The Rise of

EDR Killers:

Why Endpoint Detection

Is No Longer Enough

How SIEM and NDR Provide

Critical Visibility When Endpoint Defenses Fall

Hani Darouich, CISSP – NextgenSoftware.eu

Contents

Executive SUMMARY

Something changed in 2024. The ransomware playbook evolved, and defenders are still catching up.

For years, Endpoint Detection and Response solutions stood as the cornerstone of modern security architecture. They watched processes, analyzed behaviors, and caught malicious activity at the point of execution. Attackers responded by developing increasingly sophisticated evasion techniques. But the latest evolution is different. Rather than sneaking past EDR, threat actors have learned to kill it outright.

EDR killers are now a commodity. On underground forums like XSS, RAMP, and Exploit.in, these tools sell for as little as $300 per month. Premium offerings with encryption capabilities fetch up to $10,000. The barrier to entry has collapsed, and even technically unsophisticated ransomware affiliates can now blind enterprise security tools before deploying their payloads.

The technique underpinning most of these tools is called Bring Your Own Vulnerable Driver, or BYOVD. Attackers load a legitimately signed but flawed Windows driver onto the target system, exploit its vulnerabilities to gain kernel-level access, and then systematically terminate security processes. Because the driver carries a valid Microsoft signature, the operating system trusts it implicitly. The result is a complete compromise of endpoint visibility.

CISA has tracked a 240% year-over-year increase in BYOVD incidents. Researchers estimate that one in four ransomware attacks during 2024 used these techniques. More than fifteen major ransomware operations now include EDR-killing capabilities as standard equipment.

The criminal ecosystem has matured rapidly. In early 2025, ESET documented how a single affiliate they call QuadSwitcher used RansomHub's custom EDRKillShifter tool to conduct attacks attributed to four different ransomware gangs: RansomHub itself, Medusa, Play, and BianLian. The walls between competing criminal enterprises are breaking down when it comes to sharing tools that work.

This whitepaper makes a straightforward argument. EDR remains necessary, but it is no longer sufficient on its own. When your primary detection layer can be disabled by the very threats it is meant to catch, you need independent visibility that persists regardless of endpoint status.

Network Detection and Response provides exactly that. Because NDR operates passively on network traffic through TAP or SPAN configurations, there is no agent for attackers to disable. The network does not lie, and it does not go silent when an endpoint is compromised.

SIEM provides the correlation and context layer. By collecting logs from diverse sources and applying detection logic across them, SIEM can identify the precursors to EDR tampering, detect the attack in progress through alternative telemetry, and orchestrate response actions.

We will examine how Cyberquest SIEM and Netalert NDR work together to close the visibility gap that EDR killers exploit. NetAlert's 32KB PCAP capture provides forensic-grade evidence of lateral movement, command-and-control traffic, and data exfiltration. Cyberquest's 500+ correlation rules and UEBA module detect anomalous driver loading, security service termination, and behavioural patterns consistent with compromise.

The threat landscape has shifted. Your defensive architecture must shift with it.

1. Introduction: A New Chapter in the Ransomware Playbook

The ransomware ecosystem experienced a seismic shift in 2024. Two of the most dominant operations in recent memory, ***LockBit*** and ***BlackCat***, effectively dropped out of the picture following sustained law enforcement pressure. ***Operation Cronos*** disrupted LockBit's infrastructure in February 2024. BlackCat collapsed amid internal disputes and an apparent exit scam following a major ransom payment. For a moment, it seemed defenders might gain ground.

That optimism proved short-lived.

The vacuum left by these giants was filled almost immediately. ***RansomHub*** emerged in February 2024, posting its first victims just eight days after advertising for affiliates on the Russian-speaking ***RAMP forum***. By the end of the year, it had become one of the most prolific ransomware operations in the world. ***Medusa*** intensified its campaigns, claiming nearly 400 victims since its emergence in January 2023, with attack volume increasing 42% between 2023 and 2024. ***Play***, ***BianLian***, and ***Embargo*** continued steady operations, while new actors entered the field.

But the real story of 2024 was not which groups rose to prominence. It was how they changed their tactics.

Ransomware operators have always understood that endpoint security is their primary obstacle. For years, the cat-and-mouse game focused on evasion: obfuscating payloads, living off the land with legitimate tools, encrypting malware in

memory. EDR vendors responded with behavioral analysis, machine learning models, and kernel-level telemetry. The arms race seemed balanced, if not tilting slightly toward defenders.

Then the attackers stopped trying to evade. They decided to eliminate the problem entirely.

The concept of disabling security tools is not new. Malware has attempted to terminate antivirus processes for decades. What changed is the sophistication and reliability of the approach. Modern EDR solutions run as protected processes with kernel-level hooks and tamper protection. They are designed to resist termination. Attackers needed a way to operate at the same privilege level as the security tools themselves.

They found it in vulnerable drivers.

The Windows operating system requires kernel-mode drivers to be digitally signed. This requirement exists to prevent malicious code from running with kernel privileges. However, the signature only validates that the driver came from a legitimate vendor. It says nothing about whether the driver contains exploitable vulnerabilities. Hundreds of legitimately signed drivers from reputable companies contain flaws that allow arbitrary code execution in kernel mode.

Attackers realized they could bring these vulnerable drivers with them. Load a signed driver, exploit its vulnerability, gain kernel access, and terminate any process on the system regardless of its protection level. EDR cannot defend against an attacker who operates with equal or greater privilege.

This technique, Bring Your Own Vulnerable Driver, existed in advanced persistent threat operations for years. Nation-state actors like the ***Lazarus Group*** used it as early as **2021.** What changed in 2024 was democratization. The technique moved from elite APT toolkits to commodity ransomware operations. It moved from bespoke development to subscription services sold openly on criminal forums.

The ransomware playbook did not just add a new chapter. It rewrote the rules of engagement.

2. Understanding EDR Killers: Techniques and Mechanics

To defend against EDR killers, security teams must first understand how they work. These tools are not magic. They exploit well-documented weaknesses in the Windows security model, and they do so with surgical precision. The techniques fall into three broad categories: driver exploitation, kernel-level manipulation, and telemetry suppression.

2.1 The BYOVD Technique

Bring Your Own Vulnerable Driver, or BYOVD, is the foundation of nearly every modern EDR killer. The concept is deceptively simple. Windows requires kernel-mode drivers to be digitally signed by Microsoft or a trusted certificate authority. This requirement exists to prevent malicious code from running in the kernel. But the requirement only validates that a driver was signed at some point by a trusted entity. It does not validate that the driver is free of exploitable vulnerabilities.

Attackers have compiled extensive lists of legitimately signed drivers that contain security flaws. These drivers were developed by reputable vendors for legitimate purposes. Graphics card utilities, overclocking tools, hardware monitoring software, and system management applications have all contributed vulnerable drivers to the attacker toolkit. The drivers were signed years ago, often before secure development practices became standard, and they remain valid because revoking a signature would break legitimate software that depends on them.

The attack sequence follows a predictable pattern. The attacker drops a vulnerable driver onto the target system. They then load the driver using standard Windows APIs, which succeeds because the driver carries a valid signature. Once loaded, the attacker exploits vulnerability within the driver to gain arbitrary kernel read and write capabilities. With kernel access established, they can manipulate any process on the system, including the EDR agent.

Microsoft maintains a blocklist of known vulnerable drivers, but the list is incomplete and updates infrequently. Attackers continually discover new vulnerable drivers, and the window between discovery and blocklisting can stretch for months. Even when a driver is blocklisted, attackers simply rotate to the next vulnerable driver in their collection.

2.2 Kernel-Level Access and Privilege

Understanding why kernel access matters requires a brief explanation of the Windows privilege model. Windows separates code execution into two distinct modes: user mode and kernel mode. Applications, including security software, typically run in user mode. The Windows kernel and device drivers run in kernel mode.

User mode code operates within strict boundaries. It cannot directly access hardware, cannot modify the memory of other processes without permission, and cannot interfere with kernel operations. These restrictions exist to maintain system stability and security. When an EDR agent runs in user mode, it relies on APIs and callbacks provided by the operating system to monitor system activity.

Kernel mode code faces no such restrictions. Code running in the kernel can access any memory address, modify any data structure, and control any process. The kernel is the ultimate authority on the system. When an attacker achieves kernel code execution through a vulnerable driver, they inherit this authority.

From the kernel, an attacker can terminate the EDR process regardless of any self-protection mechanisms the EDR has implemented. They can unload the EDR's kernel-mode components. They can modify the data structures that the EDR uses to receive notifications about system events. They can even patch the EDR's code in memory to disable specific detection routines while leaving the process running, creating the illusion of continued protection.

2.3 ETW and AMSI Bypass Techniques

Not all EDR evasion requires kernel exploitation. Some techniques operate entirely in user mode by targeting the telemetry sources that security tools depend on.

Event Tracing for Windows, or ETW, is the primary mechanism through which Windows reports security-relevant events to monitoring tools. EDR solutions subscribe to ETW providers to receive notifications about process creation, network connections, registry modifications, and other activities. Attackers have developed techniques to blind these providers by patching the functions responsible for generating events. When the patch is applied, events simply stop flowing to the EDR, even though the underlying activity continues.

The Antimalware Scan Interface, or AMSI, provides a standardized way for applications to submit content to security tools for scanning. PowerShell, for example, uses AMSI to send scripts to the installed antivirus before execution. Attackers routinely patch the AMSI scanning function in memory, causing it to return a clean result for all submissions regardless of actual content.

These user-mode techniques are often used in combination with BYOVD attacks. The attacker first blinds ETW and AMSI to prevent detection of their initial activities, then deploys the vulnerable driver and escalates to kernel-level control to neutralize the EDR entirely.

3. The Dark Web Marketplace: Commoditization of EDR Bypass

Five years ago, bypassing enterprise EDR required significant technical expertise. Attackers needed to understand Windows internals, driver development, and kernel exploitation. The barrier to entry was high, which limited these capabilities to sophisticated threat actors and nation-state groups.

That barrier has collapsed. EDR bypass tools are now sold openly on criminal forums with the same marketing polish as legitimate software products. Complete solutions come with documentation, customer support, and satisfaction guarantees. The commoditization of EDR evasion represents one of the most significant shifts in the threat landscape since the emergence of ransomware-as-a-service.

3.1 Pricing Structures and Accessibility

The economics of EDR killers favor the attacker. Prices start remarkably low. Entry-level tools capable of disabling common EDR solutions sell for as little as $300 for a single-use license or $350 per month for ongoing access. These prices place EDR bypass capabilities within reach of virtually any threat actor, regardless of technical skill or financial resources.

Mid-tier offerings range from $500 to $1,500 and typically include broader EDR coverage, more reliable evasion techniques, and basic customer support. The ***AlphaGhoul group***, for example, sells their ***NtKiller*** tool in this price range, offering different tiers based on the target EDR vendor.

Premium packages command prices between $7,500 and $10,000. These bundles often combine EDR bypass with additional capabilities such as ransomware lockers, data exfiltration tools, and post-exploitation frameworks. The premium tier targets established ransomware affiliates who need turnkey solutions for high-value operations.

To put these numbers in perspective, a single ransomware payment can exceed several million dollars. The cost of EDR bypass tooling represents a trivial investment against potential returns. Even a moderately successful attack generates returns measured in thousands of percent.

3.2 Key Vendors and Forums

The market for EDR killers operates across multiple platforms. Forums such as ***XSS*** and ***Exploit*** remain primary venues for tool sales and technical discussion. These forums require vetting for membership and maintain reputations that encourage a degree of accountability among sellers. Rippers, as scammers are known in this ecosystem, face bans and public exposure.

Telegram channels have emerged as an alternative distribution mechanism, offering faster communication and easier operational security. Some vendors operate invitation-only channels where they announce updates, share bypass success rates

against specific EDR products, and negotiate bulk purchases with ransomware-as-a-service operators.

The vendor landscape includes both established groups and new entrants. ***Spyboy*** gained notoriety with their ***Terminator*** tool, which they marketed aggressively across multiple forums. The developer behind ***EDRSandBlast*** released their tool publicly, enabling others to build commercial offerings on top of the open-source code. ***FIN7***, a financially motivated threat group with years of experience, developed ***AuKill*** for their own operations before the tool proliferated to other actors.

3.3 The Subscription Model

The most significant market evolution has been the shift toward subscription-based licensing. Rather than selling tools outright, vendors now offer ongoing access with regular updates. This model benefits both parties. Buyers receive continuous improvements and new bypasses as EDR vendors patch existing techniques. Sellers generate recurring revenue and maintain ongoing relationships with their customer base.

Subscription packages typically include several components. The core bypass tool receives updates whenever EDR vendors release new versions or implement new protections. Vulnerable driver collections expand as researchers discover new candidates. Documentation and tutorials help less technical buyers deploy the tools effectively. Some subscriptions include access to private forums or chat channels where buyers can request features and report issues.

The subscription model has also enabled a support ecosystem that mirrors legitimate software. Vendors offer installation assistance, troubleshooting for failed deployments, and guidance on evading specific EDR products. Some even provide testing services, allowing buyers to submit samples for validation against a panel of EDR solutions before deployment.

This professionalization of the market has lowered the skill threshold dramatically. An attacker no longer needs to understand kernel exploitation or driver vulnerabilities. They simply need enough funds to purchase a subscription and

enough patience to follow the documentation. The tools handle the technical complexity, transforming sophisticated attacks into point-and-click operations.

The implications for defenders are severe. Organizations can no longer assume that advanced evasion techniques will only be used by advanced adversaries. The same capabilities once reserved for nation-state operations are now available to any affiliate willing to pay a modest monthly fee.

4. The Arsenal: Prominent EDR Killer Tools

The commoditization of EDR bypass has produced a recognizable cast of tools, each with distinct characteristics, target profiles, and threat actor associations. Understanding these tools helps defenders recognize attack patterns and prioritize detection efforts. The following represents the most significant EDR killers currently circulating in the threat landscape.

4.1 EDRKillShifter

EDRKillShifter emerged as the signature tool of the RansomHub ransomware operation and has since become one of the most widely deployed EDR killers in active incidents. The tool demonstrates thoughtful engineering, incorporating multiple evasion layers that complicate both static and dynamic analysis.

The execution flow begins with a loader component that requires a command-line password to proceed. This simple measure prevents automated sandbox analysis, as security researchers must first extract the correct password before the malicious payload will execute. The loader decrypts an embedded payload using the provided password, then executes the decrypted code in memory.

The core payload cycles through a collection of vulnerable drivers until it finds one that successfully loads on the target system. This approach provides resilience against driver blocklisting. If one driver fails to load due to revocation or policy restrictions, EDRKillShifter simply attempts the next driver in its collection. Once a suitable driver

loads, the tool exploits its vulnerability to gain kernel access and systematically terminates EDR processes.

EDRKillShifter has been observed in attacks attributed to multiple threat actors beyond RansomHub, including affiliates associated with Medusa, Play, and BianLian ransomware operations. This cross-pollination suggests either shared tooling agreements between groups or, more likely, that affiliates operate across multiple ransomware programs and carry their preferred tools with them.

4.2 Terminator

Terminator gained notoriety through aggressive marketing by its developer, known as Spyboy, who promoted the tool across criminal forums throughout 2023 and 2024. The marketing materials made bold claims about bypass capabilities against 24 different EDR and antivirus products, complete with demonstration videos showing successful termination of security processes.

The tool relies primarily on the **zam64.sys** driver from **Zemana Anti-Malware**, a legitimate security product with an unfortunate vulnerability in its process termination functionality. Terminator exploits this vulnerability to kill arbitrary processes with SYSTEM privileges, effectively weaponizing a security tool against other security tools.

Spyboy offered Terminator at multiple price points: $300 for a single bypass, $500 for a package covering five target products, and $3,000 for an all-inclusive license covering all supported EDR solutions. The tiered pricing model attracted buyers across the skill and resource spectrum, from opportunistic criminals to organized ransomware affiliates.

Security vendors have since added detections for the specific driver and exploitation patterns used by Terminator. However, variants continue to appear with modified loaders and alternative vulnerable drivers, maintaining the tool's relevance despite increased defender awareness.

4.3 AuKill and AvNeutralizer

AuKill, also distributed under the name AvNeutralizer, traces its origins to **FIN7**, a financially motivated threat group responsible for billions of dollars in fraud and cybercrime losses. FIN7 developed the tool for their own operations before it proliferated to other actors, most notably the **Black Basta** ransomware operation.

The tool exploits vulnerabilities in the Process Explorer driver published by Microsoft as part of the Sysinternals suite. This choice of target driver is particularly insidious. Process Explorer is a trusted system administration utility used by IT professionals worldwide. Many organisations explicitly whitelist Sysinternals tools, inadvertently creating an opening for AuKill to operate without triggering policy-based restrictions.

AuKill implements multiple termination methods to ensure reliability. If direct process termination fails, the tool attempts to disable the EDR service, corrupt its configuration, or remove its kernel callbacks. This persistence in the face of resistance makes AuKill particularly effective against EDR solutions with self-protection mechanisms.

The connection between FIN7 and Black Basta operations has led researchers to investigate potential organizational links between the groups. Whether through direct collaboration, shared membership, or tool sales, the AuKill lineage demonstrates how capabilities developed by one threat actor eventually propagate across the broader criminal ecosystem.

4.4 NtKiller

NtKiller represents a newer entrant to the market, developed and sold by a group operating under the name **AlphaGhoul**. The tool distinguishes itself through modularity and vendor-specific targeting. Rather than offering a single bypass approach, NtKiller provides customized attack modules optimised for specific EDR products.

The pricing structure reflects this specialization. Base licenses start at $500 for single-vendor bypass capability, scaling to $1,100 for packages covering multiple EDR solutions. AlphaGhoul maintains an active development program, releasing updates

as EDR vendors implement new protections and advertising success rates against current product versions.

NtKiller employs several anti-analysis techniques beyond standard driver exploitation. T**he tool checks for virtualization indicators, debugging attachments, and known sandbox environments before executing its payload.** If analysis conditions are detected, NtKiller terminates silently without revealing its capabilities. These checks frustrate security researchers attempting to study the tool in controlled environments.

The modular architecture also enables rapid adaptation. When an EDR vendor patches a vulnerability that NtKiller exploits, AlphaGhoul can update the relevant module without rewriting the entire tool. This agility has allowed NtKiller to maintain effectiveness despite active countermeasures from the security industry.

4.5 MS4Killer and ABYSSWORKER

MS4Killer emerged alongside the **Embargo** ransomware operation in mid-2024. The tool follows the established BYOVD pattern but incorporates several refinements that indicate professional development practices. Error handling is robust, logging is comprehensive, and the code demonstrates awareness of edge cases that trip up less mature tools.

The driver selection in MS4Killer focuses on lesser-known vulnerable drivers that had not yet appeared in public blocklists at the time of deployment. This choice extended the tool's operational lifespan by avoiding immediate detection through signature-based blocking. The Embargo operators clearly invested in driver research, identifying candidates that security vendors had not yet catalogued.

ABYSSWORKER represents an evolution of the EDR killer concept, combining process termination with broader system manipulation capabilities. Beyond killing security software, ABYSSWORKER can disable Windows Defender, modify security policies, and establish persistence mechanisms that survive reboots. The tool effectively combines EDR bypass with post-exploitation functionality in a single package.

5. Threat Actor Ecosystem: Who Is Behind This?

EDR killers do not exist in isolation. They are components within broader attack chains operated by organized criminal enterprises, state-sponsored groups, and opportunistic affiliates. Understanding who deploys these tools, and why, helps defenders anticipate targeting patterns and prioritise protection for likely victims.

The threat actor ecosystem has grown increasingly interconnected. Tools flow between groups through sales, sharing, and personnel movement. Affiliates work simultaneously for multiple ransomware operations, carrying techniques and tooling across organizational boundaries. Attribution has become difficult not because attackers have grown more sophisticated at hiding, but because the boundaries between groups have blurred to the point of irrelevance.

5.1 RansomHub

RansomHub emerged in early 2024 and rapidly established itself as a dominant force in the ransomware landscape. The operation filled the vacuum left by law enforcement actions against ALPHV/BlackCat and LockBit, absorbing displaced affiliates and offering competitive commission structures. Within months of launch, RansomHub claimed responsibility for attacks against hundreds of organizations across multiple sectors.

The group's technical sophistication is evident in their tooling choices. EDRKillShifter, their primary EDR bypass tool, demonstrates engineering quality that exceeds typical

criminal malware. The tool's resilience against analysis, its driver rotation capabilities, and its reliable operation across diverse target environments suggest experienced developers with deep Windows internals knowledge.

RansomHub operates as a ransomware-as-a-service platform, providing affiliates with encryption tools, negotiation infrastructure, and leak sites in exchange for a percentage of ransom payments. The provision of EDRKillShifter to affiliates represents a competitive advantage, enabling less technical operators to succeed against hardened targets. This democratization of capability has contributed significantly to the proliferation of EDR killer techniques across the threat landscape.

ESET researchers have documented RansomHub's influence on the broader ecosystem, noting that EDRKillShifter has appeared in attacks attributed to affiliates with no apparent direct connection to the core RansomHub operation. The tool has become a de facto standard, spreading through affiliate networks like a franchise model.

5.2 Medusa

Medusa ransomware has operated since late 2022, maintaining a consistent tempo of attacks against education, healthcare, and government targets. **The group runs a leak site where they publish stolen data from victims who refuse payment, applying public pressure alongside technical disruption.**

The Medusa operation has demonstrated particular interest in EDR bypass capabilities, incorporating multiple tools into their attack playbooks. Analysts have observed Medusa affiliates deploying EDRKillShifter, suggesting either direct acquisition from RansomHub or access through shared affiliate relationships. The group has also developed custom bypass scripts targeting specific EDR products common in their preferred victim sectors.

Medusa's targeting patterns reveal strategic thinking about EDR deployment. Education and healthcare organisations often run standardised security stacks due to budget constraints and compliance requirements. By developing bypasses for the specific EDR products common in these sectors, Medusa achieves reliable access

without maintaining capabilities against the full spectrum of enterprise security solutions.

The group's operational security has proven robust. Despite sustained attention from law enforcement and security researchers, Medusa has avoided the disruptions that have plagued competitors. This resilience suggests experienced operators who have learned from the mistakes of predecessors.

5.3 Play and BianLian

Play ransomware, also known as ***PlayCrypt***, has operated since mid-2022 with a focus on Latin American and European targets. The group eschews the affiliate model employed by most ransomware operations, maintaining a closed membership that executes attacks directly. This structure provides tighter operational control, but limits scaling compared to affiliate-based competitors.

Play operators have demonstrated consistent interest in EDR bypass, incorporating techniques from multiple sources into their toolkit. The group has been observed using EDRKillShifter alongside custom scripts and publicly available tools. This tool diversity suggests a pragmatic approach: Play operators use whatever works against the target environment rather than committing to a single bypass methodology.

BianLian represents an interesting evolution in the ransomware space. The group originally operated as a traditional encryption-based ransomware but shifted in early 2023 to pure data extortion. Rather than encrypting victim files, BianLian now focuses exclusively on data theft and extortion, threatening to publish stolen information unless payment is received.

This operational shift has implications for EDR bypass requirements. BianLian still needs to evade detection during the data theft phase, but the technical requirements differ from encryption-focused operations. The group has invested in stealth-oriented techniques, including EDR blinding approaches that suppress telemetry without terminating security processes. By leaving the EDR running but blind, BianLian reduces the likelihood of alerting security teams to the ongoing intrusion.

5.4 FIN7 and Black Basta

FIN7 occupies a unique position in the threat landscape. The group has operated since at least 2013, originally focusing on point-of-sale malware targeting retail and hospitality organizations. Over the years, FIN7 has evolved through multiple phases, demonstrating remarkable adaptability and technical capability.

The group's development of AuKill, later known as AvNeutralizer, represents a significant investment in EDR bypass research. FIN7 identified the vulnerable Process Explorer driver, developed reliable exploitation techniques, and packaged the result into a deployable tool. This capability development reflects resources and expertise beyond typical criminal operations.

The relationship between FIN7 and Black Basta has attracted significant researcher attention. Black Basta emerged in early 2022 and quickly established itself as a major ransomware threat, attacking organizations across multiple sectors with notable success. The group's use of AuKill, combined with other technical and operational overlaps, has led analysts to conclude that former FIN7 members play significant roles in Black Basta operations.

Black Basta's attack methodology demonstrates the effectiveness of combining EDR bypass with rapid execution. The group typically moves from initial access to ransomware deployment within hours, leaving defenders minimal time to detect and respond. AuKill's reliable EDR neutralization enables this speed by removing the primary detection mechanism that might otherwise alert security teams to the ongoing attack.

5.5 North Korean State-Sponsored Activity

The inclusion of nation-state actors in the EDR killer ecosystem reflects the blurring boundaries between criminal and state-sponsored operations. North Korean threat groups, operating under various names including Lazarus Group, have deployed BYOVD techniques since at least 2021, predating the widespread adoption of these methods by criminal actors.

North Korean operations serve dual purposes: generating revenue for the regime and conducting espionage against strategic targets. The revenue motivation has driven North Korean actors toward ransomware and cryptocurrency theft, bringing them into direct competition with criminal groups. The espionage motivation requires persistent access to target networks, making EDR evasion essential for long-term operations.

The ***FudModule rootkit***, attributed to North Korean actors, demonstrates sophisticated kernel manipulation capabilities that exceed most criminal tooling. **The rootkit disables security monitoring at a fundamental level, blinding not just EDR but also kernel-level security features built into Windows itself. This capability represents the high end of EDR bypass sophistication.**

North Korean groups have also shown willingness to exploit zero-day vulnerabilities in their BYOVD operations. While criminal actors typically rely on known vulnerable drivers, state-sponsored groups have the resources to identify and exploit previously unknown vulnerabilities. This capability gap provides North Korean operations with bypass options unavailable to purely criminal actors.

5.6 The Affiliate Web: QuadSwitcher and CosmicBeetle

The affiliate model that dominates modern ransomware has created a fluid ecosystem where individual operators move between groups, carrying tools and techniques with them. Tracking specific affiliates has become as important as tracking ransomware brands, as the same individuals often drive attacks attributed to different operations.

QuadSwitcher exemplifies this affiliate mobility. The actor, tracked by multiple security vendors under various names, has been linked to attacks deploying RansomHub, Play, and other ransomware variants. QuadSwitcher consistently employs EDRKillShifter across operations regardless of the ransomware payload, demonstrating personal tool preferences that transcend group affiliations.

CosmicBeetle, also known as ***NoName***, represents a different affiliate archetype. The actor has struggled with technical implementation, deploying ransomware with encryption flaws and operational errors that have allowed some victims to recover without payment. Despite these failures, CosmicBeetle has successfully incorporated

EDR killer tooling, demonstrating how commoditised tools enable even less skilled actors to overcome enterprise security controls.

The affiliate ecosystem creates attribution challenges for defenders and law enforcement alike. When an attack occurs, determining responsibility requires untangling relationships between the ransomware brand, the affiliate who executed the attack, the developers who created the tools, and the infrastructure providers who enabled communication and payment. Each layer may involve different individuals or groups, complicating response efforts.

6. By The Numbers: Statistics That Demand Attention

The threat posed by EDR killers is not theoretical. The data from incident response engagements, threat intelligence reporting, and security vendor telemetry paints a clear picture: these tools have moved from novelty to mainstream within the ransomware ecosystem. The following statistics quantify the scale and trajectory of the problem.

Growth in BYOVD Incidents

The United States Cybersecurity and Infrastructure Security Agency documented a 240% year-over-year increase in BYOVD-related incidents between 2023 and 2024. That trajectory continued into 2025. Researchers observed a 23% increase in BYOVD

attacks between the first and second quarters of 2024 alone, and the technique has only become more entrenched since.

In August 2025, Sophos reported that **at least eight distinct ransomware operations were actively deploying a shared EDR killer framework derived from RansomHub's EDRKillShifter.** The groups identified included Blacksuit, Medusa, Qilin, Dragonforce, Crytox, Lynx, and INC. The Cyber Security Agency of Singapore issued a dedicated advisory warning organizations about this collaborative weaponization, noting that the tool's modular architecture and vendor-specific targeting represented a significant advancement in ransomware tactics.

CYFIRMA's August 2025 tracking report recorded 522 global ransomware victims in a single month, a figure that remains far above 2023 and 2024 baselines despite minor month-over-month fluctuations. The report specifically highlighted BYOVD weaponisation advances, including Akira's abuse of Intel's rwdrv.sys driver to disable Microsoft Defender at the kernel level.

Overall Ransomware Volume

The broader ransomware landscape provides context for EDR killer proliferation. Analysis from late 2025 documented 4,701 ransomware incidents for the year, representing a 46% increase compared to the prior year. This growth occurred despite sustained law enforcement pressure and improved organizational defenses in other areas.

Kaspersky's Q1 2025 threat statistics identified nearly 12,000 new ransomware variants during the quarter, with over 85,000 users experiencing ransomware attacks. RansomHub maintained its position as the leading operation, accounting for approximately 11% of all victims whose data appeared on leak sites. Akira and Clop followed closely at roughly 11% each.

The Q1 2025 data also revealed continued BYOVD innovation. Researchers documented ransomware groups exploiting a series of vulnerabilities in Paragon Partition Manager, assigned CVE identifiers *CVE-2025-0288, CVE-2025-0287, CVE-2025-0286, CVE-2025-0285*, and *CVE-2025-0289.* These vulnerabilities enabled

attackers to gain Windows SYSTEM privileges through BYOVD attacks, adding yet more drivers to the already extensive vulnerable driver inventory.

Ransomware Integration Rates

Analysis of ransomware incidents in 2024 indicated that approximately 25% incorporated BYOVD methods specifically to disable endpoint detection and response systems. The 2025 data suggest this figure has increased further as EDR killer frameworks have become shared infrastructure across the ransomware ecosystem.

The Logpoint Emerging Threats Report identified over 15 major ransomware operations incorporating EDR killing modules into their standard attack chains. By mid-2025, Sophos confirmed that the number of groups using shared EDR killer tooling had expanded to at least eight, with the tool representing not leaked code but collaborative development across criminal organizations.

Attack Methodology Evolution

The 2025 threat landscape data reveal how attackers gain initial access before deploying EDR killers. Vulnerability exploitation accounts for 32% of initial access, targeting unpatched VPN appliances and content management systems. Stolen credentials, obtained through information stealers and phishing campaigns, account for 23%. Phishing emails have increased to 18% of initial access vectors, up from 11% in 2024, reflecting improved AI-generated content that bypasses traditional filters.

Living-off-the-land techniques and BYOVD have become standard components of the attack chain rather than exceptional capabilities. The triple extortion model, combining encryption, data theft, and distributed denial of service attacks, appeared in 29% of 2025 ransomware incidents.

Time to Impact

The operational efficiency of modern attacks compounds the defensive challenge. **Modern ransomware can encrypt 220,000 files in 4.5 minutes once deployed.** When

combined with EDR bypass that completes in under 60 seconds, the window for detection and response has narrowed to almost nothing.

This speed has profound implications for security operations. Traditional workflows assume that alerts will fire, analysts will triage, and responders will investigate. When the EDR goes blind in under a minute and encryption completes minutes later, none of these steps have time to occur.

Economic Impact

IBM's 2025 study reported that the average cost of an extortion or ransomware incident reached $5.08 million when disclosed by an attacker. This figure encompasses investigation costs, downtime, legal exposure, and reputational damage. Average ransom demands now exceed $1.2 million per case, though actual payments average around $250,000.

Recovery costs remain substantial even when organizations refuse to pay. The mean recovery cost excluding ransom payments reached $1.53 million in 2025, though this represented a 44% decrease from the prior year, suggesting improved organisational resilience. In the United States, average ransomware insurance claims rose 68% to $353,000, signaling rising remediation expenses despite improved recovery capabilities.

Average downtime per attack now extends to approximately 30 days. Healthcare attacks increased 45% in 2025, with education seeing a 30% rise and finance experiencing a 25% increase. These sectors share characteristics that make them attractive targets: valuable data, operational sensitivity to disruption, and security budgets that trail behind threat evolution.

Victim Response Trends

Not all trends favor attackers. I**BM's 2025 study found that 63% of organizations refused to pay ransoms, up from previous years.** This shift suggests that attackers face lower success rates and shrinking returns, forcing them to increase pressure tactics or target higher-value victims capable of larger payments.

Recovery capabilities have also improved. Despite ongoing threats, 97% of organizations with encrypted data successfully recovered it through some method, demonstrating improved resilience and preparedness. Encryption may be declining in importance as a coercion mechanism, but data exposure and extortion leverage remain central to modern ransomware strategies.

Detection Gap

The most concerning statistics involve detection rates. When EDR killers succeed, they create blind spots that persist until the attack concludes. Organizations cannot respond to threats they cannot see. The primary visibility tool goes dark precisely when defenders need it most.

This detection gap explains why layered visibility has become essential. Network-level monitoring, centralised log analysis, and behavioral detection provide the redundancy necessary to maintain situational awareness when endpoint protection fails.

7. Case Studies: EDR Killers in the Wild

The statistics tell part of the story. The case studies tell the rest. The following incidents, drawn from published incident response reports and threat intelligence analysis, illustrate how EDR killers function in real attacks against real organisations. Each case reveals patterns that defenders can use to improve their own security posture.

Case Study 1: The Webcam That Encrypted the Network

In early 2025, cybersecurity firm S-RM responded to an Akira ransomware incident that demonstrated just how far attackers will go to circumvent endpoint protection. The attack began conventionally enough. Akira gained initial access through an externally facing remote access solution, likely using stolen credentials. They deployed AnyDesk for persistence and began exfiltrating data in preparation for double extortion.

When the attackers attempted to deploy their ransomware payload on a Windows server, packaging it as a password-protected ZIP file, the organization's EDR solution detected and quarantined the binary. The attack should have ended there. Instead, the attackers adapted.

Having been blocked by EDR, Akira conducted an internal network scan to identify alternative attack paths. They discovered several Internet of Things devices on the network, including webcams and a fingerprint scanner. The attackers selected a webcam as their pivot point for three reasons: it had critical vulnerabilities enabling remote shell access, it ran a lightweight Linux operating system compatible with Akira's Linux ransomware variant, and critically, it lacked any EDR protection.

From the compromised webcam, the attackers mounted Windows SMB network shares belonging to other systems on the network. They then launched their Linux encryptor directly from the webcam, encrypting files across network shares without ever executing code on a protected Windows endpoint. Because the webcam was not monitored, the organization's security team remained unaware of the malicious SMB traffic flowing from the device to their servers.

S-RM noted that patches were available for webcam vulnerabilities, meaning the attack vector was entirely preventable. The case demonstrates that EDR, while essential, cannot protect devices it cannot see. Network visibility and IoT security have become prerequisites for comprehensive defense.

Case Study 2: Legitimate Software Turned Weapon

Cisco Talos incident responders encountered a troubling pattern across multiple 2024 engagements: attackers using legitimate commercial software to disable endpoint protection. In one case involving GlobeImposter ransomware, the attackers gained administrative access and immediately executed HRSword, a monitoring tool developed by Beijing Huorong Network Technology.

HRSword is legitimate software designed for system monitoring and management. However, its capabilities include the ability to interact with and disable security products. Ransomware operators recognized this dual-use potential and incorporated the tool into their attack chains. Because HRSword is a signed, legitimate application, it was far less likely to trigger security alerts than purpose-built malware.

After deploying HRSword to blind the organization's EDR, the GlobeImposter attackers proceeded with their operation unimpeded. They deployed NetSupport RAT for remote access, then used Smbexec and Wmiexec to move laterally through the network. The entire sequence, from EDR neutralisation to data theft and ransomware deployment, proceeded without generating the alerts that should have notified the security team.

Talos observed the same pattern in a separate Phobos ransomware incident. The attackers again led with HRSword, using it to disable endpoint protection before deploying additional tools from the same software suite for malicious purposes. The consistency across incidents suggests that HRSword has become a standard component in certain ransomware affiliate toolkits.

Kendall McKay, strategic lead at Cisco Talos, explained the appeal: "Using HRSword is a way to hide in plain sight because it's a legitimate tool, and it should be occurring legitimately on many systems. With threat actors using that to kick off their operations, it's much more likely to go undetected."

Case Study 3: The Shared EDR Killer Framework

In August 2025, Sophos published research documenting a disturbing development: at least eight distinct ransomware operations were deploying variants of the same EDR killer tool. The operations included Blacksuit, RansomHub, Medusa, Qilin, Dragonforce, Crytox, Lynx, and INC. Each group used customised builds rather than identical binaries, indicating collaborative development rather than simple code theft.

The tool traced its lineage to EDRKillShifter, originally developed by RansomHub and first observed in August 2024. However, the version Sophos documented had evolved significantly. All variants were packed using HeartCrypt, a subscription-based packer-as-a-service that complicated analysis. The drivers were signed with expired or compromised certificates, including one from Fuzhou Dingxin Trade Co., Ltd. that had been invalid since 2012.

In one January 2025 case, Sophos observed the EDR killer deployed as part of a Medusa ransomware attack. The attackers created a file in the Windows Temp directory, deployed the HeartCrypt-packed dropper, and successfully disabled security products from six vendors: ESET, Symantec, Sophos, HitmanPro, Webroot, and Kaspersky. Within minutes of EDR neutralization, the Medusa ransomware binary executed.

A June 2025 case proved particularly interesting because the attackers had added an additional layer of packing to the EDR killer, demonstrating ongoing development efforts. The tool loaded a driver with a randomized five-character name, exploited it for kernel access, and terminated security processes. This was followed by INC ransomware deployment.

The cross-group adoption of shared tooling represents a maturation of the ransomware ecosystem. Development costs are distributed across multiple operations, updates benefit all participants, and individual groups can focus on their core competencies while relying on shared infrastructure for common challenges like EDR bypass.

Case Study 4: When EDR Worked, But Nothing Else Did

Not every case study ends in encryption. In an incident documented by Palo Alto Unit 42 in early 2025, an attacker attempted to use an AV/EDR bypass tool against an organization protected by Cortex XDR. The tool failed. The EDR detected and blocked the bypass attempt, preventing the attacker from proceeding with their operation.

What made this case notable was what happened next. Because the bypass attempt was logged and alerted, the incident response team gained visibility into the attacker's activities. They were able to examine the attacker's tooling, understand their targeting patterns, and gather intelligence about the threat actor's persona. The failed EDR bypass became an intelligence windfall.

The case illustrates an important principle: EDR bypass attempts, even unsuccessful ones, generate telemetry. Organizations that monitor for these attempts can detect attacks earlier in the kill chain, before the EDR is neutralized. The attempt itself becomes an indicator of compromise, provided someone is watching for it.

Lessons from the Field

These cases share common threads that inform defensive strategy.

First, EDR bypass has become routine rather than exceptional. Attackers expect to encounter endpoint protection and plan accordingly. Organizations that rely solely on EDR are planning for a threat landscape that no longer exists.

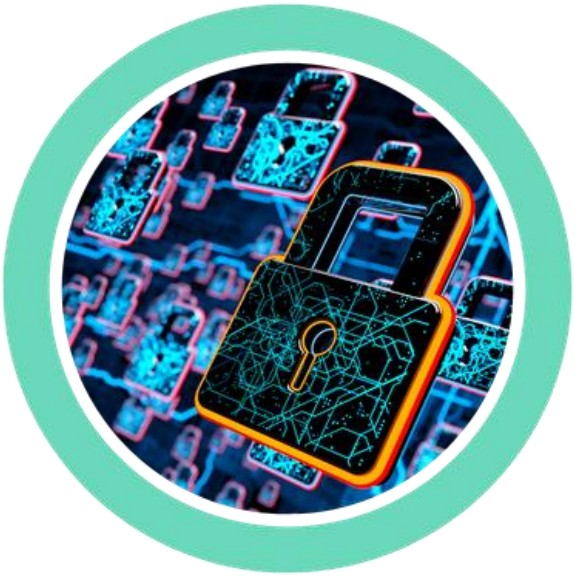
Second, attackers demonstrate remarkable adaptability. When one path is blocked, they find another. The Akira webcam case shows that attackers will exploit any connected device to achieve their objectives. Comprehensive security requires visibility beyond traditional endpoints.

Third, legitimate tools have become attack tools. The distinction between malicious software and dual-use utilities has blurred. Detection strategies must account for the misuse of legitimate applications, not just the presence of known malware.

Fourth, shared tooling has accelerated capability proliferation. Techniques that once required significant development investment are now available through criminal marketplaces and collaborative frameworks. Defenders face not individual threat actors but an ecosystem with shared resources and distributed development.

Finally, detection opportunities exist throughout the attack chain. EDR bypass attempts, driver loading events, service modifications, and unusual network traffic all provide potential detection points. Organisations with layered visibility can identify attacks even when individual security controls fail.

8. Why EDR Alone Is No Longer Sufficient



The evidence is now overwhelming. **Endpoint detection and response, once considered the cornerstone of modern security architecture, cannot be trusted as a standalone defense against sophisticated ransomware operations.** This is not a criticism of EDR technology itself. EDR solutions remain valuable and necessary components of a comprehensive security strategy. But the threat landscape has evolved, and defensive strategies must evolve with it.

Understanding why EDR alone falls short requires examining both the technical limitations inherent to endpoint protection and the operational realities that attackers have learned to exploit.

The Kernel Privilege Problem

EDR solutions face a fundamental architectural constraint: they operate within the same system they are trying to protect. Most EDR agents run primarily in user mode, relying on kernel callbacks and API hooks to monitor system activity. This design makes sense from a stability perspective. Kernel-mode code that crashes can bring down the entire system, so vendors minimize their kernel footprint to reduce risk.

The problem is that attackers who achieve kernel access operate at a higher privilege level than the EDR itself. From the kernel, an attacker can manipulate the data structures that EDR relies on, terminate protected processes, and remove the hooks that provide visibility into system events. The EDR cannot defend against an adversary who has already bypassed the privilege boundary it depends on.

BYOVD attacks exploit this asymmetry directly. By loading a vulnerable but signed driver, attackers gain kernel access through a path that Windows considers legitimate. Once in the kernel, they have the authority to neutralize any user-mode security control, including the EDR agent. The EDR may detect the initial driver load, but if the attacker moves quickly enough, the detection never reaches an analyst before the agent is disabled.

Some EDR vendors have responded by implementing kernel-mode protections and self-defense mechanisms. These measures raise the bar for attackers but do not eliminate the fundamental problem. Determined adversaries continue to find ways around these protections, whether through novel driver vulnerabilities, timing attacks during updates, or exploitation of configuration weaknesses.

The Visibility Gap

EDR provides deep visibility into endpoint activity but limited visibility into everything else. **Network traffic between endpoints, communications with external systems, and activity on devices that cannot run EDR agents all fall outside the EDR's field of view.**

The Akira webcam case discussed earlier illustrates this gap perfectly. The organization's EDR successfully detected and blocked the ransomware on Windows endpoints. But the EDR had no presence on the IoT devices sharing the network. When the attackers pivoted to the webcam, they moved outside the EDR's visibility entirely. The subsequent SMB traffic from the webcam to network shares went unmonitored because no endpoint agent was watching that traffic path.

This visibility gap extends beyond IoT devices. Legacy systems that cannot support modern EDR agents, operational technology environments with stability requirements that preclude security software, and cloud workloads with ephemeral lifecycles all create blind spots. Attackers have learned to identify and exploit these gaps, moving through unmonitored paths to reach their objectives.

Even on systems where EDR is deployed, visibility depends on proper configuration and continuous operation. Cisco Talos reported that almost 20 percent of incidents they investigated involved organizations without protection against EDR uninstallation. Attackers simply removed the agent and proceeded without interference. Misconfigured EDR, EDR left in audit-only mode, and EDR with disabled components all create exploitable weaknesses.

The Telemetry Dependency

EDR detection capabilities depend on telemetry sources provided by the operating system. Event Tracing for Windows, the Antimalware Scan Interface, and various kernel callbacks feed information to the EDR agent, which analyses this data to identify threats. When attackers blind these telemetry sources, the EDR loses its ability to see what is happening on the system.

ETW patching has become a standard technique in sophisticated attacks. By modifying the functions responsible for generating ETW events, attackers can suppress specific event types while leaving others intact. The EDR continues running and may even report that the system is healthy, but critical events never reach the detection engine. **The attack proceeds in a manufactured blind spot.**

AMSI bypass techniques similarly undermine script-based detection. PowerShell, JavaScript, and other scripting languages submit content to AMSI for scanning before execution. Attackers who patch the AMSI scanning function cause it to return clean results regardless of actual content. Malicious scripts execute without triggering the alerts that should have stopped them.

These telemetry attacks often precede BYOVD exploitation. The attacker first blinds the EDR to their initial activities, then deploys the vulnerable driver and escalates to kernel control. By the time the EDR might have detected the driver load, its ability to report that detection has already been compromised.

The Speed Asymmetry

Modern ransomware operations move faster than human response cycles can accommodate. The statistics are stark: EDR bypass completes in under 60 seconds, ransomware can encrypt 220,000 files in under five minutes, and **attackers routinely move from initial access to full domain compromise in hours rather than days.**

Traditional security operations assume that alerts will fire, analysts will investigate, and responders will contain threats before significant damage occurs. This model requires time that attackers no longer provide. When the EDR is neutralized in the first minute of an attack, the entire response timeline collapses. There are no alerts to triage, no indicators to investigate, no opportunity to intervene.

Even organizations with mature security operations centers struggle with this speed asymmetry. Staffing limitations mean that alerts outside business hours may wait until morning for review. **Alert fatigue from false positives can delay response to genuine threats.** And the sheer volume of security telemetry in large environments makes it impossible to investigate every anomaly in real time.

The speed problem compounds the visibility problem. Attackers who move quickly through blind spots may complete their objectives before any detection mechanism has an opportunity to fire. The attack is discovered only after the damage is done, when encrypted files or ransom notes make the compromise undeniable.

The Configuration Challenge

EDR effectiveness depends heavily on proper deployment and configuration. Out-of-the-box settings rarely provide optimal protection for specific environments. Policies must be tuned to balance security against operational requirements. Exclusions must be carefully managed to prevent attackers from abusing them. And configurations must be maintained as environments change and new threats emerge.

Many organizations struggle with this configuration burden. Security teams are stretched thin, managing multiple tools across complex environments while responding to ongoing incidents. EDR tuning becomes a lower priority than immediate threats, leading to configurations that drift from best practices over time.

Attackers actively probe for configuration weaknesses. They test whether specific directories are excluded from scanning, whether certain process names bypass monitoring, and whether self-protection mechanisms are enabled. Poorly configured EDR may provide a false sense of security while offering little actual protection against determined adversaries.

Cisco Talos specifically highlighted this issue in their 2024 analysis, noting that attackers were targeting *"out-of-the-box products that had not been configured specifically for that organization."* The gap between EDR capability and EDR effectiveness creates opportunities that attackers readily exploit.

The Single Point of Failure

Perhaps **the most fundamental problem with EDR-centric security is structural: it creates a single point of failure.** When all detection and response capabilities concentrate in one technology, neutralizing that technology neutralizes the entire

defensive posture. Attackers who bypass EDR face no additional obstacles on their path to objectives.

Robust security architecture avoids single points of failure through redundancy and defense in depth. Multiple independent detection mechanisms ensure that the failure of any single control does not leave the organization blind. **Layered defenses force attackers to bypass multiple obstacles, increasing the likelihood of detection at some point in the attack chain.**

EDR remains an essential layer in this architecture. Its deep endpoint visibility and response capabilities address threats that other controls cannot see. But i**t must be complemented by network-level detection** that persists when endpoint visibility fails, centralized log analysis that correlates events across the environment, and monitoring capabilities that extend to devices and systems beyond the EDR's reach.

9. The Case for Defence-in-Depth

The previous sections documented a problem. This section begins to outline the solution.

Defense-in-depth is not a new concept. Military strategists have understood for centuries that a single defensive line, however strong, can be breached. **The solution is multiple independent layers, each capable of detecting and delaying an adversary, buying time for response and limiting the damage from any single failure.**

Applied to cybersecurity, defence-in-depth means deploying controls that operate independently and compensate for each other's weaknesses. When one layer fails, others continue to provide protection and visibility. The attacker who defeats one control must still contend with the rest.

The Three Pillars

Effective defence against EDR killers rests on three complementary capabilities: **endpoint detection, network detection**, and **centralized log analysis**. Each addresses threats the others cannot see.

- Endpoint detection provides the deepest visibility into individual system behavior. Process execution, file operations, registry modifications, and memory manipulation all occur at the endpoint level. No other vantage point offers comparable granularity for host-based activity.
- Network detection provides visibility that persists regardless of endpoint status. Traffic flows across the network whether or not the source system is compromised. An attacker who has blinded the EDR still generates network activity when moving laterally, communicating with command infrastructure, or exfiltrating data. That traffic is visible to properly positioned network sensors.
- Centralized log analysis correlates events across both domains, identifying patterns that would be invisible when examining either source in isolation. A driver load on one endpoint might be innocuous. The same driver load followed by security service termination, then anomalous SMB traffic to sensitive file shares, then DNS queries to newly registered domains represents a clear attack pattern. Correlation transforms isolated events into actionable intelligence.

Independence as a Design Principle

The three pillars must be genuinely independent to provide meaningful redundancy. If network detection depends on endpoint agents to capture traffic, an EDR killer that disables those agents also blinds the network layer. If log analysis relies solely on EDR telemetry, silencing the EDR silences the SIEM.

True independence requires architectural separation. Network detection must operate through passive capture mechanisms that function regardless of endpoint health. Log collection must include sources beyond the EDR: Windows Event Logs, authentication systems, DNS servers, proxy logs, and infrastructure devices. Each layer

must be capable of detecting attacks even if the other layers are compromised or unavailable.

This independence creates the redundancy that defeats EDR killer strategies. The attacker who successfully neutralizes endpoint protection still faces network-level detection of their lateral movement, SIEM correlation of their preparatory activities, and log-based detection of the security service manipulation that preceded the EDR shutdown.

The Visibility Matrix

Different attack phases generate different types of observable activity. **Initial access typically produces network indicators: connections from unexpected sources, authentication attempts against external services, or traffic patterns consistent with exploitation.** Privilege escalation and defense evasion generate endpoint indicators: driver loads, process manipulation, and service modifications. Lateral movement produces both: endpoint process execution on newly accessed systems and network traffic between internal hosts. Data exfiltration manifests primarily at the network level: unusual outbound data volumes, connections to cloud storage services, or traffic to previously unseen destinations.

A defensive architecture that covers all cells in this matrix maintains visibility throughout the attack lifecycle. **When endpoint visibility fails, network visibility persists. When network visibility is limited, endpoint telemetry fills the gap. The SIEM correlates across both, identifying attacks that manifest partially in each domain.**

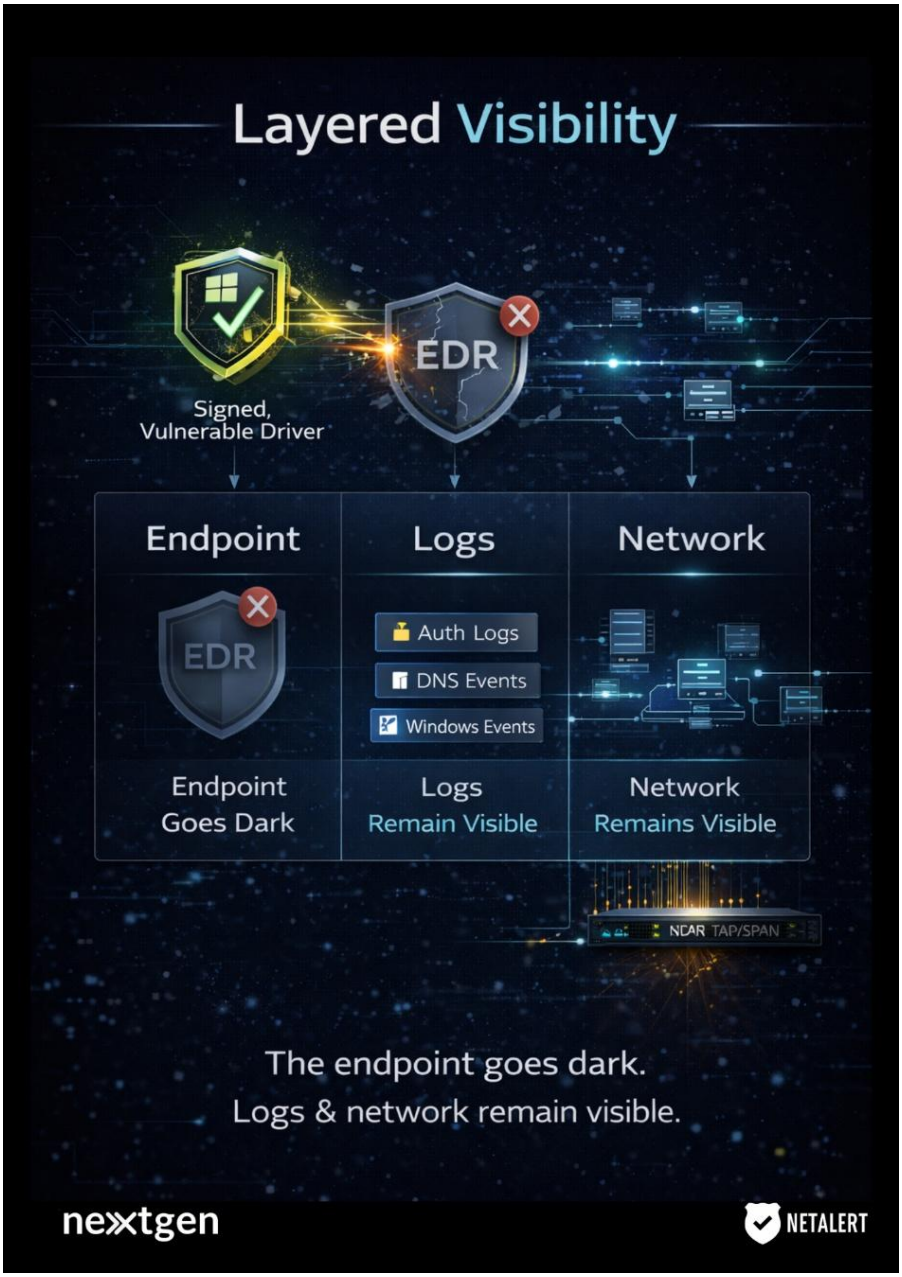
Compensating Controls in Practice

Consider a concrete scenario. An attacker gains initial access through a vulnerable VPN appliance, establishes persistence, and prepares to deploy ransomware. Their playbook includes EDRKillShifter to neutralize endpoint protection before encryption begins.

In an EDR-only architecture, the attack proceeds as follows: the attacker loads the vulnerable driver, exploits it for kernel access, terminates the EDR process, and deploys

ransomware without further detection. The security team discovers the attack only when ransom notes appear.

In a defense-in-depth architecture, the attack unfolds differently. The initial VPN exploitation generates authentication logs collected by the SIEM. The attacker's internal reconnaissance produces DNS queries and network scanning activity visible to NDR. The vulnerable driver download may trigger network-based detection. The driver load generates Windows Event Log entries collected independently of EDR.



The service termination appears in system event logs. The lateral movement to additional systems generates both authentication events and network traffic. The ransomware communication with its infrastructure produces detectable network patterns.Any single detection might be missed or dismissed. But the cumulative pattern across multiple independent sources creates high-confidence alerting that triggers investigation before encryption completes. The attacker's EDR bypass succeeds, but the attack itself fails because visibility persisted through alternative channels.

10. Netalert NDR: Network-Level Visibility That Persists

Netalert NDR operates from a fundamentally different vantage point than endpoint security tools. Rather than monitoring individual systems from within, **Netalert observes traffic flows across the network infrastructure.** This architectural distinction provides detection capabilities that remain intact regardless of endpoint compromise.

10.1 Architecture and Deployment

Netalert deploys through passive network taps or SPAN port configurations. The sensor receives a copy of network traffic without sitting inline with production flows. T**his passive architecture eliminates latency concerns and ensures that sensor failures cannot disrupt business operations.**

The deployment model also means there is **no agent for attackers to disable.** Netalert's visibility comes from network infrastructure, not from software running on potentially compromised endpoints. **An attacker** who has achieved SYSTEM privileges and kernel access on a Windows server **has no mechanism to prevent NetAlert from observing that server's network communications.**

Sensors can be positioned at network boundaries to monitor ingress and egress traffic, at internal segmentation points to observe east-west flows, or at critical junctions where sensitive systems communicate. Strategic placement ensures visibility into the traffic paths that attackers must traverse to achieve their objectives.

10.2 32KB PCAP Recording

Netalert captures and retains the first 32 kilobytes of every network session. This capture size balances forensic utility against storage efficiency. The initial bytes of a connection contain protocol headers, authentication exchanges, and often enough payload data to characterize the communication's purpose.

For incident response, these PCAP fragments provide evidence that telemetry summaries cannot match. Analysts can examine actual packet contents rather than

relying on metadata abstractions. Protocol anomalies, malformed headers, and suspicious payload patterns are directly observable.

The 32KB threshold captures complete transactions for many protocols. DNS queries and responses, LDAP authentication exchanges, SMB session establishment, and HTTP request headers typically fit within this window. For longer sessions, the initial capture still provides protocol identification, source and destination characterization, and often enough context to determine whether the communication warrants further investigation.

Retention policies determine how long these captures remain available. Organisations can tune retention based on compliance requirements, storage capacity, and incident response timelines. **The forensic value of packet captures often exceeds their storage cost, particularly when investigating sophisticated attacks that evade other detection mechanisms.**

10.3 ML-Based Anomaly Detection

Netalert incorporates machine learning models that establish behavioral baselines for network activity. These models learn normal communication patterns: which systems talk to which, using what protocols, at what volumes, during what time windows. Deviations from established baselines generate anomaly scores that feed into detection logic.

The ML approach complements signature-based detection. Signatures catch known bad patterns but miss novel attacks. Anomaly detection catches unusual activity regardless of whether it matches a known signature. The combination provides coverage across the spectrum from commodity threats to zero-day techniques.

Baseline learning occurs continuously, adapting to legitimate changes in network behavior. A new application deployment that changes communication patterns will initially generate anomalies, but the model adapts as the new pattern becomes established. Tuning parameters control the sensitivity of this adaptation, allowing organizations to balance detection sensitivity against alert volume.

10.4 Detection Capabilities

Netalert's detection library addresses multiple threat categories relevant to EDR killer scenarios.

- **Command and control detection** identifies communication between compromised systems and attacker infrastructure. Beaconing patterns, domain generation algorithms, and protocol anomalies associated with common C2 frameworks all trigger detection logic. When an attacker maintains access after disabling EDR, their C2 traffic remains visible to network monitoring.
- **Lateral movement detection** identifies internal reconnaissance and propagation activity. Port scanning, service enumeration, and authentication attempts against multiple systems produce network patterns distinct from normal administrative activity. SMB traffic from unexpected sources, RDP connections outside established patterns, and WMI-based remote execution all generate detectable signatures.
- **Data exfiltration detection** monitors outbound traffic for indicators of data theft. Unusual volumes to cloud storage, connections to file sharing services, and protocol tunnelling techniques designed to bypass security controls all produce alerts. Attackers who successfully disable EDR still need to extract stolen data, and that extraction produces network evidence.
- **Encrypted traffic analysis examines metadata and behavioral characteristics of TLS-encrypted sessions.** While payload content remains opaque, certificate information, connection patterns, and timing characteristics provide substantial analytical value. Many C2 frameworks produce distinctive TLS fingerprints that enable detection despite encryption.

10.5 Detecting Threats When EDR Is Blind

The specific value proposition for EDR killer scenarios centres on Netalert's ability to detect activity that endpoint tools cannot see.

When an attacker loads a vulnerable driver and terminates the EDR process, the endpoint goes dark. But the attacker's subsequent activities still traverse the network.

Lateral movement to additional systems generates authentication traffic and connection establishment visible to Netalert. **Ransomware deployment across network shares produces SMB traffic patterns distinct from normal file server activity.** Encryption of network-accessible files generates anomalous access patterns detectable through traffic analysis.

The Akira webcam case from Section 7 illustrates this detection opportunity. The IoT device that served as the encryption platform had no endpoint protection, **but it communicated across the network to reach its targets.** SMB traffic from an unexpected source, accessing file shares on multiple servers in rapid succession, would generate clear alerts in a properly configured NDR deployment.

NetAlert also detects the preparatory stages that precede EDR neutralisation. The vulnerable driver downloads, the command and control communication that delivers attack instructions, and the reconnaissance activity that identifies security tools all produce network indicators. Detection at these earlier stages enables response before the EDR goes offline.

11. Cyberquest SIEM: Centralised Detection and Correlation

Where Netalert provides network-level visibility, **Cyberquest SIEM provides the correlation and context layer that transforms raw events into actionable intelligence.** By collecting logs from diverse sources and applying detection logic across them, Cyberquest identifies attack patterns that would be invisible when examining any single data source in isolation.

11.1 Log Collection and Normalisation

Cyberquest ingests log data from across the enterprise environment. Windows Event Logs, Linux syslogs, application logs, authentication systems, network infrastructure, cloud platforms, and security tools all feed into the centralized collection infrastructure. **This breadth ensures that detection logic can draw on the full range of available telemetry.**

Log normalisation transforms disparate formats into a common schema. A Windows logon event, a Linux SSH authentication, and a cloud platform sign-in all represent fundamentally similar activities but arrive in completely different formats. Normalisation maps these variations to consistent field structures, enabling correlation rules to operate across heterogeneous environments.

The collection architecture supports multiple ingestion methods. Agent-based collection deploys lightweight forwarders to source systems. Agentless collection uses native protocols like syslog, Windows Event Forwarding, or API integrations. **The flexibility accommodates diverse infrastructure requirements and ensures coverage even for systems where agent deployment is impractical.**

11.2 Correlation Engine and UEBA

Cyberquest's correlation engine applies detection logic across the normalized event stream. Rules can reference events from multiple sources, across variable time windows, with complex conditional logic. A single rule might correlate a failed authentication attempt from a Windows domain controller with subsequent successful authentication from the same source, followed by service installation on a remote system, all within a defined time window.

The rule library includes over 500 pre-built correlation rules addressing common attack patterns. These rules provide immediate detection value while serving as templates for environment-specific customization. Security teams can modify existing rules or develop new ones to address threats specific to their infrastructure.

User and Entity Behavior Analytics extends detection beyond rule-based logic. UEBA models establish baseline behaviour patterns for users and systems, then identify deviations that may indicate compromise. An account that suddenly accesses systems outside its normal scope, or a server that begins communicating with unusual destinations, triggers UEBA alerts even if no specific rule matches the activity.

The combination of rule-based and behavior-based detection provides coverage across the threat spectrum. Rules catch known attack patterns efficiently. UEBA catches novel patterns that rule authors have not anticipated.

11.3 Detection Capabilities for EDR Killer Scenarios

Cyberquest's detection capabilities directly address the EDR killer threat through multiple detection approaches.

Driver loading events appear in Windows Event Logs independently of EDR telemetry. Event ID 7045 records service installations, including kernel-mode driver services. Correlation rules can identify driver loads from unusual paths, with suspicious names, or at unexpected times. The vulnerable drivers used in BYOVD attacks often exhibit characteristics distinguishable from legitimate driver installations.

Security service manipulation generates multiple log events. Service stop and start events, process termination events, and security log tampering all produce records that Cyberquest collects and analyses. **A rule correlating driver installation with subsequent security service termination provides high-confidence detection of EDR killer deployment.**

Authentication anomalies associated with privilege escalation and lateral movement generate log evidence across multiple sources. Unusual service account activity, authentication from unexpected sources, and access patterns inconsistent with normal operations all produce detectable events. These indicators often precede EDR neutralization, enabling detection before endpoint visibility is lost.

Windows Defender and other built-in security components generate their own event streams. Attackers who disable EDR often overlook or incompletely address these secondary sources. Correlation rules that monitor Defender events, Windows Firewall logs, and AppLocker records can identify attacks that the primary EDR has been prevented from reporting.

11.4 Automation and Response

Detection without response provides limited value. Cyberquest integrates with response orchestration through playbooks that automate containment and remediation actions.

When correlation rules identify high-confidence threats, automated playbooks can execute predefined response actions. Network isolation of compromised systems, account disablement for compromised credentials, and blocking of malicious infrastructure can all proceed without waiting for analyst intervention. For EDR killer scenarios where speed is critical, automated response may be the only mechanism fast enough to prevent damage.

Playbooks support conditional logic that adapts response based on context. A potential EDR bypass on a workstation might trigger investigation and monitoring. The same indicator on a domain controller might trigger immediate isolation given the higher impact potential. Contextual response ensures that automation does not cause unnecessary disruption while still providing rapid containment for genuine threats.

Integration with Netalert enables cross-platform response coordination. A Cyberquest detection can trigger Netalert to increase monitoring sensitivity for the affected network segment, capture additional traffic for forensic analysis, or feed IP addresses into blocking policies. The combination provides response capabilities that neither platform could achieve independently.

12. Detection Strategies: Catching EDR Killers in Action

The previous sections described what Cyberquest and Netalert can do. This section details how to configure them for EDR killer detection. The strategies fall into three categories: SIEM-based detections using log correlation, NDR-based detections using network traffic analysis, and combined detections that leverage both platforms.

12.1 SIEM-Based Detections

Vulnerable Driver Loading

Windows Event ID 7045 records service creation events, including driver services. A detection rule should trigger when a driver service is created meeting any of these conditions:

The service binary path points to a temporary directory, user profile path, or other unusual location for legitimate drivers. Legitimate drivers typically install System32\drivers or program-specific directories.

The driver name matches known BYOVD candidates. Maintaining a list of driver names associated with EDR killer tools enables signature-based detection. The list should include variations and partial matches to account for attacker attempts at evasion.

The driver file was recently created. Correlation between the driver load event and file creation timestamps can identify drivers dropped immediately before loading, a pattern consistent with attack tooling rather than legitimate software installation.

The rule should exclude known legitimate driver paths and correlate with contextual factors like time of day, source user, and recent system activity to manage false positive rates.

Security Service Termination

Windows Event ID 7036 records service state changes. EDR killer activity produces a distinctive pattern: driver service start followed rapidly by security service stops. A correlation rule should identify:

Multiple security-related services stop within a short time window, particularly outside maintenance windows. EDR products, antivirus services, and Windows security components rarely stop simultaneously under normal operation.

Security service termination preceded by driver service creation within a defined time window. This sequence directly represents the BYOVD attack pattern.

Security service termination without corresponding scheduled maintenance or administrative change records.

Process Termination Patterns

EDR killers terminate security processes in predictable sequences. Sysmon Event ID 5, or equivalent process termination logging, can identify:

- Termination of multiple security-related processes within seconds. Legitimate administrative actions rarely require terminating multiple security tools simultaneously.
- Process termination by unusual parent processes. A driver or service that was recently created terminating established security processes represents highly suspicious activity.
- Termination of protected processes. EDR agents often run as protected processes that cannot be terminated through normal means. Successful termination indicates kernel-level manipulation.

ETW and AMSI Tampering

While ETW and AMSI bypass occur in memory and may not generate direct log evidence, their effects can be detected indirectly:

Gaps in expected telemetry streams. If a system normally generates consistent PowerShell logging and that logging suddenly stops while the system remains active, **the gap itself is an indicator.**

Process creation for known bypass tools. Many ETW and AMSI bypass techniques require initial code execution that may be logged before the bypass takes effect.

Registry modifications to telemetry configuration. Some bypass techniques modify registry keys that control event generation. Monitoring these keys provides detection opportunity.

12.2 NDR-Based Detections

Vulnerable Driver Download

BYOVD attacks require the vulnerable driver to reach the target system. Unless the driver is already present, it must be downloaded. Netalert can detect:

- Downloads of known vulnerable driver files by hash or name from external sources.
- File transfers over SMB or HTTP from internal systems may be staging attack tools.
- Connections to infrastructure associated with EDR killer distribution, including known criminal forums and file hosting services.

Post-Compromise C2 Traffic

After disabling EDR, attackers typically maintain command and control communication. Netalert detection opportunities include:

- Beaconing patterns indicating periodic check-in with attacker infrastructure. Regular intervals, consistent packet sizes, and predictable timing all contribute to beacon identification.
- DNS queries for suspicious domains. Newly registered domains, DGA patterns, and lookups for known malicious infrastructure all warrant investigation.
- Protocol anomalies suggest tunnelling or covert channels. HTTP traffic with unusual header patterns, DNS queries with encoded data, and HTTPS connections with suspicious certificate characteristics all indicate potential C2.

Lateral Movement Detection

With EDR disabled, attackers proceed to their objectives through lateral movement that generates network evidence:

- SMB traffic to administrative shares from unexpected sources. The C$ and ADMIN$ shares used for remote execution produce distinctive access patterns.
- RDP connections outside established baselines. New RDP relationships, particularly to sensitive systems, warrant investigation.
- WMI and PowerShell remote traffic. Remote management protocols used for lateral movement produce identifiable network signatures.
- Authentication traffic anomalies. Kerberos ticket requests, NTLM authentication, and pass-the-hash attempts all generate network-visible evidence.

Exfiltration Indicators

Data theft following EDR bypass produces network evidence regardless of endpoint status:

- Unusual outbound data volumes. Baseline comparison identifies systems transmitting significantly more data than normal.
- Connections to cloud storage and file sharing services. While legitimate use is common, unusual patterns or new destinations warrant investigation.
- Protocol tunnelling. Data exfiltration through DNS, ICMP, or other protocols designed to evade controls produce detectable anomalies.

12.3 Combined Detection Scenarios

The highest-confidence detections correlate evidence across both platforms. Several scenarios illustrate this approach:

Scenario: Driver Load Plus Network Anomaly

Cyberquest detects a suspicious driver service creation on a workstation. Within the next hour, Netalert identifies unusual SMB traffic from that workstation to multiple file servers. Neither event alone might trigger high-priority response, but the combination strongly suggests an EDR bypass followed by ransomware staging.

Scenario: Service Termination Plus C2 Traffic

Cyberquest detects security service termination on a server. Netalert identifies new beacon-like outbound traffic from that server to an external destination. The correlation confirms that the service termination was malicious rather than administrative, and the C2 traffic indicates active attacker presence requiring immediate response.

Scenario: Authentication Anomaly Plus Lateral Traffic

Cyberquest detects unusual service account authentication from an unexpected source system. Netalert identifies subsequent administrative traffic from that source to multiple internal destinations. The pattern suggests credential theft followed by lateral movement, with EDR bypass likely either completed or imminent.

12.4 Sample Correlation Logic

The following pseudocode illustrates correlation rule structure for Cyberquest:

```
Rule 1: BYOVD_Attack_Sequence
Description: Detects driver load followed by security service termination

Condition A: Event ID 7045 (Service Creation)
  WHERE ServiceType = "kernel driver"
  AND ImagePath NOT IN (known_legitimate_paths)
  AND ImagePath MATCHES (temp_directory OR user_profile)

Condition B: Event ID 7036 (Service State Change)
  WHERE ServiceName IN (security_service_list)
  AND State = "stopped"

Correlation: A followed by B
  WHERE B.Timestamp - A.Timestamp < 300 seconds
  AND A.ComputerName = B.ComputerName

Alert: Critical
Response: Initiate isolation playbook, notify SOC
```

```
Rule 2: Network_Exfil_After_EDR_Bypass
Description: Correlates EDR bypass indicators with network exfiltration

Condition A: BYOVD_Attack_Sequence fired
  (references previous rule)

Condition B: Netalert alert
  WHERE AlertType IN (data_exfiltration, unusual_outbound_volume)
  AND SourceIP = A.ComputerName.IP

Correlation: A followed by B
  WHERE B.Timestamp - A.Timestamp < 3600 seconds

Alert: Critical
Response: Block destination IP, initiate full IR
```

13. Practical Implementation Recommendations

Strategy without execution remains theoretical. This section provides actionable recommendations for organizations seeking to implement defense-in-depth against EDR killer threats.

Phase 1: Assessment

Begin by mapping current visibility. Document which systems have EDR coverage, which generate logs collected by SIEM, and which network segments have NDR visibility. Identify gaps where attacks could proceed undetected.

Inventory the log sources feeding your SIEM. Windows Security and System event logs from all domain-joined systems represent the minimum baseline. Extend collection to include Sysmon where deployed, PowerShell logging, authentication system logs, and DNS query logs.

Evaluate NDR sensor placement. Coverage should include the network boundary, connections to sensitive internal segments, and paths between user systems and critical infrastructure. Identify blind spots where traffic could traverse without observation.

Phase 2: Detection Development

Implement the SIEM detection rules described in Section 12. Start with high-confidence, low-false-positive rules and expand coverage as tuning progresses.

Build a vulnerable driver reference list. Published resources like the LOLDrivers project maintain catalogues of known BYOVD candidates. Import these into detection rules as negative indicators.

Configure Netalert detection policies for lateral movement, C2 traffic, and exfiltration. Baseline the network to establish normal patterns before enabling anomaly-based alerts.

Develop correlation rules that span both platforms. The scenarios in Section 12.3 provide templates that can be adapted to specific environments.

Phase 3: Response Integration

Map detection rules to response playbooks. High-confidence detections should trigger automated containment. Lower-confidence detections should trigger investigation workflows.

Test response automation in controlled conditions before enabling in production. Verify that isolation actions work as expected and that appropriate personnel receive notifications.

Establish escalation procedures for EDR bypass scenarios. When endpoint visibility is compromised, response coordination becomes more complex. Clear procedures ensure that responders know how to proceed when their primary tools are unavailable.

Phase 4: Validation

Test detection coverage through controlled exercises. Purple team engagements that simulate BYOVD attacks validate whether detections fire as expected and whether response playbooks execute correctly.

Verify that log collection continues when EDR is unavailable. The independence principle requires that SIEM visibility persist even when endpoint agents are disabled. Test this assumption directly.

Evaluate detection latency. If detections take longer to fire than attacks take to complete, the detections provide forensic value but limited prevention capability. Identify opportunities to reduce detection and response time.

Ongoing Operations

Update vulnerable driver lists as new candidates are discovered. **The BYOVD landscape evolves continuously, and detection signatures must evolve with it.**

Review detection rule performance regularly. Rules that generate excessive false positives will be disabled or ignored. Rules that never fire may indicate gaps or environmental differences from rule assumptions.

Maintain independence between detection layers. Infrastructure changes that inadvertently create dependencies between EDR, NDR, and SIEM undermine the redundancy that defense-in-depth provides.

14. Regulatory and Compliance Considerations

EDR killer techniques create compliance implications beyond the immediate security concerns. Regulatory frameworks increasingly mandate specific security capabilities that BYOVD attacks can undermine.

Data Protection Requirements

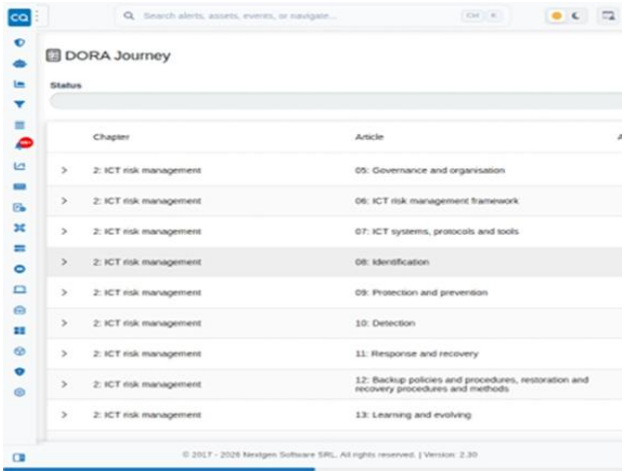
GDPR, CCPA, and similar regulations require appropriate technical measures to protect personal data. When EDR bypass enables ransomware operators to access and exfiltrate sensitive data, organizations face potential regulatory liability in addition to operational impact.

Defense-in-depth architectures support compliance by demonstrating that security investments extend beyond single points of failure. **Network monitoring and SIEM correlation provide the "appropriate technical measures" that regulators expect, even if any single control can be defeated.**

Breach notification timelines create urgency around detection capability. Regulations typically require notification within 72 hours of discovering a breach. Detection capabilities that identify compromises quickly enable organizations to meet notification deadlines and limit regulatory exposure.

Industry-Specific Mandates

Financial services regulations like PCI DSS require continuous monitoring and logging of security events. The logging capabilities of Cyberquest SIEM directly address these requirements while providing detection value against EDR killer techniques.



Healthcare regulations under HIPAA require security incident procedures and audit controls. Network monitoring provides the audit trail that demonstrates compliance while enabling detection of threats that endpoint tools may miss.

Critical infrastructure regulations increasingly mandate specific security capabilities. The layered visibility provided by combined SIEM and NDR deployment addresses regulatory expectations while providing genuine security improvement.

Cyber Insurance Considerations

Insurers have grown more sophisticated in evaluating security posture. Many now require specific controls as conditions of coverage. EDR deployment has become a common requirement, but insurers are beginning to recognize that EDR alone is insufficient.

Organizations that can demonstrate defense-in-depth architectures may qualify for better coverage terms. The ability to detect and respond to threats even when primary controls fail represents the resilience that insurers seek to underwrite.

Claims documentation benefits from the forensic capabilities that NDR packet capture provides. When investigating incidents for insurance purposes, actual network evidence carries more weight than reconstructed timelines based solely on endpoint telemetry.

15. Conclusion: The Imperative for Layered Visibility

The ransomware ecosystem has evolved. EDR killers have moved from advanced technique to commodity capability. The tools are available, affordable, and effective. Defenders who rely solely on endpoint protection are betting their organizations on a single point of failure that attackers have demonstrated they can defeat.

This whitepaper has documented the threat in detail: the techniques that enable EDR bypass, the marketplaces where these tools trade, the threat actors who deploy them, and the real-world incidents where they have succeeded. The evidence is clear. EDR alone is no longer sufficient.

The solution is not to abandon EDR. Endpoint visibility remains valuable and necessary. The solution is to complement EDR with independent detection capabilities that persist when endpoint protection fails.

Network Detection and Response operates from a vantage point that attackers cannot disable from compromised endpoints. The network does not go silent when an EDR agent terminates. Traffic continues to flow, and properly positioned sensors continue to observe it. Netalert provides this persistent visibility through passive deployment, comprehensive traffic capture, and detection capabilities tuned for the threats that emerge when endpoints are compromised.

SIEM provides the correlation layer that transforms isolated events into actionable intelligence. Cyberquest collects logs from sources beyond EDR, applies detection logic across them, and identifies attack patterns that no single data source reveals. When EDR goes dark, the SIEM maintains visibility through Windows Event Logs, authentication systems, and network telemetry that continue generating data regardless of endpoint agent status.

Together, these capabilities create the defense-in-depth architecture that modern threats demand. Attackers who successfully bypass EDR still face network-level detection of their lateral movement, correlation-based identification of their attack patterns, and automated response capabilities that can contain threats before damage spreads.

The ransomware operators understand this. They continue investing in EDR bypass because it works against organizations that have not invested in layered visibility. The question for defenders is straightforward: will you be the target where EDR bypass is sufficient, or will you be the target where attackers discover that disabling the endpoint was only the beginning of their problems?

The threat landscape has shifted.

Your defensive architecture must shift with it.

Appendix A: MITRE ATT&CK Mapping

EDR killer techniques map to multiple ATT&CK tactics and techniques (not exhaustive):

Defence Evasion (TA0005)

- T1562.001: Impair Defenses: Disable or Modify Tools
- T1562.002: Impair Defenses: Disable Windows Event Logging
- T1562.004: Impair Defenses: Disable or Modify System Firewall
- T1014: Rootkit
- T1112: Modify Registry
- T1218: System Binary Proxy Execution

Privilege Escalation (TA0004)

- T1068: Exploitation for Privilege Escalation
- T1543.003: Create or Modify System Process: Windows Service

Execution (TA0002)

- T1569.002: System Services: Service Execution
- T1106: Native API

Persistence (TA0003)

- T1547.006: Boot or Logon Autostart Execution: Kernel Modules and Extensions
- T1543.003: Create or Modify System Process: Windows Service

Lateral Movement (TA0008)

- T1021.002: Remote Services: SMB/Windows Admin Shares
- T1021.001: Remote Services: Remote Desktop Protocol
- T1047: Windows Management Instrumentation

Exfiltration (TA0010)

- T1041: Exfiltration Over C2 Channel
- T1567: Exfiltration Over Web Service

Appendix B: Indicators of Compromise

Vulnerable Drivers (Partial List)

Driver Name	Associated Tool	CVE/Vulnerability
zam64.sys	Terminator	Process termination
procexp.sys	AuKill	Arbitrary process termination
gdrv.sys	Multiple	Arbitrary memory read/write
dbutil_2_3.sys	EDRSandBlast	Arbitrary memory read/write
asio64.sys	Multiple	Memory access
mhyprotect.sys	Multiple	Process termination
ene.sys	Multiple	I/O control
BS_HWMIO64.sys	MS4Killer	Memory access

File Path Indicators

EDR killers commonly deploy from:

- C:\Windows\Temp\
- C:\Users[user]\AppData\Local\Temp\
- C:\ProgramData\
- User profile directories with randomised names

Registry Indicators

Driver service creation modifies:

- HKLM\SYSTEM\CurrentControlSet\Services[driver_name]
- Values: ImagePath, Type, Start

Security service manipulation may modify:

- HKLM\SYSTEM\CurrentControlSet\Services[security_service]\Start

Network Indicators

Post-compromise traffic patterns:

- Beaconing intervals: 30-60 second cycles common
- C2 destinations: newly registered domains, dynamic DNS

- Exfiltration: connections to cloud storage, unusual outbound volumes
- Lateral movement: administrative share access, RDP from workstations to servers

References

1. CISA. "BYOVD Attacks on the Rise." Cybersecurity Advisory, 2024.
2. ESET. "RansomHub and the QuadSwitcher Connection." ESET Research, 2025.
3. Sophos X-Ops. "Multiple Ransomware Groups Share EDRKillShifter Framework." Sophos Labs, August 2025.
4. Cisco Talos. "Trends in Ransomware: EDR Bypass and Defense Evasion." Talos Intelligence, 2024.
5. S-RM. "Akira Ransomware Pivots Through IoT Device." Incident Response Report, 2025.
6. Kaspersky. "IT Threat Evolution Q1 2025." Securelist, 2025.
7. CYFIRMA. "Global Ransomware Trends Report." August 2025.
8. IBM Security. "Cost of a Data Breach Report 2025." IBM, 2025.
9. Palo Alto Unit 42. "Ransomware and Extortion Report." Unit 42, 2025.
10. Logpoint. "Emerging Threats: EDR Killers in the Ransomware Ecosystem." 2024.
11. Microsoft. "Driver Block Rules." Microsoft Learn Documentation, 2025.
12. LOLDrivers Project. "Living Off The Land Drivers." https://www.loldrivers.io/
13. Cyber Security Agency of Singapore. "Advisory on EDR Killer Tools." August 2025.
14. MITRE ATT&CK. "Enterprise Tactics and Techniques." https://attack.mitre.org/