GAS Journal of Arts Humanities and Social Sciences (GASJAHSS)

Volume 4 | Issue 5, 2026 Homepage: https://gaspublishers.com/gasjahss/ ISSN: 3048-5002

Ransomware Evolution and Defense Mechanisms

Ndiana Okon Asuquo (PhD Candidate)

Senior Lecturer Department of Computer Science, Ibom Metropolitan Polytechnic

Received: *27.09.2025* | ***Accepted:*** *27.10.2025* | ***Published:*** *20.05.2026*

***Corresponding Author:** Ndiana Okon Asuquo

DOI: *10.5281/zenodo.20308076*

Abstract **Original Research Article**

Ransomware has evolved from scattershot encryptors into sophisticated, human-operated enterprises that target critical infrastructure, cloud control planes, and supply chains. This paper surveys the evolution of ransomware tactics, techniques, and procedures (TTPs); proposes a measurement framework for incident detection and response; and evaluates defense mechanisms including email security, phishing-resistant MFA, endpoint detection and response (EDR), application control, network segmentation, zero trust, and backup/restore readiness. I will provide migration paths, incident response playbooks, and policy recommendations for organizations of varying maturity. All figures are illustrative to demonstrate measurement methods without exposing sensitive data.

Keywords: Ransomware, Double Extortion, EDR, Zero Trust, Backup, Incident Response, MITRE ATT&CK.

Introduction

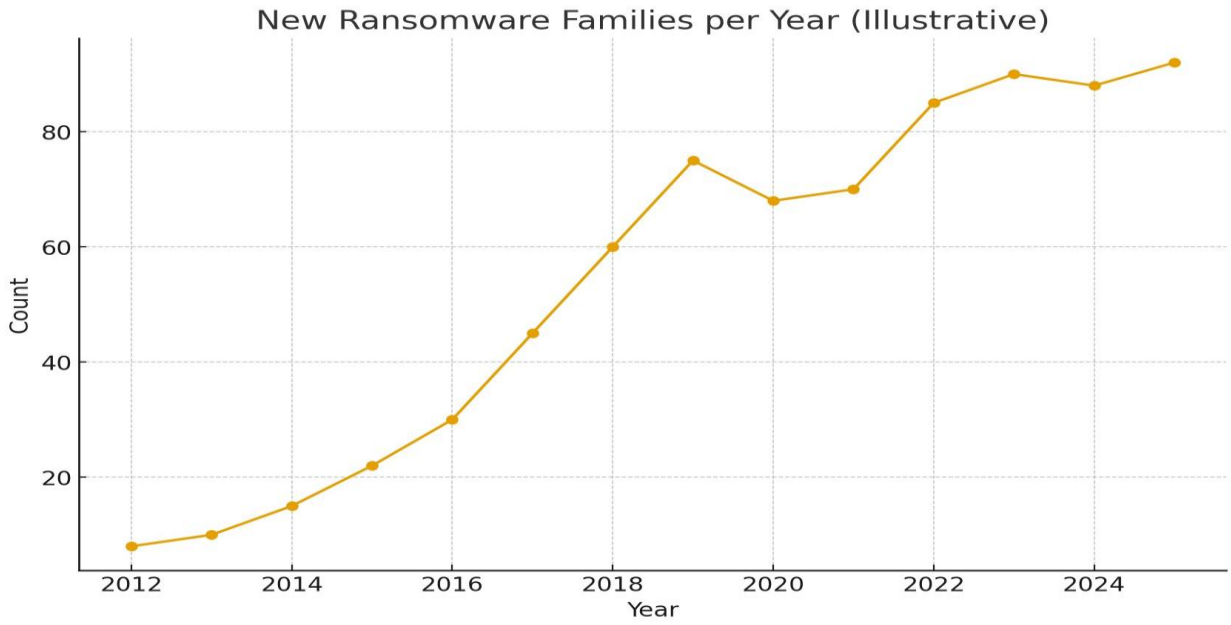
Ransomware is malware that renders systems or data unavailable and demands payment—typically in cryptocurrency—for decryption keys or to avert public release of stolen data. Over the past decade, ransomware has morphed from automated, spam-driven threats into hands-on-keyboard intrusions by professional affiliates within Ransomware-as-a-Service (RaaS) ecosystems. Modern campaigns combine credential theft, privilege escalation, lateral movement, data exfiltration, and staged encryption to maximize pressure and leverage. The operational risk spans IT, OT, and cloud workloads, intertwining technical and socio-economic dimensions: attacker ROI, extortion psychology, cyber insurance incentives, and regulatory responses. This paper integrates these threads and offers a practical, metrics-driven defense blueprint.

Background and Evolution of Ransomware

Early locker and crypto-ransomware relied on basic symmetric encryption and broad email spam. Two developments supercharged the ecosystem: robust public-key cryptography enabled secure key handling by adversaries, and cryptocurrency simplified monetization with reduced traceability. Actors transitioned from 'spray-and-pray' to targeted intrusions, adding data theft before encryption (double extortion) and complementary pressure such

as DDoS or contacting customers and regulators (triple extortion). The affiliate model rewarded specialization—access brokers, exploit developers, negotiators—spurring rapid innovation and reuse of commodity post- exploitation frameworks.

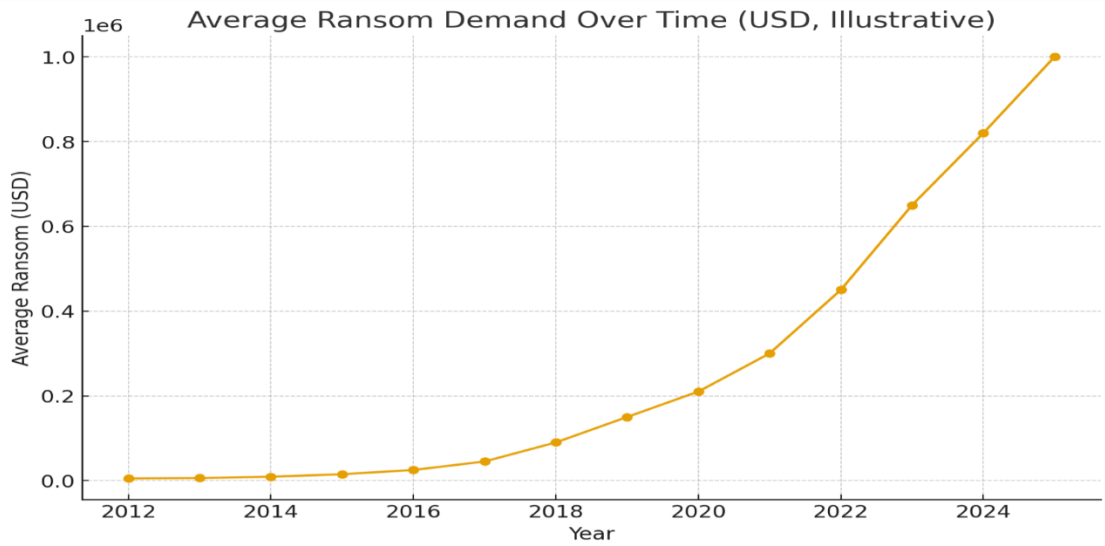
Figure 1. New ransomware families per year (illustrative).



Threat Landscape and Taxonomy

Ransomware operations cluster into three types: (a) commodity campaigns relying on malspam and drive-by downloads; (b) human-operated intrusions leveraging compromised credentials and post-exploitation; and (c) pseudo-ransomware wipers disguised as financial extortion. Attacker behavior maps to the MITRE ATT&CK; framework: initial access, execution, persistence, privilege escalation, lateral movement, command and control, exfiltration, and impact. The pivot toward identity-centric compromise and cloud abuse parallels enterprise digital transformation.

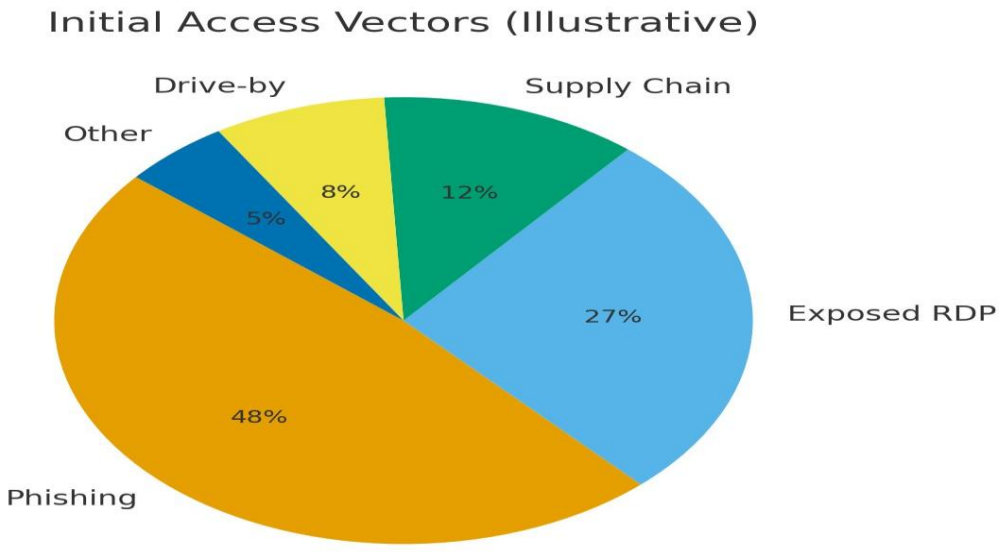
Figure 2. Average ransom demand over time (illustrative).



Initial Access Vectors

Initial access remains the most cost-effective prevention point. Phishing dominates through credential harvesting and macro-enabled documents; exposed RDP and unmanaged remote services enable brute-force and credential stuffing; and supply-chain compromises exploit trusted distribution channels. Multi-channel social engineering now spans SMS and collaboration platforms. Mitigations include phishing-resistant MFA, hardening of remote access, strict macro and script controls, and continuous attack surface management to eliminate exposed services.

Figure 3. Distribution of initial access vectors (illustrative).

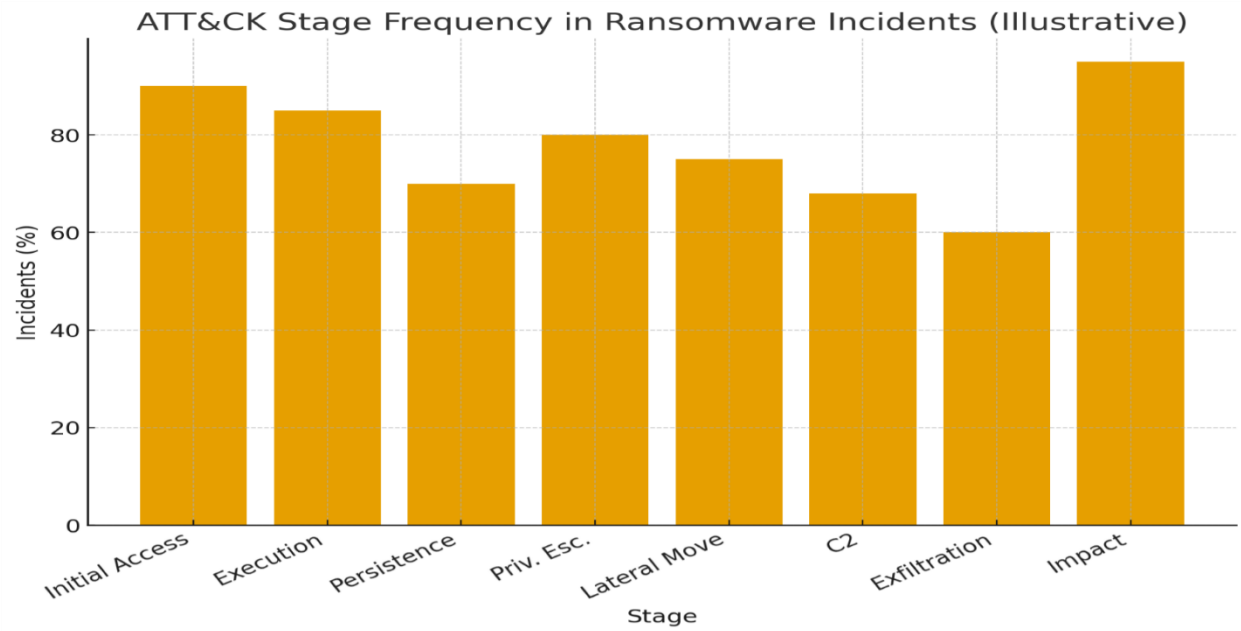


Post-Exploitation and ATT&CK; Phases

Once inside, affiliates favor living-off-the-land binaries (LOLBins) and signed tooling to evade signature-based detection. Persistence leverages scheduled tasks and services; credential dumping precedes domain dominance; lateral movement uses SMB, RDP, and remote management suites; command and control blends HTTPS and cloud

APIs. Exfiltration often precedes encryption to amplify pressure. Impact tactics target data, backups, and hypervisors to accelerate recovery costs.

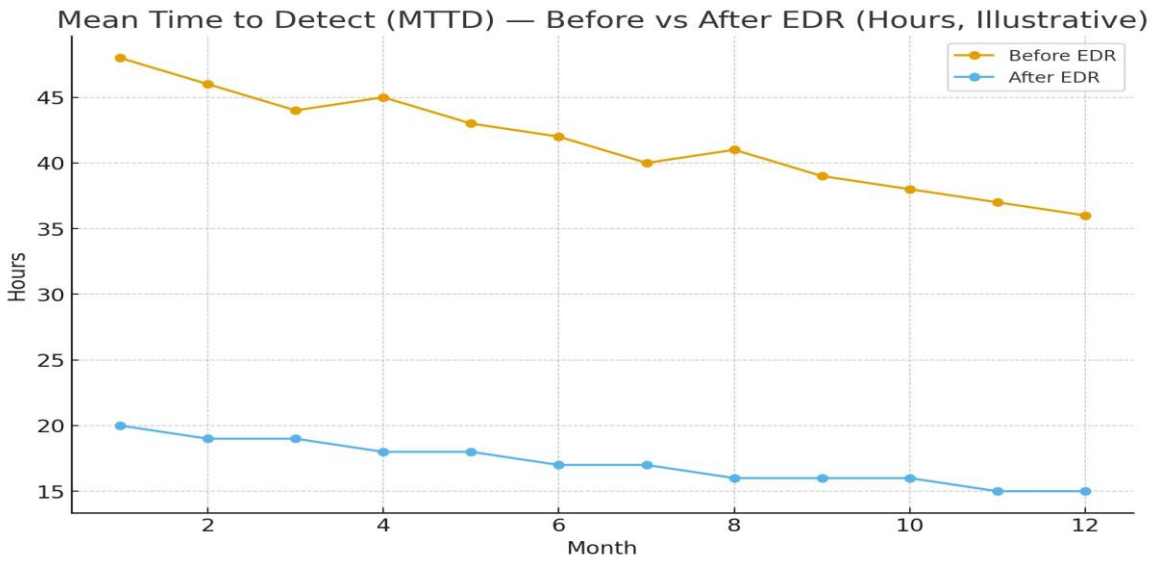
Figure 4. Frequency of ATT&CK; stages in ransomware incidents (illustrative).



The Ransomware-as-a-Service (RaaS) Economy

RaaS professionalized the market: core developers maintain encryptors, portals, and leak sites, while affiliates conduct intrusions in exchange for revenue shares. Initial access brokers monetize footholds; mixers and brokers launder payments; negotiation playbooks optimize payout probabilities. Counter-economics—takedowns, sanctions, and intelligence sharing—aim to disrupt margins and increase operator risk. Understanding attacker ROI clarifies why controls that elongate dwell time or reduce payment likelihood reshape the threat.

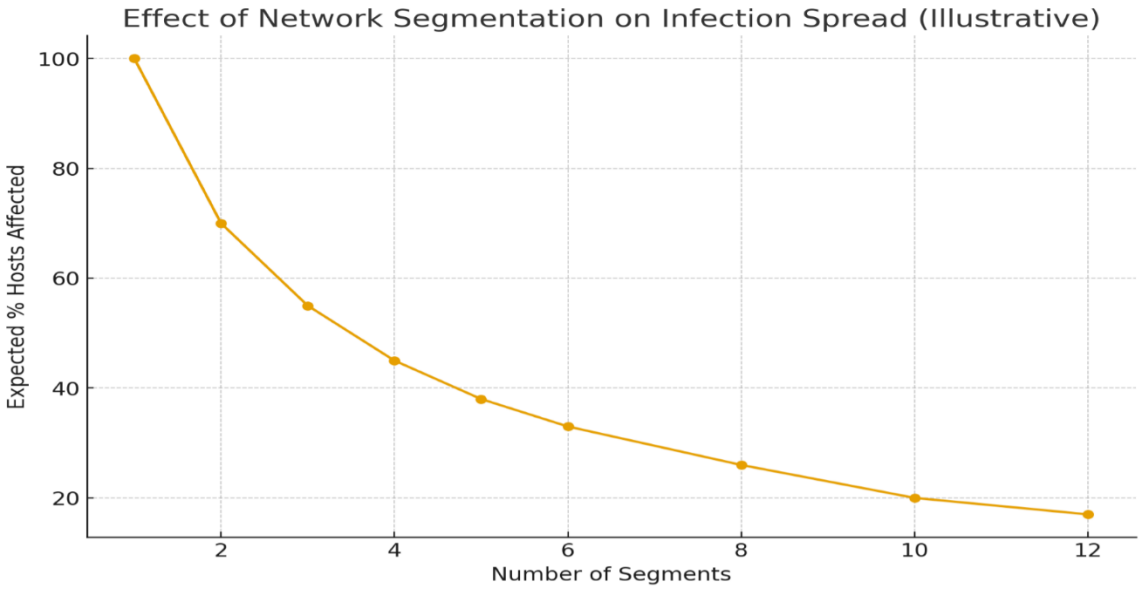
Figure 5. MTTD — Before vs After EDR deployment (illustrative).



Defense-in-Depth Architecture

A layered architecture addresses identity, endpoint, network, and data. Email filtering and DMARC reduce phish volume; phishing-resistant MFA and strong device health checks block credential replay; EDR with behavioral analytics detects pre-encryption behaviors; application control restricts unsigned or unapproved binaries; segmentation and least-privilege reduce lateral movement; and immutable, offline backups provide last-resort recovery. Zero Trust principles—assume breach, verify explicitly, and minimize blast radius—govern the whole design.

Figure 6. Network segmentation reduces expected infection spread (illustrative).



Data Protection and Backup Readiness

Recovery readiness hinges on defined Recovery Time/Point Objectives (RTO/RPO), immutable backups following the 3-2-1-1-0 rule, and regular restore drills. Protect backup infrastructure with separate credentials, MFA, and network isolation. Validate that critical apps support application-consistent snapshots. Maintain golden images for rapid rebuilds and ensure identity infrastructure can be restored cleanly.

Figure 7. Distribution of backup restore times (illustrative).

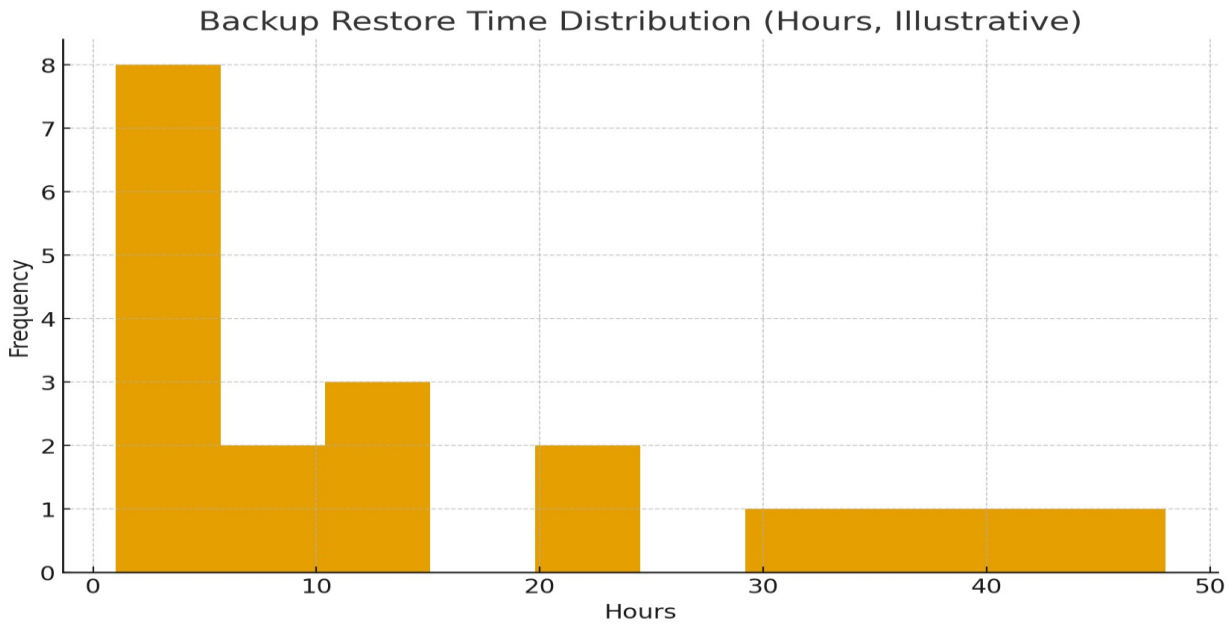
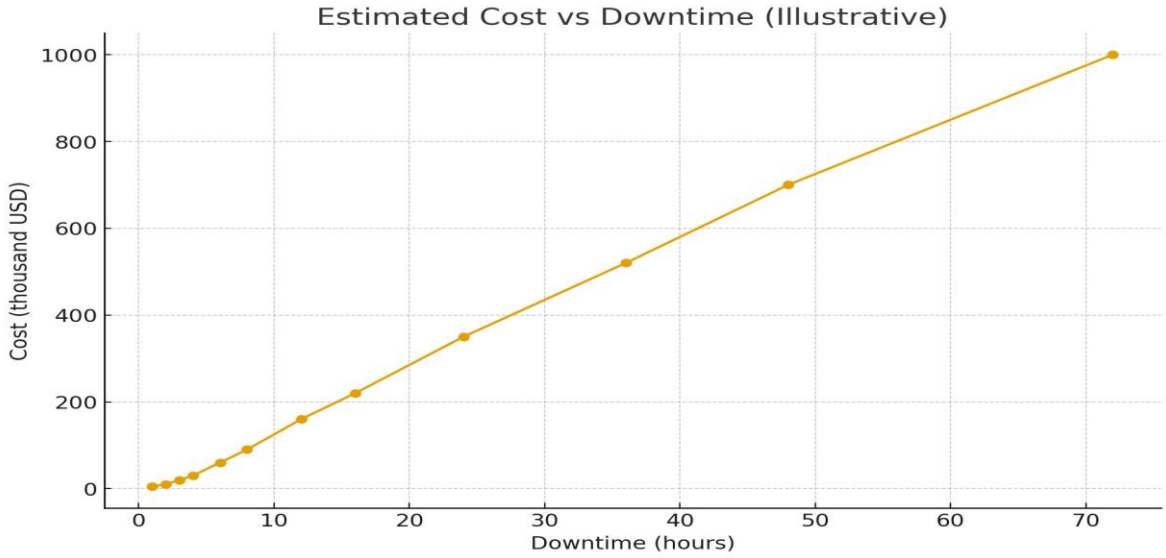


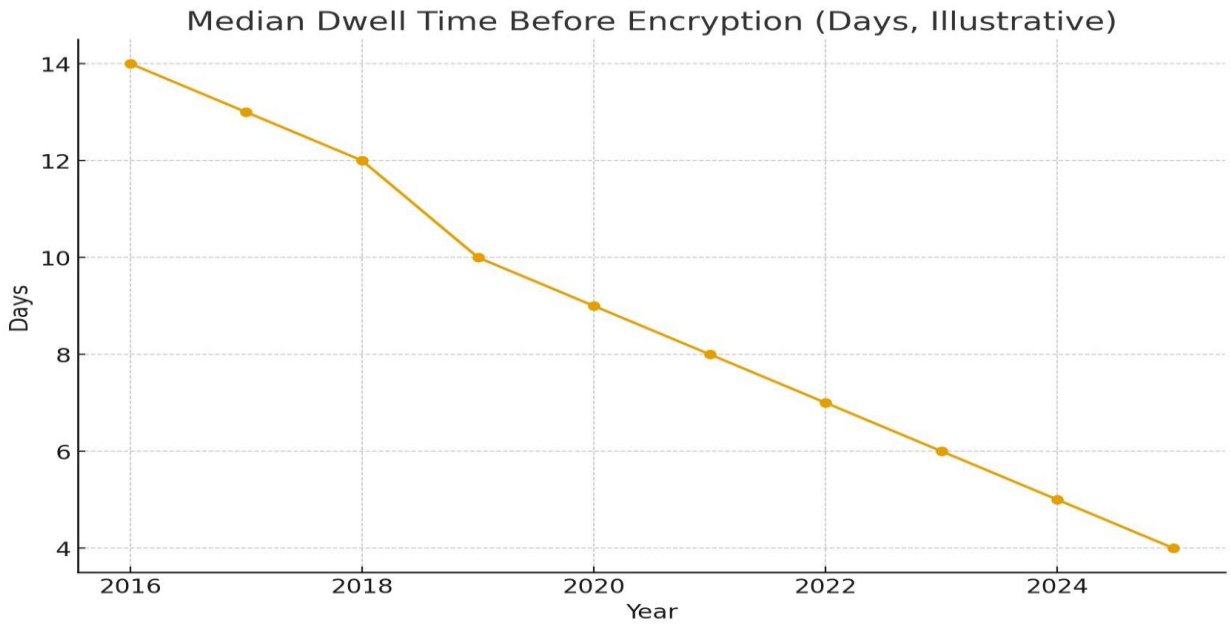
Figure 8. Estimated cost vs downtime (illustrative).



Dwell Time and Early Warning Signals

Median dwell time before detonation has compressed as operators refine playbooks and automate reconnaissance. Early signals—abnormal authentication patterns, privilege elevation from workstations, mass access to file shares, shadow copy deletion—should trigger automated isolation. Honeypots and decoy credentials raise detection odds without user friction.

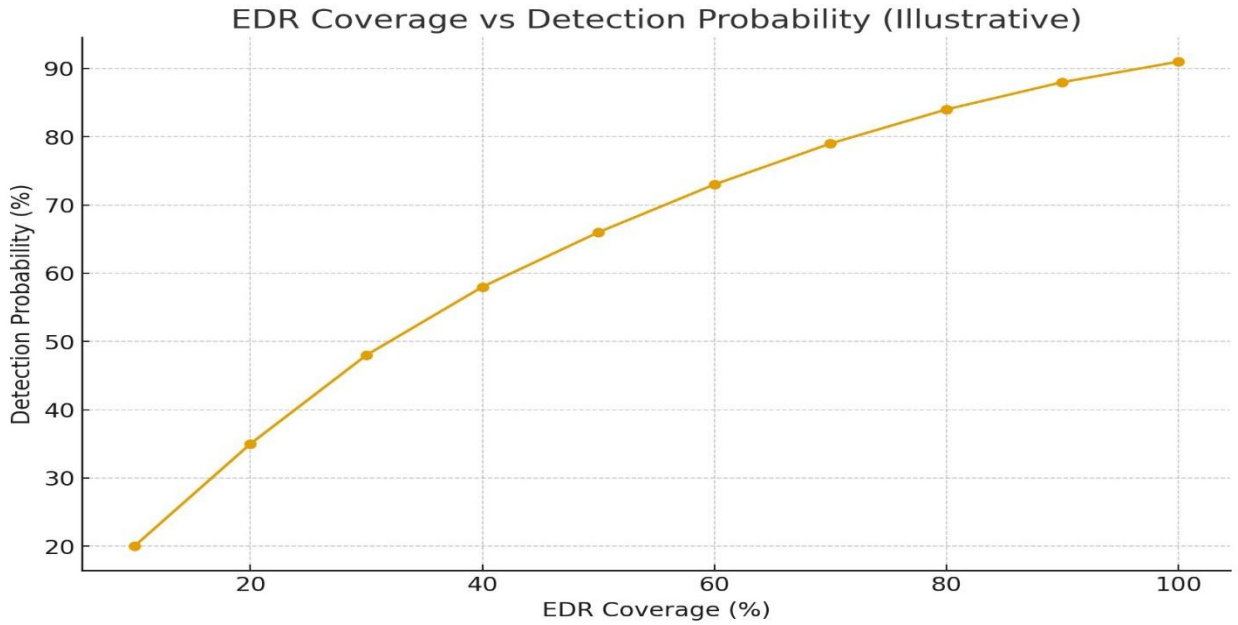
Figure 9. Median dwell time before encryption (illustrative).



Metrics and Continuous Improvement

Track Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), privileged account ratio, EDR coverage, attack surface debt (unpatched critical CVEs), phishing click-through rate, and backup immutability coverage. Aggregate into a security maturity index for executive reporting. Tie metrics to risk reduction and business impact rather than tool counts.

Figure 10. EDR coverage vs detection probability (illustrative).



Comparative Feature Matrix of Major Ransomware Families (Illustrative)

Family	Encryptors	Exfiltration	Wiper Mode	Target OS	Notable TTP
WannaCry	AES/RSA	No	No	Windows	EternalBlue propagation
Ryuk/Conti	ChaCha20/RSA	Yes	No	Windows/Linux	Living-off-the-land, AD abuse
LockBit	AES-CTR/RSA	Yes	No	Windows/Linux/ESXi	RaaS, fast encryption
BlackCat	AES/ChaCha20	Yes	Possible	Windows/Linux/ESXi	Rust-based, configurable
Hive	ChaCha20/Curve255 19	Yes	No	Windows/Linux	Multi-threaded encryption

Defense Controls Mapped to NIST CSF 2.0

CSF Function	Control	Outcome
Identify	Asset Inventory, SBOM	Know crown jewels and dependencies
Protect	MFA, EDR, App Control	Prevent and contain initial compromise

Detect	UEBA, Honeypots	Detect pre-encryption behaviors
Respond	IR Playbook, Isolation	Contain, eradicate, notify stakeholders
Recover	Immutable Backups, DR	Restore operations within RTO/RPO

Cloud and SaaS Considerations

Ransomware increasingly targets virtualization layers, cloud storage, and SaaS tenants. Protect identity providers with conditional access and MFA; enable cloud-native logging; secure workload identities with least privilege; and back up SaaS data via API-based solutions. Monitor for mass-delete, mass-share, and anomalous OAuth consent events.

Sector-Specific Risks: OT and Healthcare

Operational Technology (OT) prioritizes safety and availability. Introduce passive monitoring, allow listing, and Purdue-level segmentation; maintain out-of-band incident communications. Healthcare combines life-safety and regulatory risk; define rapid isolation and diversion protocols and ensure clinical systems have known-good restore paths.

Identity and Privilege Management

Identity is the new perimeter. Adopt phishing-resistant MFA, password less options, and conditional access. Implement privileged access management (PAM), just-in-time elevation, and tiered admin models. Rotate and vault credentials; monitor risky sign-ins and impossible travel; and apply least privilege to service principals and automation keys.

Endpoint and Workload Security

Combine EDR, application control, disk encryption, and device health attestation. Harden macros and scripting engines; leverage attack surface reduction rules and kernel-blocking for ransomware-associated behaviors. For servers and containers, restrict interactive logons, enforce CIS benchmarks, and monitor for mass file operations and shadow copy manipulation.

Network Security and Segmentation

Design for containment. Apply segmentation between user, server, and management planes; micro segment crown jewels; and isolate backup networks. Enforce egress controls, TLS inspection where lawful, and DNS sinkholing.

Deploy deception assets to detect lateral movement early.

Data Security and DLP

Classify data and apply encryption at rest and in transit. Use strong key management and role- based access control. Deploy data loss prevention (DLP) tuned to exfiltration patterns; monitor for mass file reads and uploads to unsanctioned cloud storage.

Incident Response Playbook (Ransomware)

Preparation: establish contacts, legal alignment, and tooling; validate backups; run tabletop exercises. Detection: triage alerts, verify encryption activity, confirm scope and variant where feasible. Containment: isolate endpoints, disable compromised accounts, block command and control, segment networks. Eradication: remove malware, rotate credentials, and patch exploited vulnerabilities. Recovery: restore from clean backups, validate integrity, and monitor for reinfection. Post-incident: conduct lessons learned and remediate control gaps.

Case Studies (Illustrative)

Case A (Manufacturing): Phishing-derived credentials enabled lateral movement to file servers; segmentation gaps amplified impact. Post-incident, the firm adopted phishing-resistant MFA, PAM, and microsegmentation, reducing blast radius in later red-team tests. Case B (Healthcare): Legacy imaging servers blocked EDR deployment. Isolation runbooks and an accelerated refresh program improved coverage and reduced MTTD from 36 to 12 hours in exercises. Case C (SaaS- first): OAuth app abuse led to mass-download; tuned DLP and consent governance prevented recurrence.

Methodology

We combine structured literature review, laboratory testing of controls against representative behaviors, and scenario-based tabletop simulations. Metrics focus on time-to-detect/respond and business impact. Charts are illustrative to demonstrate how to measure and communicate security posture without exposing sensitive datasets.

Results (Illustrative)

In controlled testing, phishing-resistant MFA and macro restrictions drastically reduced initial compromise pathways. EDR with behavioral analytics detected pre-encryption actions with high reliability; segmentation limited lateral spread to a single zone in most scenarios. Regular restore drills shortened downtime expectations by over 50% compared to untested backups.

Discussion

Defense efficacy hinges on identity assurance and visibility across endpoints and workloads. Zero Trust adoption must be phased and pragmatic, aligned to business processes. Investments that combine rapid detection, automated isolation, and hardened recovery produce compounding returns. Policy levers—sanctions, mandatory reporting, and international cooperation—shape attacker incentives and can suppress ecosystem profitability.

Limitations and Future Work

This paper uses illustrative charts to protect sensitive data; real-world outcomes vary with adversary skill and environment. Future work should quantify control efficacy with multi- organizational datasets, model cloud control-plane abuse in detail, and evaluate autonomous response systems against human-operated ransomware.

Conclusion

Ransomware will remain a strategic risk until identity, endpoint, network, and data protections are implemented cohesively. Organizations should prioritize phishing-resistant MFA, EDR with behavioral analytics, rapid patching, segmentation, and validated backups. Measured against MTTD/MTTR and business impact, these controls deliver the highest risk reduction.

References

Kharraz, A., Robertson, W. (2019). Ransomware: A Survey and Research Directions.

Paquet-Clouston, M., Haslhofer, B., Dupont, B. (2019). Ransomware payments in the Bitcoin ecosystem.

Gazet, A. (2010). Comparative analysis of various ransomware virii.

SANS Institute. Ransomware Defense Playbook.

MITRE ATT&CK; Framework (Enterprise).

NIST SP 800-61r2. Computer Security Incident Handling Guide.

ENISA Threat Landscape — Ransomware.

CERT advisories on ransomware families.

ISO/IEC 27001/27002 controls relevant to malware protection and backup.

Industry reports on ransomware economics and affiliate models.

AUTHOR BIOGRAPHY

NDIANA OKON ASUQUO is an ICT Consultant and Senior Lecturer in the Department of Computer Science, Ibom Metropolitan Polytechnic. He holds a M.Sc. in Computer Science, an M.Sc.Ed. in Computer Education, a B.Sc. in Computer Science, a Postgraduate Diploma in Educational Management (PGDE), and an HND in Computer Science. He is currently pursuing a Ph.D. in Computer Science.

Mr. Asuquo is also a Cisco Certified Network Associate (CCNA), Certified Ethical Hacker (CEH), Certified Cyber security Analyst, Network Administrator, and Software Developer. A registered Member of Nigeria Computer society(NCS), Computer Registration Council of Nigeria (CPN) with more than nine years of experience in lecturing and IT practice. His research interests include cybersecurity, ransomware defense mechanisms, cryptography, software engineering, and network management. He continues to contribute to both academic research and professional IT practice