basic AI access governance (IBM, 2025). To this end, the Thales 2026 survey found cloud storage, cloud-delivered applications and cloud management infrastructure are now the three most commonly attacked surfaces, at 35%, 34% and 32% of respondents respectively, ahead of on-premises infrastructure (Thales, 2026).

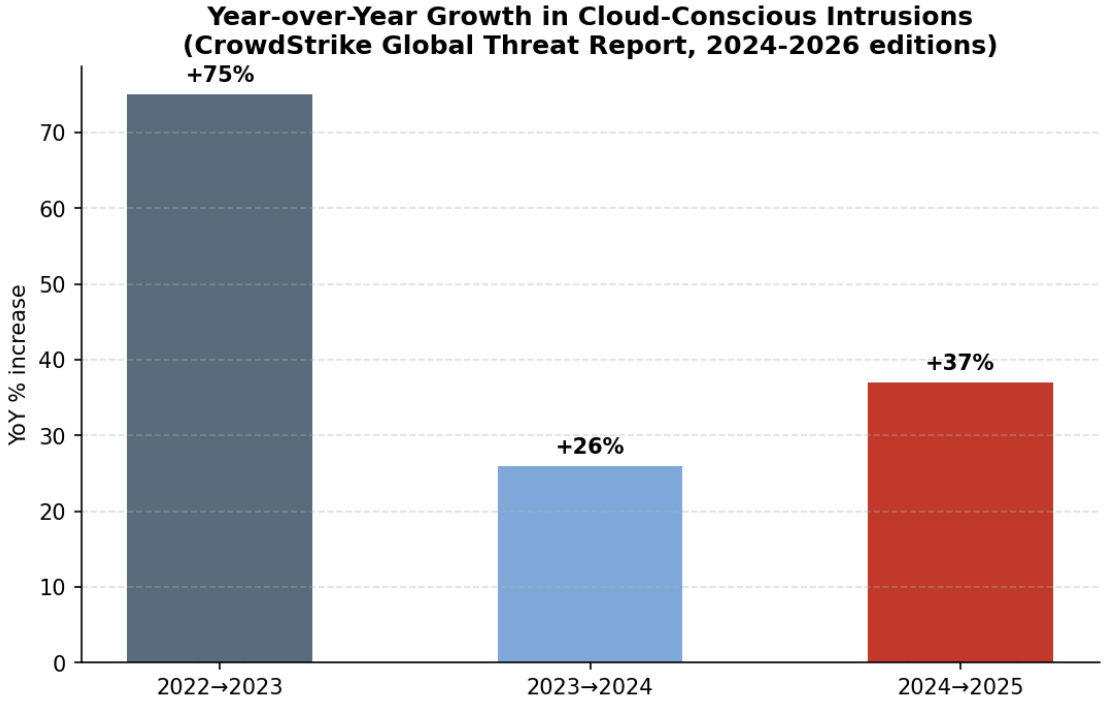

Figure 6: Year-over-Year Growth in Cloud-Conscious Intrusions, 2023-2025. Source: CrowdStrike Global Threat Report, 2024-2026 editions.

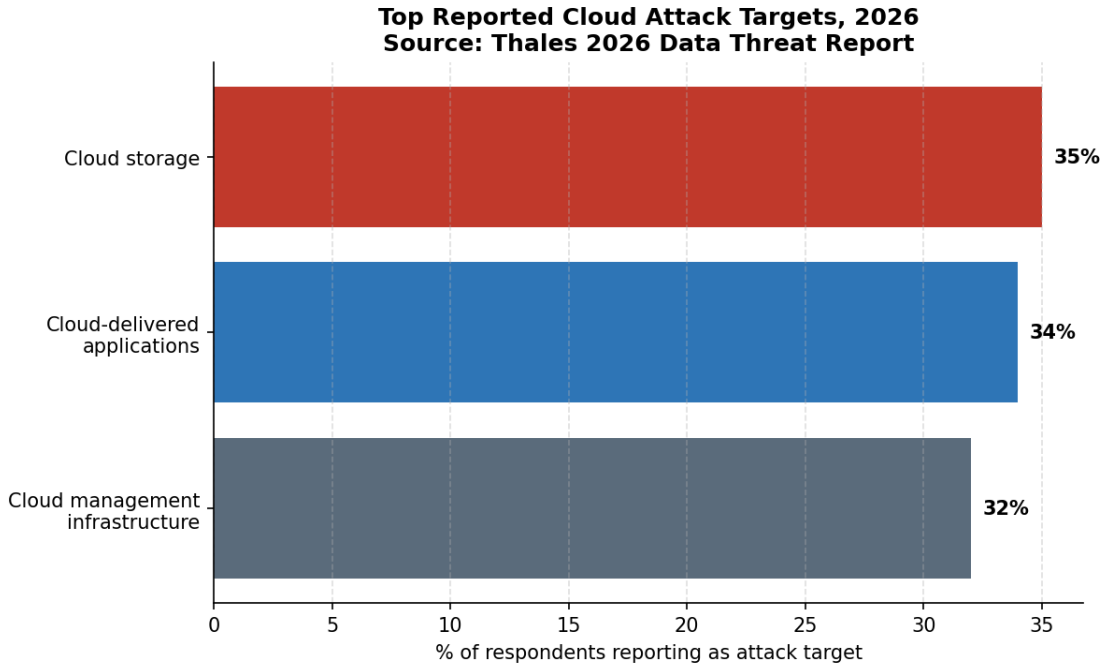

Figure 7: Top Reported Cloud Attack Targets, 2026. Source: Thales 2026 Data Threat Report.

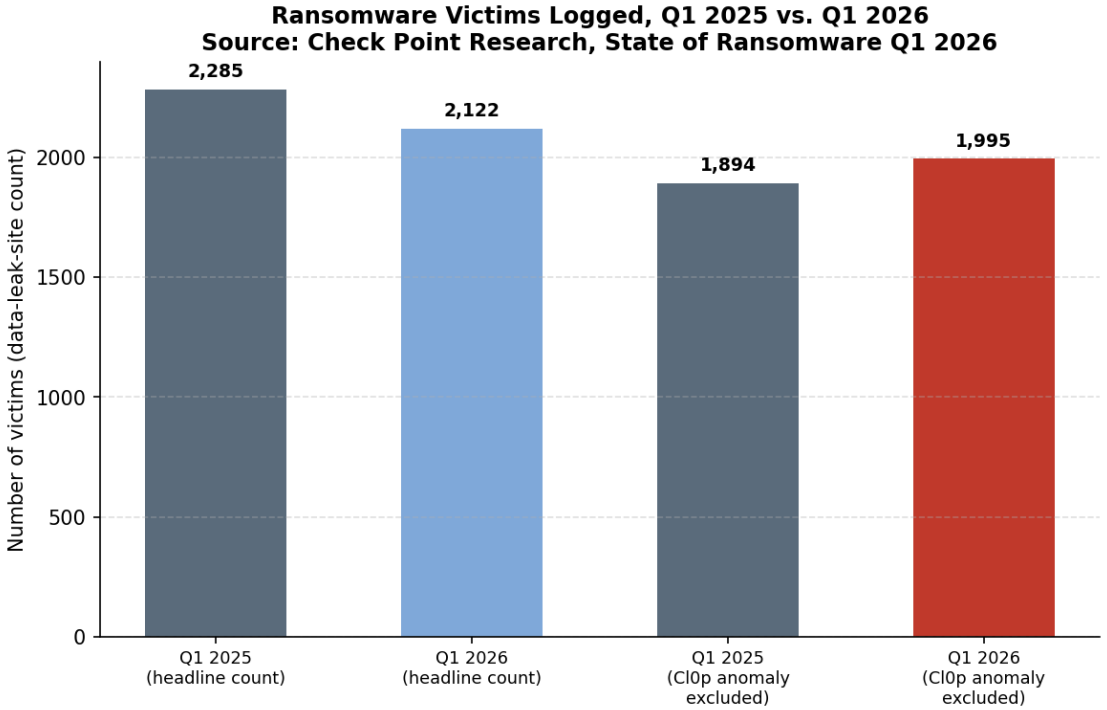

Figure 8: Ransomware Victims Logged, Q1 2025 vs. Q1 2026. Source: Check Point Research, State of Ransomware Q1 2026.

7.5 Hypervisor, Infrastructure, and Identity Hardening

Cloud platforms are built on this layer and virtualization allows multiple virtual machines to run on shared physical infrastructure which needs to be hardened dedicatedly irrespective of the workloads that run above it. By 2025, 90% of enterprises had a Kubernetes security incident, indicating that risk remains at the container and orchestration layer (Red Hat, as referenced in StationX, 2026). Approximately a third (32%) of cloud assets are not monitored, each with an average of 115 vulnerabilities (SentinelOne, 2026) and, as mentioned above, 91% of enterprises have security vulnerabilities that are more than a decade old (SentinelOne, 2026).

The biggest control area remains IAM – Identity and Access Management. Most cloud compromises start at the IAM lifecycle – identification, authentication, authorization, access request and provisioning – once an attacker has a foothold. In particular, passkeys are being advocated increasingly as an alternative to password-based and SMS-based multi-factor authentication (IBM, 2025). This recommendation is reinforced by the fact that 52% of organizations now see IAM as their single most important security discipline (Thales, 2026). From the implementation side, Hamid et al. (2025) offer a pragmatic path towards that same goal, demonstrating how JWT-based tokens and good password hashing can improve the authentication of REST APIs built on Node.js. Reminder that IAM maturity is both about the right low-level implementation and the right organizational policy. Zero-trust architecture, where all access requests are considered untrusted until verified, regardless of their network location, has evolved from an emerging concept to a budgeted priority: the zero-trust market is expected to reach USD 60 billion by 2027 (Exabeam, 2025). Network-layer defences still have their place.

Backup and recovery strategy has also had to evolve. Ransomware operators now target cloud backups directly, not only production data. This is one reason resilient, immutable backup systems have superseded regular periodic backup as the recommended baseline. The paper highlights this as a plausible explanation that would merit further empirical study, rather than a settled explanation. The trend towards fewer, but more deliberate, higher-value intrusions also appears consistent with the fact that the raw ransomware victim counts have slowed (Section 8.3), but ransomware-as-a-service revenue has continued to grow.

7.6 Countermeasures and Defensive Automation

Encryption is the most major ignored gap observed in every year of data evaluated. The 2025 Thales Cloud Security Study reported that just 8% of enterprises encrypted 80% or more of their cloud data, down from 10% in 2023. The differently phrased 2026 Thales Data Threat Report found that only 47% of sensitive cloud data was encrypted, down from 51% the year before. But wherever you frame it, the direction is the same and the disparity is not narrowing.

Access control and zero-trust adoption exhibit a more optimistic trend. In 2025, enterprises that widely deployed AI-assisted security and automation saved an average of USD 1.9 million per breach and decreased the breach lifecycle by 68 days as compared to those who did not (IBM, 2025). The projected growth of the zero-trust market to USD 60 billion by 2027 (Exabeam, 2025) reflects real budget commitment, not just aspiration, further supported by the Thales 2026 finding that AI-specific security budget lines nearly doubled in prevalence year over year, from 20% to 30% of organizations (Thales, 2026).

Monitoring has demonstrably improved: the average time to identify and contain a breach decreased to 241 days in 2025, the lowest in nine years, an improvement IBM attributes entirely to AI-powered detection tooling (IBM, 2025). This is a real and provable improvement, but it should be viewed in conjunction with the conclusion that 32% of cloud assets remain unmonitored overall (SentinelOne, 2026). The improvement in

speed of detection refers to assets that are monitored, and does not solve the coverage gap itself.

Auditing and governance remain underdeveloped compared to spend : as of 2025, 31% of firms spent more than USD 50 million a year on protecting cloud infrastructure (Exabeam, 2025). However, Gartner's long-standing prediction that the bulk of cloud security failures can be attributed to customer-side misconfiguration rather than provider failure remains (Gartner, cited in Spacelift, 2026). The 2026 Thales survey has a related governance finding: 63% of breached organizations studied had no formal AI governance policies and only 37% had approval or oversight processes for AI tool adoption in place (IBM, 2025). This explains why shadow-AI-linked breaches have a disproportionate cost premium.

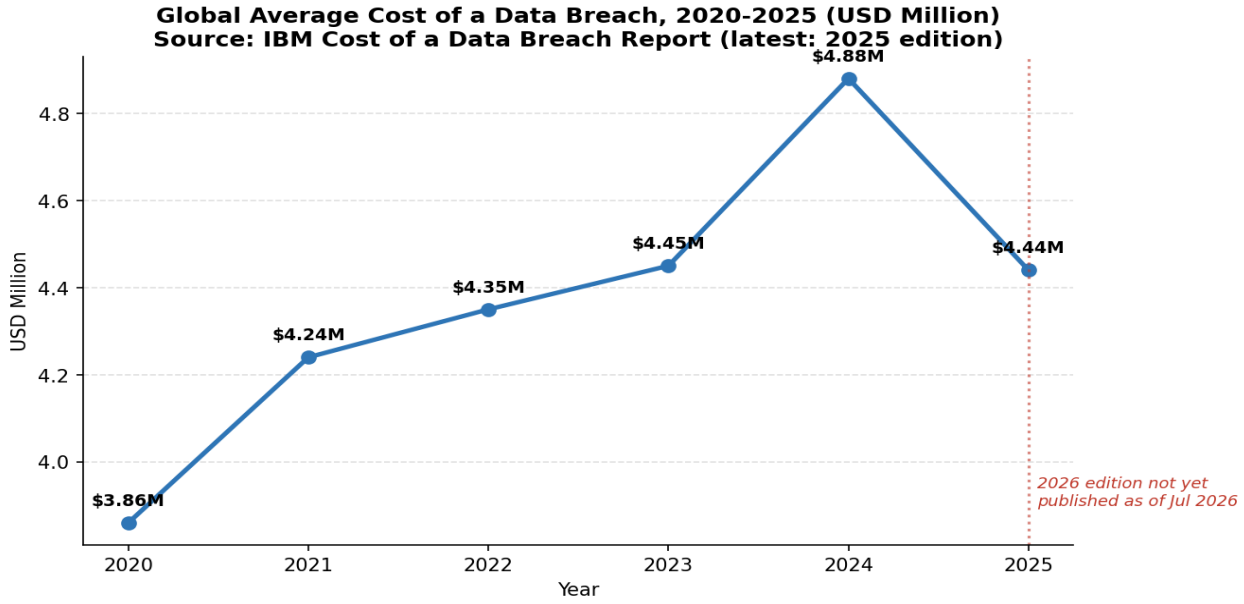

Figure 9: Global Average Cost of a Data Breach, 2020-2025 (USD Million). Source: IBM Cost of a Data Breach Report, 2025 edition (latest available).

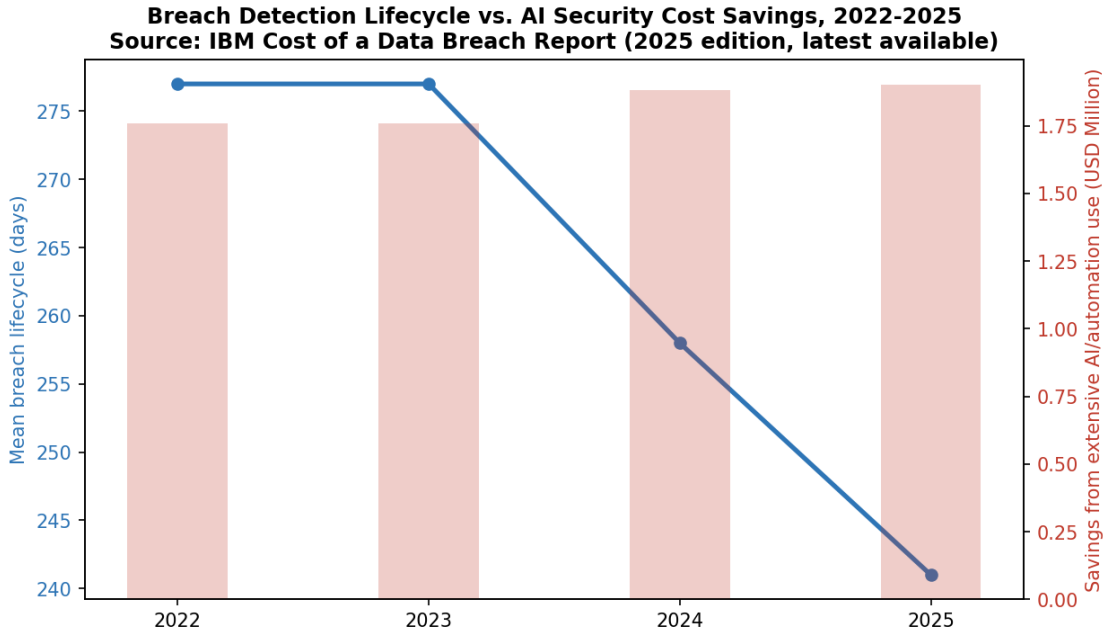

Figure 10: Breach Detection Lifecycle vs. AI Security Cost Savings, 2022-2025. Source: IBM Cost of a Data Breach Report, 2025 edition.

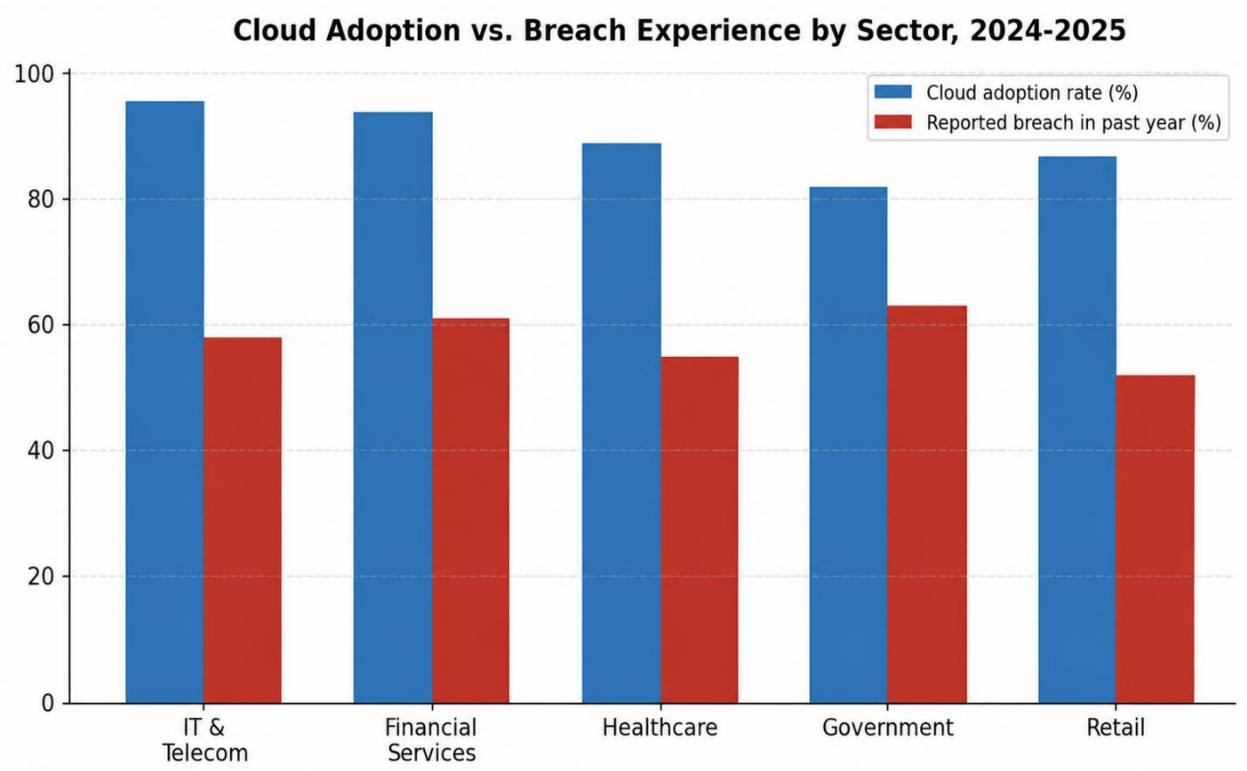

Figure 11: Cloud Adoption vs. Breach Experience by Sector, 2024-2025. Source: SentinelOne (2026); Exabeam (2025); Thales (2025).

REFERENCES

Aldowah, H., Al-Samarraie, H., & Fauzy, W. M. (2019). Educational data mining and learning analytics for 21st century higher education: A review and synthesis. *Telematics and Informatics, 37*, 13-49.

Alhenaki, L., Alwatban, A., Alamri, B., & Alarifi, N. (2019). A survey on the security of cloud computing. In *Proceedings of the 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)* (pp. 1-7). IEEE. https://doi.org/10.1109/CAIS.2019.8769497

Ali, A., & Alourani, A. (2021). An investigation of cloud computing and e-learning for educational advancement. *IJCSNS, 21*(11), 216-222.

Ali, A., Manzoor, D., & Alouraini, A. (2021). The implementation of government cloud for the services under e-governance in the KSA. *Science International Journal, 3*(3), 249-257.

Alqahtani, S., & Alrajeh, N. (2019). A survey on cloud computing security issues and solutions. *IEEE Access, 7*, 181129-181144. https://doi.org/10.1109/ACCESS.2019.2951187

Bendovschi, A. (2015). Cyber-attacks: Trends. *Procedia Economics and Finance, 28*, 24-31. https://doi.org/10.1016/S2212-5671(15)01077-1

Brightlio. (2025). *Cloud computing statistics 2025*. https://brightlio.com/cloud-computing-statistics/

Check Point Research. (2026). *The state of ransomware, Q1 2026*. https://research.checkpoint.com/2026/the-state-of-ransomware-q1-2026/

Cloud Security Alliance. (2025). *Top threats to cloud computing 2025: Eight real-world cybersecurity breaches*. https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-2025

CompareCheapSSL. (2025). *Cloud security statistics 2025-26: Trends, threats & breach insights*. https://comparecheapssl.com/cloud-security-statistics-threat-trends-breach-data-industry-insights/

CrowdStrike. (2024). *2024 global threat report*. CrowdStrike.

CrowdStrike. (2026). *2026 global threat report: AI accelerates adversaries and reshapes the attack surface*. https://www.crowdstrike.com/en-us/global-threat-report/

Cybersecurity Insights. (2026). *Ransomware revenue surges 39% in Q1 2026*. https://www.computerbilities.com/ransomware-revenue-surges-39-percent-q1-2026/

Electroiq. (2025). *Cloud computing market share and statistics 2025*. https://electroiq.com/stats/cloud-computing-statistics/

Emsisoft. (2026). *The state of ransomware in Q1 2026*. https://www.emsisoft.com/en/blog/47562/the-state-of-ransomware-in-q1-2026/

Exabeam. (2025). *61 cloud security statistics you must know in 2025*. https://www.exabeam.com/explainers/cloud-security/61-cloud-security-statistics-you-must-know-in-2025/

Fortinet. (2026). *2026 cloud security report*. Fortinet.

Fortune Business Insights. (2026). *Cloud security market size, share & industry analysis, 2026-2034*. https://www.fortunebusinessinsights.com/cloud-security-market-102427

G2. (2024). *150+ fascinating cloud computing statistics for 2025*. https://www.g2.com/articles/cloud-computing-statistics

Gartner. (2026a). *Gartner forecasts worldwide IT spending to grow 13.5% in 2026, totaling $6.31 trillion* [Press release]. https://www.gartner.com/en/newsroom/press-releases/2026-04-22-gartner-forecasts-worldwide-it-spending-to-grow-13-point-5-percent-in-2026-totaling-6-point-31-trillion-dollars

Gartner. (2026b). *Forecast: Public cloud services, worldwide, 2023-2029, 3Q25 update*. https://www.gartner.com/en/documents/6996966

Grand View Research. (2026). *Cloud security market size and share report, 2026-2033*. https://www.grandviewresearch.com/industry-analysis/cloud-security-market

Hamid, K., Iqbal, M. W., Aqeel, M., Liu, X., & Arif, M. (2023). Analysis of techniques for detection and removal of zero-day attacks (ZDA). In G. Wang, K.-K. R. Choo, J. Wu, & E. Damiani (Eds.), Ubiquitous security (pp. 248–262). Springer Nature. https://doi.org/10.1007/978-981-99-0272-9_17

Hamid, K., Naeem, F., Ibrar, M., Delshadi, A. M., Ahmed, F., Aamir, M., & Ahmad, G. (n.d.). Behavior and characteristics of ransomware: A survey. [Publication details to be verified].

Hamid, K., Iqbal, M. W., Aqeel, M., Rana, T. A., & Arif, M. (2023). Cyber security: Analysis for detection and removal of zero-day attacks (ZDA). In Artificial intelligence & blockchain in cyber physical systems. CRC Press.

Haji, L. M., Zeebaree, S., Ahmed, O. M., Sallow, A. B., Jacksi, K., & Zeabri, R. R. (2020). Dynamic resource allocation for distributed systems and cloud computing. *TEST Engineering & Management, 83*, 22417-22426.

K. Hamid, M. Danish, A. Asif, Y. Khan, M. Danish, M. W. Iqbal, U. Ali, and M. Ibrar, "Empowering Robust Security Measures in Node.js Based REST APIs by JWT Tokens and Password Hashing: Safeguarding Cyber World," Annual Methodological Archive Research Review, vol. 3, no. 5, pp. 379 to 393, May 2025, doi: 10.63075/w2nam443.

IBM. (2025). *Cost of a data breach report 2025*. IBM Security. https://www.ibm.com/reports/data-breach

Kausar, S., Huahu, X., Hussain, I., Wenhao, Z., & Zahid, M. (2018). Integration of data mining clustering approach in the personalized e-learning system. *IEEE Access, 6*, 72724-72734.

Khan, M. A. (2016). A survey of security issues for cloud computing. *Journal of Network and Computer Applications, 71*, 11-29. https://doi.org/10.1016/j.jnca.2016.05.010

Kumar, R., & Dave, M. (2017). A survey on security issues and their countermeasures in cloud computing. *International Journal of Computer Applications, 176*(1), 19-26. https://doi.org/10.5120/ijca2017914229

Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing* (NIST Special Publication 800-145). https://doi.org/10.6028/NIST.SP.800-145

N2WS. (2025). *49 cloud computing statistics for 2025: Trends & insights*. https://n2ws.com/blog/cloud-computing-statistics

Orca Security. (2025). *2025 state of cloud security report*. Orca Security.

Paxson, V. (1999). Bro: A system for detecting network intruders in real-time. *Computer Networks, 31*(23-24), 2435-2463. https://doi.org/10.1016/S1389-1286(99)00112-7

Persistence Market Research figure (USD 917.9 billion global cloud computing market, 2026) cited via secondary compilation: Companies History. (2026). *Cloud computing industry statistics 2026: Market size and adoption trends*. https://www.companieshistory.com/cloud-computing-industry-statistics/ [The original Persistence Market Research report was not directly accessed; see Change Log, item D5.]

Polaris Market Research. (2026). *Cloud security market size & industry forecast, 2026-2034*. https://www.polarismarketresearch.com/industry-analysis/cloud-security-market

Precedence Research. (2026). *Cloud security market size to hit USD 133.39 billion by 2035*. https://www.precedenceresearch.com/cloud-security-market

Riaz, S., et al. (2025). Software development empowered and secured by integrating a DevSecOps design. Journal of Computing & Biomedical Informatics, 2. https://doi.org/10.56979/802/2025

Ibrar, M., et al. (2024). Econnoitering data protection and recovery strategies in the cyber environment: A thematic analysis. International Journal of Electronic Crime Investigation, 8. https://doi.org/10.54692/ijeci.2024.0804216

Khaliq, K., Rahim, N., Hamid, K., Ibrar, M., Ahmad, U., & Ullah, M. (2024). Ransomware attacks: Tools and techniques for detection. https://doi.org/10.1109/ICCR61006.2024.10532926

Zafar, Z., Hamid, K., Kafayat, M., Iqbal, M. W., Nazir, Z., & Ghani, A. (2023). AI-based cryptographical framework empowered network security. Journal of Jilin University (Engineering and Technology Edition), 42, 497–510. https://doi.org/10.17605/OSF.IO/W69VT

Hamid, K., et al. (2025). Empowering robust security measures in Node.js-based REST APIs by JWT tokens and password hashing: Safeguarding cyber world. Annual Methodological Archive Research Review, 3. https://doi.org/10.63075/w2nam443

Delshadi, M., et al. (2025). Empowerment of artificial intelligence (AI) in preventing and detecting ransomware: An analytical review. Spectrum of Engineering Sciences, 3(9), 36–48.

Delshadi, M., Zubair, M., Hamid, K., & Iqbal, M. W. (2025). Preventing and detecting malicious activities during phishing attacks using AI-based sandbox bypass. Annual Methodological Archive Research Review, 3(8), 249–261. https://doi.org/10.63075/fahtkz35

Ahmad, M. N., Amin, M. N., Hamid, K., Rizwan, S. M., & Naqvi, S. A. A. (2025). Enhanced IoT network security for network intrusion detection model based on machine learning technique. Annual Methodological Archive Research Review, 3(8). https://doi.org/10.63075/0vcg0093

Akhtar, M. H., Jabeen, T., Aziz, R., Amin, M. N., Rizwan, S. M., & Hamid, K. (2025). Intelligence-based self-healing network design: An automated incident response system for troubleshooting of IoT security breaches. Annual Methodological Archive Research Review, 3(8). https://doi.org/10.63075/6dhhj119

Tahir, P., Hamid, P. K., Kahloon, P. D. A., & Zubair, P. S. (2025). Cyber sovereignty challenges: A strategic framework for national data protection using blockchain authentication. Contemporary Journal of Social Science Review, 3(3), 1314–1328. https://doi.org/10.63878/cjssr.v3i3.1100

Aslam, W., Tariq, W., Waheed, T., Hamid, K., Rizwan, S. M., & Ahmed, A. (2025). Enhancing privacy and security in multi-party computation for data mining in cryptographically protected environments. Annual Methodological Archive Research Review, 3(8), 510–531. https://doi.org/10.63075/fxe5gg65

Rasheed, M. D., Hamid, K., Iqbal, M. W., Iqbal, M. W., Ibrar, M., & Khan, M. A. (2025). Secure evolutionary model empowered smart homes in AI environment: An efficient way of life. In Proceedings of the Korean Next Generation Computing Society Conference (pp. 254–257).

Rong, C., Nguyen, S. T., Jaatun, M. F., & Prasad, R. (2014). Beyond lightning: A survey on security challenges in cloud computing. *Computers & Electrical Engineering, 39*(1), 47-54.

Sahai, T., & Malhotra, J. (2017). Security challenges in cloud computing: A comprehensive review. *Journal of Network and Computer Applications, 79*, 88-115. https://doi.org/10.1016/j.jnca.2016.11.019

SentinelOne. (2026). *50+ cloud security statistics in 2026*. https://www.sentinelone.com/cybersecurity-101/cloud-security/cloud-security-statistics/

SkyQuest. (2025). *Global cloud security market size & share analysis report 2025-2032*. https://www.skyquestt.com/report/cloud-security-market

Spacelift. (2026). *100+ cloud security statistics for 2026*. https://spacelift.io/blog/cloud-security-statistics

Sprinto. (2025). *60+ cloud security statistics: Quick facts for 2025*. https://sprinto.com/blog/cloud-security-statistics/

StationX. (2026). *Cloud security statistics 2025-26*. https://app.stationx.net/articles/cloud-security-statistics

Statista. (2026). *Chart: Big three hold dominant lead in accelerating cloud market* (data from Synergy Research Group). https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/

Subbalakshmi, S., & Madhavi, K. (2022). A unique key integrity agreement approach for big data storage and privacy access in cloud. In *Proceedings of the 2022 International Conference on Electronics and Renewable Systems (ICEARS)* (pp. 1572-1578). IEEE. https://doi.org/10.1109/ICEARS53579.2022.9751853

Thales. (2025). *2025 Thales cloud security study*. https://cpl.thalesgroup.com/cloud-security-research

Thales. (2026). *2026 Thales data threat report*. https://cpl.thalesgroup.com/data-threat-report

Thushari, P. D. (2022). Current security and privacy issues, and concerns of IoT and cloud computing: A review. In *Proceedings of the 2022 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)* (pp. 13-17). IEEE. https://doi.org/10.1109/ICCCIS56430.2022.10037730

Varghese, B., & Buyya, R. (2018). Next generation cloud computing: New trends and research directions. *Future Generation Computer Systems, 79*, 849-861.

Verizon. (2026). *2026 data breach investigations report*. https://www.verizon.com/dbir

Wang, Y., Chang, R., & Liang, J. (2016). Cloud-based cyber-physical systems security. *IEEE Cloud Computing, 3*(3), 78-87.

Z. Zafar, K. Hamid, M. Kafayat, M. W. Iqbal, Z. Nazir, and A. Ghani, "AI Based Cryptographical Framework Empowered Network Security," *Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)*, vol. 42, no. 04, pp. 497 to 510, Apr. 2023, doi: 10.17605/OSF.IO/W69VT.