Journal of Information Technology and Computer Science (INTECOMS)
Volume 8 Nomor 6, Tahun 2025
e-ISSN : 2614-1574
p-ISSN : 2621-3249

PENERAPAN KEAMANAN JARINGAN ZERO TRUST NETWORK ACCESS BERBASIS CLOUDFLARE ZERO TRUST DALAM LAYANAN BERBASIS INTERNET

IMPLEMENTATION OF CLOUDFLARE ZERO TRUST NETWORK ACCESS SECURITY IN INTERNET-BASED SERVICES

Nandang Sutisna[1], Hilmi Muhammad Dafa[2]
Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika[1,2]
nandang.sutisna@gmail.com[1], dafa.hilmi22@gmail.com[2]

ABSTRACT

Internal data security is a crucial aspect in addressing the increasing cyber threats on internet-based services. Zero Trust Network Access (ZTNA) provides a modern security approach with the principle of "never trust, always verify," offering strict identity verification and minimal access permissions. This research aims to implement and evaluate ZTNA using Cloudflare Zero Trust to enhance the security of digital services. The methodology involves designing a virtual lab environment using Proxmox, testing access to several internal applications via Cloudflare Tunnel and Cloudflare Access, and configuring authentication based on SSO and OTP. The results show that the Zero Trust policies successfully prevent unauthorized access and improve identity control efficiently. This study offers practical contributions for small to medium-sized organizations in implementing an efficient and cost-effective Zero Trust security model.

Keywords: *Zero Trust, ZTNA, Cloudflare Zero Trust, Identity Verification, Multi-Factor Authentication*

ABSTRAK

Keamanan data internal merupakan aspek fundamental dalam menghadapi eskalasi ancaman siber pada layanan berbasis internet. Zero Trust Network Access (ZTNA) hadir sebagai pendekatan keamanan modern dengan prinsip *never trust, always verify*, yang menekankan verifikasi identitas secara ketat dan pembatasan akses minimal. Penelitian ini bertujuan mengimplementasikan serta mengevaluasi ZTNA berbasis Cloudflare Zero Trust untuk meningkatkan keamanan layanan digital. Metode yang digunakan meliputi perancangan lingkungan virtual berbasis Proxmox, konfigurasi akses aplikasi internal melalui Cloudflare Tunnel dan Cloudflare Access, serta penerapan autentikasi berbasis *Single Sign-On* (SSO) dan *One-Time Password* (OTP). Hasil pengujian menunjukkan bahwa penerapan kebijakan Zero Trust mampu mencegah akses tidak sah, memperkuat kontrol identitas, dan meningkatkan efisiensi pengelolaan keamanan. Temuan ini memberikan kontribusi praktis bagi organisasi berskala kecil hingga menengah dalam menerapkan model keamanan berbasis Zero Trust yang efektif dan terjangkau.

Kata Kunci: Zero Trust, ZTNA, Cloudflare Zero Trust, Identity Verification, Multi-Factor Authentication

PENDAHULUAN

Keamanan data dan akses jaringan menjadi salah satu prioritas utama di era digital, terutama ketika organisasi mengadopsi layanan berbasis internet, platform cloud, dan pola kerja jarak jauh. Kondisi ini meningkatkan risiko pelanggaran data yang umumnya terjadi melalui kompromi identitas. Laporan Verizon Data Breach Investigations Report (2023) mencatat bahwa lebih dari 80% insiden pelanggaran data disebabkan oleh pencurian kredensial atau penyalahgunaan identitas [1]. Fakta ini menunjukkan lemahnya mekanisme autentikasi sebagai titik lemah utama pertahanan siber.

Di Indonesia, banyak organisasi skala kecil hingga menengah masih mengandalkan model keamanan tradisional berbasis perimeter, seperti penggunaan firewall dan Virtual Private Network (VPN), untuk melindungi layanan internal. Pendekatan ini mengasumsikan bahwa semua entitas di dalam jaringan adalah tepercaya setelah berhasil melewati perimeter. Namun, pola ini tidak lagi relevan untuk menghadapi ancaman modern, karena tidak melakukan verifikasi identitas secara berkelanjutan. Akibatnya, serangan seperti *credential theft* dan *lateral movement* tetap memungkinkan meskipun proteksi perimeter diterapkan [2]. Selain

itu, solusi VPN/firewall tradisional memerlukan biaya lisensi dan perangkat keras tambahan, serta konfigurasi yang kompleks, sehingga kurang sesuai untuk organisasi dengan sumber daya terbatas [3].

Sebagai respons terhadap kelemahan ini, Zero Trust Network Access (ZTNA) muncul sebagai paradigma baru dengan prinsip never trust, always verify. Pendekatan ini mengganti kepercayaan implisit dengan verifikasi identitas ketat setiap kali akses dilakukan, menggunakan mekanisme kontrol berbasis identitas, Multi-Factor Authentication (MFA), metode passwordless, dan validasi postur perangkat [4][5]. Dokumen NIST SP 800-207 menegaskan bahwa arsitektur keamanan berbasis perimeter tidak lagi memadai untuk melindungi sistem modern [6].

Namun, implementasi ZTNA pada penelitian sebelumnya umumnya berfokus pada organisasi berskala besar, dengan model arsitektur yang kompleks seperti Software Defined Perimeter (SDP) atau solusi berbasis broker [7][8]. Hal ini menimbulkan kesenjangan (gap) bagi organisasi kecil-menengah yang memerlukan solusi ringan, hemat biaya, dan mudah diimplementasikan tanpa investasi infrastruktur yang besar.

Cloudflare Zero Trust merupakan salah satu platform yang menawarkan implementasi ZTNA secara praktis, dengan integrasi penyedia identitas populer (Google, GitHub), dukungan MFA dan passwordless, serta pengelolaan kebijakan berbasis identitas tanpa memerlukan perangkat keras tambahan [9]. Dengan arsitektur cloud-native, platform ini mampu mengurangi kompleksitas sekaligus meningkatkan keamanan akses aplikasi internal.

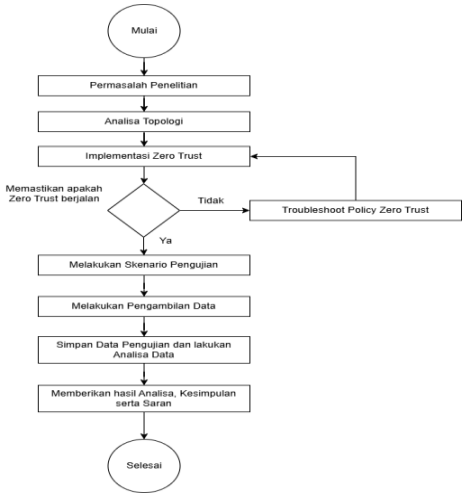
Penelitian ini berkontribusi dengan mengimplementasikan dan mengevaluasi efektivitas Cloudflare Zero Trust dalam memperkuat keamanan akses terhadap layanan internal berbasis internet, khususnya pada lingkungan jaringan berskala kecil hingga menengah. Fokus utama penelitian mencakup penerapan autentikasi berlapis, verifikasi identitas berbasis konteks, serta analisis kelebihan Cloudflare Zero Trust dibanding pendekatan tradisional dari sisi keamanan dan efisiensi operasional. Dengan demikian, hasil penelitian ini diharapkan dapat memberikan alternatif yang relevan dan praktis bagi organisasi yang menghadapi keterbatasan sumber daya, namun tetap membutuhkan penguatan keamanan jaringan.

METODE PENELITIAN

Penelitian ini menggunakan metode kuantitatif, yang bertujuan untuk mengukur dan menganalisis efektivitas penerapan Zero Trust Network Access (ZTNA) berbasis Cloudflare Zero Trust pada layanan berbasis internet. Data numerik diperoleh dari log Cloudflare, statistik autentikasi, dan performa layanan untuk mendukung hasil penelitian secara objektif dan terukur serta pengukuran secara manual. Lingkungan lab dibangun menggunakan Proxmox Virtual Environment untuk menjalankan aplikasi internal seperti WordPress CMS, LibreNMS, Zabbix, dan Omada Controller.

Implementasi dilakukan melalui pembuatan Cloudflare Tunnel, konfigurasi Cloudflare Access dengan autentikasi Single Sign-On (SSO) menggunakan Google dan One-Time Password (OTP), serta penerapan kebijakan akses berbasis wilayah (regional-based policy) dan alamat IP (IP-based policy).

Pengujian dilakukan dengan mengukur: (1) jumlah autentikasi berhasil/gagal, (2) waktu respons OTP, (3) performa loading aplikasi setelah autentikasi, dan (4) perbandingan biaya dengan solusi firewall tradisional. Data diperoleh dari log Cloudflare, dan pencatatan manual, kemudian dianalisis secara deskriptif kuantitatif menggunakan tabel dan grafik.

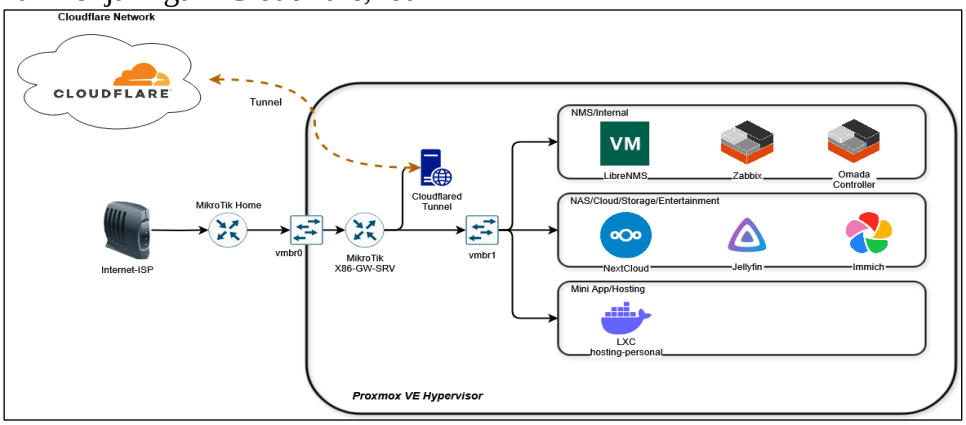


Gambar 2.1 Flowchart Penelitian

HASIL DAN PEMBAHASAN

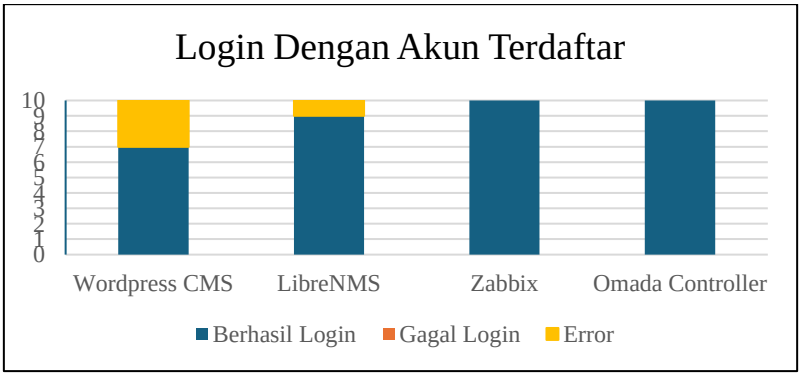
Implementasi Cloudflare Zero Trust

Lab virtual dibangun pada Proxmox Virtual Environment dengan 4 aplikasi internal yang di install: WordPress CMS, LibreNMS, Zabbix, dan Omada Controller. Akses ke aplikasi tersebut melalui Cloudflare Tunnel yang menghubungkan server lokal ke jaringan Cloudflare, dan Cloudflare Access untuk mengelola autentikasi pengguna serta policy. Dua metode autentikasi diterapkan, yaitu Google SSO dan OTP melalui email. Kebijakan akses dibatasi menggunakan regional-based policy dan IP-based policy untuk memfilter lokasi serta sumber koneksi.



Gambar 3.1 Topologi Jaringan lab virtual

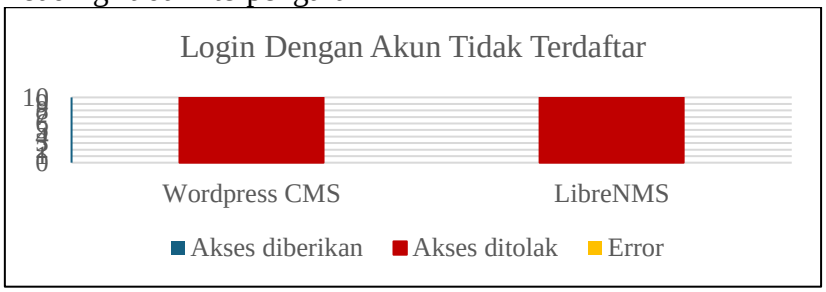
Hasil Pengujian



Gambar 3.2 Hasil Parameter Pengujian Autentikasi dengan Akun Terdaftar

Pengujian dilakukan terhadap 4 layanan yang telah dibatasi aksesnya menggunakan Cloudflare Access, yakni WordPress CMS, LibreNMS, Zabbix, dan Omada Controller. Setiap layanan diuji dengan akun yang telah terdaftar di daftar email ‘allowed team’, untuk mengetahui seberapa ampuh Cloudflare Access dalam mengautentikasi akses yang sah. Pengujian waktu pengiriman kode OTP menunjukkan rata-rata durasi 5–7 detik, yang dinilai cukup responsif untuk proses autentikasi multifaktor. Uji performa pemuatan aplikasi setelah autentikasi menunjukkan bahwa waktu loading tidak terpengaruh signifikan oleh penerapan Cloudflare Zero Trust.

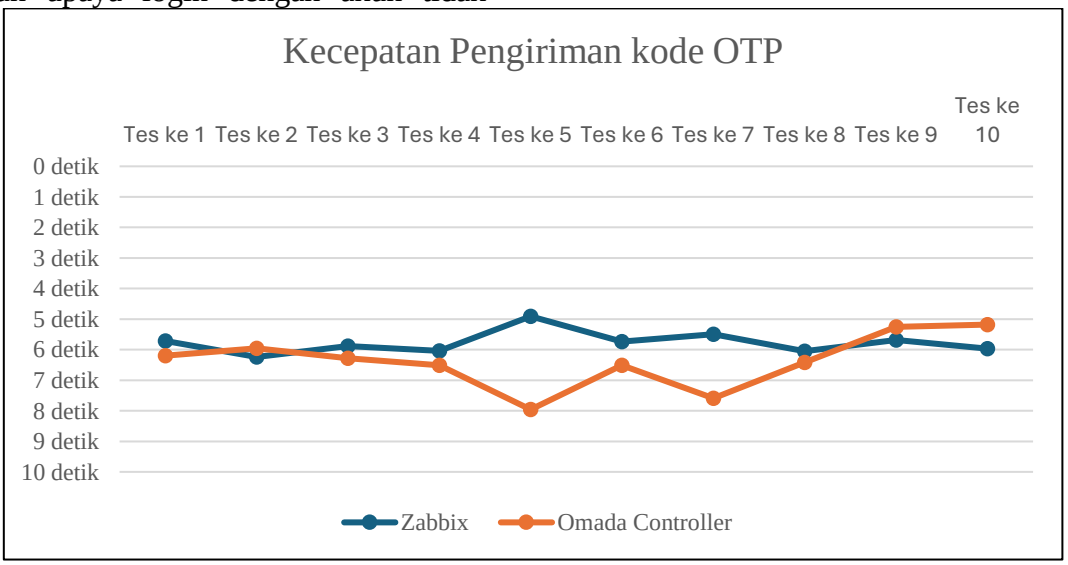
Berdasarkan grafik yang ditampilkan, seluruh layanan berhasil memproses autentikasi dengan tingkat keberhasilan tinggi. Pada Zabbix dan Omada Controller, seluruh login berhasil tanpa adanya kegagalan atau error. Sementara itu, pada LibreNMS dan WordPress CMS, ditemukan sejumlah kecil kegagalan login dan error. Error yang ditampilkan adalah ‘Current authentication token is expired’ padahal pada kenyataannya muncul histori berhasil login pada log Cloudflare Access.



Gambar 3.3 Hasil Hasil Parameter Pengujian Autentikasi dengan Akun tidak Terdaftar

Pengujian difokuskan pada 2 layanan, yakni WordPress CMS dan LibreNMS, yang menggunakan metode autentikasi via Single Sign-On (SSO) Google. Pengujian dengan metode OTP tidak dilakukan karena akun yang tidak terdaftar tidak akan menerima kode autentikasi, sehingga skenario pengujian menjadi tidak relevan.

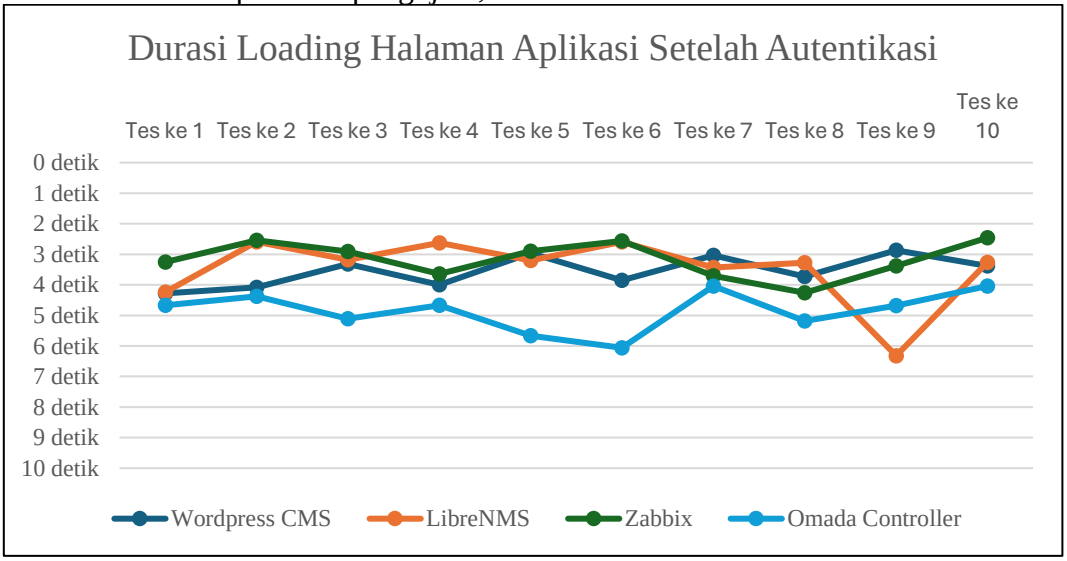
Hasil pengujian menunjukkan bahwa seluruh upaya login dengan akun tidak terdaftar berhasil ditolak oleh sistem, sebagaimana ditunjukkan pada grafik. Masing-masing layanan dilakukan 10 percobaan login dan hasilnya tidak ada akses yang diberikan maupun error selama proses autentikasi.



Gambar 3.4 Hasil Parameter Pengujian Durasi Pengiriman Kode OTP

Dari hasil diatas dapat disimpulkan bahwa Cloudflare Access mampu mengirimkan OTP dengan waktu yang cukup cepat dan konsisten. Tidak terdapat

keterlambatan ekstrem atau error pengiriman selama proses pengujian, sehingga sistem dinilai responsif dan andal dalam skenario autentikasi OTP.



Gambar 3.5 Hasil Durasi Loading Halaman Aplikasi Setelah Autentikasi

Setelah proses autentikasi berhasil dilakukan, pengujian difokuskan pada pengukuran waktu loading halaman depan dari masing-masing aplikasi yang diuji. Tujuan utama dari pengujian ini adalah untuk mengevaluasi apakah penerapan Cloudflare Access, yang merupakan bagian dari arsitektur Cloudflare Zero Trust Network Access (ZTNA), memberikan dampak terhadap kecepatan akses pengguna terhadap aplikasi yang bersangkutan. Parameter yang digunakan dalam pengujian ini adalah Largest Contentful Paint (LCP), yaitu waktu yang dibutuhkan untuk menampilkan konten utama terbesar pada halaman, yang dianggap sebagai indikator penting dalam menghitung kecepatan dari sisi pengguna.

Masing-masing aplikasi menjalani sepuluh kali pengujian, dan waktu LCP dicatat pada setiap percobaan. WordPress CMS dan LibreNMS menggunakan metode autentikasi berbasis akun Google, sedangkan Zabbix dan Omada Controller menggunakan metode autentikasi berbasis OTP (One-Time Password).

Tabel 3.1 Perbandingan Biaya Cloudflare dengan Firewall Tradisional

Platform/Model	Estimasi Harga
Cloudflare Zero Trust Free	Gratis, hingga 50 pengguna (ZTNA & Cloudflare Gateway)
Cloudflare Zero Trust Access	$3 per pengguna dan per bulan
Sophos XGS 87 dengan lisensi Statefull	Sekitar $430-$520
Sophos XGS 2100	Sekitar $2360-$2410 (Belum termasuk lisensi)
Fortinet Fortigate 40F	Sekitar $411 (Belum termasuk lisensi)
Fortinet Fortigate 101F + lisensi 5 tahun	Sekitar $16150

Tabel diatas menyajikan perbandingan estimasi harga antara platform Cloudflare Zero Trust dengan beberapa solusi firewall tradisional dari vendor ternama seperti Sophos dan Fortinet. Dari sisi biaya, Cloudflare Zero Trust menawarkan model harga yang jauh lebih fleksibel. Untuk skala kecil hingga

menengah, Cloudflare menyediakan paket gratis yang mendukung hingga 50 pengguna, mencakup fitur Zero Trust Network Access (ZTNA) dan Cloudflare Gateway. Sementara untuk kebutuhan yang lebih kompleks atau pengguna yang lebih banyak, tersedia paket Cloudflare Zero Trust Access dengan biaya sekitar $3 per pengguna per bulan.

Sebaliknya, solusi firewall tradisional seperti Sophos dan Fortinet umumnya membutuhkan investasi awal yang cukup besar. Misalnya, perangkat Sophos XGS 87 dengan lisensi stateful firewall dibanderol sekitar $430 hingga $520, sedangkan model Sophos XGS 2100, yang ditujukan untuk skala lebih besar, dijual pada kisaran $2360 hingga $2410 dan belum termasuk lisensi tambahan. Fortinet juga menawarkan berbagai model seperti Fortigate 40F dengan harga sekitar $411 (belum termasuk lisensi), hingga Fortigate 101F dengan lisensi 5 tahun yang diperkirakan mencapai $16.150.

KESIMPULAN

Berdasarkan hasil penelitian dan pengujian yang telah dilakukan, dapat disimpulkan bahwa penerapan Zero Trust Network Access (ZTNA) berbasis Cloudflare Zero Trust mampu meningkatkan keamanan akses terhadap layanan berbasis internet, khususnya dalam konteks pengelolaan identitas pengguna dan perangkat. Dengan menerapkan kebijakan autentikasi seperti SSO (single sign-on) dan IdP (identity provider) menggunakan Google dan metode tanpa kata sandi (passwordless) seperti OTP ataupun one-time link, sistem dapat memberikan perlindungan yang lebih baik terhadap ancaman akses tidak sah.

Pengujian terhadap parameter autentikasi menunjukkan bahwa layanan yang dilindungi oleh kebijakan Zero Trust berhasil menolak akses dari akun tidak terdaftar, serta mampu memberikan proses autentikasi yang cepat dan stabil melalui OTP maupun SSO. Selain itu, dari sisi biaya dan kemudahan implementasi, Cloudflare Zero Trust terbukti menjadi solusi yang efisien dan praktis, khususnya bagi organisasi atau individu dengan sumber daya terbatas. Implementasi tidak memerlukan perangkat keras tambahan dan dapat diintegrasikan langsung dengan layanan yang sudah berjalan.

Dengan pendekatan ini, penelitian ini berhasil menyajikan kerangka implementasi ZTNA yang dapat digunakan oleh organisasi kecil hingga menengah sebagai referensi dalam membangun sistem keamanan modern yang lebih adaptif terhadap ancaman siber.

DAFTAR PUSTAKA

1. Verizon. (2023). Data Breach Investigations Report (DBIR).
2. Kipkoech, R., & Ng'etich, S. (2023). A Survey of Security in Zero Trust Network Architectures. Journal of Cybersecurity, 12(2), 45-59.
3. Gartner. (2022). Market Guide for Zero Trust Network Access.
4. Kang, H., Liu, G., Wang, Q., Meng, L., & Liu, Y. (2023). Theory and Application of Zero Trust Security: A Brief Survey. IEEE Access, 11, 56023-56040.
5. NIST. (2020). SP 800-207: Zero Trust Architecture.
6. ENISA. (2022). Zero Trust Architecture: State of Play.
7. Yeoh, W., Liu, M., Shore, M., & Jiang, F. (2023). Zero Trust Cybersecurity: Critical Success Factors and a Maturity Assessment Framework. Computers & Security, 129, 103199.
8. Google. (2014). BeyondCorp: A New Approach to Enterprise Security.
9. Cloudflare Inc. (2023). Cloudflare Zero Trust Documentation.
10. IBM Security. (2023). Cost of a Data Breach Report 2023.
11. Microsoft. (2022). Zero Trust Adoption Report.
12. Palo Alto Networks. (2022). Zero Trust Best Practices.

13. CISCO. (2023). Zero Trust Model Explained.
14. Forrester. (2022). The State of Zero Trust Security.
15. Trend Micro. (2023). Implementing Zero Trust for SMBs