OS SECURITY

When Your OS Starts Working for the Hacker

The fundamental premise of legacy endpoint security is that the operating system itself can be trusted to report accurate telemetry. The data indicates that this assumption is a dangerous fallacy.

Dennis Underwood, Founder & CEO, Cyber Crucible · November 2026

EXECUTIVE SUMMARY

The cybersecurity market is currently experiencing a profound structural failure. For the past decade, the industry has relied upon a "collect and analyze" paradigm, wherein endpoint detection and response (EDR) platforms function as lightweight sensors that ship telemetry to cloud-based servers for human or algorithmic analysis.[1] This architecture is fundamentally reactive and heavily dependent on the underlying stability and integrity of the host operating system.[1] However, as cyber adversary tradecraft has evolved from file-based malware to hyper-automated, in-memory exploits targeting foundational operating system libraries, the legacy security stack has been rendered effectively blind.[1]

01 The Catalyst for Change: The Failure of Foundational Operating Systems

To understand the strategic necessity of the OS Independence pivot, one must first deeply examine the deteriorating state of the environment in which modern cybersecurity tools operate. The fundamental premise of legacy endpoint security is that the operating system itself can be trusted to report accurate telemetry.[1] The data indicates that this assumption is a dangerous fallacy.

02 The Weaponization of Core OS Libraries and Memory-Based Attacks

In recent years, a dramatic shift in cybercriminal tradecraft emerged. Attackers ceased dropping standalone executable files onto hard drives—a tactic easily thwarted by traditional Application Whitelisting (AWL) and legacy antivirus—and instead began hiding malicious code directly within the memory of legitimate, running processes.[1] This tradecraft bypasses file-based checks entirely, turning the system's own trusted applications into vehicles for exploitation. Industry analysis indicates that 79% of targeted attacks now utilize these "Living Off the Land" (LotL) binaries and scripts.[1]

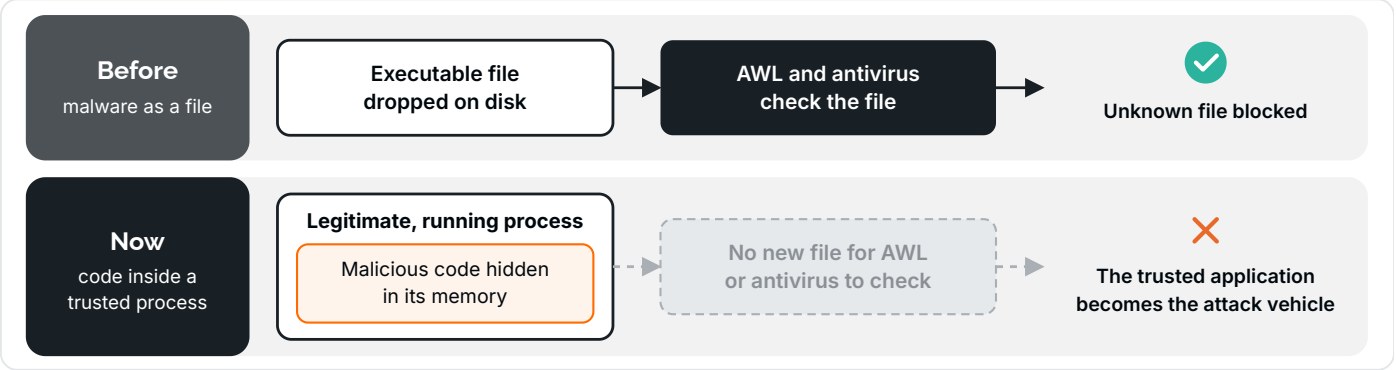

Figure 1. How attackers ride trusted OS components instead of dropping files

The most sophisticated of these attacks specifically target the core coding libraries known as System32 DLLs (System32 is the folder of core Windows system files), which run the Windows operating system and all applications that operate within it.[1] Because legacy EDR tools rely on these exact same libraries to function, collect data, and communicate with the cloud, attackers who infect these libraries in memory achieve near-omnipotence.[1] They gain the power to inspect, alter, or destroy data with untraceable stealth, all while the EDR tool reports to the cloud that the system is functioning normally.[1]

The analogy is straightforward: traditional EDR relies on the building's own security cameras to spot an intruder, but the modern intruder has already rewired the cameras to loop old footage.

Furthermore, adversaries have learned to weaponize the stability of the security tools themselves.[1] By manipulating the compromised OS libraries, attackers can cause the EDR agent to consume massive amounts of CPU or memory, degrading system performance to the point where the frustrated end-user intentionally disables their own defenses.[1] Incumbent security

vendors remain exasperated and blind to this tactic, unable to replicate the "poor customer experience" in their labs because they cannot see the root-level manipulation occurring beneath their user-space sensors.[1]

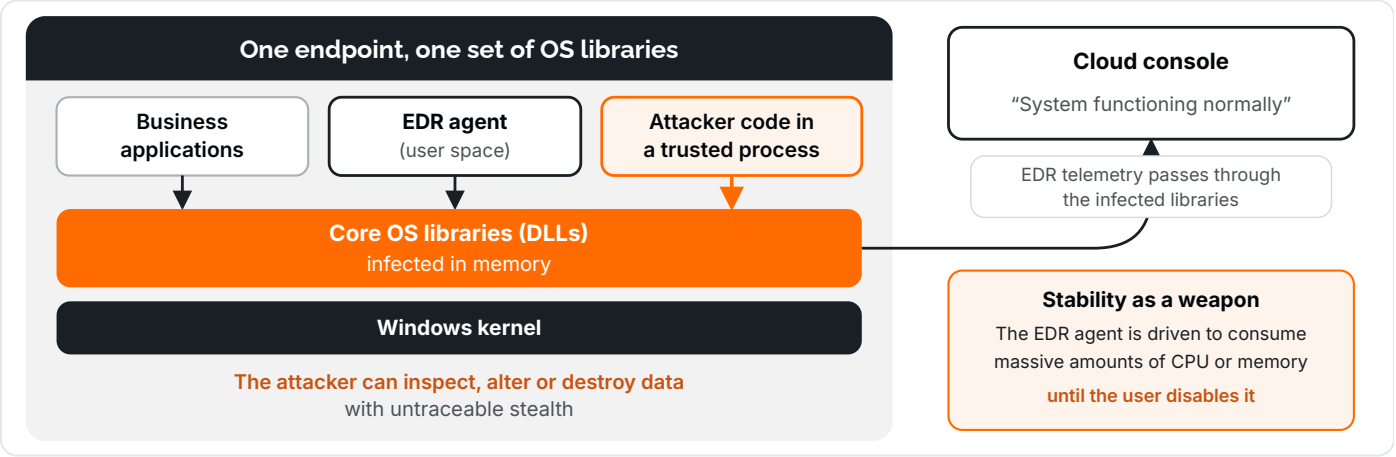

Figure 2. Why security tools that depend on the same OS libraries go blind

03 Surging Vulnerability Metrics and OS Fragility

The quantitative data regarding operating system stability validates the decision to decouple security operations from Microsoft's foundational libraries. The vulnerability landscape has accelerated well beyond the capacity of traditional patch management, creating an environment of perpetual exposure.

In 2024, the industry recorded 39,936 Common Vulnerabilities and Exposures (CVEs).[2] By the end of 2025, that number had surged by 20.6% to an unprecedented 48,175 CVEs, meaning an average of 132 new vulnerabilities were disclosed every single day.[2] More alarmingly, approximately 38% of these vulnerabilities were rated as High or Critical severity.[2]

Year	Total CVEs Disclosed	Year-Over-Year Growth	Average CVEs per Day
2021	20,177	+9.9%	~55
2022	25,000	+23.9%	~68
2023	28,848	+15.4%	~79
2024	39,936	+38.4%	~109
2025	48,175	+20.6%	~132

Focusing specifically on the Microsoft ecosystem, the metrics reveal a highly fragile foundation. While the total number of Microsoft-specific vulnerabilities hovered around 1,273 in 2025, the severity of these flaws escalated dramatically.[3]

Microsoft Vulnerability Metric (2025)	Data Point	Market Implication
Critical Vulnerabilities	157	A 100% year-over-year increase from 78 in 2024, indicating severe flaws are becoming more common.[3]
Elevation of Privilege (EoP) Flaws	509	Accounting for 40% of all vulnerabilities, these allow attackers to bypass user-space security and access the kernel.[3]
Windows OS Vulnerabilities	612	Representing almost half of all Microsoft flaws, ensuring constant instability at the OS layer.[3]
Windows Server Vulnerabilities	780	Critical infrastructure is highly exposed, with 50 of these rated as Critical.[3]

The proliferation of Elevation of Privilege (EoP) vulnerabilities is the most critical metric for security engineering. These flaws allow an attacker with standard user access to escalate their permissions to the administrative or kernel level. Once an attacker has kernel access, any security product operating in the user-space is instantly defeated.

References

1. Cyber Crucible, white papers (compilation, 24 February 2026), Intelligence Hub. https://www.cybercrucible.com/intelligence-hub
2. Mondoo, "2026 State of Vulnerabilities: Annual Security Report," accessed May 1, 2026. https://mondoo.com/vulnerability-intelligence/state-of-vulnerabilities-2026
3. BeyondTrust, "2026 Microsoft Vulnerabilities Report," 13th edition, accessed May 1, 2026. https://www.beyondtrust.com/resources/whitepapers/microsoft-vulnerability-report

Related papers

- **Part 2 of 4:** Patch Regressions and Ecosystem Fragility www.cybercrucible.com/intelligence-hub/patch-regressions-and-ecosystem-fragility
- **Part 3 of 4:** Case Studies: The Axios NPM Compromise and the 'BlueHammer' Defender Zero-Day www.cybercrucible.com/intelligence-hub/axios-npm-compromise-and-bluehammer-defender-zero-day
- **Part 4 of 4:** Autonomous Kernel Prevention vs the Telemetry Model www.cybercrucible.com/intelligence-hub/autonomous-kernel-prevention-vs-telemetry-model
- **In-Memory Attacks:** A Trojan Horse in the RAM www.cybercrucible.com/intelligence-hub/a-trojan-horse-in-the-ram
- **Attack Tradecraft:** DLL Side-Loading: How Attackers Hide Inside Trusted Software www.cybercrucible.com/intelligence-hub/dll-side-loading-how-attackers-hide-in-trusted-software

Read online (six languages): www.cybercrucible.com/intelligence-hub/when-your-os-starts-working-for-the-hacker
Book a live technical demo: www.cybercrucible.com/demo