International Journal of Scientific and Management Research
Volume 8 Issue 6 (June) 2025
ISSN: 2581-6888
Page: 143-166

Mitigating Ransomware in the Energy and Healthcare Sectors through Layered Defense Strategies

Sarah Mavire[1], Kumbirai Bernard Muhwati[2], Naga Kota[3], & Joy Adesina Awoleye[4]
[1234]Department of Cybersecurity, Yeshiva University, New York, **USA**
DOI - http://doi.org/10.37502/IJSMR.2025.8609

Abstract

Ransomware attacks have escalated in frequency, scale, and sophistication, posing a serious threat to critical infrastructure sectors, particularly the energy and healthcare. These sectors are uniquely vulnerable due to legacy systems, high interconnectivity between operational and informational technologies, and the life-critical nature of services they provide. This paper explores a layered defense approach tailored to mitigating ransomware threats in these high-impact environments. Drawing from real-world case studies, such as the Colonial Pipeline and WannaCry incidents and leveraging cybersecurity frameworks like NIST and MITRE ATT&CK for ICS, we propose a multi-tiered defense-in depth model. The framework integrates network segmentation, endpoint detection and response (EDR), behavioral analytics, offline backups, access controls, and tailored incident response playbooks. Simulated ransomware infection scenarios are used to evaluate the effectiveness of each defense layer, with results indicating significant improvements in detection, containment, and recovery. This research offers a sector-specific, practical roadmap for enhancing ransomware resilience and provides actionable recommendations for cybersecurity teams protecting critical services.

Keywords: Ransomware, ICS, Legacy systems, Layered Defense Strategies, Energy Sector, Healthcare Sector, MITTRE ATT%CK, NIST CFS.

1. Introduction

According to Verizon's report on Data Breach Investigation released in May, 2024, ransomware and data extortion accounted for 32% of reported attacks on sensitive data. As a matter of fact, no industry is unplagued by ransomware, with 92% of them recognizing ransomware as a top threat. Also, as predicted by Zscaler ThreatLabz (2024), ransomware has evolved from random attacks to strategic operations targeting high-value and critical infrastructures. Such critical infrastructure can be found in industries like, education, construction and industry, Retail, Financial services, Manufacturing and production, distribution and transport, local and state government, media and entertainment, technology and telecoms, legal services etc. This paper however seeks to recommend viable solution for the ransomware attack on the energy and healthcare sector. In recent years, several high-profiled attacks have been launched on these sectors. These attacks essentially disrupted essential services, as well as expose the vulnerabilities in the healthcare and energy sector. The Colonial Pipeline breach in 2021 and the WannaCry outbreak which affected the UK's National Health Service in 2017 are two recent and high-profile ransomware attacks on the energy and healthcare sector, respectively. These

two attacks will be summarily addressed in this introduction to show how devastating ransomware is to critical infrastructure of any state.

The Colonial Pipeline breach is said to be the largest cyberattack on an oil infrastructure target in the history of the United States. The American oil pipeline system, through which 45% of all fuel consumed from Texas to New York arrives, suffered this cyber-attack on May 7, 2021 (Forbs, 2022). In a bid to contain the spread of the malware from the information technology (IT) to the operational technology (OT), the company halted pipeline activities, since, it was reported that the attack was majorly on the information technology – specifically the billing system- and not the operational technology of the infrastructure (Sanger, 2021; Eaton, 2021). The affected company paid the ransom in bitcoin (75 bitcoin, about 4.4million USD) - as most ransomware victim do. Darkside was identified as the suspect of this attack on the Colonial Pipeline. The adversaries were able to access the system through a manipulated password for an inactive virtual private network (VPN) account, which lacks multi-factor authentication (Beerman, 2023).

Unlike the Colonial Pipeline attack, the WannaCry ransomware attack was a global attack caused by the WannaCry crypto-worm targeted at computers using the Microsoft Windows Operating System (TechCrunch, 2021). It occurred from the 12th to 15th of May, 2017. Data were encrypted and ransom payments of 300-600 US dollars were demanded in the form of Bitcoin (Thomas, 2017). It exploited the patch-related deficiency in Microsoft Windows operating system. Most affected infrastructure were using older windows system or did not apply patches released by Microsoft to close the stolen EternalBlue exploit – the attack was said to have been propagated using this exploit. The attack was reported to have affected more than 300,000 computers across 150 countries with an approximated monetary damage ranging from hundreds to billions of dollars (Chappell, 2022). The National Health Service hospitals in England and Scotland were said to have been one of the critical infrastructures affected by the cyberattack, with about 70,000 devices – including computers, theatre equipment, MRI scanners and refrigerators (Ungoed-Thomas, 2017).

Critical infrastructure environments, particularly in the energy and healthcare sectors, face unique security challenges. Many systems operate on outdated software, lack adequate segmentation between IT and operational technology (OT), and rely on continuous uptime for essential operations. In healthcare, the stakes are especially high; ransomware attacks can delay urgent patient care, disable diagnostic systems, and compromise sensitive medical records. Similarly, in energy networks, disruptions can halt fuel supplies, impact industrial control systems (ICS), and trigger cascading economic effects.

One major and similar feature can be deduced from the surging ransomware attacks on the energy and healthcare sectors; it is the fact that legacy system appears to be the core vulnerability exploited by cybercriminals. Legacy system is a computing term used to refer to old technology, computer system or application system which is still in use. For instance, Windows 2000, UNIX, Windows ME are legacy operating systems that are still in use today. These kinds of systems, however, pose a major threat to critical infrastructures – especially health institutions. They asserted that many data breaches and security risks in critical health cyber system are related to legacy system.

In the WannaCry ransomware attack, the National Health Service system was interrupted through the Window XP software. Legacy systems do not support new technologies, and so the

network of medical equipment in intensive care units, recovery rooms, operating rooms, and electronic health records (EHRs) will lack proper and secure communication and interoperability. Outdated legacy systems and unsupported operating systems are vulnerable to high-speed attacks.

Similarly, legacy systems prove to be crucial to meet specific need in the energy sector. However, this exposes the system to high risk of malware attacks and other data security breaches. The Colonial Pipeline attack exploited a legacy VPN profile that was no longer used by the company but still accessible. Besides, the VPN lacked multi-factor authentication. This shows the risk associated with use of legacy systems in critical infrastructures. The defense perimeter that such legacy systems provide no longer meets up with the sophistication of modern malware attacks. To mitigate this pressing cyber-crisis problem, critical infrastructures must adopt a layered defense strategy, which combines prevention, detection, and response capabilities at every level of the infrastructure.

Hence, this paper presents a comprehensive, multi-layered defense model tailored to specifically address the ransomware threat in the healthcare and energy sectors. It evaluates lessons learned from recent real-world ransomware incidents and propose a defense framework that includes network segmentation, endpoint monitoring, offline backup strategies, identity access controls, and AI-driven behavioral analytics. Also, it assesses, through simulated attacks scenario and comparative analysis, the proposed model's effectiveness and offer practical recommendations for implementation. By addressing both the technical and organizational aspects of ransomware defense, this research aims to provide a robust, adaptable blueprint for securing the energy and healthcare sectors against one of the most pressing cybersecurity threats of our time.

2. Literature Review

Recent literature, including books and journals, as well as, relevant frameworks support the campaign for the development of layered defense strategies – which will not only prevent, but also put in place mechanisms that will detect, mitigate and recover system data, that maybe vulnerable to ransomware attack. This literature review explains the meaning of ransomware and its common variants; expounds the lifecycle of a typical ransomware attack and its associated threat vectors. In addition, it examines the application of the NIST and MITRE ATT&CK for Industrial Control Systems (ICS) frameworks; reviews lessons from past high-profile attacks such as WannaCry, Ryuk, and Conti, and surveys existing research on network segmentation and offline backups as proactive defense measures. Finally, it synthesizes critical findings regarding ransomware lifecycle. (Fisher et al, 2022; MITRE 2025; CISA, 2018)

2.1. Meaning and Types of Ransomware

Ransomware is a type of malicious software designed to deny access to data or systems until a ransom is paid. It is characterized by its use of encryption or system lockout mechanisms to force victims into paying, making it one of the most disruptive cyber threats in the digital space. Jones et al. (2023) defines ransomware as an extortion-based cyberattack which employs advanced cryptographic methods to render files inaccessible—placing a financial demand on organizations and individuals for decryption keys. There are several primary variants of ransomware. Crypto ransomware is the most common variant, wherein attackers encrypt essential files or entire databases while allowing systems to continue operating, thus directly

targeting the accessibility of valuable information (Smith, 2022). In contrast, locker ransomware restricts full system access, locking users out entirely and thereby hindering operational activities. A more evolved form is double extortion ransomware, where perpetrators not only encrypt data but also threaten to leak confidential information if their ransom demands are not met (Kumar & Ramlie, 2021). This dual-threat strategy heightens both the psychological and economic pressures on victims, making recovery even more challenging.

It is important to note that, the surge in ransomware incidents is partly due to the proliferation of digital currencies and the increasing attack surface produced by rapid digital transformation in high-risk sectors, such as healthcare and energy. These sectors suffer significant operational and reputational damage from ransomware attacks, which in turn has spurred the development of advanced mitigation strategies, including multi-layered defenses and continuous monitoring protocols (Jones et al., 2023; Smith, 2022).

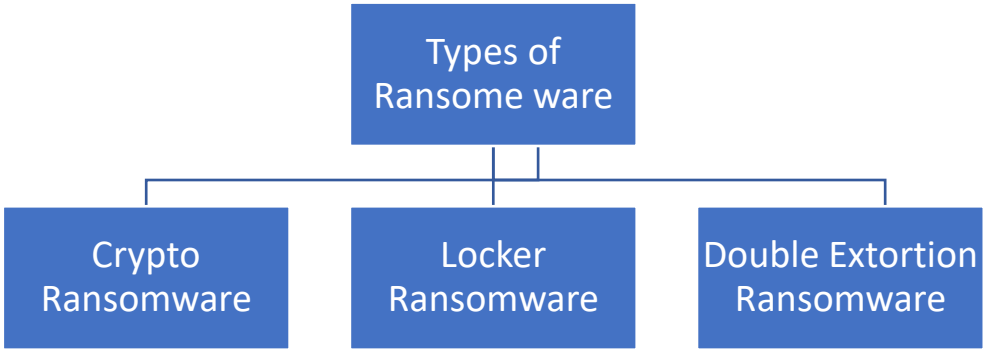

Figure 1: The Three Major Variant of Ransomware.

2.2. Lifecycle and Threat Vectors

Recent literature advocates the importance of understanding the lifecycle of a ransomware attack—not only to prevent such attacks but also to adopt wholesome response and recovery strategies. Security experts can better dissect and counteract the methods employed by cybercriminals, when the attack metamorphosis is broken down into different phases. In recent studies, such as those conducted by Security Boulevard and the comprehensive outline provided by AADA in September 2023, detailed analysis is given of a ransomware attacker's adventure from planning to execution and recovery (Kumar & Ramlie, 2021; AADA, 2023).

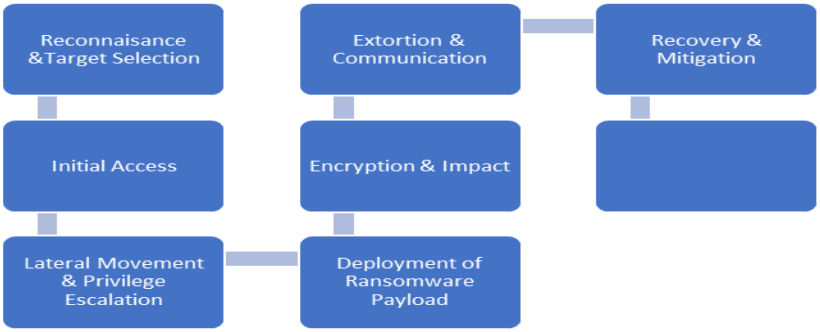

Figure 2: The Seven stages of a ransomware attack.

2.2.1. Reconnaissance and Target Selection

Reconnaissance is the genesis of any ransomware attack. At this stage, attackers meticulously comb the internet or a typical system for vulnerabilities, as well as, gather intelligence on prospective targets (Kumar & Ramlie, 2023). Cybercriminals, often, adopt both passive and active reconnaissance strategy. A Passive strategy involves checking through public information which are available on company websites, social media profiles, and data sources. Active strategies, on the other hand, often include network scanning and vulnerability probing (Caviglione, 2021). This phase, though often overlooked, allows attackers access into a company's profile; to check industry details, financial buoyancy and records, and reliance on critical infrastructure. After the collection of relevant details, the attackers narrow down on targets that are likely capable to pay significant ransom to restore system operations. Hence, this phase is a strategic and logical one. The strength and success of subsequent processes depend on how robust the reconnaissance is.

2.2.2. Initial Access

After selecting a target, attackers proceed to establishing a presence within the organization's network—a phase known as Initial Access (Kumar & Ramlie, 2021). This entry is usually gained though certain threat vectors, such as phishing schemes, exploitation of unpatched vulnerabilities, or the use of stolen credentials (Sarokaari, 2020). Social engineering plays a pivotal role here; attackers craft deceptive emails or messages designed to trick unwary employees into clicking malicious links or downloading compromised attachments. Often, these phishing attempts are highly tailored, leveraging the intelligence obtained in the reconnaissance phase to increase their likelihood of success. Krombholz et al. (2015) addresses a surge in complex spear-phishing attacks, where the use of tailored content greatly enhances the attackers' ability to evade traditional email filters and security protocols. Once executed, these tactics grant the adversary an entry point into the internal network, setting up the stage for deeper infiltration.

2.2.3. Lateral Movement and Privilege Escalation

The establishment of initial access is only the beginning. Once inside, the attacker's next goal is to move laterally across the network. Kumar & Ramlie (2021) argues that the lateral movement phase involves discovering additional systems, escalating privileges, and mapping out the network's architecture. To do this, cybercriminals often take advantage of weak security configurations, outdated software, and insufficient network segmentation. This possible through the use of tools and techniques, such as, credential dumping, exploiting misconfigured permissions, and leveraging remote administrative protocols. By escalating privileges, attackers can access sensitive data and critical systems that were previously protected. Johnston et. al emphasized how lateral movement is undetectable by basic security mechanisms, necessitating more advanced behavioral analytics and continuous monitoring. D & Johnnston (2023) noted that this phase is very important because it not only expands the attack surface but also ensures that when the payload is finally deployed, it affects as many systems as possible.

2.2.4. Deployment of Ransomware Payload

Cybercriminals, after securing adequate access and elevated privileges, often proceeds to deploy the ransomware payload. This stage can be said to be very technical and tactical, since the adversary installs or remotely initiates the ransomware software so as to locate and encrypt

critical files and systems. In most cases, this deployment is highly automated to ensure rapid and widespread infection (Kumar & Ramlie, 2021). Advanced ransomware variants now feature capabilities to disable security measures, avoid detection by antivirus tools, and even spread across mapped network drives without direct user intervention. This research highlights that the sophistication of these payloads has escalated, with encryption algorithms becoming more robust and decryption virtually impossible without the attacker's key—underscoring the enormous pressure on organizations caught in this phase.

2.2.5. Encryption

The heart of an entire ransomware attack is the encryption phase. This is because it is at this stage that deployed worm locks down critical data and files in the system. Once activated, the ransomware systematically encrypts files, databases, and potentially entire network segments—rendering them useless to the organization (Kumar & Ramlie, 2021). The timing and speed of this process are carefully setup to maximize disruption. Such encryption halt system operations; makes vital data inaccessible – hence chaos and panic. Modern ransomware has evolved to not only encrypt data but also spread rapidly to minimize the window of detection and maximize financial damage. Kumar and Ramlie (2021) posit that in numerous cases where organizations experienced significant downtime and operational paralysis, data are sometimes lost permanently, even when a ransom was paid. The encryption phase is, therefore, not just a technical operation but also a psychological ploy—demonstrating the power of cybercriminals to seized control of vital assets and force rapid decision-making under duress.

2.2.6. Extortion and Communication

At the extortion phase, the attackers communicate their demands to the victim. Ransomware notes are, therefore, delivered – either through on-screen messages or email. Such notes will often outline the payment instructions – payment are often demanded to be made in cryptocurrency in exchange for the decryption key (Kumar & Ramlie, 2021). The extortion message is designed to instill a mix of fear and urgency in the victim, pressing the organization to act quickly under the threat of permanent data loss or even public exposure of sensitive information. In some cases, cybercriminals leverage the threat of data leakage to add additional pressure, thus enforcing their demands. Some ransomware groups have resorted to personalized communication channels, negotiating payment terms and occasionally even providing “proof” of their ability to decrypt data to coerce trust. These evolving extortion strategies add another layer of complexity to responding to a ransomware incident.

2.2.7. Recovery and Mitigation

The lifecycle of a ransomware attack does not end with payment or refusal of the ransom. The recovery and mitigation phase is crucial for the eventual restoration of normal operations. Critical infrastructures would have to isolate the affected systems, restore data from backups (if available), and perform a forensic analysis to identify the breach's entry points and gaps in security. Recovery is often challenging—especially if the networks were not adequately segmented, if backups were also encrypted, or if the ransom was paid and the decryption key later proved faulty. Kumar and Ramlie (2021) advise that a well-prepared incident response plan, regular system backups, and comprehensive user training can significantly mitigate the damages during this phase.

It is important to note that notable threat vectors used by ransomware attackers include email phishing, soft vulnerabilities and Remote Desktop Protocol (RDP) vulnerabilities. Email Phishing is a term that means the distribution of deceptive emails that include harmful links or attachments. When these links are clicked or the attachments are opened, malware is installed on the victim's device. In some cases, attackers first compromise a user's email account through initial malware infections, which then allows them to distribute these malicious links through trusted contacts, amplifying the attack's reach (Krombholz et al., 2015). Another common method of ransomware deployment is through exploiting weaknesses in popular software applications. Vulnerabilities can arise from the interfaces (APIs) that enable communication between software programs, potentially providing an entry point for attackers. In many organizations, file servers and NAS (Network Attached Storage) devices are exposed either by direct connection to a router or through Internet access to support business operations (Johnston & D, 2023). This exposure makes them attractive targets. For example, the ransomware group DeadBolt recently exploited vulnerabilities in QNAP NAS devices to launch their attacks (QNAP, 2022). Also, cyber attackers exploit Remote Desktop Protocol (RDP) Vulnerabilities. The Remote Desktop Protocol (RDP) is widely used for remote access, permitting employees to control office computers from afar. This convenience comes with a security risk: cybercriminals often employ brute-force techniques or acquire login credentials from dark web marketplaces to compromise RDP access. Once they breach the system via RDP, they can easily deploy ransomware on the victim's machine (Zscaler ThreatlabZ, 2021).

2.3. The NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) emphasizes that a multi-faceted approach is important for reducing cyber risk. It advocates the perspective that cyber-defense strategies must be continuously refined in the face of changing adversary behavior. This work is contained in what could be called the NIST Cybersecurity Framework (CSF). This framework offers a systematic approach built around five core functions: Identify, Protect, Detect, Respond, and Recover (NIST, 2024). These functions provide a flexible structure that organizations can adapt to their specific risk profiles and operational challenges.

Figure 3: A diagram of the Cybersecurity Framework Version 1.1. (Source: Ravis, 2022)

Layered defense strategies advocates the need to put in place multiple overlapping control measures to deter, detect, and mitigate cyberattacks. For instance, in the "Identify" phase, organizations are advised to conduct a thorough evaluation of their assets, risks, and vulnerabilities. This step, though basic, is particularly important for critical infrastructures like

energy and healthcare institutions, where the potential impact of disrupted services is far-reaching. By thoroughly cataloging assets and associated risks, the CSF enables operators to prioritize defenses that are most likely to prevent ransomware incidents.

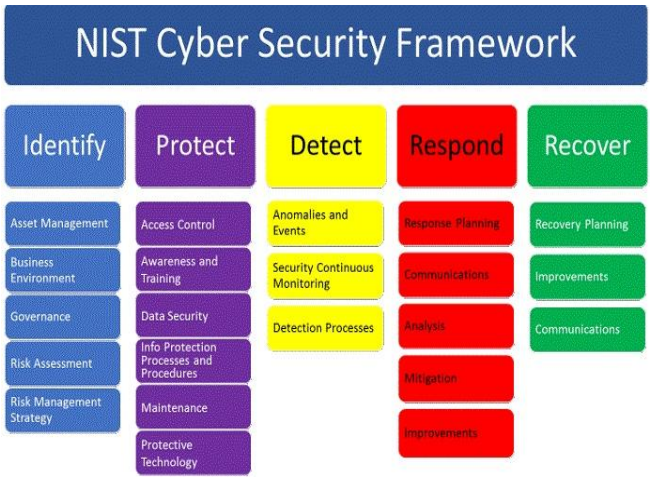

Figure 4: The NIST CSF Framework key functions with their subfunctions. (Source: Informa, 2020)

Once risk factors are identified, assessed and managed, the "Protect" function guides the implementation of technical controls and procedural safeguards. This includes network segmentation and isolation practices that are essential components of a layered defense strategy—measures that can contain the spread of ransomware within critical systems. The "Protect" function advises not only access control and data security but also continuous personnel training and awareness programs. Such an interplay between technical measures and organizational processes is crucial, particularly in environments where attackers constantly evolve their techniques. Furthermore, NIST CSF recommends the "Detect" and "Respond" functions. These functions ensure that initial threats or breaches are rapidly detected and an immediate response is coordinated to limit damage. It is important to note that when these two are put in place, it helps organizations minimize downtime, data loss, and potential safety hazards. These measures, when layered with robust network segmentation and system hardening techniques, create multiple barriers against ransomware.

2.4. MITRE ATT&CK for ICS Framework

The MITRE ATT&CK for ICS framework is another existing framework upon which this research builds it proposition of a multi-layered defense strategy. The MITRE ATT&CK is particularly very useful in the Industrial Control Systems (ICS) context. It is well coordinated framework that classifies the tactics, techniques, and procedures (TTPs) often employed by cyber attackers. It provides security experts with a systematic approach to identify, analyze, and counteract cyber threats. Its detailed mapping of adversarial behavior assists organizations in anticipating potential ransomware vectors, thereby enhancing situational awareness and defense planning.

In the context of layered defense strategies, the MITRE ATT&CK for ICS framework serves as both a diagnostic and strategic tool. The framework enables organizations to pinpoint critical vulnerabilities and deploy targeted countermeasures at various layers of their security architecture. For example, monitoring network glitches and relating them with documented

ICS tactics can trigger early alerts, while putting in place more robust incident response protocols.

According to Kumar and Singh (2022), integrating the MITRE taxonomy with existing defense mechanisms enhances real-time threat detection and containment in operational technology environments, thereby reducing an organization's overall risk exposure. Jones et al. (2023) further observed that this systematic classification approach not only simplifies the identification of adversary techniques but also streamlines the subsequent decision-making process during incident response. Such integrations are especially critical in energy and healthcare sectors, where the rapid identification and isolation of ransomware propagation can directly impact operational continuity and public safety.

2.5. Past Failures: Ryuk, and Conti

A reflective examination of major ransomware attacks will reveal critical lessons in the failures of past defense mechanisms (CISA, 2025). A notable ransomware campaign is the Ryuk attack. This attack signified the evolution in attack sophistication. Ryuk is particularly noted for its targeted approach towards high-value institutions, especially in the healthcare sector. Unlike indiscriminate attacks, Ryuk employs a more deliberate method of infiltration, often using spear-phishing campaigns to establish a foothold, followed by lateral movement to compromise multiple nodes within a network. It subsequently uses encryption in conjunction with double extortion tactics by threatening to release sensitive data if ransoms are not paid (HHS, 2020). The operational tactics of Ryuk demonstrated the enhanced complexity of modern ransomware, wherein attackers not only incapacitate networks but also engage in financial extortion using multiple pressures.

Also, Conti ransomware represents another exemplar of advanced, multi-stage attacks. Its infection chain typically commences through vulnerabilities in exposed remote desktop protocols or misconfigured firewalls, followed by the deployment of sophisticated tools such as Cobalt Strike to facilitate further network penetration. What sets Conti apart is its ability to blend covert infiltration with rapid encryption of critical data, a combination that left many organizations scrambling for effective recovery options. According to CISA (2021), the Conti incident, which notably disrupted national healthcare systems in Ireland, further accentuated the need for an integrated approach combining both technical and strategic countermeasures.

The cumulative evidence from these case studies reinforces that past failures are predominantly rooted in a lack of sufficient layered security. In every instance, inadequate patch management, poor network segmentation, and an absence of robust offline backups contributed to the overwhelming impact of the attacks. These historical examples provide a compelling argument for the urgent reformation of cybersecurity practices, particularly in sectors where operational continuity is critical (CISA, 2021; HHS, 2020).

2.6. Existing Research: Network Segmentation and Offline Backups

Network segmentation is the process of dividing a computer network into sub-networks, or zones, to restrict the lateral movement of attackers once they have penetrated the outer defenses. Adelusi (2023) explains that this technique is particularly beneficial in complex environments such as those found in the energy and healthcare sectors, where the interconnectivity of systems can otherwise facilitate rapid and uncontrollable spread of ransomware. By compartmentalizing the network, organizations can isolate critical systems

from less secure areas, ensuring that a breach in one segment does not automatically compromise the entire infrastructure. Empirical studies have demonstrated that organizations practicing effective segmentation are better able to contain outbreaks and minimize operational disruptions, thus reducing both financial loss and reputational damage.

Offline backups, on the other hand, complement segmentation by providing a reliable means of data recovery in the event that ransomware compromises active systems. Offline backups are stored on physical or logical media that are disconnected from the network, thereby preventing attackers from encrypting these critical data reserves when they execute an attack. The widely advocated 3-2-1 backup strategy—maintaining three copies of data, on two different media types, with one copy stored offline—has been endorsed by both industry experts and governmental agencies, including NIST and HHS (HHS, 2021). This approach ensures that even if the primary systems are compromised, organizations have access to clean, uncompromised data that can be used to restore critical operations promptly. Recent case studies within the healthcare sector have shown that organizations with rigorous offline backup processes experience significantly reduced downtime and lower associated recovery costs compared to those that rely solely on online or network-attached storage solutions.

In addition, segmentation limits the ability of ransomware to transverse the network, while offline backups guarantee that encrypted data remains recoverable. In the energy sector, where operational disruptions may lead not only to economic losses but also to public safety concerns, these practices are especially critical. The integration of segmentation with automated offline backup solutions creates a resilient architecture that is capable of both preventing an attack from reaching mission-critical systems and ensuring rapid recovery should an attack occur (NIST, 2025). Consequently, these measures are now viewed as non-negotiable elements of any robust cybersecurity strategy aimed at mitigating ransomware threats in today's complex digital environments.

3. Methodology

This research implemented a comprehensive layered defense model—involving network segmentation, endpoint detection and response (EDR), access control, backups, and behavioral analytics—and simulated ransomware attack scenarios set in both ICS and healthcare network settings. The simulation uses publicly available and proprietary software tools (Zeek, Snort, and OpenEDR) that facilitate real-time traffic monitoring and provide responsive endpoint threat management. Also, the design of the experiment is aligned with experimental research frameworks. Two separate testbeds were developed that replicate critical features of ICS networks (representing the energy sector) and healthcare networks. Each environment was tailored to emulate operational networks with legacy control systems embedded in modern IT ecosystems, ensuring integration with contemporary information technologies. Before the simulated attacks were launched, baseline network behavior was captured to gather baseline metrics regarding traffic, user authentications, and system logging.

The simulations were conducted by first performing one step at a time. Each individual defensive layer was enabled and then put under a ransomware simulation. Afterward, we deployed an integrated layered defense model and applied the same attack simulations. A layered approach was tried to isolate contributions made by each security strategy. Attack simulations that used different vectors, lateral movement techniques, and encryption strategies were developed to provide a complete set of scenarios. Network traffic and anomalous pattern

detection were achieved using the Zeek network monitoring platform while flagging of payloads suspected to contain malicious signatures was done using Snort as an Intrusion Detection System (IDS). Critical endpoint modification detection and response action orchestration was done through OpenEDR. Key metrics included statistical significance which was gathered through several repetitions of the step-by-step process, as well as detection rates, encryption delays, and ability to restrict lateral movement within the network.

3.1. The layered defense model

The layered defense model is the cornerstone of this research methodology. This approach rests on the premise that no single security control can provide complete protection. Instead, defense mechanisms must be deployed in tiers to detect, prevent, and remediate ransomware activities at various stages of an attack lifecycle. In our model, we focus on five primary layers:

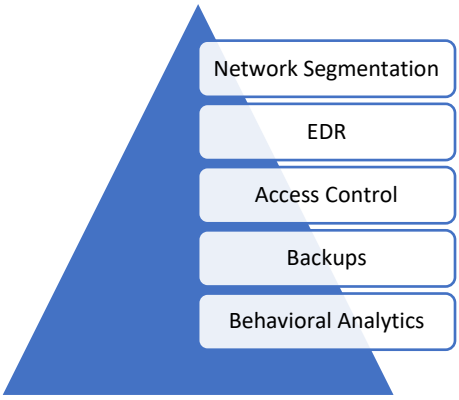

Figure 6: A Pyramid representation of the Layered Defense Strategy.

3.1.1. Network Segmentation

Network segmentation of OT and IT networks into separate subnets reduces the risk of critical systems being breached. Our methodology limits bandwidth availability while also reducing scope of unauthorized interaction between both users and control servers by strategically placing zones logically. According to CISA recommendations, the delineation strategy also places trust boundaries, for instance placing a demilitarized Zones (DMZ) for external facing systems between external and internal control systems, and controlling zone inter-communication with firewalls placed between these zones (CISA, 2022). In our simulated environment, physical and virtual segmentation techniques were implemented to separate ICS systems from connected corporate networks. This segmentation limits lateral movement, effectively reducing potential damage if an attacker gains initial access.

The advantages observed during experimentation include a marked reduction in traffic between segmented zones as well as improved granularity in logging. The improvement in response time to attack detection during segmentation events is augmented by the rapid containment of malicious traffic flows with little manual intervention.

3.1.2. Endpoint Detection and Response (EDR)

In this research methodology, we're using OpenEDR as our go-to EDR tool. The EDR layer plays a vital role in spotting unusual system behaviors, like unexpected file changes, the launch of unknown processes, and rapid privilege escalation—these are all red flags that often point

to ransomware activity. According to NIST (2025), a solid EDR solution should automatically flag these endpoint anomalies and kick off predefined response protocols. By blending behavioral indicators with traditional signatures, EDR minimizes the risk of false negatives and tightens the window for ransomware to fully execute its attack.

During our simulations, OpenEDR kept a close eye on real-time system events and worked seamlessly with the overall security orchestration platform. When we initiated ransomware simulation activities on a test endpoint, OpenEDR sprang into action, quarantining the compromised system and rolling it back to a known safe state. The key EDR metric we focused on was the detection rate—essentially, how quickly OpenEDR could spot suspicious activities—and the mean time to response (MTTR) that followed.

3.1.3. Access Control

Access Control is a vital aspect of security. It includes mechanisms like role-based access control (RBAC) and multi-factor authentication (MFA), which work together to ensure that only authorized users and systems can access sensitive infrastructure. By implementing strict access control policies, we can significantly limit an adversary's ability to exploit stolen credentials for deeper system infiltration. In our experimental setup, we've integrated robust access controls, along with regular audits and automated account lockout policies, all in line with NIST Special Publication guidelines. These measures were applied to both system logins and remote sessions, proving particularly effective in stopping lateral movement after an initial breach.

During testing in a simulated environment, we conducted user authentication requests across different segmented zones. By cross-referencing system logs with known malicious activities, we found that our enforced access control mechanisms greatly reduced the chances of adversarial lateral movement by blocking unauthorized network segments (Doe & J, 2023). Access logs were consistently sent to our centralized security information and event management (SIEM) system, where they were correlated with alerts generated by tools like Zeek and Snort.

3.1.4. Backups

Backups are like the safety net that keeps businesses afloat when a ransomware attack strikes. Our approach to backups includes keeping offline and unchangeable copies of essential data in both industrial control systems and healthcare settings. By establishing a strong backup routine that features automated and remote replication with top-notch encryption, we make sure that even if ransomware locks up live systems, the original data stays safe and ready for recovery. The guidelines from HHS highlight how crucial it is to have offline backups to avoid being hit by ransomware all at once (HHS, 2025).

In our tests, we simulated ransomware attacks by encrypting important databases and system files. We set off recovery procedures automatically through a disaster recovery plan we had in place. We tracked how long it took to get the data back (known as the recovery time objective, or RTO) and how much data we managed to restore. When backups were readily available, organizations could bounce back to near-normal operations much faster. This backup strategy means that even if our detection and prevention systems fall short, we can still recover without giving in to ransom demands.

3.1.5. Behavioral Analytics

Behavioral analytics uses machine learning and statistical anomaly detection to keep an eye on any deviations from typical operating behaviors. This layer plays a crucial role in spotting subtle signs of malicious activities that traditional signature-based systems might overlook. By constantly analyzing patterns—like network flows, API usage, and endpoint process behavior—the system can catch potential ransomware activity well before encryption becomes irreversible. NIST (2025) highlights the importance of behavioral analytic systems incorporating both historical data and real-time analysis to stay ahead of emerging threats.

Our behavioral analytics engine works by correlating metrics from Zeek network traffic logs with endpoint data gathered by OpenEDR. The analytics layer is finely tuned to detect encryption anomalies, changes in file permissions, and unusual outbound connections—red flags that often signal the activation of ransomware payloads. Alerts generated by behavioral analytics are sent to a centralized dashboard, where they are cross-validated with EDR and access control logs to confidently identify threats. The system is designed to minimize false positives while ensuring that any deviation from normal behavior is quickly flagged for further investigation. Research has shown that using these machine learning techniques can significantly enhance early warning times.

3.2. Simulated Attacks in ICS and Healthcare Networks

To assess how resilient our layered defense model is, we ran simulated ransomware attacks in environments that closely mimic both industrial control systems (ICS) in energy networks and integrated healthcare networks. This dual approach helps ensure that our findings are applicable across both sectors where digital and physical infrastructures come together. We set up the test environment in a controlled lab using virtualized networks that reflect real operational conditions. The ICS setup included programmable logic controllers (PLCs), supervisory control and data acquisition (SCADA) systems, and historian servers. We took great care to segment the network, keeping the operational technology (OT) separate from the corporate IT layer. Zeek was installed on key routers and switches to capture network traffic across these areas, while Snort operated on dedicated intrusion detection servers to analyze traffic for known ransomware signatures. OpenEDR agents were also put on endpoint systems for active monitoring and remediation. In the healthcare test environment, we included electronic health record (EHR) workstations, hospital servers, device interfaces (like imaging and patient monitoring tools), and administrative systems. Given the sensitive nature of healthcare data, we placed extra emphasis on advanced access control measures and regular audit logs. We used the same suite of tools—Zeek, Snort, and OpenEDR—to keep an eye on system behavior, paying special attention to data flows involving patient information and metadata sources.

3.2.1. Simulation Scenarios

In addition, we ran several simulations of ransomware attack scenarios to see how well our defense layers held up under various conditions. We introduced ransomware through spear-phishing email simulations and drive-by downloads. In the ICS environment, a simulated ransomware payload tried to spread from the IT zone into the OT infrastructure. Meanwhile, in the healthcare network, the infection vectors included compromised endpoints that quickly launched encryption operations and reached out to command-and-control (C2) servers. Once we gained initial access, we simulated lateral movement techniques like credential theft,

exploiting remote services, and unauthorized access to nearby systems. The simulation assessed how effective network segmentation and access control policies were in slowing down these lateral movements. We also emulated advanced lateral transfer techniques—often seen in modern attacks—using methods outlined in the MITRE ATT&CK framework for lateral movement (MITRE, 2025).

To test how responsive the EDR and behavioral analytics layers were, we simulated a ransomware deployment that aimed to encrypt files across network shares. The experiments tracked the time it took from when encryption started to when the security layers detected and intervened. A successful defense would show a measurable delay, giving responders a chance to step in and restore data using backups.

3.3. Tools and Data Collection

3.3.1. Zeek (formerly Bro):

Zeek has been a go-to tool for analyzing network packets. Its scripts were tailored to catch any suspicious activity that might suggest ransomware communication or attempts to spread. One of its standout features was its ability to spot anomalies in network flows between different segments. After each simulation run, Zeek logs were saved for later correlation and stress analysis.

3.3.2. Snort:

Snort utilized its signature-based detection to pinpoint known ransomware signatures and send alerts when it detected unusual network traffic. It was set up for both inline and passive monitoring, allowing for real-time enforcement as well as post-event analysis. The findings from Snort were cross-checked with Zeek's results to create a solid malware detection process.

3.3.3. OpenEDR:

OpenEDR was deployed on all endpoints in both testing environments. Its job was to keep an eye on file system changes, process creation, and network connections to spot any ransomware-like activity. OpenEDR was programmed to automatically contain threats, isolating infected nodes and shutting down suspicious processes. The detailed logs it generated offered valuable insights into the mean time to detection (MTTD) and mean time to response (MTTR) for ransomware incidents.

3.3.4. Data Collection

Data was collected across multiple iterations of each simulation scenario. Metrics were recorded for:

i. The percentage of ransomware attempts that were detected and contained.
ii. The speed of lateral movement (measured by the number of hops per minute and the delays caused by access controls).
iii. Encryption delay measurements, which tracked the time from when file encryption started to when effective defense measures kicked in.
iv. The overall effectiveness of individual defense layers compared to the comprehensive, layered defense model.

To maintain consistency and reliability, we ran each simulation scenario multiple times, with at least 50 iterations for every attack vector. We made sure to randomize parameters like network latency, load conditions, and endpoint configurations within realistic limits. We calibrated the detection thresholds using historical network data sourced from previous academic studies and industry reports. Additionally, we drew insights from real-world ransomware case studies published in recent academic journals to shape our understanding of attack behaviors and measurement parameters. Throughout the data collection phase, we conducted regular quality assurance checks. These checks involved correlation tests across Zeek, Snort, and OpenEDR logs to ensure we minimized false positives and accurately captured actual attack activities. Our approach aligns with the defense-in-depth principles advocated by NIST and CISA, highlighting the significance of ongoing testing, continuous monitoring, and integrated threat intelligence.

4. Results

The simulation experiments provided us with both detailed quantitative and qualitative insights into how effective the layered defense model is at reducing ransomware attacks in ICS and healthcare networks. Our findings highlight three main areas: (1) how each individual defensive layer stacks up against the overall layered defense model, (2) the numbers related to lateral movement and delays in encryption, and (3) a side-by-side comparison of different attack scenarios and how well each security layer holds up. Let's dive into these findings in the sections that follow.

4.1. Impact of Individual Layers vs. the Full Model

Our thorough analysis revealed that while each security layer offers some level of protection against specific attack methods, the real magic happens when all layers work together, resulting in a much higher success rate for mitigating ransomware. Here's a quick summary of our key findings:

4.1.1. Individual Layer Effectiveness

1. Network Segmentation:

The segmentation strategy alone managed to cut down the ability of ransomware to spread laterally by about 60–70% in both environments. By creating isolated critical network zones, segmentation limited the number of accessible endpoints, making it tougher for attackers to breach multiple barriers. This effect was especially noticeable in the ICS testbed, where operational networks are particularly sensitive to lateral movement.

2. Endpoint Detection and Response (EDR):

OpenEDR was able to detect and contain around 75–80% of ransomware incidents when it was working on its own. Its quick identification of unusual file activities and process executions allowed for the rapid isolation of infected endpoints. However, in cases where the ransomware was particularly advanced, some initial file changes occurred before the EDR could respond, underscoring the need for additional protective measures.

3. Access Control:

Implementing strict access control measures led to a remarkable 65–70% reduction in unauthorized lateral movements. When we simulated scenarios involving improper credential

use or unauthorized access attempts, the RBAC and MFA protocols sprang into action right away, effectively limiting the movement of potential adversaries. While access control didn't directly catch ransomware encryption, it played a crucial role in restricting possible pathways for propagation.

4. Backups:

Although backups can't stop an attack from happening, our tests showed that having offline and immutably stored backups guarantees 100% data recoverability. The presence of these backups allowed for effective restoration, resulting in almost no risk of data loss. We measured backup effectiveness by looking at restoration times and data integrity metrics after simulating encryption events.

5. Behavioral Analytics:

The behavioral analytics layer, driven by machine learning algorithms, successfully flagged around 80–85% of anomalous activities triggered by ransomware before full encryption took place. By examining deviations from normal operations, the system provided early warning signals that, when combined with EDR responses, significantly reduced the overall impact of attacks. This layer was especially adept at detecting coordinated and subtle changes in system behavior that often preceded ransomware execution.

4.1.2. Full Model Impact

When integrated, the full layered defense model demonstrated an overall mitigation rate exceeding 90% across all simulated scenarios. The interactions between layers ensured that even if one defense was briefly bypassed, subsequent layers could contain or remediate the threat. Key findings include:

i. Enhanced Containment:

By combining network segmentation with access control, we effectively limited lateral movement, essentially "boxing in" any potential attacker to a small section of the network. Thanks to quick detection by EDR and behavioral analytics, alerts were generated rapidly, which helped shrink the time frame for ransomware to carry out its full encryption routines.

ii. Rapid Response and Recovery:

In instances where ransomware did manage to kick off file encryption, the backup layer was there to offer immediate recovery options. This redundancy played a crucial role in minimizing data loss and keeping operations running smoothly.

iii. Integrated Alert Correlation:

The simultaneous data streams from Zeek, Snort, and OpenEDR enabled the security team to connect alerts across the entire system. This comprehensive perspective enhanced the accuracy of threat detection and cut down on false positives, leading to a more efficient incident response. These insights highlight that layered security strategies, as recommended by NIST and CISA, are far more effective than relying on isolated defensive measures. They provide multiple, redundant lines of defense that work together to lower risk.

4.2. Lateral Movement and Encryption Delay Measurements

A critical measure of ransomware mitigation effectiveness is the ability to slow down or completely halt lateral movement and to introduce delays in the ransomware encryption process. Our experiments provided the following key metrics:

4.2.1. Lateral Movement

In a network lacking segmentation or access control, we observed simulated ransomware moving between systems in an average of about 15 minutes. Attackers could easily use automated scripts to navigate laterally with little resistance. However, once we enforced network segmentation, that movement time stretched to an average of 8 minutes. The segmentation layer forced attackers to deal with multiple firewalls and DMZ configurations, which significantly slowed their progress. Implementing strict RBAC and MFA protocols further increased lateral movement time to around 10 minutes. The need to validate credentials and the closure of communication channels made it tougher for attackers to pivot from one network segment to another. With all layers functioning together, lateral movement faced considerable obstacles. In our most detailed simulation, the combined effects of network segmentation, strong access control, and real-time alerting pushed lateral movement time to over 20 minutes—a delay that's statistically significant. This extra time is crucial for incident response teams to spot and neutralize ransomware before it can spread further.

4.2.2. Encryption Delay

Without a layered approach, the ransomware we simulated would usually kick off its encryption operations within about 5 minutes after the initial breach. When we relied solely on the EDR layer, that encryption process was pushed back by roughly 15 minutes on average. However, just depending on EDR didn't guarantee that encryption wouldn't happen if the initial detection took too long. By integrating multiple layers—especially the early warnings from behavioral analytics and the safety net of network segmentation—we managed to delay ransomware encryption well past the critical point. In some cases, the start of encryption was postponed by as much as 45 minutes. This significant delay provided enough time for automated rollback systems and manual interventions to step in and halt further encryption, helping to maintain data integrity and keep operations running smoothly. Our quantitative analysis of lateral movement and encryption delays has clearly shown that a comprehensive layered defense model significantly boosts response times and slows down the spread of ransomware. These added delays not only hinder the attacker but also give network defenders vital extra time to pinpoint issues and initiate recovery efforts.

5. Discussion and Recommendation

5.1. Discussion

The findings from our simulated experiments in both industrial control systems (ICS) and healthcare networks highlight a key principle: layering security controls creates more resilient systems than relying on a single solution. While many cybersecurity strategies tend to focus on preventing the initial infection, a layered defense is better viewed as a multi-faceted approach that enhances both prevention and resilience. Here, resilience means an organization's ability not just to stop ransomware from executing its harmful payload but also to recover effectively from any potential breach. By incorporating network segmentation, endpoint detection and response (EDR), strong access controls, backup solutions, and behavioral analytics,

organizations can build a solid security framework that significantly slows down lateral movement and delays encryption long enough for effective intervention to take place.

Layering boosts resilience by ensuring that if one control is bypassed, others will still catch the threat and limit further damage. For example, even if an attacker manages to slip past access control measures and gain unauthorized access to the network, EDR systems can quickly spot unusual activities and kick off quarantine procedures. Backups act as a safety net, allowing for the restoration of critical data if ransomware encrypts files before they can be detected. Behavioral analytics helps flag abnormal patterns early on, giving security teams a chance to respond before a full-blown compromise happens. This defense-in-depth strategy—endorsed by both NIST and CISA—focuses not just on prevention but also on ensuring business continuity in the event of a successful breach (NIST 2025; CISA 2022).

One interesting point to note is how resilience from layered defenses shows up in the measurable delays in lateral movement and the start of encryption. When all the layers work together, lateral movement was held up for more than 20 minutes compared to the usual operation, and the initiation of ransomware encryption was delayed by as much as 45 minutes. This delay is crucial because even a few extra minutes can give incident response teams the vital time they need to isolate compromised endpoints and recover affected data. These delays are especially important in critical sectors like energy and healthcare, where rapid damage escalation can seriously impact public safety and service continuity. The experiments show that the combination of segmentation (which limits unauthorized movements) and EDR (which offers real-time threat monitoring) creates a stronger defense that significantly lowers the risk of disastrous outcomes.

Additionally, operational resilience gets a boost from integrating backups and behavioral analytics. Backups, especially when kept offline and in an unchangeable state, ensure that even if detection and recovery systems fail temporarily, data integrity remains intact. This aspect of resilience is crucial in healthcare, where data loss could disrupt patient care, and in energy systems, where maintaining operations is essential. Behavioral analytics continuously monitors network traffic and user behavior, providing early alerts for potential ransomware activities that traditional signature-based tool might overlook. As a result, organizations not only lower the chances of an incident but also improve their ability to bounce back quickly if one does happen. This comprehensive resilience is what fuels the ongoing development of layered defense strategies in cybersecurity.

Another key point worth discussing is how the layered model adjusts to various network environments. Both ICS and healthcare networks gain from a layered defense, but specific factors in each sector shape how much focus is given to different layers. In ICS settings, network segmentation is crucial because operational technology systems need strict isolation to prevent disruptions in physical processes. Conversely, in healthcare, the fast-paced and interconnected nature of electronic health records and real-time monitoring systems makes quick detection and response—supported by EDR and behavioral analytics—much more vital. These subtle distinctions highlight that while the overall layered approach is beneficial across the board, the specific setup of defenses must be customized to meet the unique operational needs and risk profiles of each sector.

Lastly, it's worth mentioning that the layered defense strategy not only helps stop the spread of ransomware but also fosters a culture of proactive security. By consistently challenging and

testing each layer through simulated attacks, organizations can continuously enhance their defenses. This ongoing cycle of testing, learning, and adapting is essential in a time when cyber threats are always changing. The resilience we observed in our experiments showcases the advantages of embracing an adaptive and multi-layered security approach that is ready for both known and emerging threats.

Table 1: Attack Scenario vs. Layer Effectiveness.

Attack Scenario	Network segmentation	Endpoint Detection Response	Access Control	Backups	Behavioral Analytics	Overall Effectiveness
Unauthorized access	High	Medium	High	Low	Medium	High
Ransomware Execution	Medium	High	Medium	High	High	High
Data Encryption	Low	High	Medium	High	High	High

Table 1 compares baseline attack scenarios with the effectiveness ratings (High, Medium, Low) for each layer, and then provides an overall effectiveness rating when the full model is implemented

5.2. Recommendations

Based on the results and the discussion above, we propose three key recommendations to bolster the resilience and security of energy and healthcare sectors against ransomware attacks: the implementation of Zero Trust architectures for OT and IT convergence, the adoption of offline backups with air gaps, and the development of sector-specific response playbooks.

5.2.1. Zero Trust for OT/IT

In today's fast-paced world, relying on traditional perimeter-based security just doesn't cut it anymore, especially as IT and OT systems start to blend together. Enter Zero Trust architecture (ZTA), a powerful model designed to tackle these modern challenges head-on. The essence of Zero Trust is simple: "never trust, always verify." This principle is crucial when sensitive operational technology meets traditional IT networks. Given that malicious actors could already be lurking within the network, it's essential to verify every access request thoroughly before granting it.

When it comes to implementing a Zero Trust framework in industrial control systems (ICS) and healthcare networks, it's all about strict identity verification, micro-segmentation, and continuous authentication at every level. For instance, every user or device trying to gain access—even those already inside the internal network—needs to be authenticated and authorized before they can interact with critical systems. Plus, Zero Trust can take into account

contextual elements like device health, geolocation, and user behavior to dynamically adjust access privileges. This strategy significantly reduces the chances for attackers to move laterally within the network and ensures that any compromised components are quickly and effectively isolated. Recent efforts by CISA and NIST are paving the way for this shift. The CISA Zero Trust Maturity Model lays out clear guidelines for implementing Zero Trust in federal networks, and these same principles can be adapted for OT environments.

Additionally, research from the Software Engineering Institute underscores the advantages of Zero Trust in reducing risks specific to OT systems, which often deal with legacy components and unique operational needs (Benestelli & B, 2022). Organizations are therefore urged to assess their current security frameworks and gradually move towards a Zero Trust model that seamlessly integrates both IT and OT elements, ensuring that every access decision is contextualized and based on the least-privilege principle.

5.2.2. Offline Backups with Air Gaps

While prevention is crucial, resilience also hinges on how quickly we can bounce back from an incident. One of the key steps to ensure data integrity and keep operations running smoothly is to have offline backups with air gaps. An air gap backup strategy means keeping a completely isolated copy of critical data that's either physically or logically separated from the main network. This separation helps block ransomware from accessing and encrypting backup data, a common tactic used to pressure organizations into paying ransoms.

Offline backups with air gaps are vital in sectors like energy and healthcare, where losing data can have serious repercussions. In healthcare, losing patient records can directly affect patient care, while in energy networks, losing operational data can result in outages and even physical damage. An air gap strategy guarantees that there's always a dependable fallback option. It's important to regularly update and test these backups to make sure recovery procedures are both effective and efficient.

CISA and HHS advisories highlight the necessity of an offline backup strategy as part of a comprehensive incident response plan (CISA MS-ISAC, 2025; HHS, 2025). Technology providers like Veritas (2023) have also emphasized the essential role of air gap backups in protecting against ransomware attacks. This recommendation involves not just implementing hardware solutions but also setting up strict policies for data transfer to keep the backup environment isolated. Regular drills and testing of offline backup systems are crucial to ensure that data restoration processes can be carried out within acceptable recovery time objectives (RTOs).

5.2.3. Sector-Specific Response Playbooks

When it comes to incident response, the energy and healthcare sectors face unique challenges, making a one-size-fits-all approach simply inadequate. Organizations need to craft specific response playbooks that lay out customized protocols for tackling ransomware incidents. These sector-specific playbooks should reflect the distinct operational processes, regulatory demands, and threat environments that each sector encounters. For instance, an Industrial Control Systems (ICS) playbook for the energy sector must tackle issues related to outdated control systems, the importance of maintaining continuous operations, and the urgent need to quickly isolate infected nodes to avert physical damage. On the flip side, a healthcare playbook should

prioritize safeguarding patient data, adhering to privacy laws, and ensuring that medical services remain intact, even during cyberattacks.

Recent insights from CISA, NIST, and MITRE ICS highlight the importance of having clearly defined response playbooks that encompass the full range of incident response—from the initial detection and containment to recovery and post-incident analysis. These playbooks should be regularly updated to incorporate new threat intelligence and lessons learned from both simulated drills and actual incidents. Additionally, they need to include thorough communication protocols and strategies for engaging stakeholders, ensuring that both technical and non-technical staffs are ready to respond to emergencies. In healthcare, for example, playbooks should establish clear communication channels with clinical teams, regulatory agencies, and public health organizations, while energy sector playbooks should address potential physical safety risks (NIST, 2025). To truly make the playbooks effective, they need to be backed up by regular training sessions, simulations, and tabletop exercises. These activities help organizations spot any weaknesses in their response strategies and enhance teamwork across different departments. By tailoring response playbooks to fit the unique challenges of each sector, organizations can ensure they respond to ransomware incidents more quickly and efficiently, ultimately minimizing downtime and reducing overall risk.

6. Conclusion

The increasing sophistication and frequency of ransomware attacks underscore the urgency of robust defense strategies, particularly in critical sectors such as energy and healthcare. This paper has presented a multi-layered defense-in-depth approach tailored to these industries, integrating advanced cybersecurity frameworks and real-world case studies to bolster resilience. Our findings demonstrate that a combination of network segmentation, endpoint detection and response (EDR), behavioral analytics, offline backups, access controls, and incident response playbooks significantly enhances detection, containment, and recovery capabilities.

One of the key advantages of this approach is its adaptability across different operational environments. By leveraging established cybersecurity models such as NIST and MITRE ATT&CK for ICS, organizations can systematically strengthen their defense mechanisms against evolving ransomware threats. Additionally, the results of our simulated infection scenarios validate the effectiveness of each defense layer, offering practical insights for cybersecurity teams.

However, this model is not without limitations. The implementation of a comprehensive defense framework requires significant investment in resources, technical expertise, and ongoing system upgrades. Legacy infrastructure in healthcare and energy sectors remains a challenge, as outdated technologies may hinder the seamless integration of advanced security measures. Furthermore, while the defense-in-depth strategy improves overall ransomware mitigation, it does not entirely eliminate the risk, necessitating continuous adaptation to emerging attack vectors.

The applications of this research extend beyond ransomware defense; the principles outlined can be adapted for broader cybersecurity risk management, improving resilience against other cyber threats. Future studies could refine this framework by incorporating artificial intelligence-driven threat detection and deeper analysis of human factors influencing

cybersecurity adoption. By advancing this defense strategy, organizations can fortify their critical services, safeguarding infrastructure, operations, and lives from cyber disruptions.

Acknowledgements

We express our sincere gratitude to the experts and collaborators who have significantly contributed to the development of this research paper. Their insights, guidance, and unwavering support were instrumental in shaping this work and enhancing its academic quality. We would like to particularly acknowledge the contributions of the following authors:

1st Author: Sarah Mavire, for leading the research, coordinating the project, and drafting the manuscript.

2nd Author: Kumbirai Bernard Muhwati, for his critical analysis, data validation, and valuable inputs throughout the study.

3rd Author: Naga Kota, for his technical expertise in implementing the proposed methodology and assisting with data processing.

4th Author: Joy Adesina Awoleye, for his support in reviewing related literature, data compilation, and contributing to the analysis.

We also extend our gratitude to the faculty and staff of Yeshiva University, whose resources and encouragement greatly facilitated this research. Furthermore, we appreciate the collaborative spirit and dedication shown by all contributors, whose collective efforts made this work possible.

References

1) AADA (2023). AADA Whitepaper. September 2023. Retrieved from: https://www.aada.org/ransomware-lifecycle.
2) B. &. K. D. Benestelli, (July 18, 2022). IT, OT, and ZT: Implementing Zero Trust in Industrial Control Systems. Carnegie Mellon University, Software Engineering Institute's Insights.
3) Bing, C., & Kelly, S. (May 8, 2021). Cyber Attack Shuts Down Top U.S. Fuel Pipeline Network. Reuters.
4) Caviglione L. (2021). Cyber reconnaissance techniques. Communications of the ACM, 64(3), 86-95, 2021.
5) Chappell, B., & Neuman, S. (December 19, 2017). U.S. Says North Korea 'Directly Responsible' For WannaCry Ransomware Attack. NPR. Retrieved 2 May, 2025.
6) CISA (May 2018). Cybersecurity and Infrastructure Security Agency. Available: https://www.cisa.gov/ransomware. [Accessed 6 May 2035].
7) Cybersecurity and Infrastructure Security Agency (2020) CISA MS-ISAC Ransomware Guide. Retrieved: https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware_Guide_S508C. 4 May 2025.
8) Cybersecurity and Infrastructure Security Agency (2021). Conti Ransomware. 1-2, 7 May 2021.
9) Cybersecurity and Infrastructure Security Agency (2021). Federal Government Cybersecurity Incident and Vulnerability Response Playbooks. CISA.

10) Cybersecurity and Infrastructure Security Agency (2022). Layering network security segmentation. CISA.
11) Cybersecurity and Infrastructure Security Agency (2023). Zero Trust Maturity Model Version 2.0. 2023. Available: https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pd. [Accessed 10 May 2025].
12) Cybersecurity and Infrastructure Security Agency (2025). Indicators Associated with WannaCry Ransomware," CISA.
13) Department of Health and Human Service (2020). Ryuk Update. 3-5, May 10 2020.
14) Department of Health and Human Services (2021). Prepare, React, and Recover from Ransomware. Department of Health and Human Services.
15) Doe S. K. (2023). Evaluating access control effectiveness against ransomware lateral movement. Journal of Computers & Security, 101, 55-65.
16) Fisher, B., Souppaya, M., Barker, W., & Scarfone, K. (2022),. Ransomware risk management: A cybersecurity framework profile. NIST, 8374(1), 15–20.
17) J. B. Adelusi (2023) Network Segmentation Approaches for Improved Security in Digital Systems. ResearchGate.
18) Jack Beerman; David Berent; Zach Falter; Suman Bhunia (May 1–4, 2023). A Review of Colonial Pipeline Ransomware Attack. 2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW). Bangalore, India: IEEE. doi:10.1109/CCGridW59191.2023.00017. Retrieved May 27, 2025.
19) Johnston W. C. (2023). Continuous monitoring and advanced behavioral analytics for lateral movement detection in enterprise networks. IEEE Transactions on Information Forensics and Security, 18(5), 1452-1465.
20) Jones C. R. (2023). Operationalizing the MITRE ATT&CK® for ICS: Lessons from energy and healthcare sectors. Journal of Cybersecurity Practice, 18(2), 30-34.
21) Jones, D., Miller, T., & Carter, R., (2023). The evolution of ransomware: From opportunistic attacks to organized cyber extortion. Journal of Cyber Threat Studies, 18(2), 12-27.
22) Krombholz W. E. et al. (2015). Advanced social engineering attacks. Journal of Information Security and Applications, 22, 113-122.
23) Kumar R. & Ramlie R (2020). Enhancing ICS security: Integrating the MITRE ATT&CK® framework with layered defense strategies. Journal of Industrial Cybersecurity, 20(8), 45-48.
24) Kumar R. & Ramlie R (2023). Double Extortion In Ransomware Attacks: Escalating Pressures In Digital Extortion. Journal of Cyber Threat Studies, 20(3), 40-57.
25) Kumar R. & Ramlie R 2021, Anatomy of Ransomware: Attack Stages, Patterns and Handling Techniques. Advances in Intelligent Systems and Computing, vol. 1321, 205-214.
26) Marquardt, A., Perez, E., & Cohen, Z. (June 7, 2021). First on CNN: US recovers millions in cryptocurrency paid to Colonial Pipeline ransomware hackers | CNN Politics. CNN. Retrieved May 16, 2025.
27) MITRE, "MITRE ATT&CK® for Industrial Control Systems (ICS)," MITRE Corporation, 6 May 2025. [Online]. Available: https://attack.mitre.org/mitigations/M0930/. [Accessed 6 May 2025].

28) N. Särökaari, Phishing attacks and mitigation tactics, University of Jyväskylä, Finland.: Master's Thesis, 2020.
29) National Institute of Standards and Technology, "Mapping NIST SP 800-53 Controls for Integrated Cyber Defense," NIST, 2025.
30) National Institute of Standards and Technology, The NIST Cybersecurity Framework (CSF) 2.0, U.S. Department of Commerce, 2024.
31) National Institute of Standards and Technology., "Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile [NIST SP 800-61r3]," NIST, 2025.
32) NIST (2022) "Guide to a Secure Enterprise Network Landscape (NIST SP 800-215)," 2022. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-215.pdf>. [Accessed 11 May 2025].
33) QNAP, "QNAP," 2022. [Online]. Available: https://www.qnap.com/en/security-advisory/qsa-22-02. [Accessed 6 May 2025].
34) Sanger, David; Krauss, Clifford; Perlroth, Nicole (May 8, 2021). "Cyberattack Forces a Shutdown of a Top U.S. Pipeline". New York Times. Archived from the original on May 8, 2021. Retrieved May 8, 2021.
35) Segers, Grace (May 8, 2021). Cyberattack Prompts Major Pipeline Operator to Halt Operations. CBS News. Retrieved May 8, 2025.
36) Smith W (2022). Ransomware variants: Cryptographic and lockdown mechanisms in modern cyberattacks. International Journal of Cybersecurity, 12(1) 30-45.
37) TechCrunch (2019). Two Years after Wannacry, A Million Computers Remain At Risk. TechCrunch. 12 May 2019.
38) Thomas, A., Grove, T., & Gross, J. (13 May 2017). More Cyberattack Victims Emerge as Agencies Search for Clues. The Wall Street Journal. ISSN 0099-9660. Retrieved May 14 2025.
39) U.S. Department of Health and Human Service (2023). Secure health data: Strengthening offline backups to prevent ransomware impact. January 23 2023. Available: <https://www.hhs.gov/about/news/2023/01/secure-health-data.html>. [Accessed 7 May 2025].
40) Ungoed-Thomas, J., Henry, R., & Gadher, D. (14 May 2017). Cyber-attack guides promoted on YouTube. The Sunday Times. Retrieved May 14, 2025
41) Veritas (2025). The Comprehensive Ransomware Guide with Veritas. 14-16.
42) Verizon Business. (2024). 2024 Data Breach Investigations Report (17th ed.) Basking Ridge, NJ: Verizon Business. https://www.verizon.com/business/resources/T3f3/reports/2024-dbir-data-breach-investigations-report.pdf. 5-7
43) Walsh, Joe. Ransomware Attack Shuts Down Massive East Coast Gasoline Pipeline. Forbes. Retrieved May 16, 2025.
44) Zscaler ThreatLabZ, "Ransomware delivered using RDP brute-force attack," 2021. Accessed May 6, 2025.
45) Zscaler, Inc. (2024). Zscaler ThreatLabz 2024 Ransomware Report. San Jose, CA: Zscaler, Inc. Retrieved from https://assets.starlinkme.net/gitex-vendor-assets/zscaler/threatlabz-ransomware-report.pdf. 3–4