AIS ARTIFICIAL INTELLIGENCE STUDIES

A Systematic Review on Evolution, Challenges, and Future Trajectories of Endpoint Security: Integrating Zero Trust and Federated Learning Perspectives

Oudoum Ali Houmed[*a], **Onur Ceran**[b]

ABSTRACT

As cyber threats evolve in complexity and frequency, endpoint security has transformed from simple antivirus solutions into comprehensive frameworks incorporating artificial intelligence, real-time behavioral analytics, and cloud-based telemetry integration. This paper presents a systematic review of the technological evolution and present challenges of endpoint security, covering the transition from signature-based antivirus software to modern systems such as Endpoint Detection and Response (EDR), Extended Detection and Response (XDR), Managed Detection and Response (MDR), and Network Detection and Response (NDR). Through a longitudinal timeline and thematic synthesis of recent developments, we analyze how endpoint protection technologies have adapted to address growing threats such as zero-day exploits, ransomware-as-a-service, and Internet of Things (IoT) vulnerabilities. Our findings reveal that while next-generation endpoint security solutions offer robust capabilities, they remain constrained by implementation complexity, data privacy regulations, and device interoperability. This study distinctively contributes to the literature by presenting a conceptual framework for integrating Zero Trust and Federated Learning principles into future endpoint defense strategies and by identifying critical, previously under-detailed research challenges associated with this integration. The paper concludes by discussing the importance of these integrations for creating scalable, privacy-preserving, and globally coordinated endpoint defense strategies.

[a,*] Gazi University Graduate
School of Natural and Applied Sciences
06560 - Ankara, Türkiye
ORCID: 0009-0006-6526-8042

[b] Gazi University,
Faculty of Applied Sciences, Department of Management Information Systems
06560 - Ankara, Türkiye
ORCID: 0000-0003-2147-0506

[*] Corresponding author.
e-mail: oudoumali23@gmail.com

Keywords: endpoint security, EDR XDR, AI in cybersecurity, IoT, zero trust, federated learning

Submitted: 02.06.2025
Revised: 27.06.2025
Accepted: 30.06.2025

doi:10.30855/ais.2025.08.01.02

Uç Nokta Güvenliğinin Evrimi, Zorlukları ve Gelecek Yörüngeleri: Sıfır Güven ve Federe Öğrenme Perspektiflerini Bütünleştiren Sistematik Bir Derleme

ÖZ

Siber tehditlerin hem karmaşıklık hem de frekans bakımından sürekli evrim geçirmesi, uç nokta güvenliğini basit antivirüs çözümlerinin ötesine taşıyarak yapay zeka destekli, gerçek-zamanlı davranışsal analizi ve bulut tabanlı telemetri entegrasyonunu içeren bütüncül çerçevelere dönüştürmüştür. Bu çalışma, imza tabanlı antivirüs yazılımlarından Uç Nokta Tespiti ve Müdahalesi (EDR), Genişletilmiş Tespit ve Müdahale (XDR), Yönetilen Tespit ve Müdahale (MDR) ile Ağ Tespiti ve Müdahalesi (NDR) gibi çağdaş sistemlere geçişi ele alarak uç nokta güvenliğinin teknolojik evrimini ve güncel zorluklarını sistematik biçimde irdelemektedir. Kronolojik bir zaman çizelgesi ve tematik bir sentez aracılığıyla yürütülen analiz, uç nokta koruma teknolojilerinin sıfırıncı gün açıkları, Hizmet Olarak Fidye Yazılımı (Ransomware-as-a-Service) ve Nesnelerin İnterneti (IoT) zafiyetleri gibi büyüyen tehdit ortamına karşı nasıl uyum sağladığını ortaya koymaktadır. Bulgular, yeni nesil uç nokta güvenliği çözümlerinin kayda değer kabiliyetler sunmakla birlikte, uygulama karmaşıklığı, veri mahremiyeti mevzuatı ve çoklu cihaz ortamlarında birlikte çalışabilirlik eksiklikleri gibi kısıtlarla karşı karşıya olduğunu göstermektedir. Çalışma ayrıca, Sıfır Güven (Zero Trust) ve Federe Öğrenme (Federated Learning) ilkelerinin geleceğin uç nokta savunma stratejilerine entegrasyonuna yönelik kavramsal bir çerçeve önererek, literatürde yeterince derinlemesine ele alınmamış kritik araştırma boşluklarını tanımlamakta ve böylelikle özgün bir katkı sunmaktadır. Sonuç bölümünde, ölçeklenebilir, mahremiyeti koruyan ve küresel ölçekte eşgüdümlü uç nokta savunma yaklaşımlarının geliştirilmesinde söz konusu entegrasyonların taşıdığı stratejik önem kapsamlı biçimde tartışılmaktadır.

To cite this article: O. A. Houmed and O. Ceran, "A Systematic Review on Evolution, Challenges, and Future Trajectories of Endpoint Security: Integrating Zero Trust and Federated Learning Perspectives," *Artificial Intelligence Studies,* vol.8, no.1, pp. 20-37, 2025. doi:10.30855/ais.2025.08.01.02

1. Introduction

In the contemporary digital ecosystem, where hyper-connectivity is the norm, endpoint devices have emerged as the central battleground in the cybersecurity landscape [1, 2]. These devices, ranging from traditional desktops and laptops to the ubiquitous network of smartphones and Internet of Things (IoT) hardware, serve as the primary entry points for a diverse and sophisticated array of malicious actors, compelling a relentless and rapid evolution of endpoint protection strategies [3]. The technological trajectory of endpoint security has been characterized by a perpetual arms race, advancing from rudimentary signature-based antivirus tools of the past to the sophisticated, AI-enhanced solutions that define the current era, such as Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR) [4, 5]. This progression highlights the dynamic and escalating nature of digital threats, which now include advanced persistent threats (APTs), fileless malware, and ransomware-as-a-service (RaaS).

Within this high-stakes environment, the establishment of robust endpoint security has become unequivocally critical for ensuring the operational continuity, data integrity, and overall resilience of modern organizations [6, 7]. The sheer volume and increasing sophistication of cyber-attacks consistently render traditional, perimeter-focused security measures insufficient, thereby underscoring an urgent need for more proactive, intelligent, and adaptive defense mechanisms capable of operating on scale [8, 9]. While modern solutions have significantly advanced threat detection and response capabilities, they are not a panacea. Persistent challenges related to implementation complexity, data privacy constraints, and cross-platform interoperability continue to limit their effectiveness.

This systematic review addresses these issues by charting technological evolution, persistent challenges, and future trajectories of endpoint security. However, its principal contribution extends beyond a mere synthesis of the existing landscape. We propose a novel conceptual framework that advocates for the deep integration of Zero Trust architectures [94] and Federated Learning [103] principles as the cornerstone for the next generation of endpoint defense. This study distinctively contributes to the literature by not only presenting this unique integrated framework but also by identifying and articulating a set of critical, previously under-detailed research challenges that arise from this synthesis. We posit that such integration is pivotal for addressing the nuanced complexities of modern threats, enhancing proactive defense while fundamentally upholding data privacy and ensuring systemic scalability [10]. By systematically identifying existing gaps and proposing this forward-looking model, this review charts a clear and actionable course for future research and development in this vital domain.

2. Historical Development of Endpoint Security

The evolution of endpoint security is a product of the continuous interaction between cyber threats and the defense mechanisms developed against them. This section examines the main stages of this evolution

2.1. Early Cybersecurity Challenges and Solutions

The emergence of malware in the 1980s led to the development of the first generation of antivirus tools [11, 12]. These initial threats were generally simple viruses and worms, and their propagation speed was low by today's standards [13]. The first antivirus programs were simple scanners focused on detecting known malware signatures (unique code sequences) [14]. During this period, with the proliferation of personal computers and increased network connectivity, new avenues for malware propagation emerged [15]. Early PC viruses like "Brain" and early network worms like the Morris Worm highlighted the vulnerability of digital assets and the need for specialized security software [16, 17]. These initial solutions were reactive; that is, they were effective only after a threat was identified and a signature was created [18].

2.2. Development of Antivirus Technologies

As cybercriminals adapted, antivirus systems evolved with heuristic and behavior-based detection methods [19, 20]. Signature-based detection was found to be ineffective against previously unseen (zero-day) malware [21]. Heuristic analysis attempted to detect unknown threats by looking for general characteristics or behavioral patterns of malware [22]. For example, a program attempting to

replicate itself or modify system files could be flagged as suspicious [23]. Behavior-based detection, on the other hand, works by monitoring a program's actions on the system (e.g., accessing specific registry keys, establishing network connections) and correlating these actions with malicious behaviors [24, 25]. During this period, additional security layers such as firewalls and intrusion detection systems (IDS) began to be integrated into antivirus software [26, 27]. The emergence of more complex malware, such as polymorphic and metamorphic viruses that constantly change their signatures, further increased the need for these more advanced detection techniques [28].

2.3. Transition to Advanced Endpoint Security

With the rise of Bring Your Own Device (BYOD) policies and complex threats like Advanced Persistent Threats (APTs), Endpoint Detection and Response (EDR) solutions introduced real-time detection and analytics capabilities [29, 30]. Traditional antivirus software was inadequate in detecting and responding to complex and targeted attacks like APTs [31]. APTs are typically carried out by sophisticated attacker groups that operate stealthily for extended periods to compromise a specific target [32]. BYOD, by allowing employees to use their personal devices on corporate networks, increased the number of uncontrolled and potentially insecure endpoints [33, 34]. EDR solutions responded to these challenges by continuously monitoring all activities on endpoints, detecting suspicious behaviors, and providing security analysts with tools to investigate and respond to threats [35, 36]. EDR went beyond merely blocking malware, focusing on understanding and intervening in the entire lifecycle of an attack [37].

3. Methodology

This study employs a systematic literature review (SLR) methodology, adhering to established guidelines [40, 41], to analyze the development, challenges, and future directions of endpoint security technologies. The SLR process involved several distinct phases:

3.1. Literature Collection and Search Strategy

Academic publications, white papers, cybersecurity vendor reports, and government frameworks (e.g., NIST [38], ENISA [39]) were systematically collected. The search was conducted across recognized digital libraries: IEEE Xplore, Scopus, ScienceDirect, and Google Scholar. The search strategy was designed to be comprehensive and reproducible. Search queries were constructed using Boolean operators (AND, OR) to combine core concepts and their synonyms. Core keywords included: "endpoint security", "antivirus", "Endpoint Detection and Response" (EDR), "Extended Detection and Response" (XDR), "Managed Detection and Response" (MDR), "Network Detection and Response" (NDR). These were combined with terms related to evolution ("evolution", "history", "development", "trends"), challenges ("challenges", "issues", "vulnerabilities", "limitations", "privacy"), and future technologies ("Zero Trust", "federated learning", "AI", "machine learning", "UBA", "IoT security"). For instance, a sample query for IEEE Xplore was: '(("endpoint security" OR "EDR" OR "XDR") AND ("evolution" OR "history" OR "trends") AND ("Zero Trust" OR "federated learning" OR "AI"))'. Similar logical structures, adapted to each database's syntax, were used. The literature search focused particularly on studies published between January 2014 and December 2024 to capture the most recent advancements and the current state of the field [40, 42].

3.2. Literature Selection Flow

The selection process for this systematic literature review was meticulously conducted following a multi-stage approach, adhering to the principles outlined in the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) statement [43]. A PRISMA flow diagram, illustrating the different phases of the information gathering and selection process, is presented in Figure 1. The key stages were as follows:

1. Identification: An initial search across the designated databases (IEEE Xplore, Scopus, ScienceDirect, and Google Scholar) using the defined search strings yielded a total of 3450 records. After automated removal of 250 duplicates by reference management software, 3200 records remained.

2. Screening: The titles and abstracts of these 3200 records were screened for relevance against the predefined inclusion and exclusion criteria. During this phase, 2850 records were excluded as they were clearly not aligned with the scope of endpoint security evolution, challenges, or future directions concerning Zero Trust and Federated Learning, or did not meet other primary criteria (e.g., language, document type). This left (350) articles for full-text assessment.
3. Eligibility: The full texts of the 350 potentially relevant articles were retrieved and thoroughly assessed for eligibility. At this stage, 179 articles were excluded for various reasons, including:
   - Lack of specific focus on endpoint security (n= 65).
   - Insufficient detail or methodological rigor (n=50).
   - Being outdated or superseded by more comprehensive works (n=31).
   - Inability to access the full text despite efforts (n=7).
   - Other reasons (e.g., focus solely on network security without endpoint implications) (n= 26).
4. Inclusion: After the eligibility assessment, a final set of [e.g., 171] studies met all inclusion criteria and were included in the qualitative synthesis of this systematic literature review.

The structured approach, as visualized in the PRISMA flow diagram (Figure 1), ensures transparency and replicability in the literature selection process for this review.

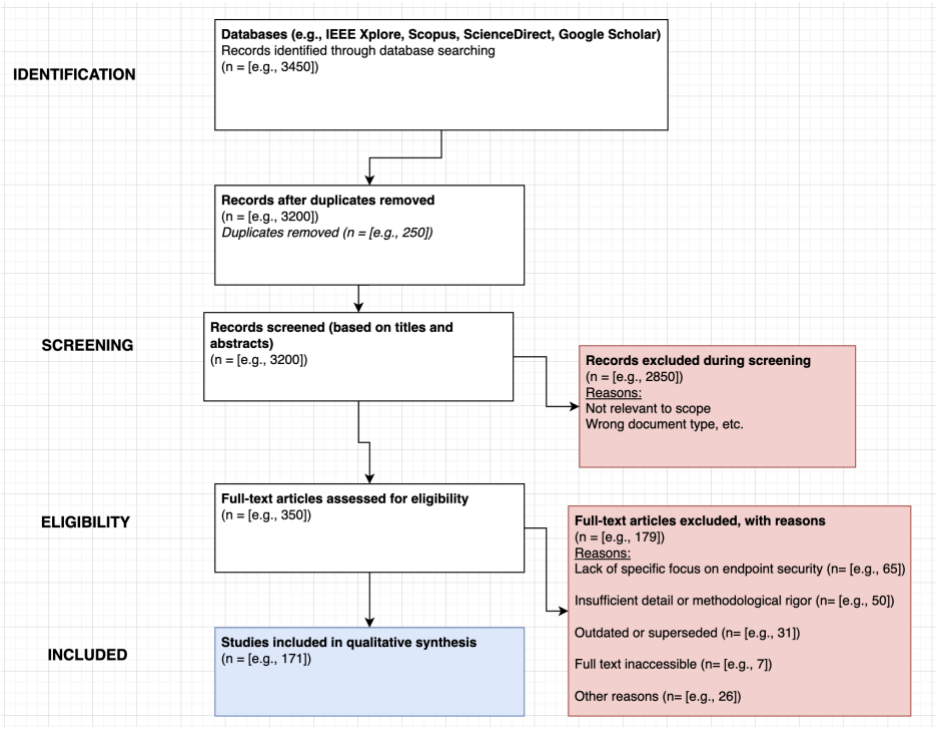

Figure 1. PRISMA Flow Diagram illustrating the study selection process

3.3. Data Extraction

Data was categorized using a chronological and thematic coding strategy. Key themes included: Technological Milestones, Architecture and Functionality of Endpoint Tools, Real-world Attack Trends (e.g., ransomware, APTs), Limitations and Bottlenecks, Emerging Trends (Zero Trust, Federated Learning, AI advancements). Information relevant to these themes was systematically extracted from each selected source and recorded in a data extraction form [44]. This process was cross-checked by multiple researchers to ensure consistency and reliability [45]. The extracted data were then synthesized to identify the evolutionary trajectory of endpoint security and the key challenges it faces [46].

3.3. Limitations of this Study

This review, while comprehensive, has certain limitations that should be acknowledged for a balanced interpretation of its findings:

- Focus on Publicly Available Literature: The review primarily relies on publicly accessible

academic papers, industry reports, and official documents. "Focusing on publicly available literature and not including private datasets or confidential security incident reports," [47] means that some cutting-edge, proprietary developments or highly sensitive incident details might not be captured. This could potentially limit the depth of analysis regarding the real-world efficacy of the very latest, non-publicly documented technologies or the full extent of certain attack vectors. Future Mitigation Strategy: Future research could aim to bridge this gap by "collaborating with industry players to gain controlled access to private datasets" or by conducting case studies within organizations, subject to non-disclosure agreements [140].

• Exclusion of Comparative Performance Benchmarks: Direct "inter-tool performance benchmarks" (e.g., specific EDR vendor A vs. EDR vendor B) are out of scope. The review focuses on technological concepts, evolution, and challenges rather than product-specific evaluations. This means the review does not offer guidance on which specific commercial tools perform best. Future Mitigation Strategy: Dedicated future studies could focus on "developing standardized testing environments and metrics for inter-tool performance comparisons," which would provide valuable data for practitioners [141].

• Qualitative Synthesis Dominance: While structured, the synthesis is predominantly qualitative. A quantitative meta-analysis of, for example, detection rates or false positive rates across different approaches was not feasible due to the heterogeneity of reported data in the source literature. This limits the ability to make statistically generalizable claims about the performance of classes of technologies. Future Mitigation Strategy: As more standardized reporting emerges in cybersecurity research, future SLRs might incorporate meta-analytic techniques for specific comparable metrics.

• Language Bias: The review was limited to English-language publications, potentially excluding relevant research published in other languages. Future Mitigation Strategy: Collaborative future reviews could involve multilingual teams to broaden the scope of included literature.

Awareness of these limitations is important for interpreting and generalizing the findings [47]. Nevertheless, the breadth of sources consulted provides a robust overview of the field [48].

4. Modern Endpoint Security Technologies

This section discusses modern endpoint security technologies such as EDR, XDR, MDR, and NDR, and how these technologies form a line of defense against cyber threats.

4.1. Endpoint Detection and Response (EDR)

EDR solutions are designed to provide comprehensive visibility, detect threats, and respond to them on endpoints (desktops, laptops, servers) [49]. The core capabilities of EDR are:

• Data Collection: Continuously records events on endpoints such as processes, network connections, file accesses, and user activities [50].

• Detection: Analyzes this data to identify anomalies, suspicious behaviors, and known indicators of compromise (IoCs). It often uses machine learning and behavioral analysis techniques [51, 52].

• Investigation: Provides security analysts with tools and context to understand the root cause and scope of an alert or incident [53].

• Response: Performs automated or manual actions to neutralize threats, such as terminating a process, isolating a device from the network, or quarantining a file [54].

EDR plays a significant role in detecting stealthy and complex attacks where traditional antiviruses fall short.

4.2. Extended Detection and Response (XDR)

XDR extends the capabilities of EDR beyond endpoints by integrating telemetry data from multiple security layers, such as network, cloud workloads, email, and identity [55, 56]. The goal of XDR is to eliminate visibility gaps created by siloed security tools and provide more holistic threat detection and response [57]. The key advantages of XDR are:

• Enhanced Visibility: Presents a more comprehensive picture by correlating different stages of the attack chain across multiple domains [58].

• Improved Detection: Enables more accurate and faster threat detection by combining weak signals from different sources [59].

• Simplified Operations: Offers security operations centers (SOCs) more efficient investigation and response capabilities through a single platform [60].

XDR typically brings together different security tools within a vendor-specific ecosystem or through open integrations [61].

4.3. Managed Detection and Response (MDR)

MDR offers outsourced expertise and services to help organizations effectively use technologies like EDR and XDR [62]. Many organizations lack the necessary skills and resources to manage advanced security tools and provide 24/7 threat monitoring and response [63]. MDR providers offer:

• 24/7 Monitoring and Threat Hunting: Expert analysts continuously monitor customer environments and proactively hunt for threats [64].

• Alert Prioritization and Analysis: Reduces false positives and ensures focus on real threats [65].

• Guided Response and Remediation: Provides expert advice and support to contain and eliminate threats [66].

MDR is a valuable solution, especially for small and medium-sized enterprises (SMEs) lacking cybersecurity expertise [67].

4.4. Network Detection and Response (NDR)

NDR solutions focus on detecting malicious activities and anomalies by analyzing network traffic [68]. It provides a complementary layer of visibility for situations where endpoint-based solutions (like EDR) may be blind or bypassed [69]. The core functions of NDR are:

• Network Traffic Analysis (NTA): Deeply inspects network packets, extracts metadata, and identifies suspicious patterns using machine learning and behavioral analysis [70, 71].

• Encrypted Traffic Analysis (ETA): May use advanced techniques to detect threats in encrypted traffic without decrypting the data [72].

• Lateral Movement Detection: Effective in detecting instances where an attacker attempts to spread within the network [73].

NDR is particularly important in networks with unmanaged devices or devices where EDR agents cannot be installed, such as IoT and operational technology (OT) environments. Comparative Architecture of Modern Endpoint Security Technologies is shown in Figure 2. And the evolution of technologies is shown in Table 1.

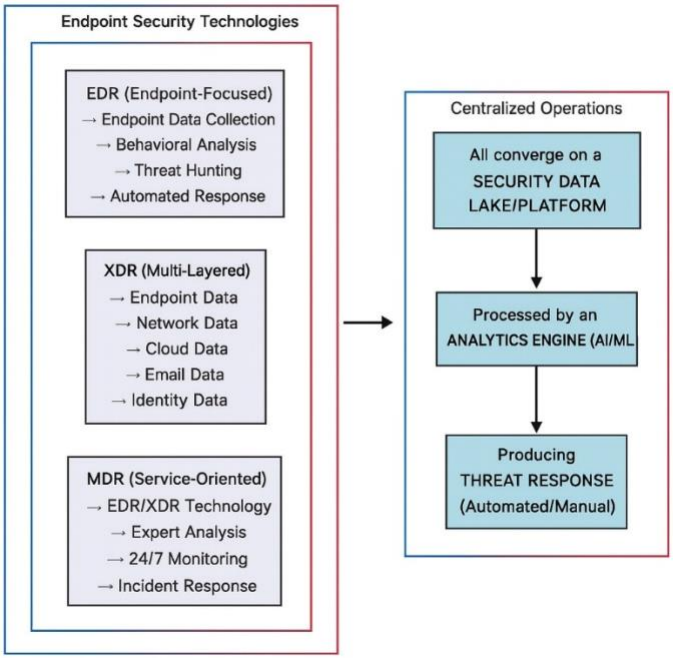

Figure 2. Comparative Architecture of Modern Endpoint Security Technologies (Conceptual Diagram)

Table 1. Evolutionary Timeline of Endpoint Security Technologies

Period	Key Threats	Prominent Technologies	Key Features
1980s	Simple viruses, worms	First-generation antivirus (signature-based)	Scanning for known malware signatures
1990s	Polymorphic/metamorphic viruses, macro viruses	Heuristic analysis, behavior-based detection (basic)	Suspicious code characteristics, basic behavior patterns
2000s	Botnets, spyware, rootkits	Antivirus suites (firewall, IDS integration)	Comprehensive protection, basic network traffic monitoring
2010s	APTs, zero-day exploits, ransomware	Endpoint Detection and Response (EDR)	Continuous monitoring, real-time analytics, threat hunting, incident response
2020s	RaaS, IoT attacks, supply chain attacks	Extended Detection and Response (XDR), Managed Detection and Response (MDR), Network Detection and Response (NDR), AI/Machine Learning integration, Emergence of Zero Trust concepts, Early exploration of Federated Learning for security	Multi-layered visibility (endpoint, network, cloud), automated response, threat intelligence, principle of least privilege, privacy-preserving model training discussions

5. Present Obstacles in Endpoint Security

Despite advancements, challenges such as IoT security, regulatory compliance, and interoperability persist. These obstacles complicate the implementation and maintenance of effective endpoint security strategies.

5.1. Internet of Things (IoT) Vulnerabilities

The rapid proliferation of IoT devices (smart home appliances, industrial sensors, medical devices, etc.) creates new and significant security risks [74, 75]. These devices often:

- Have Limited Resources: They are constrained in terms of processing power, memory, and energy, making it difficult to run complex security software [76].
- Are Designed Without Security in Mind: Many IoT devices are released to the market without basic security features (e.g., strong passwords, regular patch management) [77].
- Are Difficult to Manage: Monitoring, updating, and securing a large number of dispersed IoT devices is complex [78].

These vulnerabilities make IoT devices easy targets for botnets and allow them to be used as entry points to infiltrate broader networks [79, 80]. Attacks like the Mirai botnet have demonstrated the significant threat posed by vulnerable IoT devices [81].

5.2. Data Privacy and Regulatory Compliance

Endpoint security solutions collect and process large amounts of data to detect and analyze threats [82]. This raises significant concerns related to the General Data Protection Regulation (GDPR) [83], the California Consumer Privacy Act (CCPA) [84], and other local data privacy regulations. Organizations must:

- Be Transparent in Data Collection and Use: They must inform users about what data is collected and how it is used [85].
- Adhere to the Principle of Data Minimization: They should only collect data that is strictly necessary for security purposes [86].
- Store and Process Data Securely: They must take appropriate technical and organizational measures against unauthorized access and data breaches [87].

Complying with these regulations can be complex and costly, especially for globally operating organizations [88]. Non-compliance can lead to hefty fines and reputational damage.

5.3. Implementation Complexity and Device Interoperability

Implementing and managing modern endpoint security solutions (especially comprehensive platforms like XDR) can be complex. Organizations may face challenges with integration into existing infrastructures, interoperability of tools from different vendors, and training of security personnel [89].

- Integration Challenges: Achieving seamless data flow and coordination between different

security tools and systems can be technically challenging [90].

• Vendor Lock-in: Some XDR solutions may perform best when working with products from a single vendor, potentially locking organizations into a specific ecosystem [91].

• Skills Gap: Effectively using advanced security tools and analyzing threat data requires personnel with specialized cybersecurity skills, but the number of professionals with these skills is limited [92, 93].

Compatibility with different operating systems, device types, and legacy systems also remains a significant interoperability issue.

6. Emerging Trends and Future Directions

Technological trends such as Zero Trust, federated learning, deeper AI integration, and user-centric security are redefining endpoint protection. These approaches promise more proactive, adaptive, and resilient security strategies.

6.1. Zero Trust Architectures

Zero Trust is a security model based on the principle of "never trust, always verify" [94, 95]. Unlike traditional perimeter-based security (where everything inside is trusted), Zero Trust does not inherently trust any user or device, regardless of whether they are inside or outside the network [96]. Every access request is strictly verified and authorized based on identity, device security posture, location, and other contextual factors [97]. In the context of endpoint security, Zero Trust includes:

• Micro-segmentation: Dividing the network into smaller, isolated segments to limit lateral movement [98].

• Strong Identity and Access Management (IAM): Robustly authenticating user and device identities using multi-factor authentication (MFA) and continuous authorization [99].

• Continuous Endpoint Compliance and Health Checking: Dynamically assessing if devices comply with security policies (e.g., up-to-date antivirus, OS patches, no known vulnerabilities) before and during access [100].

• Least Privilege Access: Granting users and applications only the minimum necessary permissions to perform their tasks.

Zero Trust provides a stronger defense against insider threats, compromised credentials, and sophisticated attacks that bypass traditional perimeters [101, 102]. Open Research Questions for Zero Trust in Endpoint Security:

RQZ1: How can dynamic and context-aware Zero Trust policies be efficiently enforced across heterogeneous and resource-constrained endpoint devices (especially IoT) without significantly impacting performance or user experience? [142]

RQZ2: What are effective and scalable mechanisms for continuous authentication and trust assessment of autonomous endpoint agents and services within a Zero Trust framework? [143]

6.2. Federated Learning for Enhanced Privacy and Collaboration

Federated learning (FL) is a machine learning technique that allows models to be trained collaboratively on decentralized data sources (e.g., directly on endpoints or local enterprise servers) without exchanging raw data [103, 104]. Only model updates (e.g., gradients or parameters) are typically shared with a central aggregator, thus enhancing data privacy [105]. Potential benefits of FL in endpoint security include:

• Privacy Preservation: Sensitive endpoint data (e.g., user behavior, application telemetry) remains on the device or within the organization's perimeter, reducing privacy risks and facilitating compliance with regulations like GDPR [106].

• Improved Model Robustness and Personalization: Models can be trained on diverse, real-world data from multiple organizations or user groups, potentially leading to more robust and generalizable threat detection. Local models can also be personalized to specific user or device contexts [107].

• Reduced Communication Overhead: Transmitting model updates instead of large raw datasets can be more efficient, especially for bandwidth-constrained endpoints [108].

• Collaborative Threat Intelligence: Enables organizations to collaboratively build better threat

detection models without directly sharing potentially sensitive threat intelligence data [109, 110].
FL is promising for building more effective global defense strategies against rapidly evolving threats while respecting data sovereignty and privacy. Open Research Questions for Federated Learning in Endpoint Security:

RQF1: How can FL systems in endpoint security be made robust against various adversarial attacks, such as data poisoning, model poisoning, and inference attacks, especially when dealing with non-IID (Independent and Identically Distributed) data from heterogeneous endpoints? [144]
RQF2: What are effective incentive mechanisms and contribution evaluation frameworks to encourage participation and ensure fairness among different entities contributing to a federated endpoint security model, while also addressing potential free-riding or malicious contributions? [145]

6.3. Deepening Role of Artificial Intelligence (AI) and Machine Learning (ML)

Artificial intelligence and machine learning have become cornerstones of modern endpoint security, and their role will continue to deepen and become more sophisticated [111, 112]. These technologies provide:

- Advanced Threat Detection: Enhanced ability to detect unknown (zero-day) and complex malware, polymorphic attacks, fileless malware, behavioral anomalies, and APT tactics [113, 114].
- Automated and Orchestrated Response: Enabling faster, more consistent, and potentially autonomous responses to threats across multiple security layers (endpoints, network, cloud) [115].
- Proactive Threat Hunting Automation: AI can assist human analysts or autonomously identify suspicious patterns, weak signals, and potential emerging threats in vast datasets [116].
- Predictive Security Analytics: Moving beyond detection to predict future attack vectors, potential targets, and the likelihood of compromise based on historical data and current threat intelligence [117].
- Explainable AI (XAI): As AI models become more complex, XAI techniques are crucial for providing transparency and interpretability into why a detection or decision was made. This builds trust and allows analysts to validate and fine-tune AI-driven security systems [118, 119].

Future AI/ML applications may include AI-driven decoy generation, automated vulnerability assessment, and AI-assisted reverse engineering of malware. Open Research Questions for AI/ML in Endpoint Security:
RQA1: How can adversarial AI techniques (e.g., evasion attacks, model extraction) targeting endpoint security ML models be effectively and adaptively defended against in real-world deployments? [146]
RQA2: What XAI methods are most effective in providing actionable and comprehensible explanations for complex AI-driven endpoint threat detections to security analysts with varying levels of expertise, and how can these explanations be integrated into SOC workflows? [147]

6.4. User and Entity Behavior Analytics (UEBA)

UEBA focuses on monitoring and analyzing user and entity (e.g., hosts, applications, services) activities to detect insider threats, compromised accounts, and anomalous behaviors indicative of an attack [120]. UEBA systems establish a normal behavior baseline for each user and entity and flag statistically significant deviations as potential threats [121]. When integrated with endpoint security telemetry, UEBA can detect:

- Anomalous Access Patterns: Unauthorized access attempts, logins at unusual times or from atypical geolocations, or access to unusual resources [122].
- Data Exfiltration Indicators: Anomalous access to sensitive data, unusual data movement, or attempts to transfer large volumes of data outside the organization [123].
- Account Compromise or Insider Misuse: Actions significantly different from a user's or entity's established normal behavior patterns, potentially indicating credential theft or malicious insider activity [124].
- Lateral Movement Indicators: A user account performing actions usually associated with system administrators or accessing an unusual number of endpoints.

UEBA adds a critical defense layer by focusing on behavioral indicators, which can detect threats that evade signature-based or rule-based defenses [125]. Open Research Questions for UEBA in Endpoint Security:
RQU1: How can UEBA systems effectively differentiate between genuinely malicious anomalous

behavior and benign behavioral drift or legitimate but unusual activities, thereby minimizing false positives and analyst fatigue in dynamic endpoint environments? [148]
RQU2: What are privacy-preserving techniques for collecting and analyzing granular user and entity behavior data for UEBA purposes, especially in the context of remote work and BYOD scenarios, while still maintaining detection efficacy? [149]

7. Discussion

The evolution of endpoint security, as traced in this review, unequivocally demonstrates a reactive-to-proactive paradigm shift, moving from signature-matching to intelligent, context-aware defense mechanisms [126, 127]. The progression from AV to EDR, XDR, and NDR, augmented by AI/ML, addresses the escalating sophistication of cyber threats [128]. However, this technological arms race introduces its own complex challenges, demanding more than just incremental improvements.

7.1. Inter-Technology Dynamics: Synergies and Conflicts

The modern endpoint security landscape is increasingly characterized by the interplay of multiple advanced technologies, such as EDR, XDR, and NDR, alongside emerging paradigms like Zero Trust (ZT) and Federated Learning (FL).

- Synergies: XDR, by its nature, aims to create synergy by correlating data from EDR (endpoint), NDR (network), cloud security, and identity systems [57]. Integrating ZT principles can further enhance XDR by providing dynamic access controls based on continuously verified trust levels from these correlated signals [150]. FL can then be used to train the AI/ML models that power XDR and ZT decision engines using diverse, privacy-preserved datasets from multiple deployments, leading to more robust and adaptive threat detection [151].
- Integration Challenges and Performance Conflicts: While synergistic in theory, integrating these diverse systems presents significant practical hurdles. For example, ensuring seamless telemetry data exchange between an EDR from vendor A, an NDR from vendor B, and a ZT framework from vendor C can be hampered by proprietary data formats and APIs [89]. Performance conflicts may arise; for instance, intensive AI processing for NDR coupled with continuous endpoint monitoring for EDR and ZT policy enforcement might strain network and endpoint resources, especially in large-scale or resource-constrained IoT environments [152].
- Managerial Complexity: Managing this complex ecosystem of interconnected tools requires highly skilled personnel and mature security operations processes. The "single pane of glass" promised by XDR can become a "single point of confusion" if not implemented and managed correctly [132]. Defining and maintaining granular ZT policies across a dynamic environment also adds significant administrative overhead.

7.2. Addressing Key Challenges: IoT, Data Privacy, and Proposed Solutions

IoT Vulnerabilities: The explosion of insecure IoT devices remains a critical weak link [129]. Traditional EDR agents are often too resource-intensive for these devices. Original Solution Proposal/Conceptual Model: We propose a lightweight, FL-based anomaly detection framework for IoT endpoint clusters. Local models on gateway devices or edge servers could be trained using FL with minimal data from IoT endpoints, focusing on deviations in network traffic patterns or essential process behaviors. A ZT approach would then enforce strict micro-segmentation and least privilege access for these devices based on anomaly scores from the FL model [153] . Research Questions Stemming from Proposal:

RQI1: How can FL model aggregation be optimized for highly heterogeneous IoT environments with varying data quality and availability?
RQI2: What are the minimal yet effective sets of features that can be extracted from resource-constrained IoT devices for FL-based anomaly detection without compromising device performance?

Data Privacy in an Era of Pervasive Monitoring: The intensive data collection by EDR/XDR systems clashes with increasingly stringent data privacy regulations like GDPR [131]. Original Solution Proposal/Conceptual Model: Beyond FL, integrating advanced privacy-enhancing technologies (PETs) such as homomorphic encryption or secure multi-party computation for specific analytics tasks within an XDR framework could allow for threat correlation without exposing raw sensitive data [153]. For instance, correlating login anomalies (from IAM) with endpoint process behavior (from EDR) could

occur in an encrypted domain. Research Questions Stemming from Proposal:

RQP1: What is the computational overhead and practical feasibility of applying PETs like homomorphic encryption for real-time threat analytics in XDR systems?
RQP2: How can organizations effectively demonstrate GDPR compliance (e.g., data minimization, purpose limitation) when using complex AI/ML models that are often "black boxes" for endpoint threat detection?

7.3. Ethical Considerations in AI-Driven Endpoint Security

The increasing reliance on AI and FL in endpoint security introduces significant ethical considerations:

- Bias and Fairness: AI models trained on historical data may inherit biases present in that data, leading to discriminatory outcomes or disproportionate false positives for certain user groups or device types [154]. In FL, if certain participants contribute biased data, it could skew the global model. Potential Solution Strategy: Implementing fairness-aware machine learning algorithms, regular bias audits of models, and ensuring diverse and representative training datasets (even in FL contexts) are crucial [155].
- Transparency and Explainability (XAI): The "black box" nature of many advanced AI models makes it difficult to understand why a particular decision (e.g., blocking a process, isolating a device) was made [119]. This lack of transparency can erode trust and hinder effective incident response. Potential Solution Strategy: Investing in and integrating XAI techniques that can provide human-understandable explanations for AI decisions is vital. This includes local and global explanations of model behavior [118].
- Model Manipulation and Security of AI: AI models themselves can be targets. Adversarial attacks can cause misclassification (evasion), and model poisoning in FL can corrupt the global model [156]. Potential Solution Strategy: Developing robust defenses against adversarial attacks, secure aggregation protocols in FL, and continuous monitoring of model integrity are necessary research areas.
- Accountability and Responsibility: When an AI-driven system makes an error (e.g., a false positive leading to system outage, or a false negative leading to a breach), determining accountability can be complex. Potential Solution Strategy: Clear governance frameworks for the development, deployment, and oversight of AI in security are needed, defining roles and responsibilities.

Addressing these ethical challenges is paramount for the responsible and sustainable adoption of AI in endpoint security.

Looking ahead, trends such as Zero Trust architectures, federated learning, and deeper integration of AI are promising [135]. However, their successful realization also entails its own challenges. Full implementation of Zero Trust requires a cultural shift, significant architectural redesign, and meticulous planning [136]. Federated learning, while privacy-enhancing, may be vulnerable to new attack vectors like sophisticated model poisoning or inference attacks if not carefully designed, and could face scalability and incentive issues in large, heterogeneous networks [137]. The quest for true XAI that balances explainability with model performance remains an active research area [119].
The overarching theme is that endpoint security will remain a continuous cat-and-mouse game. As threat actors innovate, so too must defense mechanisms. Future success will depend not only on technological innovations but also on strategic planning, development of skilled personnel, establishment of robust processes, and achieving an optimal balance between security, usability, and privacy [138]. Global collaboration, standardized threat intelligence sharing, and public-private partnerships are also vital for an effective collective defense in an increasingly interconnected and complex digital world [139].

8. Conclusion

This systematic review has provided a comprehensive and longitudinal analysis of the evolution of endpoint security, meticulously tracing its transformative journey from the foundational principles of signature-based antivirus to the sophisticated, AI-driven architectures of modern Endpoint Detection and Response (EDR), Extended Detection and Response (XDR), Managed Detection and Response (MDR), and Network Detection and Response (NDR) solutions. Our analysis has illuminated the historical progression of defense mechanisms in response to an ever-advancing threat landscape, critically evaluated the capabilities and inherent limitations of contemporary technologies and

underscored the persistent challenges that continue to confront the field, namely the vulnerabilities of IoT ecosystems, the complexities of data privacy compliance, and the significant hurdles of implementation and interoperability. A key finding of this work is that while endpoint security has successfully adapted to the dynamic nature of cyber threats, each successive generation of solutions paradoxically introduces its own set of operational burdens and strategic limitations.

The primary and most significant contribution of this study is the formulation and proposal of an integrated conceptual framework designed to guide the next paradigm of endpoint defense. This framework is architected upon the synergistic integration of Zero Trust principles and Federated Learning methodologies. By systematically identifying and articulating a detailed set of open research questions pertinent to the successful implementation of Zero Trust, Federated Learning, advanced AI/ML, and UEBA, this paper moves beyond description to establish a concrete agenda for future scientific inquiry. Our analysis underscores a powerful synergy: Zero Trust provides the stringent, "never trust, always verify" policy framework for access control, while Federated Learning offers the privacy-preserving, collaborative machine learning mechanism needed to train the intelligent models that can enforce these policies dynamically and effectively. This combination is poised to foster more scalable, adaptive, and resilient defense postures that are designed with privacy at their core.

Furthermore, this review provides a forward-looking perspective by discussing the intricate interactions, potential benefits, and inherent risks associated with these future trends. We have highlighted how Zero Trust policies can be dynamically informed by AI models trained via Federated Learning, creating a proactive security posture that would otherwise be unattainable. Simultaneously, we have acknowledged the significant integration complexities, the emergence of new adversarial attack vectors against the learning models themselves, and the profound ethical dilemmas surrounding bias, fairness, and transparency in AI-driven security.

Ultimately, navigating the future of endpoint security demands more than just technological innovation; it requires a holistic strategy that addresses these technical hurdles, confronts the ethical and privacy considerations head-on, and fosters a culture of continuous adaptation within the cybersecurity community. Endpoint security will undoubtedly remain the critical frontline in the defense of our digital assets. Therefore, sustained, focused, and collaborative research and development efforts, particularly within the open research areas identified herein, are not merely recommended; they are imperative for realizing a more secure, resilient, and trustworthy digital future.

Conflict of Interest Statement

No conflict of interest was declared by the authors.

References

1. Amtra Solutions, "The evolving landscape of endpoint security" *Blog*, Amtra Solutions Jan 29, 2024. [Online]. Available: https://www.amtrasolutions.com/blog/the-evolving-landscape-of-endpoint-security-in-2024-a-comprehensive-guide.

2. A. B., "The Evolution of Endpoint Security in the Age of Cyber Warfare," *Cybersecurity Insights Blog*, U.S. Cybersecurity Institute, 19, Sep, 2024. [Online]. Available: https://www.uscsinstitute.org/cybersecurity-insights/blog/the-evolution-of-endpoint-security-in-the-age-of-cyber-warfare.

3. European Union Agency for Cybersecurity (ENISA), "ENISA Threat Landscape 2022," *Publications*, European Union Agency for Cybersecurity, Nov. 3, 2022. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022.

4. Robert Short, "The Evolution of Endpoint Security: From Basics to Advanced Protection," *Blog*, Liquid Networx, Nov. 11, 2023. [Online]. Available: https://www.liquidnetworx.com/the-evolution-of-endpoint-security-from-basics-to-advanced-protection/.
5. Microsoft, "What Is the Difference Between EDR and XDR?," Microsoft Security. [Online]. Available: https://www.microsoft.com/en-gb/security/business/security-101/edr-vs-xdr.

6. Verizon, "2023 Data Breach Investigations Report," Verizon, Public Sector Snapshot, 2023. [Online]. Available: https://www.verizon.com/business/resources/Ta5a/reports/2023-dbir-public-sector-snapshot.pdf.

7. IBM, "Cost of a Data Breach Report 2023," *IBM Reports*, IBM Security, 2023. [Online]. Available: https://www.ibm.com/reports/data-breach.

8. SentinelOne, "What is Next Generation Endpoint Security?," *Cybersecurity 101*, SentinelOne, Jun. 3, 2025. [Online]. Available:https://www.sentinelone.com/cybersecurity-101/endpoint-security/next-generation-endpoint-security/.

9. Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J. A., Invernizzi, L., Kallitsis, M., Kumar, D., Lever, C., Ma, Z., Mason, J., Menscher, D., Seaman, C., Sullivan, N., Thomas, K., & Zhou, Y. Understanding the mirai botnet. (2017), *USENIX Security Symposium*, 1093–1110. Available:https://elie.net/static/files/understanding-the-mirai-botnet/understanding-the-mirai-botnet-paper.pdf

10. Salah, K., Rehman, M. H. U., Nizamuddin, N., & Al-Fuqaha, A. (2019). Blockchain for AI: Review and open research challenges. *IEEE Access*, *7*, 10127–10149. Available: https://doi.org/10.1109/access.2018.2890507

11. Fred Cohen. Computer viruses—theory and experiments. In *Van Nostrand Reinhold Co. eBooks,(1985)* (pp. 356–378). Available: https://all.net/books/DissertationOCR.pdf

12. Spafford, E. H. The internet worm program: an analysis. *ACM SIGCOMM Computer Communication Review*, (1989), *19*(1), 17–57. https://doi.org/10.1145/66093.66095

13. David Harley,Urs E. Gattiker,Robert Slade. *Viruses Revealed*. (2001) McGraw-Hill. Available:https://dl.acm.org/doi/abs/10.5555/559413

14. Szor, P. The art of computer virus research and defense. *Choice Reviews Online*, (2005), *43*(03), 43–1613. Available:https://www.informit.com/store/art-of-computer-virus-research-and-defense-9780321304544

15. Denning, D. An Intrusion-Detection model. (1987), *IEEE Transactions on Software Engineering*, *SE-13*(2), 222–232. Available:https://doi.org/10.1109/tse.1987.232894

16. S Solomon, A. (1991). PC viruses. In *Springer eBooks*. https://doi.org/10.1007/978-1-4471-1031-6

17. Rochlis, J. A., & Eichin, M. W. With microscope and tweezers: the worm from MIT's perspective. (1989) *Communications of the ACM*, *32*(6), 689–698. Available:https://doi.org/10.1145/63526.63528

18. Kephart, J. O., Sorkin, G. B., Arnold, W. C., Chess, D. M., Tesauro, G. J., & White, S. R. Biologically inspired defenses against computer viruses. (1995), *International Joint Conference on Artificial Intelligence*, 985–996. Available: http://ijcai.org/Proceedings/95-1/Papers/127.pdf

19. Nachenberg, C. Computer virus-antivirus coevolution. (1997), *Communications of the ACM*, *40*(1), 46–51. Available: https://doi.org/10.1145/242857.242869

20. Tesauro, G., Kephart, J., & Sorkin, G. Neural networks for computer virus recognition. (1996), *IEEE Expert*, *11*(4), 5–6. Available:https://doi.org/10.1109/64.511768

21. Wagener, G., State, R., & Dulaunoy, A. Malware behaviour analysis. (2007), *Journal in Computer Virology*, *4*(4), 279–287. Available: https://doi.org/10.1007/s11416-007-0074-9

22. Forrest, S., Hofmeyr, S. A., Somayaji, A., & Longstaff, T. A. (1996). A sense of self for unix processes. *Proceedings 1996 IEEE Symposium on Security and Privacy*, 120–128. Available: DOI: 10.1109/SECPRI.1996.502675

23. Christodorescu, M., & Jha, S. Static analysis of executables to detect malicious patterns. (2003), In *Proceedings of the 12th USENIX Security Symposium* (Vol. 12, pp. 12-12). Available: https://www.usenix.org/legacy/events/sec03/tech/full_papers/christodorescu/christodorescu.pdf

24. Kirda, E., Kruegel, C., Banks, G., Vigna, G., & Kemmerer, R. A. Behavior-based spyware detection. (2006), *USENIX Security Symposium*, 19. Available:http://auto.tuwien.ac.at/~chris/research/doc/usenix06_spyware.pdf

25. Bayer, U., Moser, A., Kruegel, C., & Kirda, E. Dynamic analysis of malicious code. (2006), *Journal in Computer Virology*, *2*(1), 67–77. Available: https://doi.org/10.1007/s11416-006-0012-2

26. Bellovin, S., & Cheswick, W. Network firewalls. (1994), *IEEE Communications Magazine*, *32*(9), 50–57. https://doi.org/10.1109/35.312843

27. Rui, Z. A survey of intrusion detection systems. (2002), *Department of Computer Science, University of California, San Diego*. https://cseweb.ucsd.edu/classes/fa01/cse221/projects/group10.pdf

28. You, I., & Yim, K. Malware Obfuscation Techniques: A Brief Survey. *2010 International Conference on Broadband, Wireless Computing, Communication and Applications*, 297–300. https://doi.org/10.1109/bwcca.2010.85

29. J. Zelonis, "The Evolution Of Enterprise Detection And Response," *Blogs*, Forrester, Feb. 5, 2020. [Online]. Available: https://www.forrester.com/blogs/the-evolution-of-enterprise-detection-response/.

30. Mandiant, "APT 1: Exposing One of China's Cyber Espionage Units," *National Security Archive*, The George Washington University, Feb. 2013. [Online]. Available: https://nsarchive.gwu.edu/document/21484-document-83.

31. Gartner, "Market Guide for Endpoint Detection and Response Solutions," Gartner, 2018. [Online]. Available: https://www.gartner.com/en/documents/3894086.

32. E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-driven computer network defense informed by analysis of

adversary campaigns and intrusion kill chains," in *Leading Issues in Information Warfare and Security Research, vol. 1*, D. Remenyi, Ed. Reading, UK: Academic Publishing International, 2011, pp. 80-99. [Online]. Available: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf.

33. Mylonas, A., Kastania, A., & Gritzalis, D. . Delegate the smartphone user? Security awareness in smartphone platforms. *Computers & Security*,(2012), *34*, 47–66. Available: https://doi.org/10.1016/j.cose.2012.11.004

34. P. A. and S. L. Lahudkar, "Bring Your Own Device (BYOD): Security Risks and Mitigating Strategies," *Research and Reviews: Journal of Engineering and Technology,* 4, April 2013. [Online]. Available: https://www.rroij.com/open-access/bring-your-own-device-byod-security-risks-and-mitigating-strategies.php?aid=38224.

35. Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet*. Academic press.
36. Chuvakin, A., Schmidt, K., & Phillips, C. (2013). *Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management*. Syngress.

37. T. D. Garvey and T. F. Lunt, "Model Based Intrusion Detection," in *Proc. of the 14th National Computer Security Conference*, Oct. 1-4, 1991, Baltimore, MD, USA, 1991, pp. 372-385. [Online]. Available:https://www.researchgate.net/publication/275641502_Model-Based_Intrusion_Detection.

38. *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. (2018). https://doi.org/10.6028/nist.cswp.04162018

39. European Union Agency for Cybersecurity (ENISA), "ENISA Threat Landscape 2020," *ENISA News*, European Union Agency for Cybersecurity, Oct. 20, 2020. [Online]. Available: https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020.
40. B. Kitchenham and S. Charters, "Guidelines for performing Systematic Literature reviews in Software Engineering," Keele University, Keele, UK, Tech. Rep. EBSE-2007-01, 2007. [Online]. Available: https://www.researchgate.net/profile/Barbara-Kitchenham/publication/302924724_Guidelines_for_performing_Systematic_Literature_Reviews_in_Software_Engineering/links/61712932766c4a211c03a6f7/Guidelines-for-performing-Systematic-Literature-Reviews-in-Software-Engineering.pdf.

41. Kitchenham, B., Pretorius, R., Budgen, D., Brereton, O. P., Turner, M., Niazi, M., & Linkman, S. (2010). Systematic literature reviews in software engineering – A tertiary study. *Information and Software Technology*, *52*(8), 792–805. Available: https://doi.org/10.1016/j.infsof.2010.03.006

42. Xiao, Y., & Watson, M. (2017). Guidance on conducting a systematic literature review. *Journal of Planning Education and Research*, *39*(1), 93–112. Available: https://doi.org/10.1177/0739456x17723971

43. Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. G. (2009). Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. *BMJ*, *339*(jul21 1), b2535. https://doi.org/10.1136/bmj.b2535

44.] J. Webster and R. T. Watson, "Analyzing the Past to Prepare for the Future: Writing a Literature Review," *MIS Quarterly*, vol. 26, no. 2, pp. xiii-xxiii, Jun. 2002. [Online]. Available: https://www.jstor.org/stable/4132319.
45. A. Fink, *Conducting Research Literature Reviews: From the Internet to Paper*, 5th ed. Los Angeles, CA: SAGE Publications, 2020. [Online]. Available: https://books.google.com.tr/books/about/Conducting_Research_Literature_Reviews.html?id=2bKI6405TXwC&redir_esc=y.
46. Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a methodology for developing Evidence-Informed management knowledge by means of systematic review. *British Journal of Management*, *14*(3), 207–222. Available: https://doi.org/10.1111/1467-8551.00375
47. Shull, F., Carver, J., & Travassos, G. H. (2001). An empirical methodology for introducing software processes. *ACM Digital Library*, 288–296. Available: https://doi.org/10.1145/503209.503248
48. Wohlin, C. (2014). Guidelines for snowballing in systematic literature studies and a replication in software engineering. *EASE '14: Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering*, 1–10. Available: https://doi.org/10.1145/2601248.2601268
49. ThreatLocker, "The evolution of endpoint security," *Blog*, ThreatLocker, Sept. 29, 2023. [Online]. Available: https://www.threatlocker.com/blog/the-evolution-of-endpoint-security.
50. R. Bejtlich, *The Practice of Network Security Monitoring: Understanding Incident Detection and Response*. San Francisco, CA: No Starch Press, 2013. [Online]. Available: https://books.google.com.tr/books?id=QdLclhJhQecC.
51. Gaurav, A., Gupta, B. B., & Panigrahi, P. K. (2022). A comprehensive survey on machine learning approaches for malware detection in IoT-based enterprise information system. *Enterprise Information Systems*, *17*(3). Available: https://doi.org/10.1080/17517575.2021.2023764
52. Microsoft, "Behavioral blocking and containment," *Microsoft Learn*, Microsoft. [Online]. Available: https://learn.microsoft.com/en-us/defender-endpoint/behavioral-blocking-containment.
53. A. Aarness, "What is Endpoint Detection and Response (EDR)?," *Cybersecurity 101*, CrowdStrike, Jan. 7, 2025. [Online]. Available: https://www.crowdstrike.com/en-us/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/.
54. Tanium Staff, "Endpoint Detection and Response 101: What EDR Is and Where It Falls Short," *Blog*, Tanium, Sept. 29, 2021. [Online]. Available: https://www.tanium.com/blog/endpoint-detection-and-response-what-edr-is/.
55. K. Guercio, "XDR Software Emerges as a Key Next-Generation Security Tool," *eSecurity Planet*, Dec. 4, 2020. [Online]. Available: https://www.esecurityplanet.com/threats/xdr-emerges-as-a-key-next-generation-security-tool/.
56. K. Cross, "The Journey to Extended Detection and Response - XDR," *Blog*, Palo Alto Networks, Dec. 10, 2021. [Online].

Available: https://www.paloaltonetworks.com/blog/2021/12/the-journey-to-xdr-technology/.
57. Gartner, "Innovation Insight for Extended Detection and Response," Gartner, 2021. [Online]. Available: https://www.gartner.com/en/documents/3982247.
58. Cisco, "Cisco XDR: At-a-Glance," *Cisco*, 2024. [Online]. Available: https://www.cisco.com/c/en/us/products/collateral/security/xdr/xdr-aag.html
59. McAfee, "McAfee Introduces MVISION XDR, the Industry-First Proactive, Data-Aware and Open Extended Detection and Response Platform," *Newsroom*, McAfee, Oct. 29, 2020. [Online]. Available: https://www.mcafee.com/ru-ru/consumer-corporate/newsroom/press-releases/press-release.html?news_id=e0959323-6ec9-46bc-b52d-ce7f1d801767.
60. Secureworks, "What is XDR (Extended Detection and Response)?," *Resource Center*, Secureworks. [Online]. Available: https://www.secureworks.com/centers/what-is-xdr.
61. Trend Micro, "One Platform - Trend Vision One," *Products*, Trend Micro. [Online]. Available: https://www.trendmicro.com/en_us/business/products/one-platform.html.
62. silindi
63. Rapid7, "What is Managed Detection and Response (MDR)?," *Fundamentals*, Rapid7. [Online]. Available: https://www.rapid7.com/fundamentals/what-is-managed-detection-and-response-mdr/.
64. Sophos, "Sophos Managed Threat Response (MTR)," *Products*, Sophos. [Online]. Available: https://www.sophos.com/en-us/products/managed-threat-response.
65. Arctic Wolf, "Managed Detection and Response," *Solutions*, Arctic Wolf. [Online]. Available: https://arcticwolf.com/solutions/managed-detection-and-response/.
66. SentinelOne, "MSSP vs MDR: Which One to Choose?," *Cybersecurity 101*, SentinelOne, May 10, 2025. [Online]. Available: https://www.sentinelone.com/cybersecurity-101/endpoint-security/mssp-vs-mdr/
67. Cybereason, "Managed Detection & Response (MDR)," *Services*, Cybereason. [Online]. Available: https://www.cybereason.com/services/managed-detection-response-mdr.
68. Bitdefender Enterprise, "MDR—What is it and Why Should SMBs Care?," *Business Insights Blog*, Bitdefender, Mar. 21, 2022. [Online]. Available: https://www.bitdefender.com/blog/businessinsights/mdr-what-is-it-and-why-should-smbs-care.
69. C. Sanders and J. Smith, *Applied Network Security Monitoring: Collection, Detection, and Analysis*. Waltham, MA: Syngress, 2014. [Online]. Available: https://books.google.com.tr/books?hl=tr&lr=&id=TTIDAQAAQBAJ&oi=fnd&pg=PP1&dq=Applied+Network+Security+Monitoring:+Collection+Detection+and+Analysis .
70. ExtraHop, "The Role of NDR in Your Security Strategy," ExtraHop, 2024. [Online]. Available: https://cloud-assets.extrahop.com/resources/whitepapers/the-role-of-ndr-r02.pdf.
71. Gigamon, "Enhancing NDR Effectiveness with the Gigamon Deep Observability Pipeline," Gigamon, Dec. 2024. [Online]. Available: https://concilium.co.za/assets/files/solution-brief-enhance-ndr-effectiveness.pdf.
72. K. Awasthi, "SSL Inspection in NDR: Unlocking Threats Hidden in Encrypted Traffic," *ThreatGeek*, Fidelis Security, Jun. 13, 2025. [Online]. Available: https://fidelissecurity.com/threatgeek/network-security/ssl-inspection-in-ndr/.
73. Corelight, "Ransomware Response," *Resources - Glossary*, Corelight. [Online]. Available: https://corelight.com/resources/glossary/ransomware-response.
74. Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDOS in the IoT: Mirai and other botnets. *Computer*, *50*(7), 80–84. https://doi.org/10.1109/mc.2017.201
75. Ronen, E., Shamir, A., Weingarten, A., & OFlynn, C. (2017). IoT Goes Nuclear: Creating a ZigBee Chain Reaction. *2022 IEEE Symposium on Security and Privacy (SP)*. dio:10.1109/SP.2017.14.
76. Airehrour, D., Gutierrez, J., & Ray, S. K. (2016). Secure routing for internet of things: A survey. *Journal of Network and Computer Applications*, *66*, 198–213. https://doi.org/10.1016/j.jnca.2016.03.006
77. Dange, S., & Chatterjee, M. (2019). IoT botnet: the largest threat to the IoT network. In *Advances in intelligent systems and computing* (pp. 137–157). https://doi.org/10.1007/978-981-15-0132-6_10
78. Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2017). Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems*, *78*, 544–546. https://doi.org/10.1016/j.future.2017.07.060
79. Yaqoob, I., Ahmed, E., Hashem, I. a. T., Ahmed, A. I. A., Gani, A., Imran, M., & Guizani, M. (2017). Internet of Things Architecture: recent advances, taxonomy, requirements, and open challenges. *IEEE Wireless Communications*, *24*(3), 10–16. https://doi.org/10.1109/mwc.2017.1600421
80. Oriwoh, E., Jazani, D., Epiphaniou, G., & Sant, P. (2013). Internet of Things Forensics: Challenges and Approaches. *9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing*. https://doi.org/10.4108/icst.collaboratecom.2013.254159
81. Griffioen, H., & Doerr, C. (2020). Examining Mirai's Battle over the Internet of Things. *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, 743–756. https://doi.org/10.1145/3372297.3417277
82. Cavoukian, A. (2011). Privacy by design. In *IGI Global eBooks* (pp. 170–208). https://doi.org/10.4018/978-1-61350-501-4.ch007
83. European Parliament and Council of the European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," *Official Journal of the European Union*, vol. L 119, pp. 1-88, May 4, 2016. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.
84. M. B. Kaya, "CCPA – California Consumer Privacy Act of 2018," *mbkaya.com*. [Online]. Available: https://mbkaya.com/it-law-ccpa-california-consumer-privacy-act-2018/
85. Hoofnagle, C. J., Van Der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, *28*(1), 65–98. https://doi.org/10.1080/13600834.2019.1573501
86. Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law Innovation and Technology*, *10*(1), 40–81. https://doi.org/10.1080/17579961.2018.1452176
87. International Organization for Standardization, *ISO/IEC 27001:2013, Information technology — Security techniques — Information security management systems — Requirements*, 2013. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

88. Tankard, C. (2016). What the GDPR means for businesses. *Network Security*, *2016*(6), 5–8. https://doi.org/10.1016/s1353-4858(16)30056-3
89. J. Moline, "The Future of Cybersecurity: Why Vendor Consolidation is the Next Big Trend," *State of Security*, Tripwire, Nov. 19, 2024. [Online]. Available: https://www.tripwire.com/state-of-security/future-cybersecurity-why-vendor-consolidation-next-big-trend.
90. B. Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. New York, NY: W. W. Norton & Company, 2015. [Online]. Available: https://www.schneier.com/news/archives/2018/05/data-and-goliath-the-hidden-battles-to-collect-your-data-and-control-your-world.html.
91. E. D. Zwicky, S. Cooper, and D. B. Chapman, *Building Internet Firewalls*, 2nd ed. Sebastopol, CA: O'Reilly Media, 2000. [Online]. Available: https://www.oreilly.com/library/view/building-internet-firewalls/1565928717/.
92. $(ISC)^2$, "Cybersecurity Workforce Study, 2023," $(ISC)^2$, 2023. [Online]. Available: https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf.
93. ISACA, "State of Cybersecurity 2023," *Resources*, ISACA, Oct. 2, 2023. [Online]. Available: https://www.isaca.org/resources/reports/state-of-cybersecurity-2023.
94. J. Kindervag, "No More Chewy Centers: Introducing The Zero Trust Model Of Information Security," Forrester Research, 2010. [Online]. Available: https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf.
95. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture*. https://doi.org/10.6028/nist.sp.800-207
96. E. Gilman and D. Barth, *Zero Trust Networks: Building Secure Systems in Untrusted Networks*. Sebastopol, CA: O'Reilly Media, 2017. [Online]. Available: https://icdt.osu.edu/zero-trust-networks-building-secure-systems-untrusted-networks.
97. Cyolo, "Preventing OWASP Top 10 with Zero Trust," *Blog*, Cyolo. [Online]. Available: https://cyolo.io/blog/preventing-owasp-top-10-with-zero-trust.
98. Keeriyattil, S. (2019). Microsegmentation and Zero trust: Introduction. In *Apress eBooks* (pp. 17–31). https://doi.org/10.1007/978-1-4842-5431-8_2
99. R. Johnny, "Identity and Access Management in Zero Trust Frameworks," ResearchGate, 2019. [Online]. Available: https://www.researchgate.net/publication/388106052_Identity_and_Access_Management_in_Zero_Trust_Frameworks.
100. Reddy, R. R. P. (2024). Enhancing Endpoint Security through Collaborative Zero-Trust Integration: A Multi-Agent Approach. *International Journal of Computer Trends and Technology*, *72*(8), 86–90. https://doi.org/10.14445/22312803/ijctt-v72i8p112
101. A. McQuaid, N. MacDonald, J. Watts, and S. Handa, "Market Guide for Zero Trust Network Access," Gartner, Feb. 17, 2022. [Online]. Available: https://www.gartner.com/en/documents/4632099.
102. Edo, O. C., Ang, D., Billakota, P., & Ho, J. C. (2023). A zero trust architecture for health information systems. *Health and Technology*, *14*(1), 189–199. https://doi.org/10.1007/s12553-023-00809-4
103. McMahan, H. B., Moore, E., Ramage, D., Hampson, S., & Arcas, B. a. Y. (2017). Communication-Efficient Learning of Deep Networks from Decentralized Data. *International Conference on Artificial Intelligence and Statistics*, 1273–1282. http://proceedings.mlr.press/v54/mcmahan17a/mcmahan17a.pdf
104. Kairouz, P., McMahan, H. B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A. N., Bonawitz, K., Charles, Z., Cormode, G., Cummings, R., D'Oliveira, R. G. L., Eichner, H., Rouayheb, S. E., Evans, D., Gardner, J., Garrett, Z., Gascón, A., Ghazi, B., Gibbons, P. B., . . . Zhao, S. (2021). *Advances and open problems in federated learning*. https://doi.org/10.1561/9781680837896
105. Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (2020). Federated Learning: challenges, methods, and future directions. *IEEE Signal Processing Magazine*, *37*(3), 50–60. https://doi.org/10.1109/msp.2020.2975749
106. Truex, S., Baracaldo, N., Anwar, A., Steinke, T., Ludwig, H., Zhang, R., & Zhou, Y. (2019). A hybrid approach to Privacy-Preserving federated learning. *AISec'19: Proceedings of the 12th ACM Workshop on Artificial Intelligence and Security*, 1–11. https://doi.org/10.1145/3338501.3357370
107. K. Bonawitz *et al.*, "Towards Federated Learning at Scale: System Design," in *Proc. of Machine Learning and Systems (MLSys)*, 2019, vol. 1. [Online]. Available: https://proceedings.mlsys.org/paper_files/paper/2019/file/7b770da633baf74895be22a8807f1a8f-Paper.pdf.
108. Lan, G., Liu, X., Zhang, Y., & Wang, X. (2023). Communication-Efficient federated learning for Resource-Constrained edge devices. *IEEE Transactions on Machine Learning in Communications and Networking*, *1*, 210–224. https://doi.org/10.1109/tmlcn.2023.3309773
109. Agrawal, S., Sarkar, S., Aouedi, O., Yenduri, G., Piamrat, K., Alazab, M., Bhattacharya, S., Maddikunta, P. K. R., & Gadekallu, T. R. (2022). Federated Learning for intrusion detection system: Concepts, challenges and future directions. *Computer Communications*, *195*, 346–361. https://doi.org/10.1016/j.comcom.2022.09.012
110. Preuveneers, D., Rimmer, V., Tsingenopoulos, I., Spooren, J., Joosen, W., & Ilie-Zudor, E. (2018). Chained Anomaly Detection Models for Federated Learning: An Intrusion Detection Case study. *Applied Sciences*, *8*(12), 2663. https://doi.org/10.3390/app8122663
111. Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from machine learning perspective. *Journal of Big Data*, *7*(1). https://doi.org/10.1186/s40537-020-00318-5
112. Buczak, A. L., & Guven, E. (2015). A survey of data mining and machine learning methods for cyber Security intrusion detection. *IEEE Communications Surveys & Tutorials*, *18*(2), 1153–1176. https://doi.org/10.1109/comst.2015.2494502
113. Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., Gao, M., Hou, H., & Wang, C. (2018). Machine learning and deep learning methods for cybersecurity. *IEEE Access*, *6*, 35365–35381. https://doi.org/10.1109/access.2018.2836950
114. Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep Learning approach for Intelligent Intrusion Detection System. *IEEE Access*, *7*, 41525–41550. https://doi.org/10.1109/access.2019.2895334
115. Husak, M., Komarkova, J., Bou-Harb, E., & Celeda, P. (2018). Survey of Attack Projection, Prediction, and Forecasting in Cyber Security. *IEEE Communications Surveys & Tutorials*, *21*(1), 640–660. https://doi.org/10.1109/comst.2018.2871866

116. Jeune, L. L., Goedeme, T., & Mentens, N. (2021). Machine Learning for MISUse-Based Network Intrusion Detection: Overview, unified evaluation and feature choice Comparison Framework. *IEEE Access*, *9*, 63995–64015. https://doi.org/10.1109/access.2021.3075066
117. Kwon, D., Kim, H., Kim, J., Suh, S. C., Kim, I., & Kim, K. J. (2017). A survey of deep learning-based network anomaly detection. *Cluster Computing*, *22*(S1), 949–961. https://doi.org/10.1007/s10586-017-1117-8
118. Arrieta, A. B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., Garcia, S., Gil-Lopez, S., Molina, D., Benjamins, R., Chatila, R., & Herrera, F. (2019). Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Information Fusion*, *58*, 82–115. https://doi.org/10.1016/j.inffus.2019.12.012
119. Das, A., & Rad, P. (2020). Opportunities and Challenges in Explainable Artificial Intelligence (XAI): a survey. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2006.11371
120. Mahdavinejad, M. S., Rezvan, M., Barekatain, M., Adibi, P., Barnaghi, P., & Sheth, A. P. (2017). Machine learning for internet of things data analysis: a survey. *Digital Communications and Networks*, *4*(3), 161–175. https://doi.org/10.1016/j.dcan.2017.10.002
121. Zafari, F., Gkelias, A., & Leung, K. K. (2019). A survey of indoor localization Systems and technologies. *IEEE Communications Surveys & Tutorials*, *21*(3), 2568–2599. https://doi.org/10.1109/comst.2019.2911558
122. Mandru, S. K. (2024). Privileged User Behavior Analytics (PUBA) for insider threat detection. *Journal of Artificial Intelligence Machine Learning and Data Science*, *2*(2), 724–727. https://doi.org/10.51219/jaimld/srikanth-mandru/181
123. Liu, W., Wang, Z., Liu, X., Zeng, N., Liu, Y., & Alsaadi, F. E. (2016). A survey of deep neural network architectures and their applications. *Neurocomputing*, *234*, 11–26. https://doi.org/10.1016/j.neucom.2016.12.038
124. Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity*, *2*(1). https://doi.org/10.1186/s42400-019-0038-7
125. Legg, P. A., Buckley, O., Goldsmith, M., & Creese, S. (2015). Automated Insider Threat Detection System using user and Role-Based Profile assessment. *IEEE Systems Journal*, *11*(2), 503–512. https://doi.org/10.1109/jsyst.2015.2438442
126. The Alan Turing Institute, "Autonomous cyber defence: A roadmap from research to practice," Centre for Emerging Technology and Security (CETaS), Jun. 2023. [Online]. Available: https://cetas.turing.ac.uk/sites/default/files/2023-06/autonomous_cyber_defence_final_report.pdf.
127. Khan, M. A. (2016). A survey of security issues for cloud computing. *Journal of Network and Computer Applications*, *71*, 11–29. https://doi.org/10.1016/j.jnca.2016.05.010
128. Lazarevic, A., Ertoz, L., Kumar, V., Ozgur, A., & Srivastava, J. (2003). A Comparative study of anomaly detection schemes in network intrusion Detection. *Proceedings of the 2003 SIAM International Conference on Data Mining*. https://doi.org/10.1137/1.9781611972733.3
129. Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I., & Guizani, M. (2020). A survey of machine and deep learning methods for internet of things (IoT) security. *IEEE Communications Surveys & Tutorials*, *22*(3), 1646–1685. https://doi.org/10.1109/comst.2020.2988293
130. Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G., & Ghani, N. (2019). Demystifying IoT Security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-Scale IoT exploitations. *IEEE Communications Surveys & Tutorials*, *21*(3), 2702–2733. https://doi.org/10.1109/comst.2019.2910750
131. Voigt, P., & Von Dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR). In *Springer eBooks*. https://doi.org/10.1007/978-3-319-57959-7
132. C. Crowley and B. Filkins, "SANS 2022 SOC Survey," SANS Institute, May 2022. [Online]. Available: https://flow.torq.io/hubfs/Content%20Assets/Survey_SOC-2022_torq.pdf.
133. Omdia, "Executive Summary: Fundamentals of Endpoint Security," Omdia. [Online]. Available: https://omdia.tech.informa.com/om025420/executive-summary-fundamentals-of-endpoint-security.
134. Cybersecurity Ventures, "Cybersecurity Jobs Report: 3.5 Million Unfilled Positions In 2025," *Cybercrime Magazine*, Nov. 9, 2021. [Online]. Available: https://cybersecurityventures.com/jobs-report-2021/.
135. Ngwenya, C., & Njenga, K. (2021). Evolving Information Security Governance Practices from Evolving Technologies: Focus on Covid-19 Lockdowns. *the African Journal of Information Systems*, *13*(3), 3. https://digitalcommons.kennesaw.edu/ajis/vol13/iss3/3/
136. Check Point Software Technologies, "What is Zero Trust Security?," *Solutions*, Check Point Software Technologies. [Online]. Available: https://www.checkpoint.com/solutions/zero-trust-security/.
137. Bhagoji, A. N., Chakraborty, S., Mittal, P., & Calo, S. B. (2019). Analyzing Federated Learning through an Adversarial Lens. *International Conference on Machine Learning*, 634–643. http://proceedings.mlr.press/v97/bhagoji19a/bhagoji19a.pdf
138. F. Cappello, "Machine Learning and Artificial Intelligence for Cyber Security," Master's thesis, Dept. of Digital Systems, Univ. of Piraeus, Piraeus, Greece, 2022.
139. Lamba, T., & Kandwal, S. (2022). Global Outlook of Cyber Security. In *Algorithms for intelligent systems* (pp. 269–276). https://doi.org/10.1007/978-981-19-2065-3_30
140. Chisty, N. M. A., Baddam, P. R., & Amin, R. (2022). Strategic Approaches to Safeguarding the Digital Future: Insights into Next-Generation Cybersecurity. *Engineering International*, *10*(2), 69–84. https://doi.org/10.18034/ei.v10i2.689
141. Kfoury, E. F., Choueiri, S., Mazloum, A., AlSabeh, A., Gomez, J., & Crichigno, J. (2024). A comprehensive survey on SmartNICs: architectures, development models, applications, and research directions. *IEEE Access*, *12*, 107297–107336. https://doi.org/10.1109/access.2024.3437203
142. Ismail, M., & El-Gawad, A. F. (2023). Revisiting Zero-Trust security for internet of things. *Sustainable Machine Intelligence Journal*, *3*. https://doi.org/10.61185/smij.2023.33106
143. S. Xenitellis and A. Tsohou, "Advancing Zero Trust Network Authentication: Innovations in Privacy-Preserving Authentication Mechanisms," *Applied Sciences*, vol. 13, no. 23, p. 12675, Dec. 2023. [Online]. Available: https://www.researchgate.net/profile/Tapomoy-Adhikari-5/publication/378745801_Advancing_Zero_Trust_Network_Authentication_Innovations_in_Privacy-Preserving_Authentication_Mechanisms/links/65e81907e7670d36abfe7b13/Advancing-Zero-Trust-Network-Authentication-Innovations-in-Privacy-Preserving-Authentication-Mechanisms.pdf
144. Li, Q., Wu, D., Zhou, D., Lin, C., Liu, S., Wang, C., & Shen, C. (2025). Robust Adversarial Defenses in Federated Learning: Exploring the Impact of data Heterogeneity. *IEEE Transactions on Information Forensics and Security*, 1.

https://doi.org/10.1109/tifs.2025.3576594
145. Zhu, F., Hu, F., Zhao, Y., Chen, B., & Tan, X. (2024). A secure and fair federated learning framework based on consensus incentive mechanism. *Mathematics*, *12*(19), 3068. https://doi.org/10.3390/math12193068
146. T. K. Chawdhury, "Beyond the Falcon: A Generative AI Approach to Robust Endpoint Security," DLYog Lab Research Services LLC, Jul. 21, 2024. [Online]. Available: https://www.dlyog.com/static/data/research_papers/ai4falcon.pdf.
147. H. A. Agoro, "Integration of Explainable AI in Security Operations Centers (SOCs)," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 24, no. 2, pp. 1-10, Feb. 2024. [Online]. Available: https://www.researchgate.net/publication/389211213_Integration_of_Explainable_AI_in_Security_Operations_Centers_SOCs.
148. Journal of Communication Engineering & Systems. (2024). *Journal of Communication Engineering & Systems*. https://doi.org/10.37591/joces
149. Sparks, R., Carter, C., Donnelly, J. B., O'Keefe, C. M., Duncan, J., Keighley, T., & McAullay, D. (2008). Remote access methods for exploratory data analysis and statistical modelling: Privacy-Preserving Analytics®. *Computer Methods and Programs in Biomedicine*, *91*(3), 208–222. https://doi.org/10.1016/j.cmpb.2008.04.001
150. Paul, N. E. M., Paul, N. E. M., Kessie, N. J. D., & Salawudeen, N. M. D. (2024). Zero trust architecture and AI: A synergistic approach to next-generation cybersecurity frameworks. *International Journal of Science and Research Archive*, *13*(2), 4159–4169. https://doi.org/10.30574/ijsra.2024.13.2.2583
151. P. Shinde, S. Mali, P. Ghodke, and T. Shelke, "Cyber AI: Empowering Cybersecurity through Artificial Intelligence," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 12, no. 2, Feb. 2024. doi: 10.15680/IJIRCCE.2024.1202029. [Online]. Available: https://www.researchgate.net/profile/Punam-Shinde/publication/389901434_Cyber_AI_Empowering_Cybersecurity_through_Artificial_Intelligence/links/67d7eeef478c5a3feda365c7/Cyber-AI-Empowering-Cybersecurity-through-Artificial-Intelligence.pdf.
152. G. Elahi and E. Yu, "A Goal Oriented Approach for Modeling and Analyzing Security Trade-Offs," Dept. of Comp. Sci., Univ. of Toronto, Toronto, ON, Canada, Tech. Rep., 2007. [Online]. Available: https://www.cs.toronto.edu/pub/eric/ER07-Elahi.pdf.
153. T. Gupta, "Revolutionary the structures for next-generation cyber security: Improving the digital defense techniques," in *Digital Transformation in Retail: Adapting to New Consumer Landscape*, 2024. [Online]. Available: https://e-sarthi.lpcps.org.in/uploads/ResearchDocument/2024/7/1082/9._DR_TARU_GUPTA.pdf.
154. Mmaduekwe, U. (2024). Bias and fairness issues in artificial intelligence-driven cybersecurity. *Current Journal of Applied Science and Technology*, *43*(6), 109–119. https://doi.org/10.9734/cjast/2024/v43i64391
155. Pendlebury, F., Pierazzi, F., Jordaney, R., Kinder, J., & Cavallaro, L. (2018). Enabling fair ML evaluations for security. *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, 2264–2266. https://doi.org/10.1145/3243734.3278505
156. Baniecki, H., & Biecek, P. (2024). Adversarial attacks and defenses in explainable artificial intelligence: A survey. *Information Fusion*, *107*, 102303. https://doi.org/10.1016/j.inffus.2024.102303