UTM UNIVERSITI TEKNOLOGI MALAYSIA
INTERNATIONAL JOURNAL OF INNOVATIVE COMPUTING
ISSN 2180-4370
Journal Homepage : https://ijic.utm.my/

A Cost-Benefit Analysis of Zero Trust Architecture (ZTA) Using Hybrid Financial Impact and Threat Mitigation Strategy

Martin Ugong[1]* & Siti Hajar Othman[2]
Universiti Teknologi Malaysia,
81310 UTM Johor Bahru, Johor, Malaysia
Email: martin.ugong83@gmail.com[1]; hajar@utm.my[2]

Submitted: 22/7/2025. Revised edition: 15/12/2025. Accepted: 5/1/2026. Published online: 10/6/2026
DOI: https://doi.org/10.11113/ijic.v16n1.572

***Abstract*—Zero Trust Architecture (ZTA) emerges as a pivotal cybersecurity paradigm, fundamentally shifting from traditional perimeter-based security models to a 'Never Trust, Always Verify' ethos, which necessitates continuous authentication and authorization for all network requests, regardless of origin. The increasing adoption of cloud technologies, Internet of Things (IoT) devices, and remote workforces has significantly expanded enterprise network perimeters, rendering conventional security methods such as Virtual Private Networks (VPNs) inadequate against modern attacks like Man-In-The-Middle and Denial of Service (DoS). Despite the growing recognition of ZTA's importance, organizations often exhibit hesitancy in committing resources due to a perceived lack of comprehensive quantitative data on its benefits, available tools, pricing structures, and efficacy rates. This research directly addresses this critical gap by conducting a rigorous cost-benefit analysis, evaluating the financial impact, cost-effectiveness, and threat mitigation outcomes of ZTA implementation. The study's methodology is structured in three phases. In Phase 1, ZTA tools, resources, and components were identified, along with the necessary investments. Vendor pricing data was collected from reputable security providers, including Microsoft, Kaspersky, IBM, CrowdStrike, Google, and BlackBerry. These vendors offer a wide range of security services such as Data Encryption, Identity and Access Management (IAM), Data Protection, Cloud Storage, and Micro-Segmentation. The selected tools and resources function as core threat mitigation strategies designed to reduce data breach risks and associated financial losses. Additionally, data-driven, quantitative methodologies are applied to estimate the total cost of implementing ZTA tools and resources. The analysis focuses on the annual budget requirements for small and medium-sized businesses (SMBs) with employee headcounts ranging from 0 to 1,000. In Phase 2, the outcome of Phase 1 is a detailed breakdown of all ZTA-related expenses. This cost dataset is then used in Phase 2 to compare the total ZTA investment against the potential financial savings from preventing data breach incidents. The cost parameters established in Phase 1 are applied consistently throughout Phase 2 to calculate the monetary benefits of risk reduction. This comparison demonstrates the potential financial savings achieved through the implementation of Zero Trust-aligned breach prevention strategies. The comprehensive cost-effectiveness analysis of ZTA is performed by comparing the financial impact of data breaches before and after ZTA implementation, along with the cost of deploying ZTA itself. The cost-effectiveness is assessed using the Annual Loss Expectancy (ALE) model, which quantifies Annual Loss Expectancy before ZTA implementation, Annual Loss Expectancy after ZTA implementation, and total ZTA implementation cost, which consists of technology and staffing. In addition, Phase 2 validates the financial Return on Investment (ROI) of implementing ZTA, incorporating a four-year projected cost reduction model. The Return on Investment (ROI) assessment establishes the financial justification required for Phase 3 by demonstrating that ZTA provides measurable long-term value to the organization. Phase 3 focuses on evaluating the extent to which Zero Trust Architecture (ZTA) contributes to reducing data breach costs. The key outcome of this phase is to demonstrate that ZTA effectively lowers the frequency and reduces data breach-related costs. This provides real-world validation that ZTA delivers on its promise to enhance organizational security, thereby reinforcing the cost-effectiveness findings established in Phase 2. The methodology for Phase 3 employs comparative case studies, such as the Uber and Utah Food Bank breach analyses, examining security incidents recorded before and after ZTA implementation in real-world organizations. This comparative approach provides empirical evidence of the tangible security improvements resulting from ZTA adoption. Key findings demonstrate that ZTA significantly**

reduces risk impact, with an average reduction of RM711K over four years for implementing organizations below 500 employees. This substantial saving highlights ZTA's economic viability in mitigating data breach risks and associated penalties, indicating that organizations with ZTA deployed experience notably lower data breach costs, with potential savings exceeding 20% and risk exposure reductions of at least 37%. The research underscores that ZTA, by enforcing rigorous identity verification, least privilege, and continuous authentication, not only enhances security posture but also serves as a powerful financial strategy, offering substantial long-term savings and improved resilience against cyber threats for organizations of all sizes. The study provides essential evidence-based guidance for informed cybersecurity investment decisions, emphasizing ZTA as an economical and effective defense against the escalating costs and impacts of cyberattacks.

***Keywords*—Zero-trust architecture, tools, cost effectiveness, cost and benefit analysis**

I. INTRODUCTION

In the current security model, one prominent concept that arises is the Zero Trust model, with the continuous proliferation of technological devices and their utilization by individuals within organizations or for personal purposes. Zero Trust Model aims to secure sensitive data, systems, and services within an organization by ensuring that no actor, network, or service is inherently trusted, whether inside or outside the security perimeter [1]. Fundament principle of Zero Trust involves authorizing secure communication between the resources, regardless of their environment and location, and assuming all network communication is a threat until it is attested, authorized and secured [2].

Cotemporary organizations are transitioning to cloud technologies from their conventional systems with remote work becoming increasingly prevalent across various sectors like software development, where professionals operate from home or any location. With the growing demand for moving work from home, organizations seed to allow more workers to access their private networks through the employer's local internet [3] The Zero Trust Architecture constitutes an innovative framework aimed at addressing the challenge of safeguarding against unauthorized access and cyber threats. This paradigm is designed to ensure that access to critical information is restricted solely to authorized individuals. Failure to adhere to best practices can lead to vulnerability exposure. The surge in Internet of Things (IoT) devices in the modern digital age prompts the need for robust, protective measures. Addressing data leakage, particularly concerning sensitive information, and evaluating the sufficiency of a singular protective mechanism are essential considerations. Moreover, the adequacy of conventional access control models such as mandatory access control, discretionary access control, role-based access control, and attribute-based access control in thwarting sophisticated attacks remains uncertain, necessitating the adoption of innovative models to counter evolving threats effectively. The allure of delving into the Zero Trust Model as a research focus lies in exploring its implementation intricacies, the associated challenges, and the intricate nature of its application within expansive device-intensive organizational settings. The guiding principle of the Zero Trust Model, encapsulated by the ethos of "*never trust, always verify*" underpins its operational framework, emphasizing the imperative of continuous user and device authentication for resource access, irrespective of the request's origin or the desired resources. A compelling aspect of interest pertains to the deployment of the Zero Trust model within organizations, encompassing crucial considerations for successful implementation and post-deployment strategies. Understanding the comprehensive policy framework underpinning the zero-trust approach is pivotal for ensuring a seamless deployment process. Post-deployment evaluations are vital to assess the model's efficacy and scalability, informing subsequent steps for ongoing protection and adaptability in the face of evolving cybersecurity challenges.

II. LITERATURE

Employees operate outside the company's secure perimeter, making their devices vulnerable to attack. BYOD is where employees use their personal gadgets, like phones or laptops for work tasks, even if the company says "No" to BYOD, employees still bring their devices to work for personal use, like checking emails, or social media, this mix of personal and work devices can create security risks [4]. The Zero Trust Architecture (ZTA) is a strategy to enhance resource protection through precise authentication, minimal authorization, and continuous verification. Zero Trust Architecture offers a contemporary approach to cybersecurity, which results in significant cost savings by reducing the necessity for comprehensive manual oversight and enhancing the efficiency of security measures [5] Furthermore, Zero Trust Architecture mitigates the occurrence of data breaches through the enforcement of rigorous identity verification protocols, the principle of least privilege, and micro-segmentation. This is predicated on the assessment of trustworthiness in devices and services before the provision of access rights. ZTA is built on the notions of least privilege, granular access control and dynamic and strict policy enforcement wherein no user or device is implicitly trusted irrespective of stature or location [6] Meanwhile**,** the least privilege principle where users or roles are granted only the specific rights necessary to perform their tasks [7] This is to reduce the potential damage from compromised accounts or insider threat, and it is widely applied in ZTA system. The growth of Zero Trust Architecture has spiked over the years, but organizations are reluctant to invest in the security approach [8]. In the contemporary digital landscape, numerous organizations encounter a critical issue known as data breaches. This can incur financial losses due to the expenses associated with rectifying the issue and may also experience a decline in customer trust, leading to potential attrition. IBM. (2024) indicates that the average cost of a data breach jumped to USD 4.88 million from USD 4.45 million in 2023, a ten per cent spike and the highest increase since the pandemic [9].

III. RELATED WORK

This section elucidates the research contribution pertinent to the adoption of Zero Trust Architecture (ZTA) within organizational frameworks. The subsequent subsection delineates the prior empirical studies focusing on the implementation strategies of ZTA, cost and budget analysis, and cost-effectiveness, highlighting its potential to reduce data breaches, analysis of various ZTA tools and costs, and discussing the challenges of adopting ZTA. However, according to this study, the current expenses associated with the implementation of Zero Trust Architecture (ZTA) tools and resources necessitate timely updates.

IV. COST AND BUDGET ANALYSIS

Implementing Zero Trust Architecture (ZTA) requires a wide range of tools and resources tailored to your organization's unique security demands. This paper provides information on various Zero Trust tools that organizations can implement. Developed by leading providers, these tools offer diverse services that significantly elevate security measures. The entities including BlackBerry Cylance, Google, Microsoft, IBM, CrowdStrike, SentinelOne, Virtru, and Kaspersky have been designated as reliable providers and align with ZTA components. This paper assertively presents the latest pricing details for all tools firmly rooted in the user count. From this information, one can undeniably assess the total yearly cost of security tools. Consequently, the organization confidently pinpointed financial investment. Table 4.1 shows the security tools and current prices for 2024.

TABLE 4.1. ZTA TOOLS AND CURRENT PRICES AS OF 2024

Tools and Resources	Category	ZTA Component	Unit Cost per User	ZTA Tool cost is based on the total number of employees			
				1 - 100	101 - 400	401 - 700	701 - 1000
CylancePROTECT (Blackberry 2024)	Endpoint Protection	Subject and Resources	RM200.23 per Endpoint for 1-250 Endpoints RM185.77 per Endpoint for 501-1000 Endpoint	RM20,023.00	RM74,308.00	RM130,139.00	RM185,770.00
Kaspersky Endpoint Security for Business Advance with encryption (All Kaspersky Lab 2024)	Endpoint Protection + Data Encryption	Data Encryption-Subject and Resources PEP Endpoint Protection-Subject and Resources	RM199.38 per node	RM19,938.00	RM79,752.00	RM139,566.00	RM199,380.00
Falcon Go – Endpoint Protection. Next-gen AV – Device control – Mobile device protection – ingress support (CrowdStrike 2024).	Endpoint Protection	Subject and Resources	RM179.00 per node	RM17,900.00	RM71,600.00	RM125,083.00	RM179,000.00
SentinelOne – Singularity Core (SentinelOne 2024)	Endpoint Protection	Subject and Resources	RM211.00 per Endpoint for 5-100 workstations	RM21,100.00	RM84,376.00	RM132,223	RM211,000.00
Virtru for Business (Virtru 2024)	Data Security Encryption	Subject, Resources and PEP	RM999.29 includes 5 user	RM19,385.20	RM77,540.20	RM133,700.40	RM193,860.00
Microsoft Entra Suite with Identity-centric ZTNA (Microsoft 2024)	Identity Access Management	PEP in PDP	RM842.24 per user	RM84,224.00	RM336,896.00	RM589,568.00	RM842,240.00
Microsoft Entra ID P2 (Microsoft 2024)	Identity Access Management	PEP in PDP	RM97.00 per user	RM9,700.00	RM38,800.00	RM67,900.00	RM97,000.00
Microsoft Entra ID P1 (Microsoft 2024)	Identity Access Management	PEP in PDP	RM118.48 per user	RM11,848.00	RM47,392.00	RM82,936.00	RM118,480.00
Microsoft OneDrive Cloud Storage and File Sharing for Business – 1TB (Microsoft 2024)	Storage and File Sharing	Access control-PE in PDP Encryption-Subject, Resources PEP Cloud Storage - Resources	RM245.28 per user	RM24,528.00	RM98,112.00	RM171,696.00	RM245,280.00
Google Workspace – Business Standard with 2TB pooled storage (Google Workspace 2024).	Collaboration tools and Storage	Access Control – PE in PDP data Encryption – Subject, Resources and PEP	RM400.00 per user	RM40,000.00	RM160,000.00	RM280,000.00	RM400,000.00
Microsoft Sentinel – Analytic Log, Basic Logs, and Auxiliary Logs (Microsoft 2022).	Security Information and Event Management (SIEM) – Monitoring and Threat Detection	PEP, PA, and PE	Estimate is calculated – Pay-As-You-Go-SB-day	Estimated: Analytic Logs: 5 per day (GB) x 30 days x 30.81 = 5. Basic Logs: 100 per day (GB) x 30 days x 0.42 = RM12,600.00 Auxiliary Logs: 100 per day (GB) x 30 days x 0.00 = RM0, 000.00. RM11, 340 months. RM181, 880.00 per year			
IBM QRadar SIEM (IBM 2024).	Security Information and Event Management – Threat detection, monitoring, and response	PEP, PA, and PE	Estimation cost by total workstation and by total server in the environment.	100 workstations and 10 servers =RM418,831.00	400 workstations and 20 servers =RM626,500.02	700 workstations and 30 servers =RM842,922.22	1000 workstations and 35 servers =RM1,045.08
Security Engineer (ERI Economic Research Institute 2024).	Resources	PA and PDP	Average Base Salary RM74.20 per hour.	Hour/week =RM17,808.00	Hour/week =RM35,616.00	Hour/week =RM71,232.00	Hour/week =RM106,848.00

Table 4.1 includes ZTA tools from providers such as BlackBerry, Microsoft, IBM, Google, Virtru, and Kaspersky, with costs calculated by multiplying employee count by the annual unit cost of each security tools.

$$\mathbf{Cp} = n_e \; x \; \Phi_{uc} \qquad (4.1)$$

Cp: Security tool price.

$\mathbf{n_e}$: The number of employees.

$\mathbf{\Phi_{uc}}$: Unit cost of each tool per user.

The **Cp** is the security tool price which is calculated based on the number of employees ($\mathbf{n_e}$) multiply by the unit cost of each tool per user ($\mathbf{\Phi_{uc}}$).

Calculation of Virtru Tool

Price: RM969.29 includes 5-user

Total User:100 (as a sample)

Total Price = 100 x $\frac{969.29}{5}$

Total Price = RM19,385.20 per year

Calculation of CylancePROTECT (Endpoint Protection)

Price: RM200.23 per Endpoint for 1-250 Endpoints and RM185.77 per Endpoint for 501-1000 Endpoints.

Total Users: 400

Total Price: 400 x 185.77

Total Price = RM74,308.00

Calculation for Security Engineer Salary

Salary: Average Base Salary RM74.20 per hour (ERI Economic Research Institute 2024).

Total Hour Work per Week: 5 hours

Total Week per Year (take 48 weeks)

Salary = 74.20 x 5 x 48 = RM17, 808.00 per year

A. Scenario 1: SMBs or Large Enterprise with Complex IT Envoronments with Remote Workplace

Fig. 4.2 illustrates the ZTA security tools proposed design for SMBs complex environments with remote workplaces. The process begins by verifying the device's trustworthiness and authenticating the user through Microsoft Entra, while Kaspersky EPP reports device health (e.g., encryption, compliance). Microsoft Entra then evaluates identity and device compliance against conditional access policies, making an approve or deny decision based on risk signals. Approved users gain access to specific resources (e.g., OneDrive, internal systems), with all access logged, while denied requests are blocked. Finally, Microsoft Sentinel provides continuous monitoring for anomalies, ensuring ongoing threat detection and response. This end-to-end flow embodies Zero Trust principles, explicit verification, least-privilege access, and assumed breach to secure modern hybrid environments.

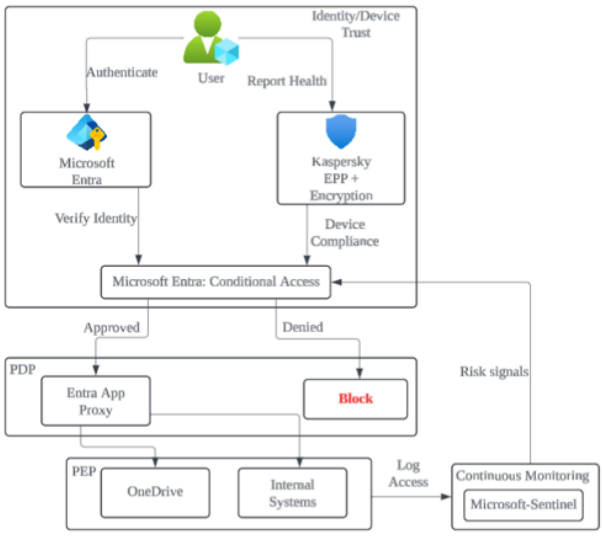

Fig. 4.2. ZTA selected security tools for SMBs with complete environments with remote workplace-proposed design

The project costs for an organization with 0-100 employees amount to RM294,906, while for those with 101-400 employees, the estimation is approximately RM595,368.00. For a workforce comprising 401-700 employees, the cost estimated to be around RM1,028,886, and for companies with an employee count ranging from 701-1000, the projected expenditure is RM1,396,548. (Fig. 4.3).

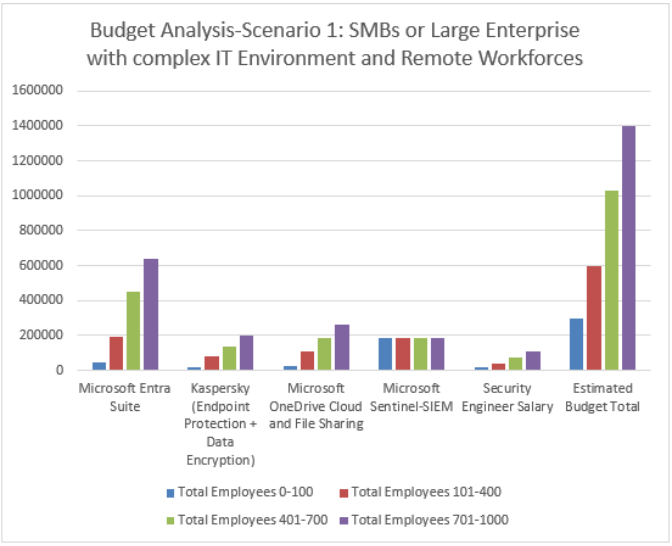

Fig. 4.3. Budget analysis for SMBs or large enterprises with complex IT environment and remote workforce

B. Scenario 2: Organization Collaborating Across Geographical Boundaries

Fig. 4.4 illustrates the proposed design of ZTA selected security tools for organization collaboration across geographical boundaries. The workflow begins with device trust verification and user authentication via Microsoft Entra, while Cylance PROTECT ensures endpoint security and encryption. Microsoft Entra then checks identity and device compliance, applying conditional access policies to either approve or deny access based on risk signals.

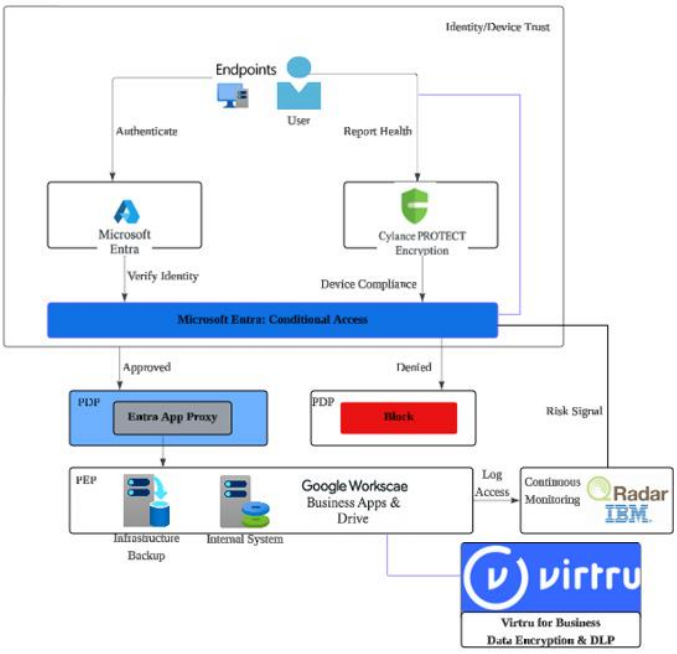

Fig. 4.4. ZTA selected security tools for organization collaborating across geographical boundaries-proposed designs

The projected expenditure for small businesses with a workforce of fewer than one hundred employees is RM159,897.20. In contrast, organizations with an employee count ranging from 701 to 1000 may incur costs of RM1,277,621.00.

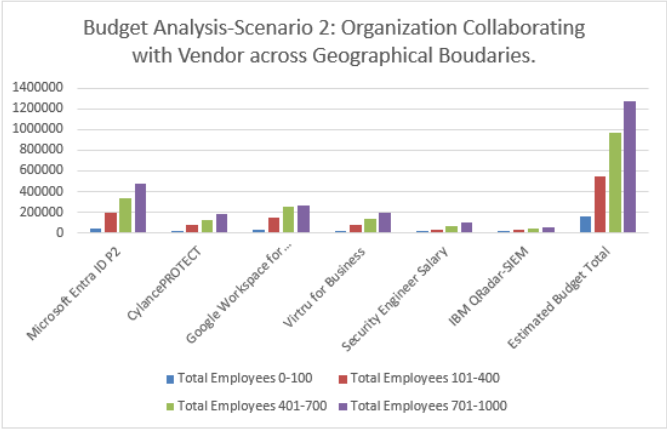

Fig. 4.5. Budget analysis for organizations collaborating with vendors across geographical boundaries

C. Scenario 3: Organization has Satelite Facilities or Branch Offices.

Fig. 4.6 illustrates a Zero Trust security architecture that begins with user and device authentication through Microsoft Entra ID P1, which enforces identity verification and multi-factor authentication. Endpoint trust is established with CrowdStrike Falcon (EPP) reporting device health and compliance status to ensure only secure devices gain access.

Microsoft Entra's conditional access policies then evaluate risk signals to either approve access to resources like OneDrive, and internal systems, or deny and block suspicious requests. Approved access is further protected by Virtru's data encryption and DLP to prevent data leaks, while Microsoft Sentinel continuously monitors and logs all access attempts for real-time threat detection and response. This end-to-end framework adheres to Zero Trust principles, explicit verification, least-privilege access, and continuous monitoring to secure hybrid environments against evolving threats.

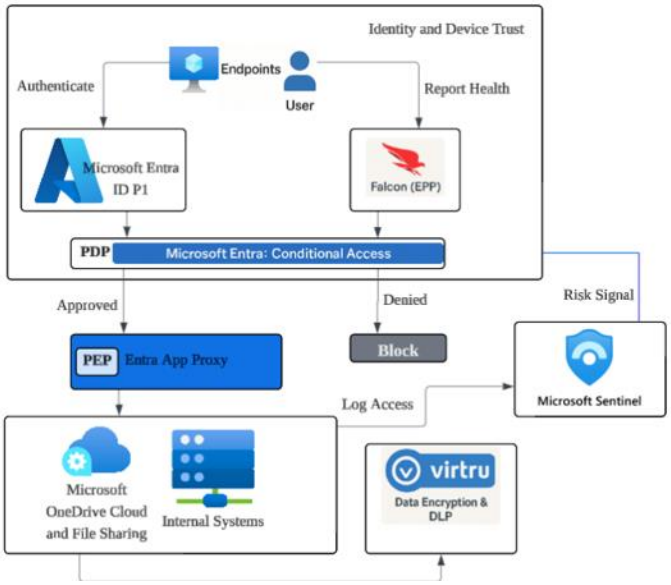

Fig. 4.6. Organization that has a satellite facility ore branch offices-proposed design

For organizations employing between 101 to 400 employees, the projected expense is RM561,506.20, which may be reduced depending on specific organizational needs. In addition, the comparison between ZTA and the traditional perimeter-based security model highlights clear advantages for organizations with satellite facilities or multiple branch offices. ZTA uses an identity-based trust model that continuously verifies every user and device, providing more efficient protection than perimeter-based security, which automatically trusts anything inside the network boundary.

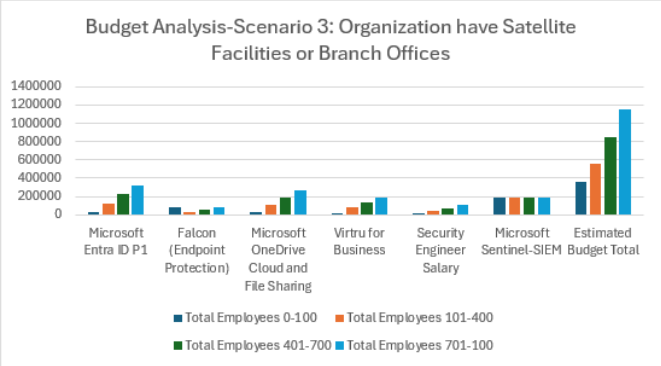

Fig. 4.7. Budget analysis for organizations that have satellite or branch offices

D. Scenario 4: Accessing Internet Resources via Organization-Managed Devices

Fig. 4.8 illustrates an identity and device trust architecture integrating Microsoft Entra P1, SentinelOne, and IBM QRadar SIEM. Users and endpoints initiate authentication through Microsoft Entra, which verifies identity and evaluates device compliance using health reports from SentinelOne Endpoint Protection. Based on conditional access policies, Microsoft Entra grants or denies access: approved users are routed through Entra App Proxy to access systems like Google Workspace for Business and internal systems, while denied attempts are blocked based on risk signals. Access logs from these systems are sent to IBM QRadar for monitoring and analysis, and data protection enforced via Virtru for Business, which handles encryption and secure access to sensitive information.

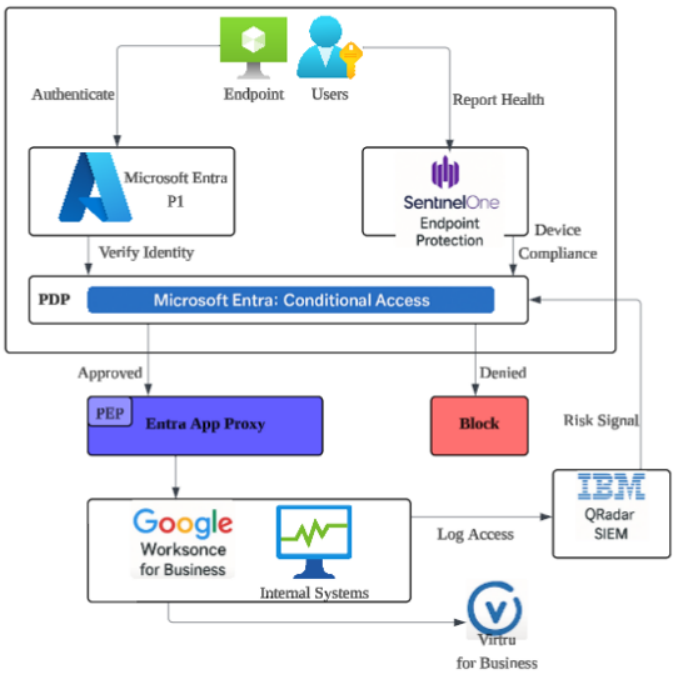

Fig. 4.8. Accessing internet resources via organization managed devices-proposed design

By evaluating the financial implications for an organization that employs 200 to 400 users, the projected expenditure estimated to be RM535,808.10 or less. From a data protection perspective, Zero Trust and IBM QRadar enforce continuous verification, encryption, and strict access controls across all locations, reducing the risk of lateral movement and insider threats. Meanwhile, perimeter-based models trust internal traffic by default, making them vulnerable once the network boundary breached. In addition, the perimeter-based lack the robust data protection and adaptability needed for modern distributed environments.

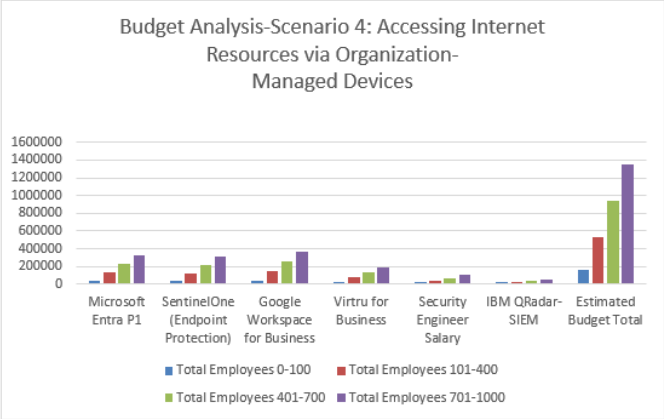

Fig. 4.9. Budget analysis for accessing internet resources via organization-managed devices

TABLE 4.2. BUDGET ANALYSIS

Tool Selection																
Access Control			Endpoint Protection				Cloud Storage		Data Encryption		Sec. Eag	SIEM		ZTA Budget-Based number of employees (RM)			
														1-100	101-400	401-700	701-1000
MS Entra Suite	MS Entra ID P2	MS Entra ID P1	Kaspersky	Cylance Protect	Falcon Go	Sentinel One	MS One Drive	Google Work-space	Kaspersky	Virtru		MS Sentinel	QRadar				
√			√				√		√		√	√		294,906	595,368	1,028,886	1,396,548
	√			√				√		√	√		√	159,897.20	549,008.10	965,703.9	1,277,621
		√			√		√			√	√	√		358,440.20	561,506.20	854,381	1,147,256
		√				√		√		√	√		√	154,248.20	535,808.10	942,603.90	1,344,621
	√		√				√		√		√	√		194,925	595,377	913,647	1,231,917

V. COST-EFFECTIVENESS OF ZTA

Cost-effectiveness (CE) is a critical metric for evaluating the financial feasibility of a security measure, specifically in the context of Zero-Trust Architecture (ZTA). This metric enables organizations to ascertain the justification for investing in ZTA by comparing the potential savings to the implementation cost. Annual Loss Expectancy (ALE) constitutes a risk assessment metric that quantifies the possible financial detriment arising from a particular threat or vulnerability. The primary objective of calculating cost-effectiveness (CE) is to evaluate whether the implementation of Zero Trust Architecture (ZTE) justified the financial investment. It provides insight into whether the expenditure on ZTA is outweighed by the savings derived from diminished risks. The cost-effectiveness calculated uses the following Equation 4.2.

$$CE = \frac{ALE_b - ALE_a}{ZTA} \quad (4.2)$$

CE: cost-effectiveness

ALE_b: annual loss expectancy before ZTA implementation

ALE_a: annual loss expectancy after ZTA implementation

ZTA: cost of implementing ZTA

(Adahman, Z., Malik, A. W., and Anwar, Z. 2022)

TABLE 4.3. ANNUAL LOSS EXPECTANCY BASED ON THE EMPLOYEE COUNT OF THE ORGANIZATION (ASSUMING AN EXCHANGE RATE OF 1 USD = 4.50 MYR)

Employees Total	2019 (USD) in million	2020 (USD) in million	2021 (USD) in million
Less than 500	2.74 (RM12.33)	2.35 (RM10.58)	2.98 (RM13.41)
500 to 1,000	2.65 (RM11.93)	2.63 (RM11.84)	2.95 (RM13.28)
1,001 to 5,000	3.78 (RM17.01)	4.09 (RM18.41	4.27 (RM19.22)
5,001 to 10,000	4.41 (RM19.85)	4.72 (RM21.24)	4.35 (RM19.58)
10,001 to 25,000	5.15 (RM23.18)	4.61 (RM20.75)	5.52 (RM24.84)
More than 25,000	5.11 (RM22.99)	4.25 (RM19.13)	5.33(RM23.99)

A. Case Study 1: Uber Data Breach

In the year 2016, unauthorized individuals infiltrated the Uber network and exfiltrated sensitive data about approximately 57 million individuals. This compromised data encompassed both clientele and operators. The intruders were able to exploit vulnerability due to the inadvertent dissemination of a critical access key on a digital repository known as GitHub. GitHub serves as a platform where software developers exchange and collaborate on programming code. This oversight facilitated the hackers' seamless entry into Uber's technological infrastructure. Based on the immediate consequences, after the breach, Uber decided to pay the hackers $100,000 (RM444,800.00).

B. Case Study 2: Utah Food Brank

Based on Utah Food Bank's total number of employees, which is below five hundred headcounts, the Annual Loss Expectancy or ALE is RM13.41 million (Table 4.3). The ZTA average cost for a headcount below five hundred employees is around RM535,808.10. This cost taken from the ZTA tools and resources from Table 4.1.

TABLE 4.4. FINANCIAL HISTORY OF UBER

Year	Total of Employees	IT, Distribution & Other Costs (RM)	Data Breach Cost (RM)	Revenue (RM)
2018	22, 263	322M	00.00M	51,742M
2019	26, 900	271.4M	00.00M	64,510.32M
2020	22, 800	2,116M	00.00M	51,244.4M
2021	29, 300	3.002.8M	706.63M	80,153M

TABLE 4.5. IMPLEMENTATION COST-UBER

Year	Total Employee	Technology Distribution & Other Cost (RM)	IT Budget (RM)	ZTA Costs (RM)	Difference (IT Budget – ZTA Cost) (RM)
2021	29,300	3,002,800,000	450,370,000	17,665, 750	435,718,180

TABLE 4.6. INITIAL ZTA IMPLEMENTATION COST-UTAH FOOD BANK

Year	Total Employee	Development Cost (RM)	IT Budget (RM)	ZTA Costs (RM)	Difference (IT Budget – ZTA Cost) (RM)
2021	50-200	9,063,826.80	1,359,574.02	**535,808.10**	823,765.92

For the Utah Food Bank case, there are 10,000 donors whose personal information was disclosed in 2015. The SLE for the year 2015 and the year 2021 is calculated as below.

SLE = Average Per-record Cost of Data Breach x 10,000 = 154 x 10,000 = USD1, 540, 000. (RM6,849,920.00).

SLE = Average Per-record Cost of Data Breach x 10,000 = 161 x 10,000 = USD1,610,000. (RM7,169,641.55).

This means that Utah Food Bank's single loss expectancy for the years 2015 and 2021 respectively RM684,992.00mand RM7,169,641.55. Based on Utah Food Bank's total number of employees, which is below five hundred headcounts, the Annual Loss Expectancy or ALE is RM13.41 million (Table 4.3). The ZTA average cost for a headcount below five hundred employees is around RM535,808.10. This cost taken from the ZTA tools and resources from Table 4.1.

VI. REDUCE DATA BREACH MODEL

The primary objective of assessing the diminished risk of data breaches is to illustrate the potential savings an organization can achieve by implementing Zero Trust Architecture over four years. This aspect is crucial, as companies investing in ZTA are keen to understand whether it will lead to long-term financial benefits. To reduce the likelihood of a compromised account, ZTA is the best alternative for the organization.

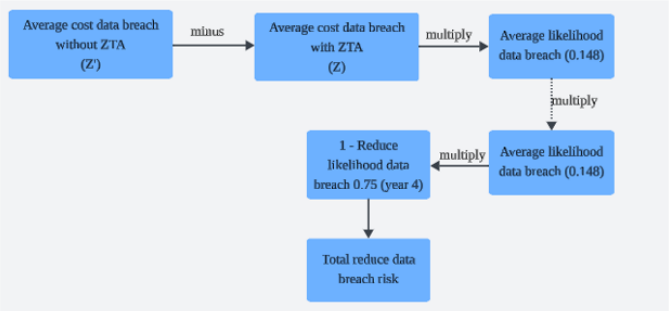

Fig. 4.11. Reduce data breach model

Ponemon Institute and IBM Security (2021) mentioned in their report that the average cost of a data breach can be calculated based on the organization's headcount. The statistical probability of an organization encountering a data breach involving 10,000 records or more stands at 29.6% over two years. Consequently, this translates to a 14.8% probability within a one-year timeframe. Implementing a zero-trust security framework can significantly decrease an organization's risk exposure by a minimum of 37 per cent and lower security expenditures by 31 per cent, thereby conserving not only financial resources and time but also minimizing unnecessary energy spent on superfluous IT investments [10]. A twenty-per-cent downward modification is explicitly implemented in relation to the diminished risk associated with the data breach metric. This modification embodies a more prudent methodology in assessing the financial advantages of enacting security measures recognizing that actual results may deviate from forecasts [11].

TABLE 4.7. REDUCED RISK ANALYSIS OF DATA BREACHES FOR ORGANIZATIONS WITH OVER 25,000 EMPLOYEES (USD1=4.45 MYR)

Component	Source	Year 1	Year 2	Years 3	Year 4
Average Cost Data Breach without ZTA (Z')	Ponemon Institute and IBM Security (2021)	23,746,053.35	23,746,053.35	23,746,053.35	23,746,053.35
Average Cost Data Breach with ZTA (Z)	Ponemon Institute and IBM Security (2021)	19,529,885.96	16,542,437.65	14,622,988.05	13,713,035.51
Difference Average Cost	-(Z' – Z)	4,216,167.39	7,203,615.70	9,123,065.30	10,033.017.84
Average Likelihood Data Breach (φ)	Forrester Research (%)	0.148	0.148	0.148	0.148
Reduced Likelihood Data Breach (ψ)	Forrester Research (%)	0.37	0.52	0.64	0.75
Reduced Data Breach Risk	−(Z' * φ - Z) * (φ * (1 - ψ))	1,493,282.43	925,510.67	591,864.72	377,348.93
Risk Adjustment	Forrester Consulting (2021)	0.20	0.20	0.20	0.20
Adjusted Reduced Data Breach Risk		298,656.49	185,102.13	118,372.94	75,469.79
Total Reduces Data Breach Risk					**3,388,006.75**
Total Adjustment Data Breach Risk					**677,601.35**

TABLE 4.8. REDUCED RISK ANALYSIS OF DATA BREACHES FOR ORGANIZATIONS WITH BELOW 500 EMPLOYEES (USD1=4.46 MYR)

Component	Source	Year 1	Year 2	Year 3	Year 4
Average Cost Data Breach without ZTA (Z')	Ponemon Institute and IBM Security (2021)	13,316,152.04	13,316,152.04	13,316,152.04	13,316,152.04
Average Cost Data Breach with ZTA (Z)	Ponemon Institute and IBM Security (2021)	19,529,885.96	16,542,437.65	14,622,988.05	7,684,888.08
Difference Average Cost	-(Z' – Z)	(6,213,733.92)	(3,226,285.61)	(1,306,836.01)	5,631,263.96
Average Likelihood Data Breach (φ)	Forrester Research (%)	0.148	0.148	0.148	0.148
Reduced Likelihood Data Breach (ψ)	Forrester Research (%)	0.37	0.52	0.64	0.75
Reduced Data Breach Risk	−(Z' * φ - Z) * (φ x (1 - ψ))	1,637,210.06	1,035,169.81	674,109.09	211,421.61
Risk Adjustment	Forrester Consulting (2021)	0.20	0.20	0.20	0.20
Adjusted Reduced Data Breach Risk		327,442.01	207,033.96	134,821.82	42,284.32
Total Reduces Data Breach Risk					**3,557,910.57**
Total Adjustment Data Breach Risk					**711,582.11**

VII. EVALUATE HOW ZTA REDUCE DATA BREACH COST

Case Study: Target's Data Breach

In 2013, a significant security incident took place at Target, a prominent retail corporation. The cybercriminals, in total, breached the credit and debit card information of around 40 million customers, along with the personal details of 70 million customers, including names, addresses, and phone numbers [12].

TABLE 4.9. TARGET'S FINANCIAL HISTORY (ADAHMAN, Z., MALIK, A. W., AND ANWAR, Z., 2022

Year	No. of Employee	IT, Distribution and other costs (million)	Data Breach Costs (ALE) (million)	Revenue (million)
2015	**347000**	**$773**	**$39**	**$74,494**
2016	341000	$587	0	$70,271
2017	**323000**	**$620**	**$292 (RM 1,305,240,000)**	**$72,714**
2018	345000	$568	0	$75,365
2019	360000	$811	0	$78,112
2020	368000	$917	0	$93,561
2021	409000	$600	0	$103,328

TABLE 4.10. TARGET'S INITIAL ZTA IMPELEMTATION COST YEAR (USD1=RM4.50)

Category	
No. of Employee	409,000
IT Budget	RM405,000,000.00
ZTA Cost (take 15% of the cost spent on data breach)	RM197,100,000.00
Difference (IT budget – ZTA Costs)	RM207,900,000.00

Total Data Breach Cost without ZTA

Annual Loss Expectancy (ALE) for Target is RM1 305 240,000

Total Data Breach costs without ZTA (ALE) over 4 years: RM 1,305,240,000 * 4 = RM5,220,960,000

Total Risk Reduction after ZTA Implemented

Risk reduction by ZTA over 4 years (table 4.7): RM3,388,066.75

Adjusted Data Breach Risk after ZTA

Adjusted data breach risk over 4 years: RM677,601.35 (table 4.7)

ZTA Implementation Cost

RM 197,100,00.00

Calculate the Net Benefit of ZTA

ZTA Net Benefit = Total Data Breach Cost Without ZTA– (ZTA Implementation Cost + Adjusted Risk After ZTA)

= 1,305,240,000 – (197,100,000 + 677,601.35)

= 1,305,240,000 – 197,777,601.35

= 1,107,462,398.65

In conclusion, ZTA implementation is expected to decrease the potential penalty or fine from a data breach by around RM1,107,462,398.65 over four years, once the implementation costs and the adjusted risk post-ZTA are considered. This indicates that the company stands to save a substantial amount by investing in ZTA, rendering it a highly economical approach to mitigating the risk and financial consequences of data breaches.

VIII. CONCLUSION AND FUTURE DIRECTION

This research provides a comprehensive cost-benefit analysis of Zero Trust Architecture (ZTA), highlighting its financial and security benefits as a threat mitigation strategy. The study's findings indicate that implementing ZTA leads to substantial financial savings, demonstrating an average reduction of RM711K in risk impact over four years for organizations. This underscores ZTA's cost-effectiveness and its potential to improve an organization's overall security posture and financial performance by reducing data breach costs and risks.

The fortcoming research may evaluate the Role of AI and Automation in mitigating data breach costs through a comprehensive cost-benefit analysis of the implementation of AI and automation within security operations. This investigation could emphasize the extent to which AI-driven preventive workflows, including attack surface management and posture management, yield substantial cost reductions in breach situations.

ACKNOWLEDGMENT

I would like to express my sincere gratitude to Associate Professor Ts. Dr. Siti Hajar Othman for her valuable guidance, continuous support, and constructive feedback throughout this research. Her expertise and insights greatly contributed to the successful completion of this study.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest regarding the publication of this paper.

REFERENCES

[1] Bertino, E., & Brancik, K. (2021). Services for zero trust architectures—A research roadmap. In *2021 IEEE International Conference on Web Services (ICWS)* (pp. 14–20). IEEE. https://doi.org/10.1109/ICWS53863.2021.00016.

[2] Lawrence, V., Pawar, M., & Sheikh, N. (2021). Zero trust using network micro segmentation. *IEEE Xplore*, 1–6.

[3] Kim, Y., & Yiliyaer, S. (2022). Secure access service edge: A zero trust based framework for accessing data securely. In *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 586–591). IEEE.

[4] Foo, E., Hussain, M., Pal, S., Kanhere, S., & Jadidi, Z. (2024). Federated zero trust architecture using artificial intelligence. *IEEE Wireless Communications, 31*(2), 30–35.

[5] Lee, S., Shieh, S. W., & Tsai, M. (2024). Strategy for implementing of zero trust architecture. *IEEE Transactions on Reliability*, 1–8.

[6] Anwar, A., Baig, Z., Doss, R., Shaghaghi, A., Shah, S. W., & Syed, N. F. (2022). Zero trust architecture (ZTA): A comprehensive survey. *IEEE Access, 10*, 57143–57179. https://doi.org/10.1109/ACCESS.2022.3174679.

[7] Brazhuk, A., & Fernandez, E. B. (2024). A critical analysis of zero trust architecture (ZTA). *Computer Standards & Interfaces, 89*, 103832. https://doi.org/10.1016/j.csi.2024.103832.

[8] Adahman, Z., Anwar, Z., & Malik, A. W. (2022). An analysis of zero-trust architecture and its cost-effectiveness for organizational security. *Computers & Security, 122*, 102911. https://doi.org/10.1016/j.cose.2022.102911.

[9] IBM. (2024). *Cost of a data breach 2024*. IBM. https://www.ibm.com/reports/data-breach.

[10] Jones, C. (2021). *5 reasons to use zero trust architecture*. Red River. https://redriver.com/security/5-reasons-for-zero-trust.

[11] Forrester Consulting. (2021). *The total economic impact™ of zero trust solutions from Microsoft* (pp. 1–40). Microsoft. https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft-Zero-Trust-TEI-Study.pdf.

[12] Young, K. (2021). *Cyber case study: Target data breach*. CoverLink Insurance. https://coverlink.com/cyber-liability-insurance/target-data-breach.