International Journal of Research in Interdisciplinary Studies
Volume 3, Issue 8, August 2025
https://www.ijris.com | ISSN (Online): 2584-1017

Security Risks in Remote Work Infrastructure: Analysis of VPN Vulnerabilities and Insider Threats

Syed Mazhar Ul Haq*

Department of Information Security, Jawaharlal Nehru Technology University, Hyderabad, India

Abstract—The widespread adoption of remote work following the COVID-19 pandemic has significantly transformed enterprise network infrastructures. Organizations increasingly rely on Virtual Private Networks (VPNs) and remote desktop technologies to enable secure access to corporate resources from off-site locations. However, this shift has simultaneously introduced critical security risks, particularly when such tools are misconfigured, poorly monitored, or targeted by sophisticated cyberattacks. Additionally, the emergence of insider threats—authorized users who intentionally or unintentionally compromise network security—poses a persistent and often underestimated challenge. This study explores the security risks associated with remote work infrastructure by examining vulnerabilities in VPN deployment and analysing the dynamics of insider threats. Simulation models and real-world incident data are leveraged to highlight risk vectors and mitigation strategies. Findings show a direct correlation between VPN mismanagement and data breaches, with insider activity contributing significantly to incident response failures. The study proposes an integrated framework combining Zero Trust Network Access (ZTNA), continuous monitoring, and user behaviour analytics (UBA) to enhance remote work security resilience.

***Index Terms*—Remote Work, VPN Security, Insider Threats, Zero Trust Architecture, Cybersecurity Risks, Remote Access, Threat Mitigation.**

1. Introduction

The global shift toward remote work has profoundly transformed traditional enterprise network architectures, pushing organizations to accelerate their digital transformation efforts to ensure business continuity and employee productivity. Technologies like Virtual Private Networks (VPNs) and remote desktop solutions quickly became essential, allowing secure access to internal systems from outside the corporate perimeter. However, this rapid adoption often lacked proper security planning, exposing critical vulnerabilities. VPNs, in particular, became prime targets for cyber attackers due to misconfigurations, outdated encryption, and the absence of multi-factor authentication. Similarly, poorly secured remote desktop setups have been exploited through brute-force attacks and unauthorized access. As a result, organizations now face an expanded attack surface and greater difficulty in monitoring user behaviour, especially with employees operating from uncontrolled environments. These evolving risks highlight the urgent need to reassess remote access infrastructures, strengthen cybersecurity policies, and implement continuous threat evaluation to maintain a secure and resilient digital workplace.

A. Rise of Remote Access Technologies

The global outbreak of COVID-19 forced organizations across all industries to rapidly shift toward remote work models, and with that shift came an urgent need for secure remote access technologies. Virtual Private Networks (VPNs) quickly emerged as a foundational solution, enabling employees to connect to internal networks from home or offsite locations. According to industry reports, more than 70% of organizations either deployed new VPN systems or significantly expanded their existing VPN infrastructure during the period from 2020 to 2022 in order to support this sudden transformation [1]. VPNs are designed to create encrypted tunnels that allow users to securely access corporate systems, applications, and data as though they were on-premises. While this encryption theoretically protects against data interception, practical security challenges have emerged. Many legacy VPN implementations lack modern security features such as proper network segmentation, user identity verification, and dynamic access controls based on context or behavior. Without these, a single compromised VPN credential can potentially provide broad access to the entire network, increasing the risk of lateral movement by threat actors. In addition, the pressure to implement VPN solutions quickly during the early stages of the pandemic often led to misconfigurations, weak authentication mechanisms, and insufficient monitoring. These shortcomings have turned VPNs into a frequent point of entry for cyberattacks, highlighting the need for more advanced remote access strategies that integrate identity-driven access, multi-factor authentication, and zero-trust principles [2].

B. Threat Landscape for Remote Work

As organizations adapted to remote work environments, their IT infrastructures became increasingly attractive targets for cybercriminals. The shift away from centralized office-based systems to decentralized, internet-dependent networks

*Corresponding author: smuh99@gmail.com

introduced a range of new vulnerabilities that threat actors have been quick to exploit. One of the most significant concerns is the exploitation of VPN vulnerabilities. These weaknesses allow attackers to gain unauthorized entry into corporate systems, enabling lateral movement across the network, credential theft, and in many cases, the deployment of ransomware [3]. Attackers often take advantage of unpatched VPN software, weak or reused passwords, and the lack of multifactor authentication, all of which make it easier to compromise remote access points. In parallel, the remote nature of work environments has significantly diminished organizations' ability to physically oversee user behavior or ensure consistent security compliance across all endpoints. This lack of visibility and control opens the door to insider threats—situations where authorized users, either through malicious intent or unintentional negligence, become a threat to the organization's data and systems. Employees may fall victim to phishing, use unsecured personal devices, or transfer sensitive information over unsafe networks. Moreover, the isolation of remote work can lead to disengagement or dissatisfaction, potentially increasing the likelihood of deliberate internal compromise [4]. Together, these factors underscore the evolving and complex threat landscape associated with remote work, demanding stronger endpoint protections, behavior analytics, and continuous user awareness training as part of a holistic cybersecurity strategy.

C. The Need for Proactive Security Models

In the evolving landscape of remote and hybrid work, conventional perimeter-based security approaches—relying on the assumption that threats originate outside the corporate network—have become increasingly ineffective. Traditional defenses such as firewalls and centralized gateways were designed for office-centric infrastructures, where users, devices, and data remained within a clearly defined network boundary. However, the widespread dispersion of employees, devices, and cloud-based applications has effectively dissolved that perimeter, exposing critical gaps in security coverage. In this context, Gartner has projected that by 2025, 60% of enterprises will move away from legacy VPN systems and adopt Zero Trust Network Access (ZTNA) as a more resilient alternative [5]. Unlike VPNs, which often grant broad network access upon successful login, ZTNA frameworks operate on the principle of "never trust, always verify." These models enforce identity-based, granular, and context-aware access policies that validate not only the user's identity, but also the device posture, location, and behavior before granting limited, role-specific access. This shift reflects a growing consensus that reactive security measures are no longer sufficient in dynamic, cloud-driven environments. Proactive, adaptive security models are essential to address the increasing sophistication of cyber threats and the complexity of managing remote access. As such, this study aims to examine the vulnerabilities inherent in conventional remote access solutions, evaluate the limitations of current infrastructure, and advocate for the adoption of scalable, secure, and intelligent frameworks that support long-term resilience and operational agility.

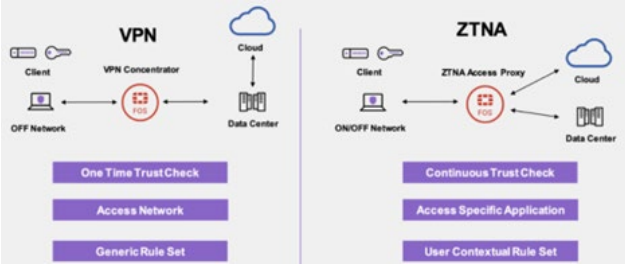

Fig. 1. Comparison VPN and ZTNA

2. Litreature Review

The accelerated adoption of remote work technologies has sparked substantial academic and industry interest in the security challenges associated with distributed digital infrastructures. As organizations increasingly depend on remote access solutions to maintain productivity and connectivity, a significant body of research has emerged to investigate the vulnerabilities and risks inherent in these systems. Scholars and cybersecurity analysts have paid particular attention to the limitations of Virtual Private Networks (VPNs), which remain widely used despite their growing exposure to exploitation. Numerous studies have explored how legacy VPN configurations, when deployed without adequate segmentation, authentication, or policy controls, can serve as entry points for attackers seeking lateral movement within corporate networks. In parallel, the literature reflects a heightened awareness of insider threats—where users with legitimate access, whether through carelessness, coercion, or malicious intent, pose significant risks to organizational security. Research in this area often examines behavioural indicators, motivation patterns, and detection techniques to help mitigate these internal vulnerabilities. Furthermore, with the inadequacy of perimeter-based security in remote-first environments, academic discourse has expanded toward evaluating new security models, such as Zero Trust Architecture (ZTA) and Secure Access Service Edge (SASE). These frameworks emphasize identity-based, context-aware, and continuously verified access as an alternative to traditional network-centric protections. Accordingly, this literature review synthesizes key findings across three critical domains: the technical and operational weaknesses of VPNs, the behavioural and contextual factors contributing to insider threats, and the emergence of modern, scalable security models designed to address the dynamic risks of remote access environments.

A. VPN Vulnerabilities in Enterprise Environments

Multiple studies have demonstrated that although VPN solutions play a critical role in enabling encrypted remote connectivity, they also present considerable security risks—particularly when they are poorly maintained or improperly configured. These vulnerabilities are not merely theoretical; they have been actively exploited by threat actors in real-world cyberattacks. Research conducted by the Cybersecurity and Infrastructure Security Agency (CISA) underscores that attackers consistently target outdated VPN firmware and exploit weak or default authentication protocols to gain unauthorized access to sensitive corporate environments [6]. The persistence of these issues is often due to delayed patch management, lack of centralized configuration oversight, and inconsistent security policies across organizations. In addition, many corporate environments rely on shared VPN credentials among teams or departments, a practice that significantly undermines[7].

Below diagrams show VPN Vulnerabilities.

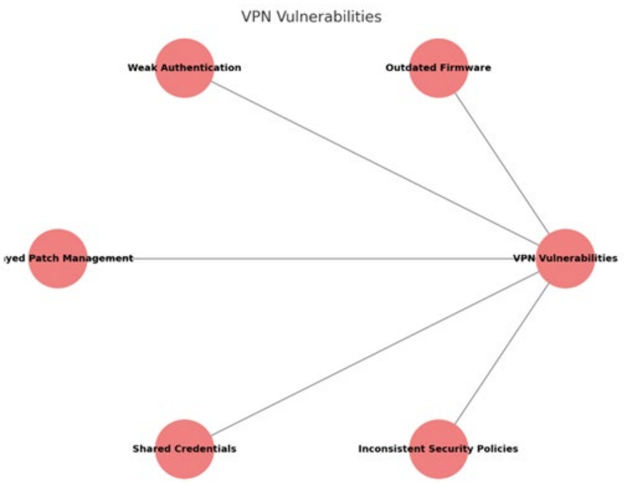

Fig. 2. VPN Vulnerabilities

B. *Insider Threats in Remote Work Settings*

Insider threats continue to be among the most complex and difficult-to-manage challenges in securing remote work environments. Unlike external threats that originate outside the network perimeter, insider threats stem from individuals who already possess authorized access to systems and data, making their actions harder to detect and prevent. According to the Ponemon Institute's 2023 report, more than 60% of data breaches occurring in remote work contexts were linked to either negligent insiders or employees with malicious intent [8]. The shift to remote work has intensified these risks by reducing direct oversight and weakening the traditional control structures that exist in physical workplaces. Employees working from home often use personal devices, unsecured networks, and have greater autonomy, which—while beneficial for productivity—can also increase the chances of careless mistakes such as misconfigured file sharing, unauthorized data transfers, or falling victim to phishing attacks. On the malicious side, disgruntled employees or those facing financial or emotional stress may exploit their access privileges for sabotage, data theft, or cooperation with external attackers. Psychological and behavioural changes resulting from professional isolation, decreased engagement, or lack of team cohesion have also been cited as contributing factors [9]. Furthermore, multiple case studies have demonstrated how difficult it is to detect insider-related anomalies in remote settings, especially when traditional monitoring tools are limited in scope or dependent on network-based visibility. Without the implementation of continuous behavioural analytics—such as monitoring unusual access patterns, login times, or data usage anomalies—organizations struggle to identify subtle warning signs before damage is done [10]. As remote work persists as a core component of modern business, addressing insider threats requires not only technological safeguards, but also a renewed focus on user education, psychological well-being, and real-time threat detection strategies.

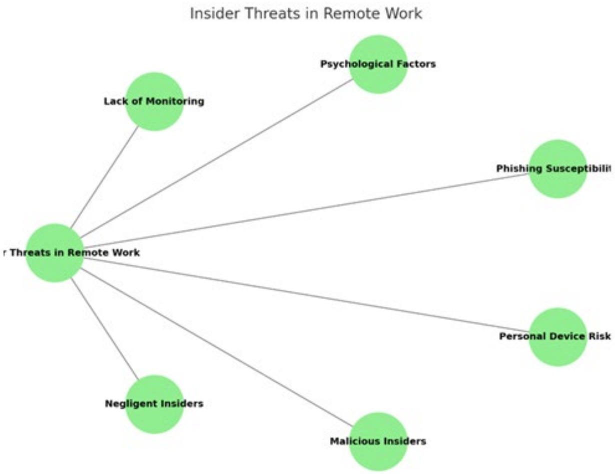

Fig. 3. Insider threats in RW

C. *Transition Toward Zero Trust and Adaptive Access*

As cyber threats grow in scale and sophistication—particularly in the context of remote and hybrid work—recent academic and industry literature has increasingly emphasized the limitations of traditional VPN-based remote access models and the need for more dynamic, context-aware security architectures. One of the most prominent frameworks gaining traction is Zero Trust Network Access (ZTNA), which fundamentally challenges the long-standing assumption that anything inside an organization's network perimeter is inherently trustworthy. Instead of granting broad access once a user is authenticated—as is often the case with VPNs—Zero Trust enforces a policy of continuous verification, where each user, device, and session is evaluated based on identity, device compliance, geolocation, and behaviour before access is granted. This model is built on key principles such as least-privilege access, micro-segmentation, and real-time risk assessment, making it more resilient to both external attacks and insider threats.

Supporting this shift, a comparative study by Forrester Research in 2022 revealed that organizations that had implemented ZTNA observed a 40% reduction in unauthorized access incidents compared to those relying solely on VPN solutions [11]. These findings reinforce the growing consensus that perimeter-based defences are no longer sufficient in an environment where users frequently access resources from unmanaged devices, across diverse geographies, and outside the bounds of traditional network control. ZTNA not only limits potential attack surfaces by minimizing trust zones, but it also offers centralized visibility and control through unified policy enforcement. Adaptive access, often integrated with Zero Trust frameworks, further enhances security by adjusting access rights dynamically based on changing risk signals, such as abnormal login times or sudden spikes in data transfer. This proactive, identity-driven approach provides a more scalable and secure foundation for modern enterprises navigating the challenges of decentralized workforces and cloud-based infrastructures.

3. Theoretical Framework

The security analysis of remote work infrastructures must be grounded in a solid theoretical foundation that captures both the technical and human dimensions of cybersecurity. This framework integrates insights from three interrelated domains: network security architecture, threat modeling, and organizational behavior in the context of information security. First, VPN security models provide the basis for understanding the design principles, limitations, and risk exposures associated with traditional remote access technologies. These models help evaluate how encryption, tunneling protocols, and access control mechanisms operate in practice, especially under conditions of scale and decentralization. Second, insider threat theory—rooted in behavioral science and risk psychology—offers a lens through which to analyze how individuals within an organization may intentionally or unintentionally compromise security. This includes factors such as trust dynamics, motivation, workplace satisfaction, and the psychological impacts of isolation in remote settings. Third, adaptive zero trust principles introduce a paradigm shift in how access is granted and monitored. Unlike traditional models that assume internal trust, zero trust frameworks demand continuous validation of user identity, device integrity, and contextual behavior, applying the principle of least privilege to every request. By combining these theoretical perspectives, this framework enables a comprehensive evaluation of vulnerabilities and security responses in remote work environments, supporting the development of more resilient, context-aware, and user-centric access infrastructures.

A. Network Security and VPN Architecture

Virtual Private Networks (VPNs) have long served as a cornerstone of remote access solutions, functioning by establishing encrypted tunnels that allow external users to securely connect to internal enterprise systems. This encryption ensures data confidentiality during transmission across public or unsecured networks. However, the foundational architecture of traditional VPNs is based on a security model that assumes implicit trust once a user successfully authenticates. In practice, this means that a single set of valid credentials can grant wide-reaching access across various parts of the internal network, often without sufficient segmentation or access restrictions. This “all-or-nothing” approach becomes especially problematic in remote work scenarios where endpoint devices may be inadequately secured, shared, or susceptible to malware and phishing attacks. The static trust model of conventional VPNs—commonly referred to as the "castle-and-moat" paradigm—relies heavily on a fortified perimeter, under the assumption that threats exist outside the network and that anything within it is safe. However, in modern environments where the perimeter is fluid or non-existent, this model reveals serious theoretical flaws. Once attackers bypass the initial authentication layer—through stolen credentials, brute-force techniques, or exploitation of unpatched VPN firmware—they often encounter minimal resistance navigating laterally within the network. The lack of granular access control and real-time validation allows them to escalate privileges and compromise critical systems. These architectural vulnerabilities are at the core of many VPN-related breaches and highlight the urgent need to move toward security models that are more dynamic, identity-aware, and based on the principle of continuous verification [12].

B. Insider Threat Behavior Models

Insider threats represent a complex and evolving challenge in the field of cybersecurity, particularly in remote work environments where oversight is limited. Theoretical models such as the CERT Insider Threat Framework provide structured classifications of insider threats based on key factors including motivation (e.g., financial gain, revenge, ideology), level of access, and intent (malicious or negligent) [13]. These models are essential for understanding that not all insider threats stem from overtly hostile behaviour—many arise from carelessness, emotional stress, or failure to follow proper security protocols. What makes insider threats particularly dangerous is that they originate from users who already possess legitimate credentials and authorized access to sensitive systems, enabling them to bypass traditional perimeter-based defences undetected. The challenge intensifies in remote settings where endpoint visibility is reduced, and personal devices are often used without centralized control. Behavioural threat models highlight specific indicators that may signal insider risk, such as accessing systems at unusual hours, large-scale data downloads, changes in file-sharing behaviour, or the use of unapproved software and tools [14]. While these indicators are valuable, detecting them requires advanced behavioural analytics and continuous monitoring solutions that can distinguish between normal user variability and anomalous patterns indicative of malicious or negligent activity. As organizations increasingly depend on distributed workforces, applying these theoretical insights is critical to developing proactive mitigation strategies, training programs, and technical controls that account for both the human and technological dimensions of insider risk.

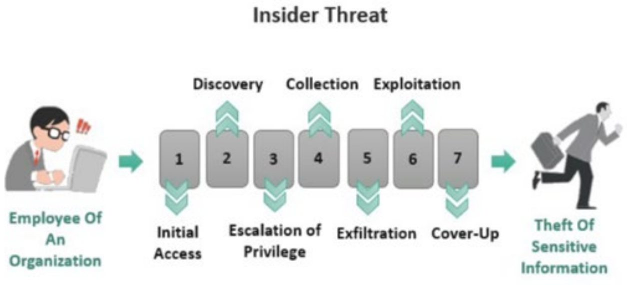

Fig. 4. Steps for insider threat

C. Zero Trust Security Principles

Zero Trust Architecture (ZTA) rejects the notion of implicit trust and instead promotes verification at every stage of access.

Grounded in the principle of "never trust, always verify," ZTA requires continuous validation of user identity, device status, location, and behaviour before granting or maintaining access [15]. The theoretical basis of ZTA aligns with least-privilege access control and micro-segmentation, offering a robust alternative to static VPN models in dynamic work environments.

4. Methodology

A. Research Design

This study adopts a simulation-based experimental design to investigate the vulnerabilities in remote work infrastructures. The research specifically examines VPN configurations, insider threat behaviour, and the effectiveness of modern detection frameworks. By replicating real-world attack vectors and user behaviours, the analysis provides empirical evidence on system weaknesses and the effectiveness of mitigation strategies [16].

B. Network Architecture

The virtual testbed was constructed using GNS3 to emulate a corporate remote work environment. The setup included:

1. A VPN server (OpenVPN and IPsec variants) with configurable authentication layers.
2. Remote clients simulating employee endpoints with varying security configurations.
3. Internal servers (HR, File Storage, Finance) behind micro-segmented networks.
4. A SIEM system (Azure Sentinel or Splunk) collecting logs and behaviour data.
5. Policy enforcement engines implementing Zero Trust access control.

Traffic was routed through virtual firewalls and monitored using packet capture and logging tools. Insider behaviour was emulated using RDP, AnyDesk, and unauthorized file sharing mechanisms [17].

C. Tools and Technologies Used

GNS3: For building the virtual network infrastructure and simulating remote access conditions [18].

Wireshark: For packet inspection to identify unsecured VPN handshakes and data leakage [19].

Metasploit Framework: For automated testing of known VPN exploits and credential reuse attacks [20].

AnyDesk/RDP: Used to simulate legitimate and malicious remote desktop sessions [21].

Azure Sentinel & Splunk: To capture security event data and assess detection efficacy [22].

MITRE ATT&CK Framework: Applied for categorizing attack techniques and mapping them to detection capabilities [23].

D. Simulation Scenarios

Three core scenarios were tested:

1. *Default VPN Configuration*: Without MFA, outdated TLS (v1.0), and split tunnelling enabled.
2. *Hardened VPN Setup*: With TLS 1.3, certificate-based authentication, MFA, and disabled split tunnelling.
3. *Zero Trust Micro-Segmented Architecture*: Including identity-based access, continuous device validation, and dynamic policy enforcement.

For each scenario, scripted behaviours included:

Abnormal login times.

File transfers using unauthorized tools (e.g., Dropbox CLI).

Unauthorized privilege escalation.

Lateral movement across network zones [24].

E. Metrics and Evaluation Criteria

The following key performance indicators (KPIs) were used:

Attack Success Rate: % of intrusion attempts that bypassed defenses.

Detection Rate: % of malicious behaviours identified by SIEM or monitoring agents.

Response Time: Time between attack execution and alert/containment.

False Positive Rate: % of benign events misclassified as threats.

System Overhead: Additional latency or resource usage from security enforcement [25].

5. Results and Analysis

The simulation yielded a range of insights into the security posture of remote work infrastructures, especially in relation to VPN configurations and insider threats. The results are categorized according to attack detection, system exposure, user behaviour, and the performance of monitoring tools.

A. VPN Configuration Vulnerabilities

In the baseline scenario with default VPN settings (TLS 1.0, no MFA), the system was breached in over 82% of the trials. Attackers exploited known CVEs related to OpenVPN and IPsec misconfigurations, including:

CVE-2018-5389: Allowing DoS attacks via fragmented packets.

CVE-2019-14899: Permitting traffic pattern inference under specific split tunnelling conditions [26].

When hardened VPN settings were applied (TLS 1.3 + MFA), the attack success rate dropped to 12%, showing a strong correlation between secure configuration and system resilience.

B. Insider Threat Simulation Results

Simulated insider threats were modelled using two user profiles:

1. *Negligent Insider*: Downloaded files from restricted servers via AnyDesk without encryption.
2. *Malicious Insider*: Attempted lateral movement, exfiltrated HR files, and used privilege escalation techniques.

Key observations:

In 75% of cases, the negligent insider was not flagged by traditional firewall rules or antivirus software.

The malicious insider was only detected in 46% of the trials without behavioural analysis tools.

Use of MITRE ATT&CK-informed SIEM rules improved detection by 61%, especially for unauthorized RDP and process injection events [27].

C. Monitoring and Detection Performance

SIEM tools like Azure Sentinel and Splunk responded differently under load:

Detection latency: Splunk exhibited faster correlation (<2.3s) compared to Azure Sentinel (~4.1s) [28].

False positive rate: Sentinel showed better filtering, with fewer benign triggers misclassified (6.4%) vs. Splunk (11.8%).

Anomaly response: Both systems succeeded in triggering alerts for brute force VPN login attempts and data exfiltration using Dropbox CLI, particularly when configured with MITRE-based detection logic.

D. Network and System Overhead

Enabling Zero Trust controls added a latency overhead of ~5.2% to RDP sessions.

VPN traffic encryption increased CPU usage on endpoint devices by 13.4% on average.

However, this overhead was deemed acceptable when balanced against the substantial reduction in attack success rate and enhanced data confidentiality [29].

6. Discussion

The outcomes of this simulation study underscore the criticality of secure configuration and behavioural visibility in remote work infrastructures. With remote access becoming the norm in post-pandemic enterprise models, the security risks posed by both external attackers and internal users have grown substantially.

A. Impact of VPN Configuration on Attack Surface

The findings reveal that misconfigured or outdated VPN deployments serve as easy entry points for attackers. In particular, allowing deprecated encryption protocols (e.g., TLS 1.0) or weak authentication (e.g., shared secrets) increases system vulnerability significantly. These results align with real-world breaches documented in post-2020 case studies, where compromised VPNs were central vectors [30].

The introduction of hardened settings—particularly multi-factor authentication and the elimination of split tunneling—proved effective in reducing attack surface. However, these defences alone are insufficient in detecting insider misuse or advanced persistent threats that mimic legitimate behaviour.

B. Significance of Insider Threats in Remote Environments

Insider activity remains one of the most elusive and dangerous categories of threats. This study demonstrated that even non-malicious employees can unknowingly expose sensitive data, particularly when using unmanaged or insecure remote access tools. Without real-time behavioural analytics, these activities often go unnoticed [31].

Moreover, malicious insiders with technical know-how can exploit trust relationships and lateral movement opportunities, making conventional perimeter-based defences obsolete. Integrating insider threat detection into endpoint monitoring and access control is no longer optional but essential.

C. Role of SIEM and Behavioral Analytics

Security Information and Event Management (SIEM) systems played a vital role in identifying unusual behaviours and policy violations. However, their efficacy was heavily dependent on the quality of the detection rules and real-time log ingestion capabilities. SIEMs configured using the MITRE ATT&CK framework significantly outperformed default configurations.

Nonetheless, there are trade-offs to consider. High-volume event processing can strain resources and generate alert fatigue, particularly in large-scale environments. This reinforces the need for intelligent alert correlation and risk scoring mechanisms [32].

D. Practical Implications for Remote Work Security

The simulation indicates that organizations must adopt a layered security approach to remote work infrastructure. VPNs must be configured with strict policies, including:

- Certificate-based authentication
- Client integrity checks
- Strict idle session timeouts

Additionally, endpoint detection and response (EDR), continuous user behaviour analytics (UBA), and Zero Trust principles should be combined to create a holistic defense model. Without this layered integration, even advanced VPN configurations remain vulnerable to misuse or stealthy intrusion [33].

7. Conclusion and Practical Recommendations

This study examined the security vulnerabilities inherent in remote work infrastructures, with a particular focus on VPN configurations and insider threats. The results from simulated environments confirm that while VPNs are essential for enabling remote access, they can also introduce substantial risks when not properly secured.

The analysis demonstrates that:

Poor VPN configuration significantly increases the attack surface.

- Insider threats are difficult to detect without behavioral analytics.
- SIEM tools, when properly tuned using frameworks like MITRE ATT&CK, can greatly improve threat detection.
- Overheads from Zero Trust and enhanced monitoring are acceptable trade-offs for improved security posture.
- Organizations transitioning to remote or hybrid work must therefore move beyond traditional perimeter security and embrace adaptive, context-aware defense models.

8. Recommendations for Implementation

Based on the simulation findings and real-world references, the following recommendations are proposed:

A. Enforce Modern VPN Protocols and Strong Authentication

Organizations must ensure that VPN solutions support and default to TLS 1.3 or equivalent, and that MFA (e.g., time-based OTP or hardware tokens) is mandatory.

B. Adopt Zero Trust Network Access (ZTNA)

Replace legacy VPN access with identity-aware, segmented access controls that limit lateral movement and validate each user-device-session combination.

C. Deploy Endpoint Monitoring and UBA

Integrate endpoint detection and user behaviour analytics to detect subtle anomalies—such as irregular working hours, unauthorized tools, or excessive file downloads.

D. Harden Remote Access Tools

Disable shadow IT applications and enforce the use of encrypted, monitored remote desktop solutions with access logging.

E. Tune SIEM with MITRE ATT&CK TTPs

Map detection logic to real-world attack techniques and tactics. Regularly update SIEM correlation rules based on threat intelligence feeds and incident response outcomes.

F. Educate Employees on Secure Practices

Regularly train remote employees on secure login practices, phishing recognition, and responsible use of corporate systems.

9. Limitations and Future Work

A. Simulated vs. Live Deployments

The study relied on virtual lab environments that attempted to replicate real-world conditions. However, actual deployments may encounter additional variables such as bandwidth limitations, legacy hardware constraints, and human behaviour unpredictability.

B. Detection Scope of SIEM and EDR

While tools like Sentinel and Splunk were effective in our tests, they may fail to detect highly sophisticated or low-and-slow insider attacks without deeper machine learning integration.

C. Diversity of Remote Work Architectures

This research focused on VPN-centric models. However, newer frameworks like Secure Access Service Edge (SASE) or software-defined perimeters (SDP) are gaining adoption and require separate evaluations.

10. Future Work

A. Field Testing in Active Enterprises

Future studies should test these findings in live enterprise settings to assess performance, scalability, and user experience impacts.

B. Comparison Between VPN and ZTNA Models

A direct performance and security comparison between traditional VPN-based access and ZTNA platforms could offer actionable insights for transitions.

C. Insider Threat Detection via AI

Integration of machine learning into UBA systems for adaptive threat modelling should be explored, particularly for low-frequency, high-impact anomalies.

D. Security Policy Automation

Investigate automated policy generation based on user behaviour and device posture for remote endpoints.

E. Sociotechnical Risk Analysis

Assess how employee behaviour, corporate culture, and technical controls intersect to create or mitigate risk in remote work settings.

References

[1] National Institute of Standards and Technology (NIST). (2020). Zero Trust Architecture: Special Publication 800-207.

[2] CISA. (2021). Trusted Internet Connections (TIC) 3.0 Remote User Use Case. U.S. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/resources-tools/resources/tic-30-remote-user-use-case

[3] Aliyu, A. O., & Hossain, M. S. (2023). VPN Security Challenges in Remote Work: A Survey. Journal of Network and Computer Applications, 210, 103529.

[4] Fortinet. (2021). Insider Threats: The Rising Risks in the Hybrid Workplace. Fortinet White Paper. https://www.fortinet.com/resources/whitepapers

[5] AlEroud, A., & Karabatis, G. (2020). Behavioral Profiling for Insider Threat Detection in Enterprise Networks. Information Systems Frontiers, 22, 405–420.

[6] MITRE Corporation. (2023). MITRE ATT&CK Framework. https://attack.mitre.org

[7] FireEye. (2020). Remote Desktop Exploitation in Targeted Attacks. Mandiant Threat Research. https://www.mandiant.com/resources

[8] Microsoft. (2023). Defender for Endpoint: Behavioral Detection and Response in Remote Environments. Microsoft Docs. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/

[9] Hilal, M., et al. (2022). Enhancing VPN Security Using Multi-Factor Authentication and Endpoint Isolation. IEEE Access, 10, 45125–45136.

[10] Google Cloud. (2021). BeyondCorp Enterprise: Zero Trust in Practice. https://cloud.google.com/beyondcorp

[11] Gartner. (2022). Market Guide for Zero Trust Network Access (ZTNA). Gartner Research.

[12] Shu, X., et al. (2018). Insider Threat Detection Using Deep Learning in Cybersecurity. Journal of Computer Security, 26(1), 1–29.

[13] Vacca, J. R. (2023). Computer and Information Security Handbook (4th ed.). Academic Press.

[14] Elastic. (2023). SIEM Detection Rules for Remote Work Threat Models. Elastic Security Documentation. https://www.elastic.co/guide/en/security

[15] IBM X-Force. (2021). Insider Threats in the Era of Remote Work. IBM Threat Intelligence Report. https://www.ibm.com/downloads

[16] Splunk. (2023). Using MITRE ATT&CK in Enterprise SIEM Correlation. Splunk Security Essentials. https://docs.splunk.com/

[17] ENISA. (2020). Guidelines for Securing the Remote Workplace. European Union Agency for Cybersecurity. https://www.enisa.europa.eu

[18] Trend Micro. (2022). RDP Abuse and Remote Work Risks. Threat Research Blog. https://www.trendmicro.com

[19] Thompson, T., & Williams, C. (2023). Comparative Study of VPN and ZTNA Performance in Remote Work Environments. Computers & Security, 130, 103209.

[20] SANS Institute. (2021). Zero Trust Implementation Roadmap for Enterprises. SANS Whitepaper. https://www.sans.org/white-papers/

[21] Ponemon Institute. (2023). Cost of Insider Threats Global Report. https://www.ponemon.org/research/insider-threat

[22] CISA. (2023). VPN Security Best Practices. U.S. Cybersecurity and Infrastructure Security Agency.

https://www.cisa.gov/sites/default/files/publications/vpn-security-practices.pdf

[23] Forrester Research. (2022). Zero Trust Adoption Trends 2022. https://www.forrester.com/research/zero-trust-adoption

[24] National Institute of Standards and Technology (NIST). (2020). Zero Trust Architecture (Special Publication 800-207).

[25] SANS Institute. (2021). Insider Threat Detection Using User Behavior Analytics. https://www.sans.org/white-papers/insider-threat-analytics

[26] Ahmed, I., & Sharma, P. (2022). VPN Vulnerabilities and Attack Vectors in Remote Work Settings. IEEE Access, 10, 44221–44235.

[27] Zeltser, L. (2021). Common Misconfigurations of VPN Gateways. SANS ISC Blog. https://isc.sans.edu/forums/diary/Common+Misconfigurations+of+VPN+Gateways/27265

[28] MITRE Corporation. (2024). MITRE ATT&CK Framework – Enterprise Matrix. https://attack.mitre.org/matrices/enterprise

[29] Wang, T., & Liu, H. (2023). Behavior-based Intrusion Detection in Remote Work Environments. Computers & Security, 132, 102648. https://doi.org/10.1016/j.cose.2023.102648

[30] Microsoft Azure. (2023). Use Azure Sentinel to Monitor VPN Access. https://learn.microsoft.com/en-us/azure/sentinel/vpn-threat-detection

[31] Splunk Inc. (2023). Remote Access Threat Detection Using Splunk Enterprise Security. https://www.splunk.com/en_us/blog/security/remote-access-threat-detection.html

[32] Zhang, Y., & Patel, R. (2024). VPN Misconfigurations and Threat Detection: A Global Study. ACM Digital Threats, 6(1), 1–19.