Partners Universal Multidisciplinary Research Journal (PUMRJ)
Volume: 03 Issue: 03 | April - May 2026 | ISSN: 3107-5789 | www.pumrj.com

Beyond the Perimeter Rethinking Enterprise Network Security in an Age of Distributed Threats

Dr.A.Shaji George[1], Dr.T.Baskar[2], Dr.P.Balaji Srikaanth[3]

[1]Independent Researcher, Chennai, Tamil Nadu, India.
[2]Professor, Department of Physics, Shree Sathyam College of Engineering and Technology, Sankari Taluk, Tamil Nadu, India.
[3]Associate Professor, Dept of Networking and Communications, School of Computing, SRM Institute of Science and Technology, Kattankulathur, Tamil Nadu, India.

Abstract - In the last 20 years enterprise network security has been transformed by the rapid growth of cloud computing, increase in remote working patterns, the growing number of connected devices and growing sophistication of cyber adversaries. The traditional perimeter-based security paradigm that's been the working paradigm for protecting organization networks for years is not sufficient anymore in a world where data, users and applications are everywhere, at the same time. This article looks back at how enterprise network security has developed over time, discusses the fundamental technologies that make up the "modern" enterprise network security stack, and examines the concept and practical applications of Zero Trust enterprise network security. The research, which references known ransomware and Monitoring software case studies, points out the financial, regulatory, and reputational ramifications of poor security postures. The latest developments in the field, such as artificial intelligence (AI) for threat detection, post-quantum cryptography, cloud-native security approaches, and behavioral analytics, are explored for their real-world applications. In addition, the human aspect of network security is covered, an aspect that is often overlooked, and it is said that culture and governance are just as important as technical solutions. This is followed by an integrated system design for organisations aiming to move from perimeter-based security to a proactive, resilience-based approach in the distributed threat environment of today and tomorrow.

Keywords: Enterprise network security, Zero Trust architecture, Cyber threat landscape, Cloud security, AI-driven threat detection, Defense in depth, Insider threats, Post-quantum cryptography.

1. INTRODUCTION

1.1 The Network Is No Longer a Castle

The prevailing mindset of enterprise network security that has been in effect for the last 30 years or so, was, to an extent, adopted from medieval military fortifications. Establish a clear perimeter, establish what is "in" and what is "out" of that perimeter as safe and focus defense at the perimeter. The drawbridge was the fire wall. The demilitarized zone was the outer courtyard. Once the outer wall held the inner wall was assumed safe and was referred to as the keep.

That was fine for the days of mainly centralized enterprise computing. Corporate applications continued to run on servers in on-premises data centers. On-premises data centers continued to host corporate applications. They had workstations attached to managed office networks and were required to work at their assigned desks. They were required to work at their assigned workstations on managed office networks. The internal trust network and the external untrusted internet seemed to be distinct and so was

Partners Universal Multidisciplinary Research Journal (PUMRJ)
Volume: 03 Issue: 03 | April - May 2026 | ISSN: 3107-5789 | www.pumrj.com

the security architecture.

The world isn't the same. The enterprise network no longer has an exact definition and is now more of a concept. Applications are deployed in hyperscale cloud environments on Amazon, Microsoft, and Google. Employees use corporate resources via home and hotel networks and cell phones that may never touch a corporate network. Internal systems are connected to third party vendors for services. Sensitive information is transmitted between applications without the involvement of humans, thanks to automated pipelines. This is a non-moated environment. There's hardly any wall. Yet, many organizations are still spending their security budget and security thinking as if the old perimeter is still in place.

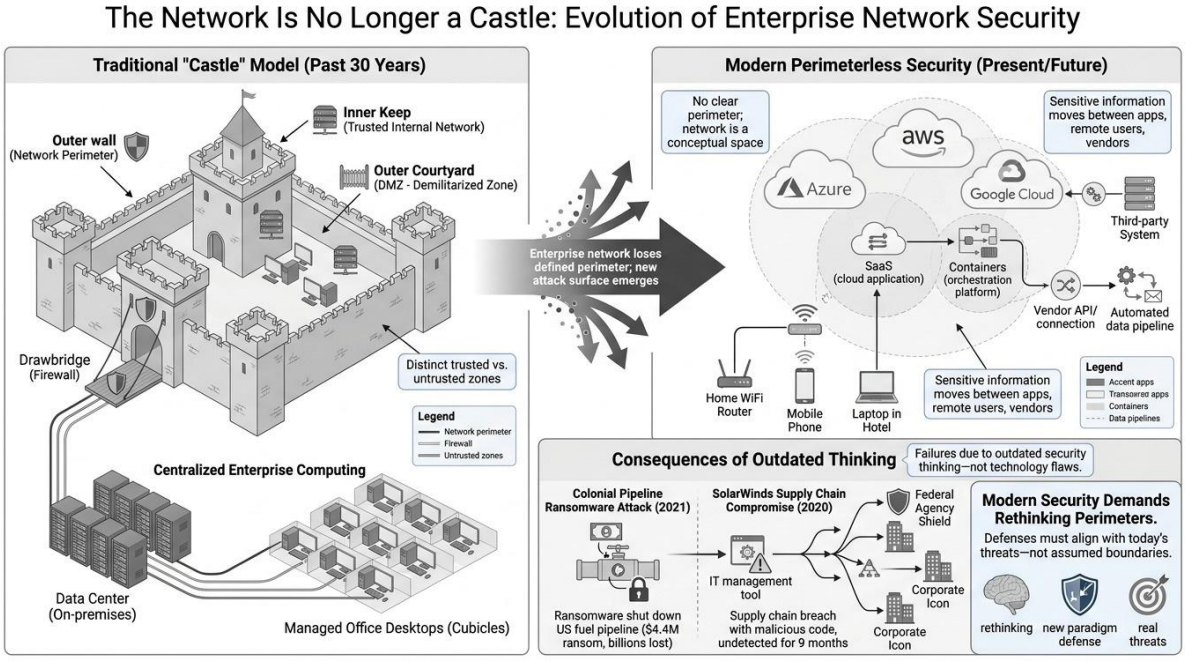

Fig -1: Evolution of Enterprise Network Security

The repercussions of this assumption of security and operational reality are far from benign and widely known. The Colonial Pipeline ransomware attack of May 2021 caused the shutdown of the largest refined fuel pipeline in the United States, and disrupted fuel supplies across the East Coast of the United States for almost a week, costing Colonial about 4.4 million dollars in ransom payments, and a total economic cost of billions of dollars. In the case of Monitoring Software, the attackers managed to infiltrate the 2020 Monitoring Software supply chain compromise, which involved inserting malicious code into a popular IT monitoring tool, and then operate within the networks of more than 18,000 companies, including several U.S. federal agencies, for up to nine months without detection. These were not flaws in security products per se. These were lapses in security thinking, in thinking that was based on assumptions that no longer exist. The intent of this article is to say that it's not just technology that is needed to rebuild enterprise network security for the present. It calls for a complete rethinking of what security is and where it can be found, as well as a new paradigm on how to create a defense that is fair and square with the threats that one has and not the threats that he/she wishes he/she had.

2. OBJECTIVES

Partners Universal Multidisciplinary Research Journal (PUMRJ)
Volume: 03 Issue: 03 | April - May 2026 | ISSN: 3107-5789 | www.pumrj.com

There are a few goals for this article.

1. First, to present the evolution of enterprise network security from perimeter-centric designs towards today's distributed network designs.
2. Second, to explain and explain the basic concepts of contemporary enterprise network security, such as the CIA triad of confidentiality, integrity, and availability.
3. Third, to review the technical elements that make up a layered, defense-in-depth security approach.
4. Fourth, to explore the Zero Trust model as a concept and business approach to replace the old paradigm of perimeter thinking.
5. Fifth, to consider the present trends that are transforming the industry, such as dual-use considerations of artificial intelligence, increasing significance of cloud security, and the future of quantum computing.
6. Sixth, to handle with human and organizational dimensions of security, contending that culture and leadership are not "extras" but key concerns in security.
7. Finally, offer practitioners, security professionals, and organizational leaders actionable frameworks and guidance to create security postures that are resilient, adaptive, and proportionate to the actual risk.

3. THE HISTORICAL EVOLUTION OF ENTERPRISE NETWORK SECURITY

To know where enterprise network security is going to be in the future, it's important to know its history. The field of complexity didn't develop overnight. It had a different stage in every era and was affected by the technology and threat levels of that era.

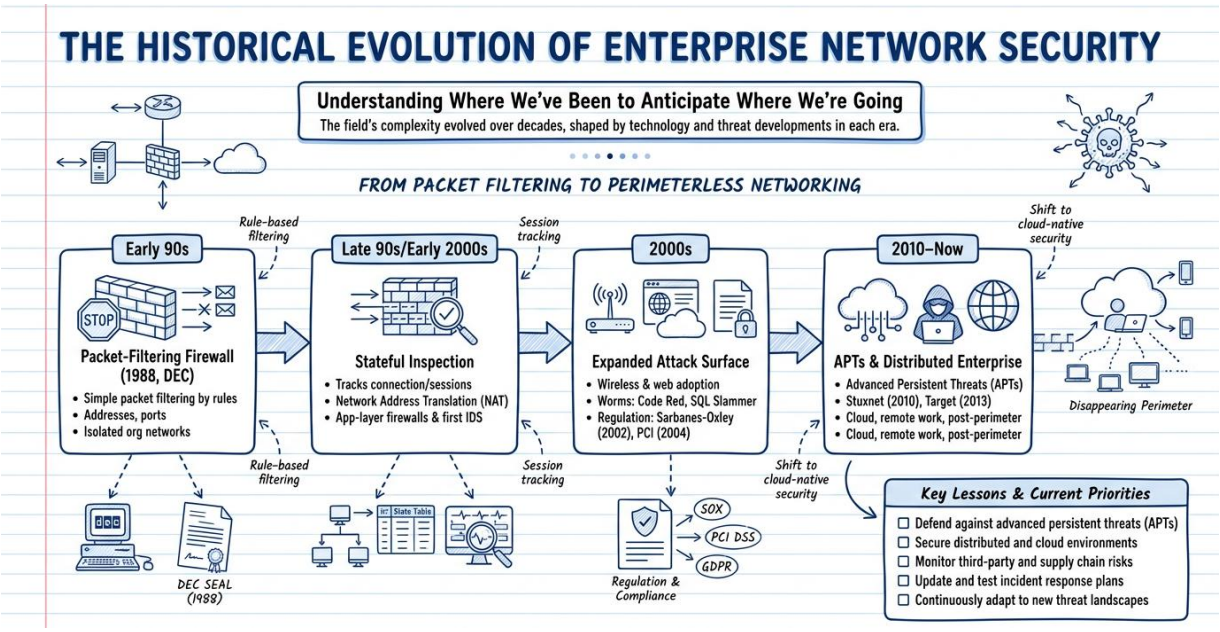

Fig -2: The Historical Evolution of Enterprise Network Security

When commercial Internet access started to become commonplace in the early 90's, organizational networks were mostly contained. The foremost security issue was to ensure that nobody could penetrate internal systems. The first-line answer to this was packet-filtering firewalls, which were developed by Digital Equipment Corporation (DEC) computer scientists in 1988. These tools analyzed network packets, by source address, destination address, and port numbers, blocked traffic that failed to match defined rules. By today's standards they were rough yet suitable for the threat environment they were intended to meet.

During the late 90's and early 2000's, stateful inspection firewalls began to monitor the state of active connections instead of evaluating each packet individually. Stateful inspection firewalls emerged in the late 90's and early 2000's that monitored the state of active connections rather than evaluating individual packets. This enabled more complex filtering and also paved the way for network address translation (NAT) to hide the internal network topology from external network observers. At the same time, the growth of web applications added new attack vectors which were hard for packet filtering to defend against, leading to the creation of application-layer firewalls and early intrusion detection systems.

The first decade of the 2000s saw a dramatic growth in attack surface and technology adoption by organizations at an incredible pace. Wireless networking, e-commerce, and the early development of Web-based applications all brought new challenges that perimeter defenses were not effective in providing security for. Perimeter defenses were already being compromised and overwhelmed on a large scale as shown by worms such as Code Red in 2001 and SQL Slammer in 2003. In 2002 the Sarbanes Oxley Act started to put pressure on organizational security postures, and the payment card industry (PCI) began to establish security standards in 2004.

There was a qualitative change in cyber threats from 2010 onwards. Advanced Persistent Threats (APTs or APTs) emerged as a mainstay of the threat profile, with patient and multi-stage attacks being a major attack method used, frequently sponsored by nation states. Cyber operations had physical effects, though, when in 2010, a far more sophisticated malware, dubbed "Stuxnet," was discovered that wreaked havoc on Iranian nuclear centrifuges. In the 2013 Target Corporation breach, a third-party HVAC provider was breached, allowing attackers to access payment card data for 40 million customers, and the lessons that should be learned is clear.

The 2010s saw the rapid uptake of cloud and the 2020 COVID-19 situation acted as a catalyst for COVID-19 and remote working adoption to take place in weeks as opposed to years. These transformations effectively marked the end of the definition of the enterprise perimeter, and set the stage for the distributed, boundary-less network computing environment that has become the hallmark of today's enterprise computing environment.

4. WHAT ENTERPRISE NETWORK SECURITY ACTUALLY MEANS THE CIA TRIAD REVISITED

The term enterprise network security denotes the comprehensive strategy, technology, policy, and human practices that an organization employs to safeguard its network(s) from unauthorized use, misuse, theft of services, disruption, and destruction. The field is conceptually grouped around three fundamental characteristics of the field, that form the CIA triad: confidentiality, integrity, and availability.

Confidentiality means limiting access to sensitive information to people, systems and processes that have explicit permission to view information. Ensuring confidentiality requires that data be encrypted, user access be restricted, and that there be monitoring systems in place that can detect unauthorized

Partners Universal Multidisciplinary Research Journal (PUMRJ)
Volume: 03 Issue: 03 | April - May 2026 | ISSN: 3107-5789 | www.pumrj.com

attempts at accessing the data.

Data integrity means that data should be accurate, consistent, and not change over the data's lifespan. Whether it's financial fraud or safety failures in operational technology environments, the impacts of unauthorized modification of data from external threats or insider threats could be far-reaching. Cryptographic hashing, Digital signatures, Version control systems, and audit logging are techniques used to ensure the integrity of a file.

Availability is the desired property of network services, applications and data that permits them to be accessed by their intended users when required. Distributed denial of service attacks, failed hardware, failed software, and natural disasters are examples of failures that can cause availability issues. Redundancy, failover, capacity management, and extensive disaster recovery planning are all critical aspects of maintaining availability.

The three objectives are difficult to achieve at the same time because, often, they compete with each other. Fine-grained access controls and strong encryption can have a negative impact on availability in terms of latency and complexity that increases the likelihood of reducing confidentiality. The more systems are configured to be available, the more they might be exposed and have less stringent access controls. The balancing act of security practitioners is always a dynamic one, and depends on the risk profile, regulatory compliance needs, and operating context of the organization.

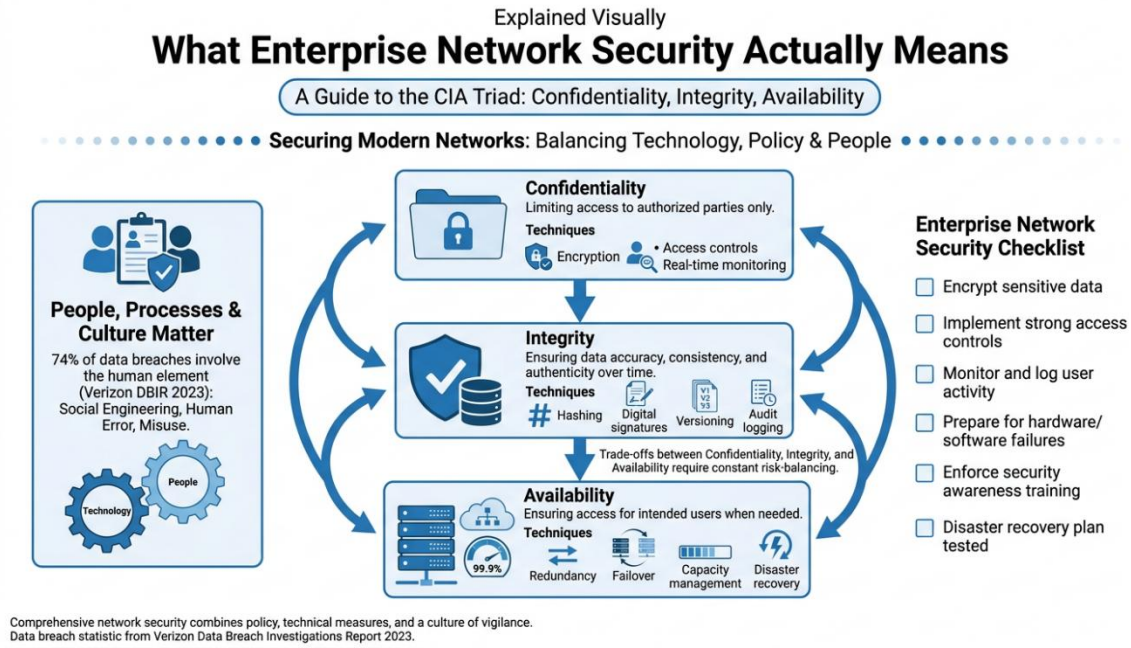

Fig -3: Enterprise Network Security Actually Means

Also, enterprise network security is not a solely technical field. As significant as any technology being implemented is the people, processes, and culture that govern the use and management of the network, as well as the culture of security awareness. Human factors have been shown to play a role in most security incidents, time and time again. According to Verizon's Data Breach Investigations Report 2023, 74 percent of data breaches occurred because of the human element, such as social engineering, human error, and misuse. Technical controls that disregard this are only dealing with part of the risk.

Partners Universal Multidisciplinary Research Journal (PUMRJ)
Volume: 03 Issue: 03 | April - May 2026 | ISSN: 3107-5789 | www.pumrj.com

5. THE CORE TECHNICAL COMPONENTS OF A LAYERED DEFENSE

A ripe enterprise network security architecture is built on a few overlapping layers of control, every one of which targets different threat vectors. The so called defence in depth is the right operational model as it allows no control can be 100 per cent infallible. If one layer is not utilized or is failed, the other layers will be in place to detect, contain, and eliminate the threat.

5.1 Firewalls and Perimeter Controls

Next generation firewalls are a significant improvement over their forebears. Next generation firewalls can do deep packet inspection, which is the ability to inspect information at the application layer, they can also incorporate real-time threat intelligence feeds, and they can add user and application identity to access decisions, instead of just IP addresses and port numbers. A well-designed firewall is a default denying type firewall, allowing only traffic that is explicitly allowed for documented business purposes and blocking everything else.

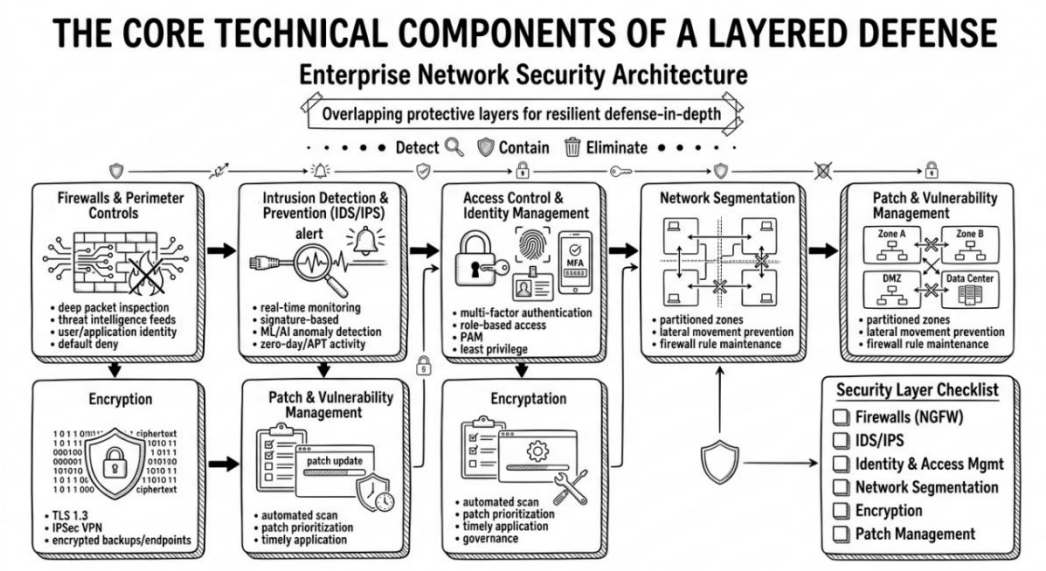

Fig -4: The Core Technical Components of a Layered Defense

5.2 Intrusion Detection and Prevention Systems

An Intrusion Detection and Prevention System (IDS/IPS) monitors network traffic in real time for signatures of known attacks and behavior patterns that are indicative of malicious activity. However, machine learning models trained using a vast amount of network telemetry data are becoming more common in modern systems and can be used for detecting anomalous behavior when there is no attack signature in the network. This is especially significant for the detection of zero day exploits and APT activity, which won't be included in signature databases by definition.

5.3 Access Control and Identity Management

One of the highest leverage investments that an organization can make is in strong identity and access management practices. The adoption of multi-factor authentication (MFA) that forces users to pass at least 2 independent factors to access accounts makes credential-based attacks much more difficult. With role-based access control, the user is only granted access to those resources that are necessary for the role they play in their organization. Privileged access management (PAM) solutions offer extra security

measures for administrative accounts, the most appealing targets for attackers. The rule of least privilege should be emphasized. All users, applications and automated processes must have only the necessary access rights to carry out their duties. This restricts damage that can be done from one failed account, thus minimizing the "blast radius" of successful intrusions.

5.4 Network Segmentation

One of the most useful architectural controls is to partition the enterprise network into distinct areas where traffic is limited to specific areas. In one network segment, there is a system compromised by the attacker, and segmentation prevents the attacker from moving laterally to another network segment. For instance, a health care provider could separate its medical network from its administrative IT systems, so that a ransomware infection on the office systems wouldn't impact medical devices. Effective segmentation depends on careful design of the network, proper maintenance of firewall rules, and validation that segmentation is really effective.

5.5 Encryption

Information should be protected when in transit, and when stored. The latest version of Transport Layer Security (TLS) is version 1.3, which is now used to encrypt web traffic. IPsec encrypts data at the network layer, thus allowing for VPN connections. Encryption for databases, endpoints and backups prevent stolen data being accessed by unauthorized users. While it is not an absolute cure, encryption is an essential control that renders stolen data harmless: it is not a data collection, but a set of ciphertexts.

5.6 Patch and Vulnerability Management

For a great many attempts, the vulnerabilities exploited are ones that are known and for which there are patches, but they haven't been installed. The WannaCry ransomware attack that infected more than 200,000 systems in 150 countries was exploiting a Windows Server Message Block (SMB) vulnerability, which Microsoft had fixed 59 days before. Organizations that were well-run patch management programs were not significantly impacted. To implement patch management, automation is needed to scan for vulnerable software, prioritization is necessary based on the exploitability and business criticality of the software, and governance is required to ensure that patches are applied within certain time limits.

6. THE ZERO TRUST REVOLUTION RETHINKING TRUST ITSELF

Since the creation of the firewall, Zero Trust has been the biggest paradigm shift in enterprise network security. Although the model was first outlined by Forrester Research analyst John Kindervag in 2010, the principles are not widely accepted in the mainstream until the last few years, fueled by the COVID-19 pandemic which forced much of the workforce to work remotely, and the significant number of perimeter-based failures.

The key principle of Zero Trust is "never trust, always verify. The traditional perimeter model was based on geographical trust based on network location. All employees within the corporate network were trusted. Zero Trust says, “no way.” In a Zero Trust architecture, no user, device, or network segment is trusted by default, no matter where they are or what they look like. All accesses must be explicitly authenticated and authorized based on verified identity and context; they must be validated continuously during access.

It has significant implications for practice. Authenticating during the session as opposed to at session initiation. Access decisions consider not only identity, but also the health of the device involved, its location, time of day, patterns displayed in use and the sensitivity of the resources currently being accessed. The access is given on a per application and per service rather than a per network segment

basis. Network microsegmentation creates small segments of network with highly defined traffic flows.

Compelling Business Cases and incident analysis support Zero Trust. The Monitoring Software attack was a prime example of the extent to which the perimeter model is completely ineffective against supply chain assaults. A breach in trusted software update channel has been used to initiate attack, which attacker had obtained legitimate credentials, and to move within a network where internal traffic is assumed to be safe. Once the attackers have gained initial access, a Zero Trust approach (where users are constantly re-authenticated and authorized as they move laterally around) would have reduced the scope of that attack considerably.

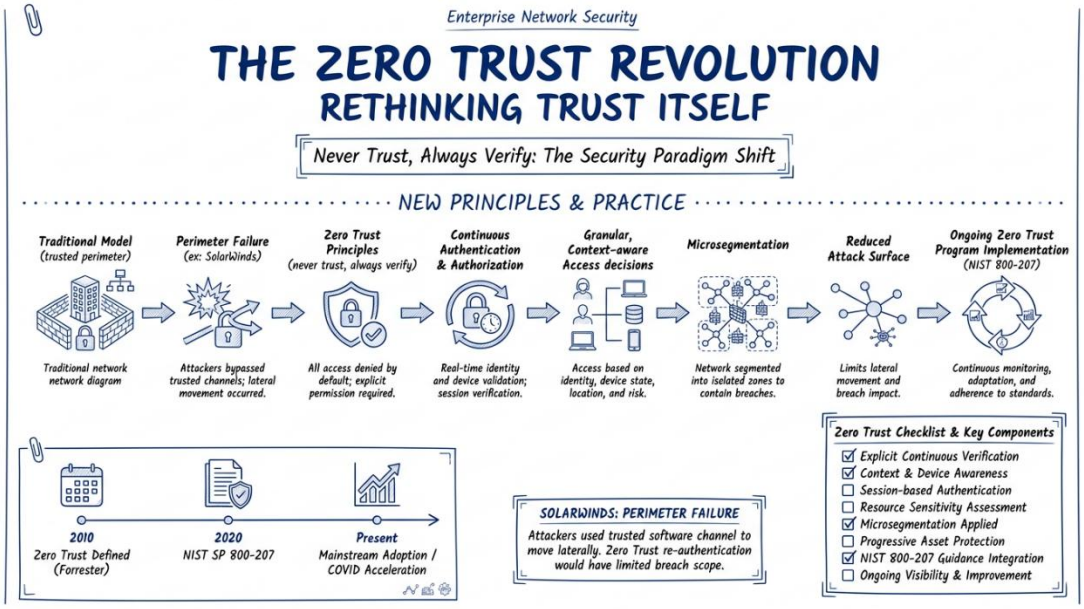

Fig -5: The Zero Trust Revolution

Most organizations view Zero Trust as not a project, but a multi-year journey. Gartner suggests it's a program for continuous improvement, starting with full visibility of how users, devices and applications are accessing existing assets, then progressively tightening access to the most sensitive assets. In 2020 the National Institute of Standards and Technology published NIST Special Publication, which offers an extensive guide to Zero Trust architecture implementation as it has become the standard for U.S. federal agencies as well as a number of private sector organizations.

7. CURRENT TRENDS RESHAPING THE ENTERPRISE SECURITY LANDSCAPE

7.1 Artificial Intelligence as Both Defense and Threat Vector

AI is putting both sides of the network fence under pressure in enterprises these days. On defense, AI and machine learning have become indispensable in today's security landscapes, where a massive amount of data is created daily. In a large enterprise security operations center, you could have millions of events coming in from logs, network sensors, endpoint agents, and cloud services every day. This volume is too large to be processed by humans in a meaningful way. AI security information and event management platforms gather information from multiple sources, detect patterns that align with common attack methodologies and bring the relevant signals to the forefront amidst the noise.

Partners Universal Multidisciplinary Research Journal (PUMRJ)
Volume: 03 Issue: 03 | April - May 2026 | ISSN: 3107-5789 | www.pumrj.com

Generative AI has made it much easier for social engineering attacks to be effective on the offensive side of the players. Phishing campaigns, whose messages were so badly written and hard to believe in the past that they were easily identified as such, can now create a message that is contextually correct, grammatically perfect, and highly personalized. According to security firm Abnormal Security, in 2019, AI-generated phishing volumes spiked 350 percent during the last 18 months. AI is also speeding up vulnerability discovery, having the ability to analyze code automatically and fuzzing at unprecedented volumes.

For security teams, the takeaway is that AI should be implemented on the defense side not for its sake of being innovative, but because it's needed. In a world where attacks are so commonplace that they are now a regular occurrence, organizations that depend on rule based detection are placed in a long-term situation of a growing and persistent detection gap.

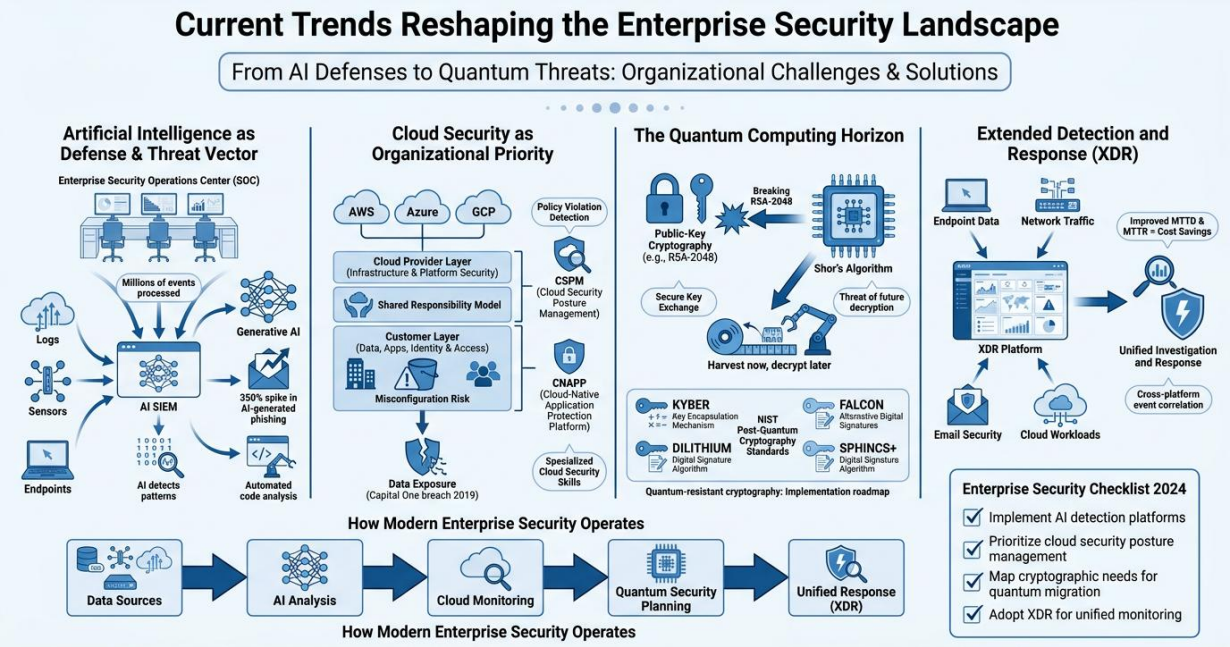

Fig -6: Current Trends Reshaping the Enterprise Security Landscape

7.2 Cloud Security as Organizational Priority

Cloud has become the baseline for most business operations and it's no longer a modernization option. But this change has in essence transformed the security model, as all three Cloud giants, Amazon Web Services, Microsoft Azure, and Google Cloud, refer to as a shared responsibility model. The cloud provider protects the clouds' base hardware, hypervisor layer, and managed services. The customer must ensure the protection of all the items placed on top of that infrastructure such as the data classification, access control, network configuration, and application security.

The primary driver of data exposures related to the Cloud has become misconfiguration of cloud resources. Back in 2019, the Capital One data breach exposed personal information of about 106 million customers, due to a misconfigured web application firewall in an AWS environment. Up Guard's Research team has reported dozens of large data leaks caused by Amazon S3 storage buckets being made public by configuration mistakes.

Cloud Security Posture Management tools are becoming a vital category, constantly monitoring cloud

landscapes for non-MOSAIC compliance, policy violations, misconfigurations and more. This is expanded to workloads, containers, and Serverless functions with Cloud Native Application Protection Platforms. Cloud security skills are not a replication of on-premises security skills, but are a specialized skill set unique to the organization that is moving significant workloads to the cloud.

7.3 The Quantum Computing Horizon

The long-term, but basic, danger to the cryptographic basis of today's security structure is quantum computing. Most modern public-key cryptography, such as RSA and elliptic curve cryptography are based on the difficulty of factoring large numbers as well as the problem of computing the discrete logarithm. These problems are impossible to solve in practical amounts of time with classical computers. If such a quantum computer with the power of Shor's algorithm were built, it would theoretically be able to break an RSA-2048 encryption in hours rather than billions of years.

This threat is not present now. The number of qubits and the number of errors are so low in quantum computers today that they are not a threat to current cryptographic systems. But the date for cryptographically useful quantum computers has been up for debate, with some estimates suggesting that they could be "practical" in a decade or even sooner. Nearer to home, there is a technique known as “harvest now, decrypt later”, where adversaries grab the encrypted traffic now and wait for quantum capability to decrypt it later. This threat is already relevant in the operating environment for data that has a long-term sensitivity (intelligence, medical, IP, etc.). In 2024, NIST finalized the standardisation process for quantum resistant cryptography, and published quantum resistant standards for four algorithms CRYSTALS-Kyber (key encapsulation) and CRYSTALS-Dilithium (digital signatures). While it might be years off for full implementation, it is time that organisations start mapping out their cryptographic need and create migration plans.

7.4 Extended Detection and Response

Known as XDR, this is a major step forward in the management of security telemetry collection, correlation, and response. Traditional security solutions worked in isolation, alerting users to incidents detected on endpoints, on the network, through email security gateways and cloud security solutions. Event correlation across platforms was done manually, and was slow, prone to errors, and tedious. XDR platforms pull in information from all parts of the security landscape and apply consistent detection logic to it and offer a unified investigation and response. This improves both MTD and MTR, which are two operational metrics that are most directly linked to financial impact caused by security incidents, by a dramatic factor. However, Ponemon Institute research has always shown that it costs significantly more to an organization to have a breach go undetected for over 200 days, so the operational efficiencies that XDR provides can be directly correlated with cost savings.

8. INSIDER THREATS THE SECURITY CHALLENGE FROM WITHIN

External attacks are more likely to be the subject of media coverage and can also be easier to imagine as a problem of adversary, making them more likely to be center stage in the conversation about security. Insider threats malicious employees, negligent user and compromised accounts of legitimate users – are an ever important category of security incidents, but they get less attention.

According to the Ponemon Institute Cost of Insider Threats Global Report 2023, insider threat incidents cost organizations an average of $16.2 million annually, and the number of insider threats had increased by 44 percent in the last two years. Significantly, most of the insider incidents were not deliberate, but were a result of negligence such as poorly configured systems, accidental data exposures, or employees

Partners Universal Multidisciplinary Research Journal (PUMRJ)
Volume: 03 Issue: 03 | April - May 2026 | ISSN: 3107-5789 | www.pumrj.com

being victims of social engineering.

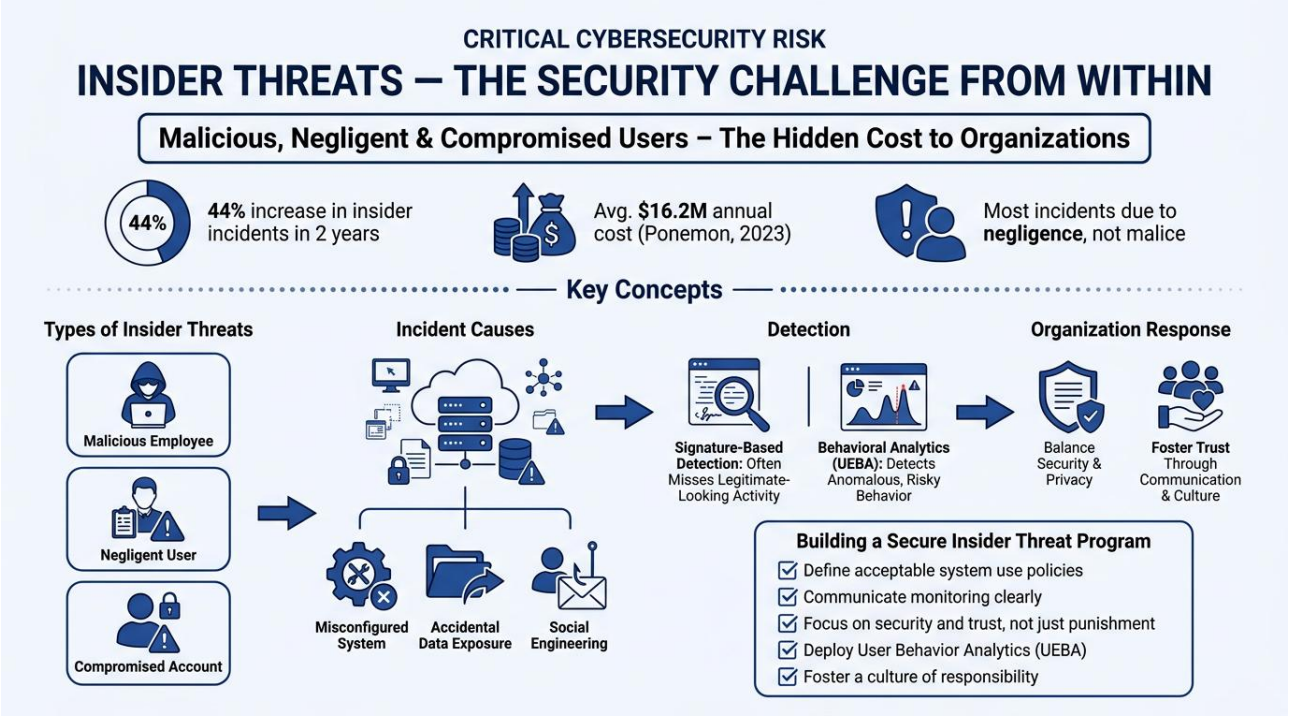

Fig -7: The Security Challenge From Within

Significant challenges exist with malicious insider detection as legitimate users accessing legitimate resources will not raise a red flag with signature-based detection. User and Entity Behavior Analytics (UEBA) addresses this by setting up user baselines and raising alarms based on user behavior that is statistically different. While there is no doubt that a system administrator suddenly accessing significant amounts of files that they've never before been granted access to, or an employee who starts copying data to external storage devices in the last few weeks that he or she has worked there, may both be exhibiting signs of behavior to be investigated, even if they are technically allowed to access these files. An organization's response to insider risk needs to be both a commitment to security and respect for privacy and trust. Defining acceptable uses, communicating clearly about what will be monitored, and messaging that involves culture, not punishment, are all crucial to the trust and cooperation that is really needed for a culture that is truly about security.

9. BUILDING SECURITY-FIRST CULTURE THE HUMAN ARCHITECTURE

Technology is the solution to the technical aspects of security issues. It does not cover social and behavioural. Any organisation that focuses solely on the technical aspects of its security program and disregards the human infrastructure will end up wasting their money on security because there are predictable human activities that will undermine their security efforts, no matter how much they spend on technology.

The figures along this line are rudimentary and convincing. Phishing was the top attack vector in the initial breach, accounting for 16 percent of breaches, according to the 2023 Cost of a Data Breach Report from IBM Security. Another 19 percent was due to stolen or compromised credentials. Combined, attacks reliant

Partners Universal Multidisciplinary Research Journal (PUMRJ)
Volume: 03 Issue: 03 | April - May 2026 | ISSN: 3107-5789 | www.pumrj.com

mainly on manipulation or exploitation of human behaviors make up over one-third of all attacks analyzed. These are issues that cannot be addressed with technical controls.

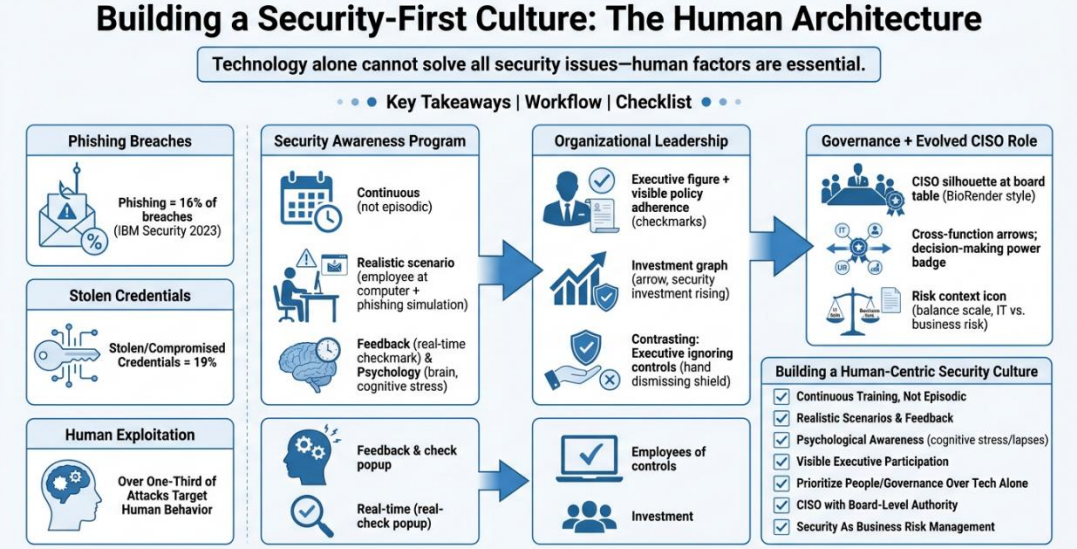

Fig -8: Building a Security-First Culture

Security awareness programs have certain traits that set them apart from the yearly compliance-oriented security training that is typically conducted in many organizations. They are not episodic, meaning that they are not all at once in the year, they are regular and create security awareness throughout the year, not just in one. These are not hypothetical but involve realistic scenarios that put employees in real-life situations to test and offer real-time feedback on learning when phishing simulations are not completed. They are psychologically savvy, aware that most security lapses are made by employees who are not negligent but simply putting the pieces together in a cognitively busy environment, under time pressure, and in an environment that has not made security signaling a priority.

Organisational leadership is a key enabler of security culture. The culture is persuasive and obvious when senior executives visibly conform to security policies, attend training and make security investments a priority in the business instead of a cost-reducing measure. If the same executives consistently ignore access controls, do not agree to implement multi-factor authentication, or consider the technical executives' concerns about security to slow down business velocity, then the organization's real culture will demonstrate those priorities even if the policy document is in place. In good organizations, the CISO job has changed dramatically from being a technical manager to a position that is cross-functional, has a direct seat at the board table, and truly has strategic decision-making power. Any organization that views security in an IT rather than a business risk management context will always spend on the people and governance aspects which are often more significant than any decision on technology.

10. BEST PRACTICES FOR BUILDING A MATURE SECURITY POSTURE

Going from a compliance-based security model to a true mature risk-based security model is a long-term effort that takes time, technology, and commitment. But there are several practices that are found in security programs that are typically the difference between a mature security program and an ever reactive security program.

Partners Universal Multidisciplinary Research Journal (PUMRJ)
Volume: 03 Issue: 03 | April - May 2026 | ISSN: 3107-5789 | www.pumrj.com

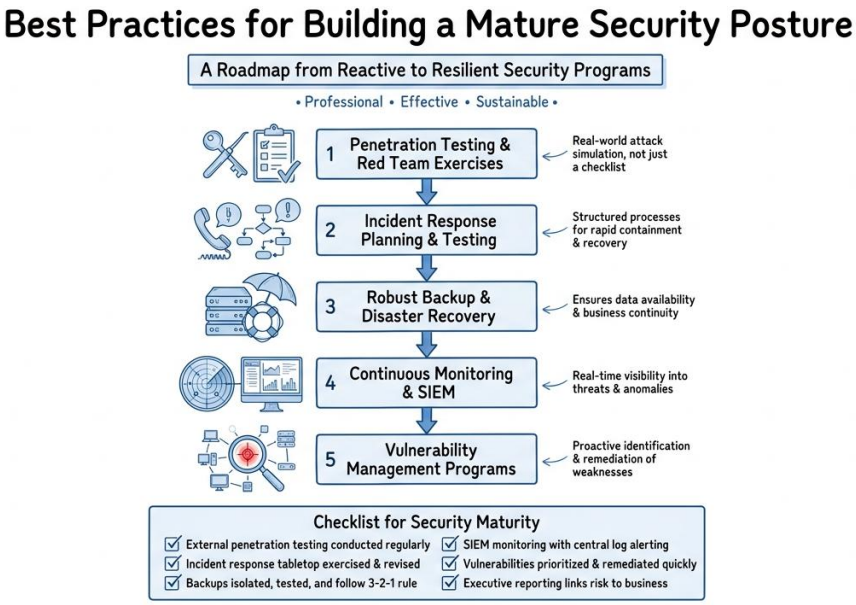

Fig -8: Best Practices for Building a Mature Security Posture

10.1 Regular Penetration Testing and Red Team Exercises

Organizations require real world data and information to show them the true area of weakness not a checklist or assumptions. This is achieved through penetration testing which is carried out by an external team in a genuine adversarial way with the same techniques used by attackers and recording which ones succeeded. Red team exercises expand on that to involve real-life attack scenarios for example, social engineering, physical access, multi-stage infiltrations and more replicated by real-world advanced persistent threat groups. These exercises should lead to specific remediation priorities, not something for which they were done, but forgotten.

10.2 Incident Response Planning and Testing

But it is not sufficient to have an incident response plan stored in a policy repository to have an effective incident response capability. Plans not used, rehearsed, and improved in a tabletop exercise will be inadequate under high stakes, full information, and time pressure in an actual incident. It is important to have tabletop exercises with scenarios that include organizations, know what is missing in their response, and ensure that everyone involved knows their responsibilities and has the authority to respond quickly in case of an incident.

10.3 Robust Backup and Disaster Recovery

As ransomware attacks have proven again, the only way for an organization to survive an attack by a ransomware is to have a reliable and tested backup to restore their data should it be encrypted. Sophisticated ransomware operators know that backup repositories are prime targets to encrypt before deployment of their main payload, so it's imperative that backups are stored in isolated locations that are inaccessible from production networks. Three copies of data on two different media types with one off-site, this is still sound advice. Perhaps most importantly, backups should be tested regularly by taking a recovery action to restore the backup. A lot of organizations have found out if their backup copies were corrupted or incomplete or could only be recovered in a time frame that did not meet the needs of their businesses.

Partners Universal Multidisciplinary Research Journal (PUMRJ)
Volume: 03 Issue: 03 | April - May 2026 | ISSN: 3107-5789 | www.pumrj.com

10.4 Continuous Monitoring and SIEM

Security information and event management platforms can centralize log data from throughout the environment, correlate events and offer visibility to identify incidents as they happen. One of the reasons for the value of continuous monitoring is because the more quickly a breach is detected, the less will be the cost of the incident. The IBM Cost of a Data Breach Report has always determined that breaches that take place within 200 days on average are about one million dollars cheaper than those that run longer. During critical times, organizations without centralized logging and alerting are flying blind.

10.5 Vulnerability Management Programs

Vulnerability management is not all about running a scanner. It needs a thorough and up-to-date Asset Inventory, regular scanning coverage, prioritization by vulnerabilities according to the risk level (exploitability and business impact), remediation service level agreements and executive vulnerability reporting that correlates the exposure of vulnerabilities to the business risk. A huge vulnerability backlog that leaves companies with a false sense of security for having a comprehensive scan and doesn't fix critical vulnerabilities for months.

11. COMPLIANCE, GOVERNANCE, AND THE DIFFERENCE BETWEEN THEATER AND SECURITY

Over the last 20 years, the number of regulatory compliance frameworks has grown exponentially, with increasingly complex obligations for companies with operations in many jurisdictions and industries. The General Data Protection Regulation is a new European Union data protection law with fines of up to four per cent of global turnover. Protected health information in the United States is under HIPAA. Any organization that handles payment card information is subject to PCI DSS. More than a dozen other states in the U.S. have been inspired to enact similar privacy laws to the California Consumer Privacy Act.

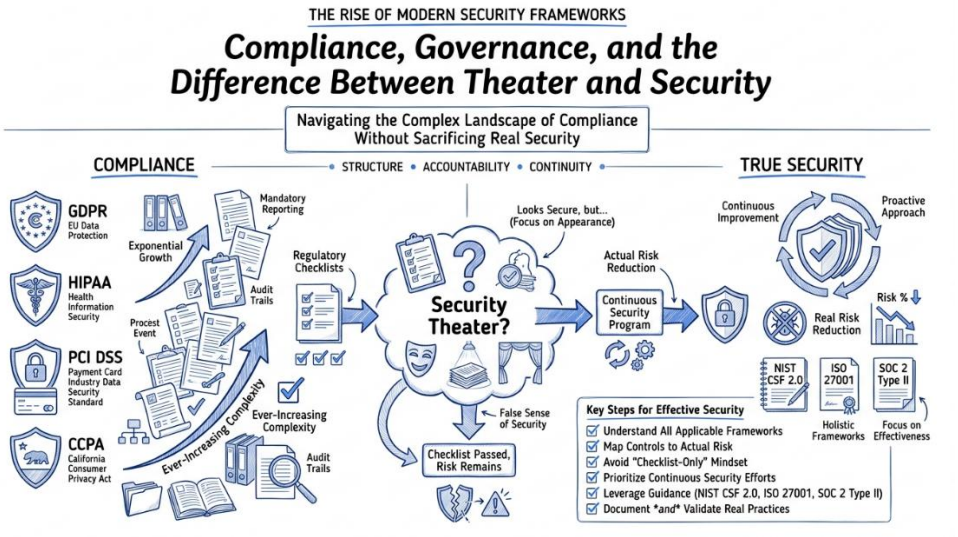

Fig -9: The Rise of Modern Security Frameworks

These frameworks offer a lot of structure and accountability, which has resulted in a boost in security investment where they would have otherwise been underinvested in the discipline. But compliance and true security are linked, but different, goals. Conformance verifies the existence of controls at a particular time. Security is a continuous way of operating. Those organizations that design their security program

Partners Universal Multidisciplinary Research Journal (PUMRJ)
Volume: 03 Issue: 03 | April - May 2026 | ISSN: 3107-5789 | www.pumrj.com

around compliance criteria, rather than what security practitioners might consider to be "what it takes," often end up creating something called "security theater" processes, documentation and tools that meet the requirements of a compliance checklist without significantly reducing the real risk of an attack. The goal is to implement a security program that lowers actual risk, and produces compliance as a byproduct, not a program that creates compliance documentation, while risks are not reduced. Tools like NIST CSF 2.0, ISO 27001 and SOC 2 Type II offer truly valuable structural direction to creating robust security programs. These are intended to be used as a guide to good security use and not as a goal to be achieved.

12. FUTURE PROSPECTS WHAT ENTERPRISE NETWORK SECURITY MUST BECOME

There are a handful of forces that will combine to affect the course of enterprise network security in the coming decade. Today's ever-growing landscape of connected infrastructure such as the Internet of Things, operational technology systems and edge computing deployments will dramatically expand the attack surface well beyond the capabilities of most organizations. Industrial control systems that were once air-gapped from corporate networks are now more connected so they can be more efficient, but the industrial sector is just starting to confront the security challenges of these connections.

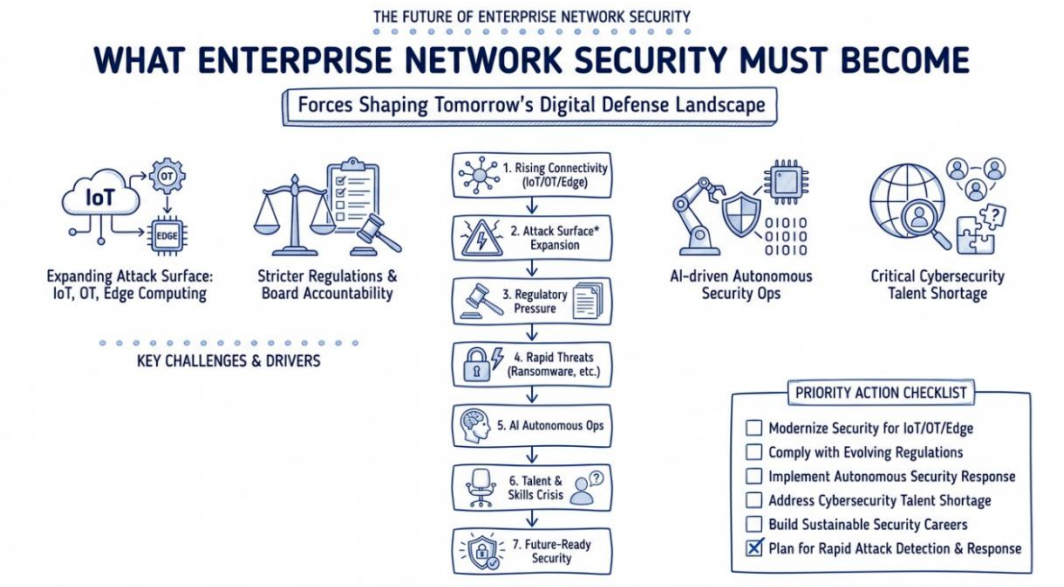

Fig -10: Enterprise Network Security

Regulatory structures will further develop, with more particularity in terms of security architecture requirements instead of just results concerning data protection. New disclosures rules for publicly traded companies under the U.S. Securities and Exchange Commission (SEC) that mandate that material cybersecurity incidents be reported to investors within four days of their occurrence mark a shift toward increased accountability of boards and senior officials in the cyber realm.

As technology advances, autonomous security operations, where AI systems identify, investigate, and respond to threats with very little human input will become increasingly viable. This is a must have because of the speed at which modern attacks occur. A lot of ransomware attacks will encrypt essential systems within minutes of gaining access, and human-speed response is insufficient in that amount of

Partners Universal Multidisciplinary Research Journal (PUMRJ)
Volume: 03 Issue: 03 | April - May 2026 | ISSN: 3107-5789 | www.pumrj.com

time. Building trustworthy autonomous response capability, with appropriate human oversight and audit trails will be a key challenge in the field as the development progresses.

The security industry will also have to face the ongoing lack of talent that will limit the capacity of their organizations. ISC2 estimated that there were 4 million cybersecurity professionals missing in the workforce globally in its 2023 Cybersecurity Workforce Study. Solving this means investing in security education and training pathways, leveraging automation to scale up the talent that is available, and building security jobs that are sustainable and attractive to be held onto by experienced security practitioners.

13. SUPPLY CHAIN SECURITY AND THIRD-PARTY RISK MANAGEMENT

Supply chain compromise might be the most structurally unmanageable attack vector, among all the ones that pose a threat to enterprise networks today. The challenge is at the core. All organizations rely on third-party vendors, software vendors, managed service providers, and cloud service providers. All these connections are a way to enter the enterprise network, and the attacked organization may have little or no visibility into, or control over, the security measures taken by the organizations it relies on.

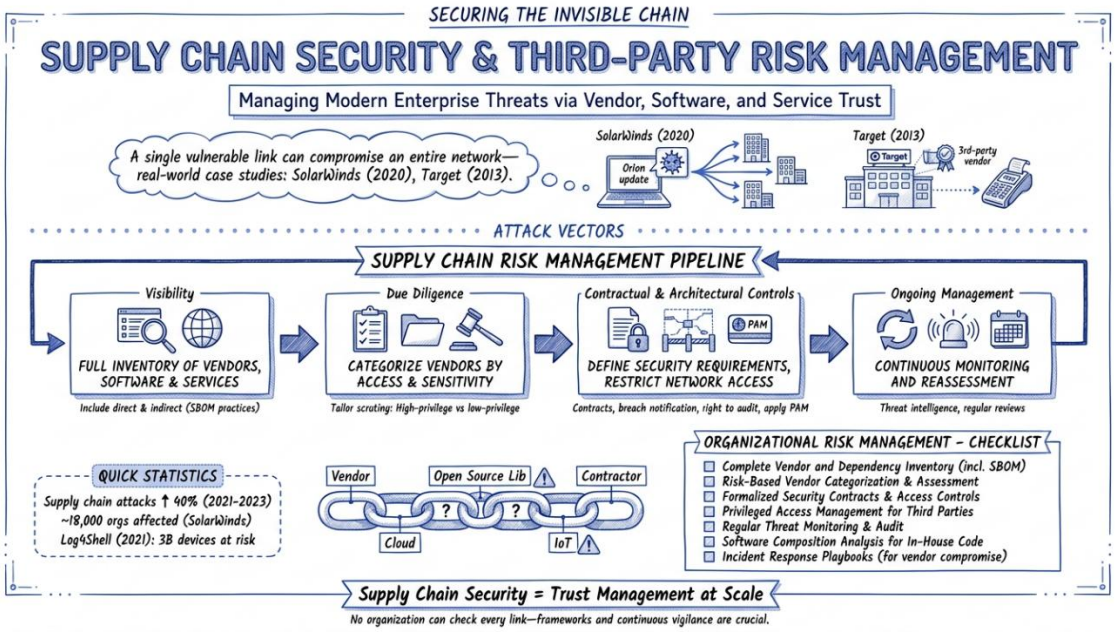

Fig -11: Supply Chain Security & Third party Risk management

This is what was done during the Monitoring Software attack in 2020. The attackers, allegedly connected to the Russian foreign intelligence service, allegedly compromised Monitoring Software' development system and added malicious code to Orion, the company's popular IT monitoring solution. About 18,000 enterprises, ranging from the U.S. Treasury to the Department of Homeland Security, to dozens of fortune 500 firms, were taking routine software updates from Monitoring Software that were an advanced form of backdoor. The attack was not a result of any of the attacked organizations having poor perimeter security, but that they relied on a vendor whose security had been breached. The link in the chain of trust was a place they couldn't physically examine.

The logic of the Target breach from 2013 was the same. The third party HVAC contractor on the network,

who had credentials to log in to Target's POS systems, was the source of the stolen credentials. It wasn't via Target's own system. It was a vendor relationship on the periphery that wasn't adequately checked for security. This is not a freak occurrence. In fact, the number of attacks on the supply chain rose 40 percent year over year from 2021 to 2023, according to CrowdStrike's 2023 Global Threat Report. European Union Agency for Cybersecurity (ENISA) recently published its 2023 Threat Landscape Report and supply chain attacks were one of the highest ranked emerging threats to any organisation in any sector.

Most organisations have not executed the necessary level of clarity and rigor into supply chain risk management processes. The first is that it be seen. Organizations require a complete list of all third-party vendors, software dependency, and service providers that are used, touch the organization network environment or have an impact on it. This will involve direct suppliers and ideally, those of suppliers, for the most critical dependencies. However, there is a new practice that has been promoted as standard practice by the U.S. Cybersecurity and Infrastructure Security Agency (CISA) that offers a way to list software dependencies to determine if systems are at risk if a vulnerability is found in a software library. This is known as a software bill of materials.

The second requirement is ‘proportionate due diligence'. Not all vendors are created equal, and it is not feasible to treat an Enterprise Security Service Provider (ESSP) with a high level of service and access and apply the same scrutiny to a software tool vendor with low access. Vendors should be categorized based on access privileges and sensitivity of systems they are able to access and then the security assessment requirements should be commensurate with the categorized access. Regular security assessment, contractual security requirements and in some cases independent auditing are all applicable to those vendors who enjoy privileged access to production systems or sensitive data.

Contractual and architectural controls are the 3rd requirement. There must be a contract with the vendor that defines minimum security requirements, breach notification requirements, and the right to audit. Network architecture should restrict vendor access to only the systems and resources that they properly need, using dedicated vendor access segments, robust authentication, and logging. Privileged access management solutions should control access to third-party vendors' resources that are used for administration and log and track access to all these resources.

The fourth important requirement is ongoing management of the vendor over the years. A vendor who makes the cut in their initial security assessment may then suffer from their own system being breached, have their security practices changed, or be acquired by a vendor with different security practices. It's important to continuously monitor the risks from third parties by utilizing threat intelligence feeds, breach notification services and by routinely reassessing the risk.

For third-party and open-source library dependencies in applications developed in-house, software composition analysis tools help mitigate the risks. In 2021, the Log4Shell vulnerability that was found in the popular Apache Log4j logging library, impacted an estimated three billion devices and necessitated emergency patching in almost every industry. Those organizations that had adopted software composition analysis were able to determine impacted systems within hours. Without this ability, it took many weeks for those without to locate all the places the library existed in their world.

Security in the supply chain is a trust management at scale issue. It is impossible for organisations to validate all elements independently and there is a need to have frameworks in place for determining the level of trust to be given to third parties, under what circumstances and with what level of follow up. The construction of these frameworks is one of the top priorities today for enterprise network security and the most under-invested enterprise network security practice.

14. CONCLUSION

The security of enterprise networks is at a turning point. The model that once prevailed in the field is no longer sufficient such as perimeter-based model, which has been replaced by distributed, boundary-less enterprise computing. The attacks that have plagued the security industry this time around Monitoring Software, Colonial Pipeline, Capital One, and dozens of others were not so many failures of individual security products as they were failures of the security industry. They were failures in architectural thinking, in the conception of the organization, and in a perimeter that had become an abstract concept. However, moving forward will mean embracing this reality and developing security plans that acknowledge the real threat landscape they are in. Zero Trust is the right conceptual model every access request is untrusted until verified and always rechecked. A Defense in Depth strategy is designed to ensure that if one control fails, there is still another one in place that will not cause any catastrophic exposure. Detecting and responding to today's challenges is too fast and too frequent for humans to keep up with, and that's where AI-assisted detection and response come in. Cloud-native security practices are safeguarding the environments where an increasing amount of data in organizations resides.

It's also important to realize that technology is essential but not enough. Any technical measure is as vital as security culture, governance frameworks, the accountability of leaders and investments in human capacities. Every organization that sees security as an IT issue will continue to outperform those organizations that view security as an organizational function that must be continuously invested in, with board-level attention, and commitment across all functions. Security is not something that an organization gets. It is ongoing, it's adaptable and it's continuously improving, all to a threat landscape that will not cease to change. Those that will prosper the most over the next decade will not be the ones with the most advanced tech stack, but those that develop the ability to intelligently respond to threats they have yet to face. Resilience is the most important security attribute in an era of distributed threats.

REFERENCES

[1] Aldabbas, M., Teufel, S., & Teufel, B. (2017). The importance of security culture for crowd energy systems. 2017 Information Security for South Africa (ISSA). https://doi.org/10.1109/issa.2017.8251783
[2] Battal, C., & Gündüz, Ş. (2025). Evaluation of authentication schemes in online exams within the framework of information security: CIA triad. The New DNA of Education: Innovation, Technology, Equity, and the Cognitive Turn. https://doi.org/10.58830/ozgur.pub1137.c4676
[3] Das, R. (2025). Real-world supply chain attacks. The Effects of Cyber Supply Chain Attacks and Mitigation Strategies. https://doi.org/10.1201/9781003585916-3
[4] Kudrati, A., & Pillai, B. (2022). Zero trust – disrupting the business model. Zero Trust Journey Across the Digital Estate. https://doi.org/10.1201/9781003225096-4
[5] Ologunde, E. (2026). Risk acceptance in critical infrastructure cyber incidents: A retrospective analysis of the colonial pipeline ransomware attack. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.6212678
[6] Ouda, A. J., Yousif, A., Hasan, A. S., Ibrahim, H. M., & Shyaa, M. A. (2022). The impact of cloud computing on network security and the risk for organization behaviors. Webology. https://doi.org/10.14704/web/v19i1/web19015
[7] Vescent, H., & Blakley, B. (2018). Shifting paradigms. Proceedings of the New Security Paradigms Workshop. https://doi.org/10.1145/3285002.3285013
[8] Zmaimita, H., Madani, A., & Zine-Dine, K. (2025). Automating cyber threat detection with AI and machine learning. AI-Driven Cybersecurity. https://doi.org/10.1201/9781003631507-13
[9] (2023). Industry and government collaboration on security guardrails for AI systems: Summary of the AI safety and security workshops. https://doi.org/10.7249/cfa2949-1
[10] Berghel, H. (2001). The code red worm. Communications of the ACM, 44(12), 15-19. https://doi.org/10.1145/501317.501328

[11] Cabric, M. (2015). Confidentiality, integrity, and availability. Corporate Security Management. https://doi.org/10.1016/b978-0-12-802934-3.00011-1
[12] El-Atawy, A., Al-Shaer, E., Tran, T., & Boutaba, R. (2009). Adaptive early packet filtering for defending firewalls against dos attacks. IEEE INFOCOM 2009. https://doi.org/10.1109/infcom.2009.5062171
[13] Marcus, J. S. (2023). COVID-19 and the shift to remote work. Beyond the Pandemic? Exploring the Impact of COVID-19 on Telecommunications and the Internet. https://doi.org/10.1108/978-1-80262-049-820231003
[14] Markov, A., & Fadin, A. (2013). Organizational and technical problems of protection against targeted malware such as stuxnet. Voprosy kiberbezopasnosti, 28-36. https://doi.org/10.21681/2311-3456-2013-1-28-36
[15] Marpaung, J. A., Bhakti, M. A. C., & Yazid, S. (2013). A study on application layer classification for firewalls using regular expression matching. 2013 International Conference on Advanced Computer Science Applications and Technologies. https://doi.org/10.1109/acsat.2013.88
[16] Mishra, S., & Dhillon, G. (2008). The impact of the sarbanes-oxley (SOX) act on information security. Information Security and Ethics. https://doi.org/10.4018/978-1-59904-937-3.ch170
[17] Pribil, K., Lassarat, J., Felicetti, A., & O'Rourke, J. (2014). Target corporation: Reputational damage from a massive data breach. https://doi.org/10.4135/9781526403421
[18] Steffens, T. (2020). Advanced persistent threats. Attribution of Advanced Persistent Threats. https://doi.org/10.1007/978-3-662-61313-9_1
[19] Vacca, J. R., & Ellis, S. R. (2005). Firewalls. Firewalls. https://doi.org/10.1016/b978-155558297-5/50003-7
[20] (2003). Enterprise security concerns in year ahead. Network Security, 2003(4), 2. https://doi.org/10.1016/s1353-4858(03)00402-1
[21] (2017). The wannacry ransomware attack. Strategic Comments, 23(4), vii-ix. https://doi.org/10.1080/13567888.2017.1335101
[22] (2019). Verizon: 2019 data breach investigations report. Computer Fraud & Security, 2019(6), 4-4. https://doi.org/10.1016/s1361-3723(19)30060-0
[23] Arun Kumar Soumya, A. (2024). Ai-powered strategies for enhanced email security and phishing defense. International Journal of Science and Research (IJSR), 13(12), 1335-1337. https://doi.org/10.21275/sr241220090939
[24] Bhagat, L., & Banerji, B. (2025). The digital shift: Remote work, gender inequalities, and the transformation of work during the COVID-19 pandemic in india. sozialpolitik.ch. https://doi.org/10.18753/2297-8224-6988
[25] Gelles, M. G. (2021). Insider threat prevention, detection, and mitigation. International Handbook of Threat Assessment. https://doi.org/10.1093/med-psych/9780190940164.003.0037
[26] Karamchand, G. (2022). ZERO TRUST SECURITY ARCHITECTURE: A PARADIGM SHIFT IN CYBERSECURITY FOR THE DIGITAL AGE. INTERNATIONAL JOURNAL OF CYBER SECURITY, 1(2), 1-20. https://doi.org/10.34218/ijcs_01_02_001
[27] Khalil, I., Dou, Z., & Khreishah, A. (2016). Your credentials are compromised, do not panic. Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security. https://doi.org/10.1145/2897845.2897925
[28] Kindervag, J. (2006). The five myths of wireless security. Information Systems Security, 15(4), 7-16. https://doi.org/10.1201/1086.1065898x/46353.15.4.20060901/95120.2
[29] Kudrati, A., & Pillai, B. (2022). Zero trust architecture components. Zero Trust Journey Across the Digital Estate. https://doi.org/10.1201/9781003225096-8
[30] Makkada, V., & Rai, I. (2024). Capital one data breach. Information Technology Security and Risk Management. https://doi.org/10.1201/9781003264415-6
[31] Md Aminul Islam (2025). Zero-trust reinforcement learning for autonomous network access decisions. Academica Global: Journal of Computer Science and Technology Studies, 4(1), 17-37. https://doi.org/10.32996/agjcsts.2025.2.1.2
[32] Parshuram Patil, S. (2020). Zero trust architecture in hybrid cloud: Theory and implementation. International Journal of Science and Research (IJSR), 1911-1915. https://doi.org/10.21275/sr20522094157
[33] Rai, A. (2026). Cloud misconfiguration as a leading cause of data breaches: A systematic analysis. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.6002874
[34] Ricci, S., Jedlicka, P., Cibik, P., Dzurenda, P., Malina, L., & Hajny, J. (2021). Towards crystals-kyber VHDL implementation. Proceedings of the 18th International Conference on Security and Cryptography. https://doi.org/10.5220/0010580400002998
[35] Wylde, A. (2021). Zero trust: Never trust, always verify. 2021 International Conference on Cyber

Situational Awareness, Data Analytics and Assessment (CyberSA). https://doi.org/10.1109/cybersa52016.2021.9478244
[36](2004). Cascade perimeter defence model in multiple VPN environment. The KIPS Transactions:PartC, 11C(1), 81-88. https://doi.org/10.3745/kipstc.2004.11c.1.081
[37](2013). Continuous improvement toolkit. Communication for Continuous Improvement Projects. https://doi.org/10.1201/b15983-14
[38](2015). Some mathematical problems in public key cryptography. Mathematical Foundations of Public Key Cryptography. https://doi.org/10.1201/b19324-14
[39](2017). 6. a worst practices guide to insider threats. Insider Threats. https://doi.org/10.7591/9781501705946-009
[40](2019). How can quantum computing break today's cryptography?. Cryptography Apocalypse, 59-83. https://doi.org/10.1002/9781119618232.ch3
[41](2019). Accenture/ponemon institute: The cost of cybercrime. Network Security, 2019(3), 4-4. https://doi.org/10.1016/s1353-4858(19)30032-7
[42](2021). IBM: Cost of a data breach report. Computer Fraud & Security, 2021(8), 4-4. https://doi.org/10.1016/s1361-3723(21)00082-8
[43]George, D. (2026c). Multi-Vendor firewall strategy: IT, OT, and edge networks. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.19630402
[44](2022). When network and security management meets AI and machine learning. AI and Machine Learning for Network and Security Management, 9-47. https://doi.org/10.1002/9781119835905.ch2
[45](2024). Cloud adoption. Conference of European Statisticians Statistical Standards and Studies. https://doi.org/10.18356/9789213587256c006
[46]George, D. (2026b). IEC 62443 Wireless Security: Deploying OT wireless controllers in industrial factory networks. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.19428491
[47]Garbis, J., & Chapman, J. W. (2021). A zero trust policy model. Zero Trust Security. https://doi.org/10.1007/978-1-4842-6702-8_17
[48]George, D. (2026d). Security Service Edge (SSE) and SASE: A complete guide to Cloud-Native Zero Trust architecture for enterprise security. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.19974566
[49]Glocker, F. (2022). Der california consumer privacy act. https://doi.org/10.1628/978-3-16-161943-4
[50]Miller, J. F. (2013). Supply chain attack framework and attack patterns. https://doi.org/10.21236/ada610495
[51]Nizich, M. (2023). Preparing the cybersecurity workforce of tomorrow. The Cybersecurity Workforce of Tomorrow. https://doi.org/10.1108/978-1-80382-915-920231009
[52]George, D. (2025b). India's new labor codes a critical analysis of promise, peril, and the path forward. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.17871778
[53]Sopariwala, S., Fallon, E., & Asghar, M. N. (2022). Log4jpot: Effective log4shell vulnerability detection system. 2022 33rd Irish Signals and Systems Conference (ISSC). https://doi.org/10.1109/issc55427.2022.9826147
[54]Sudharani, S. (2025). Decision supported framework for regulatory compliance. https://doi.org/10.31274/cc-20260223-54
[55]George, D. (2024). Personal privacy at risk: The security threats of sharing boarding passes online. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.14503012
[56]George, D. (2025a). Cyber resilience in an AI-Driven world: a Strategic framework. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.18002783
[57](2010). Layer upon layer (defense in depth). Security Strategy. https://doi.org/10.1201/ebk1439827338-16
[58](2011). ASPECTS OF PCI DSS COMPLIANCE. PCI DSS. https://doi.org/10.2307/j.ctt5hh6b2.13
[59]George, D. (2025c). Sanchar Saathi Digital Security versus Civil Liberty in India 's Smartphone Era. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.17838468
[60]George, D. (2026a). Architectural Convergence in Security Operations: a technical framework for AI-Augmented Threat Detection, Automated response, and Organizational cyber resilience. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.19986642
[61]George, D., & Dr.T.Baskar. (2025). Security and privacy comparison of Arattai, WhatsApp, and WeChat: India's messaging app landscape and digital sovereignty. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.17483067

[62] George, D., Dr.T.Baskar, & Dr.M.M.Karthikeyan. (2026). Cloud Security Architecture: A comprehensive guide to zero trust, governance, and operational resilience. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.19551592

[63] George, D., Dr.T.Baskar, & Srikaanth, P. B. (2025). Bridging the Security Skills Gap: A comprehensive framework for developing application security competencies in modern software engineering. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.15616416

[64] (2014). Confidentiality: HIPAA regulations. https://doi.org/10.4135/9781529727722

[65] George, D., Dr.T.Baskar, Srikaanth, P. B., & Dr.M.M.Karthikeyan. (2025). Building resilient API security through a Five-Dimensional Framework for data breach prevention in modern digital ecosystems. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.15862111

[66] (2014). ENISA: Top cyber-bedrohungen im threat-landscape-report 2013. Datenschutz und Datensicherheit - DuD, 38(2), 134-134. https://doi.org/10.1007/s11623-014-0058-0

[67] (2021). IBM: Cost of a data breach report. Computer Fraud & Security, 2021(8), 4-4. https://doi.org/10.1016/s1361-3723(21)00082-8

[68] George, D., George, A., & Dr.T.Baskar. (2023). SD-WAN Security Threats, Bandwidth Issues, SLA, and Flaws: An In-Depth Analysis of FTTH, 4G, 5G, and Broadband technologies. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.8057014

[69] (2023). Art. 83: General conditions for imposing administrative fines. General Data Protection Regulation, 1051-1064. https://doi.org/10.5040/9781509932535.0127

[70] Khan, N., & Al-Yasiri, A. (2018). Cloud security threats and techniques to strengthen cloud computing adoption framework. Cyber Security and Threats. https://doi.org/10.4018/978-1-5225-5634-3.ch016

[71] Kudrati, A., & Pillai, B. (2022). Zero trust – disrupting the business model. Zero Trust Journey Across the Digital Estate. https://doi.org/10.1201/9781003225096-4

[72] Nizich, M. (2023). Preparing the cybersecurity workforce of tomorrow. The Cybersecurity Workforce of Tomorrow. https://doi.org/10.1108/978-1-80382-915-920231009

[73] Olorunlana, T. J., & Mohammed, H. (2025). Analysis of the colonial pipeline cybersecurity incident. International Journal of Science, Architecture, Technology and Environment, 9-13. https://doi.org/10.63680/jngh0767as

[74] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture. https://doi.org/10.6028/nist.sp.800-207

[75] Scarfone, K. A., Grance, T., & Masone, K. (2008). Computer security incident handling guide. https://doi.org/10.6028/nist.sp.800-61r1

[76] Sethuraman, S. C., V S, D. P., Reddi, T., Reddy, M. S. T., & Khan, M. K. (2024). A comprehensive examination of email spoofing: Issues and prospects for email security. Computers & Security, 137, 103600. https://doi.org/10.1016/j.cose.2023.103600

[77] Thompson, E. E. (2018). Insider cybersecurity threats to organizations. The Insider Threat. https://doi.org/10.1201/9781315368627-2

[78] Truong, Q. D., Nguyen, H., Nguyen, T. T., & Lee, H. (2026). NIST post-quantum cryptography standards: A comprehensive review of theoretical foundations and implementations. IEEE Access, 14, 14069-14097. https://doi.org/10.1109/ACCESS.2026.3654142

[79] Tóth, Á. (2025). Zero trust network access az ipari (OT) kiberbiztonságban. Hadmérnök, 20(4), 87-102. https://doi.org/10.32567/hm.2025.4.6

[80] Yang, S. (2023). Backdoor attack in autonomous vehicles. https://doi.org/10.31274/cc-20240624-276

[81] (2009). "shared responsibility". https://doi.org/10.1377/hpb20090813.812963

[82] (2019). Verizon: 2019 data breach investigations report. Computer Fraud & Security, 2019(6), 4-4. https://doi.org/10.1016/s1361-3723(19)30060-0

[83] Dr.A.Shaji George, Dr.S.Sagayarajan, Dr.T. Baskar, & Digvijay Pandey. (2024). Assessing the Security and Privacy Implications of India's DigiYatra Initiative. Partners Universal Innovative Research Publication (PUIRP), 02(06), 36–45. https://doi.org/10.5281/zenodo.14599297

[84] (2021). IBM: Cost of a data breach report. Computer Fraud & Security, 2021(8), 4-4. https://doi.org/10.1016/s1361-3723(21)00082-8

[85] (2025). MITRE att&ck: MITRE adversarial tactics, techniques, and common knowledge. Encyclopedia of Cryptography, Security and Privacy. https://doi.org/10.1007/978-3-030-71522-9_300601