Inside the Attacker's Playbook: How EDR Evasion Really Works

Jeff Wheat
Lumu CTO
jwheat@lumu.io

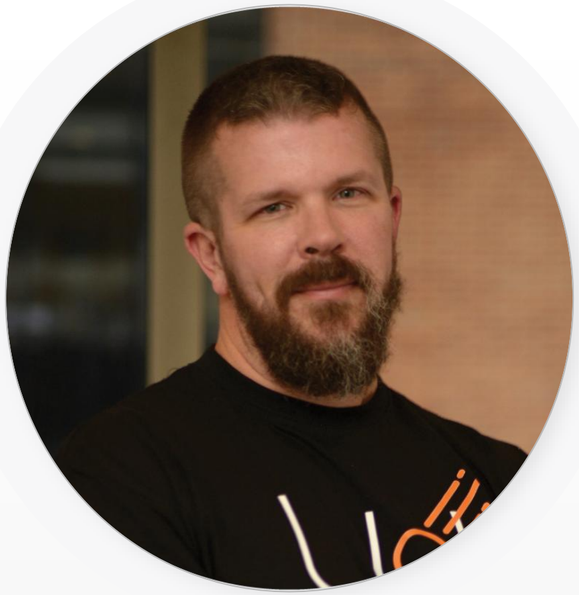
Dr. Chase Cunningham
Field CISO
ccunningham@lumu.io

LUMU

Jeff Wheat

Field CISO, Lumu

- CISO, Blue Team Alpha
- VP of Solutions Engineering, Gradient Cyber
- NSA



Dr. Chase Cunningham

Field CISO, Lumu

- Principal Analyst, Forrester
- Cyber Research and Development Lead, Accenture
- Chief Cryptographic Technician, NSA

LUMU

Overview of
Key Topics

- The Healthcare Threat Landscape
- Medical OT
- EDR Bypass & Evasion
- Combating Defense Evasion

LUMU

Hospitals Under Attack

Brockton Hospital Ransomware Attack: Downtime Procedures to Continue for Two Weeks

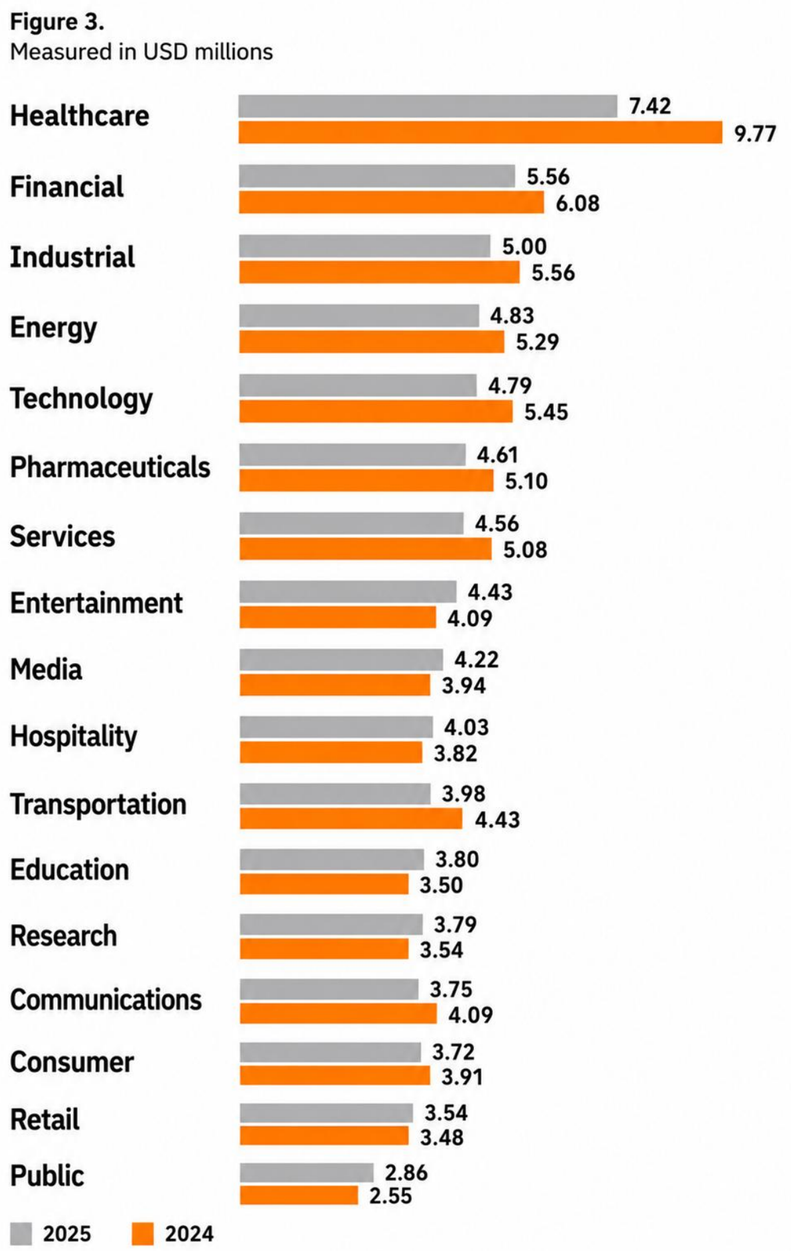
Stryker warns of earnings fallout from March cyberattack

State AG Sues Change Healthcare in 2024 Ransomware Attack

The Healthcare Threat Landscape

Healthcare remained the most expensive industry for breaches

At USD 7.42 million, healthcare recorded the highest average breach cost among industries for the 12th consecutive year—even as it saw a sharp reduction from last year (USD 9.77 million). Attackers continue to value and target the industry's patient personal identification information (PII), which can be used for identity theft, insurance fraud and other financial crimes. Healthcare breaches took the longest to identify and contain at 279 days. That's more than five weeks longer than the global average. **See Figure 3.**



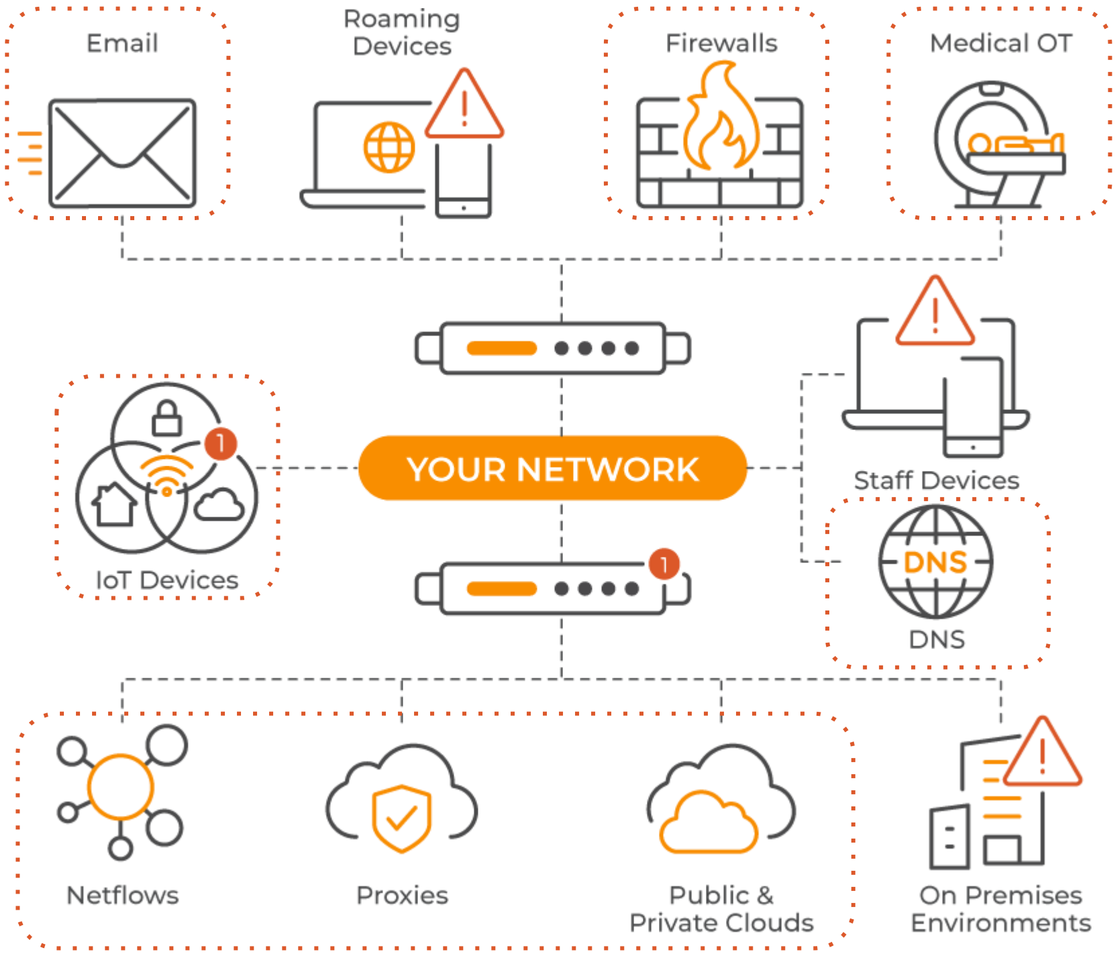
Source: IBM Cost of a Data Breach Report 2025

“No **EDR** caught all Living-off-the-Land attacks”

2026

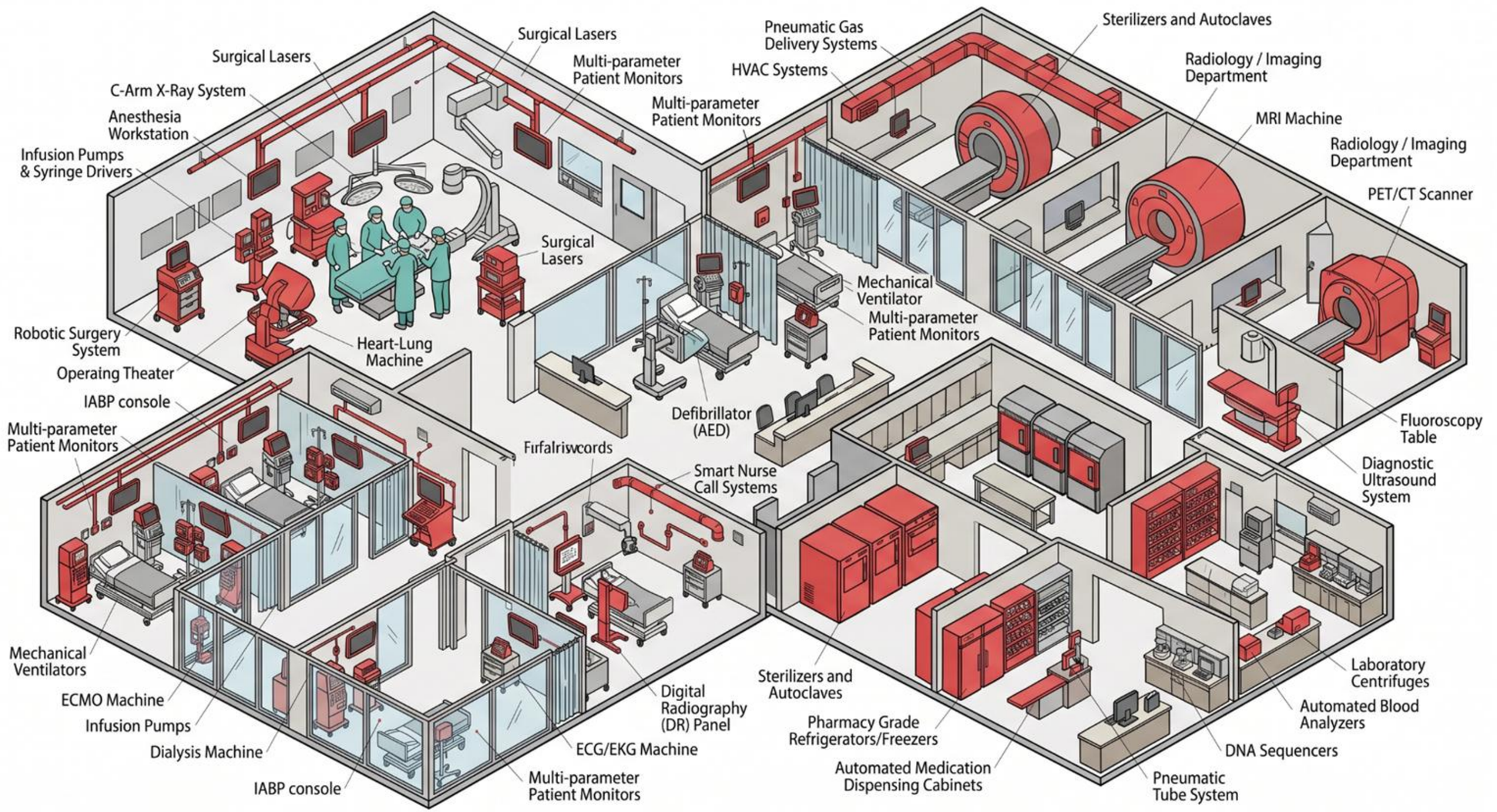
Your **EDR** Is Leaving **Critical Blind Spots in the Network**

Most EDR solutions, while valuable for responding to threats, leave blind spots that attackers often exploit in the network.



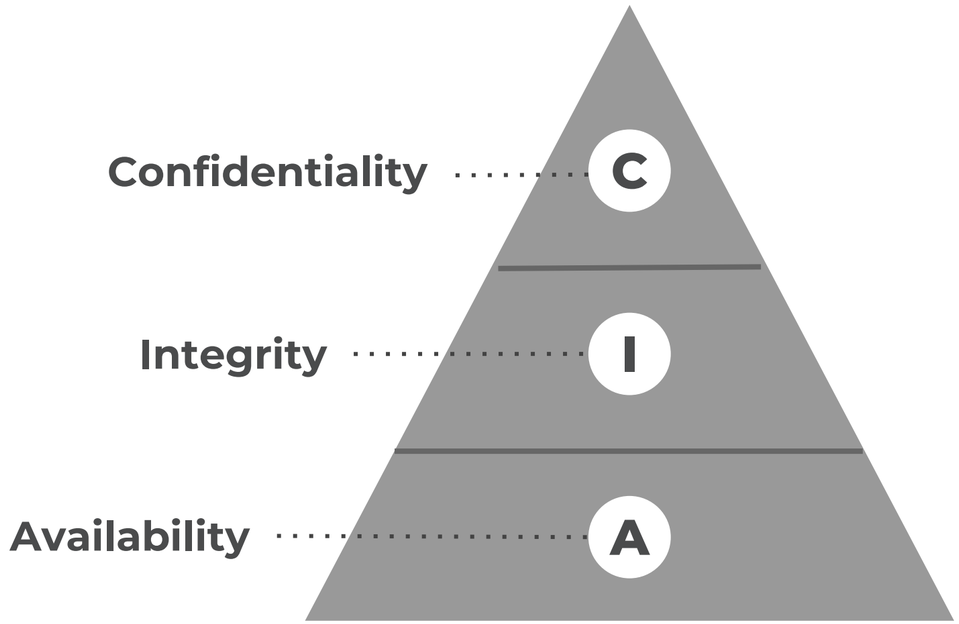
LUMU

The Medical OT Attack Surface

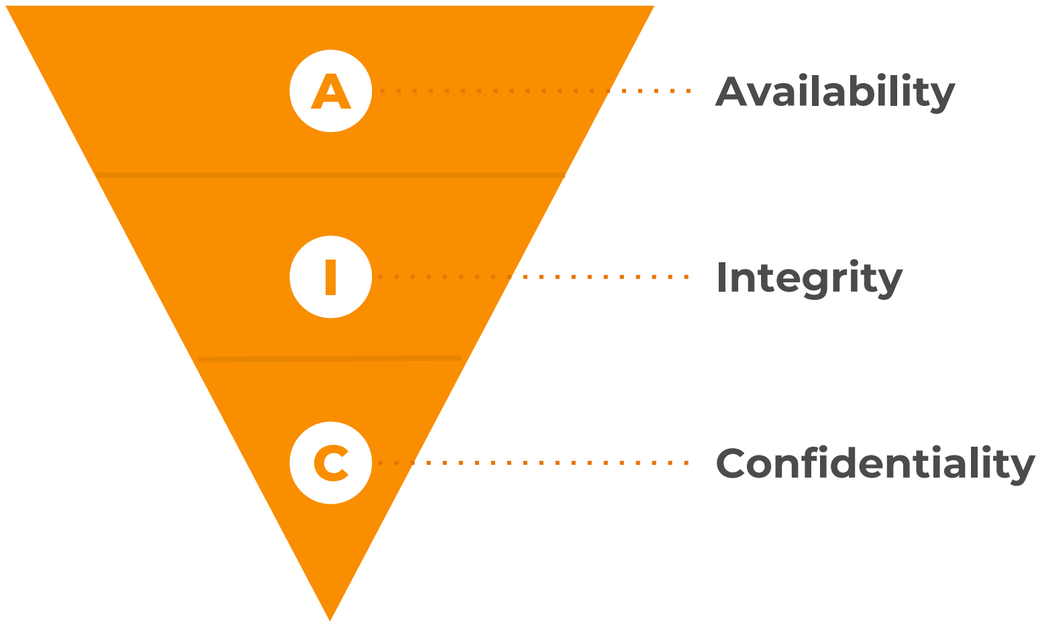


Cybersecurity Priorities

Other Industries: CIA



Healthcare: AIC

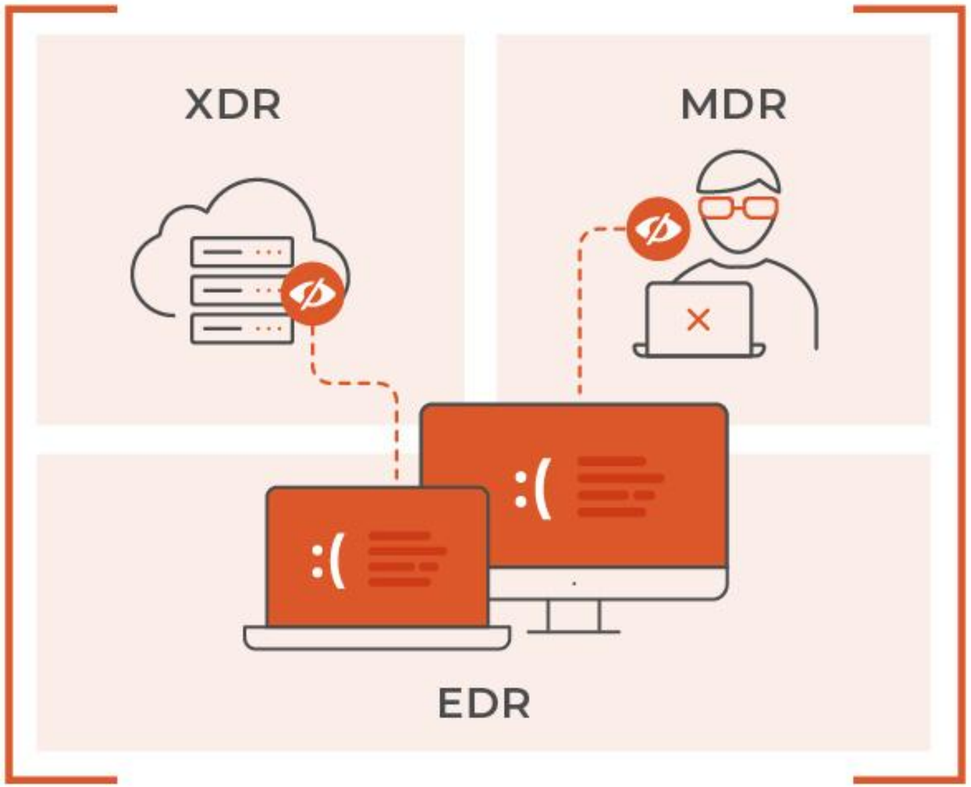


Consequences of EDR Evasion
& Medical OT Infection

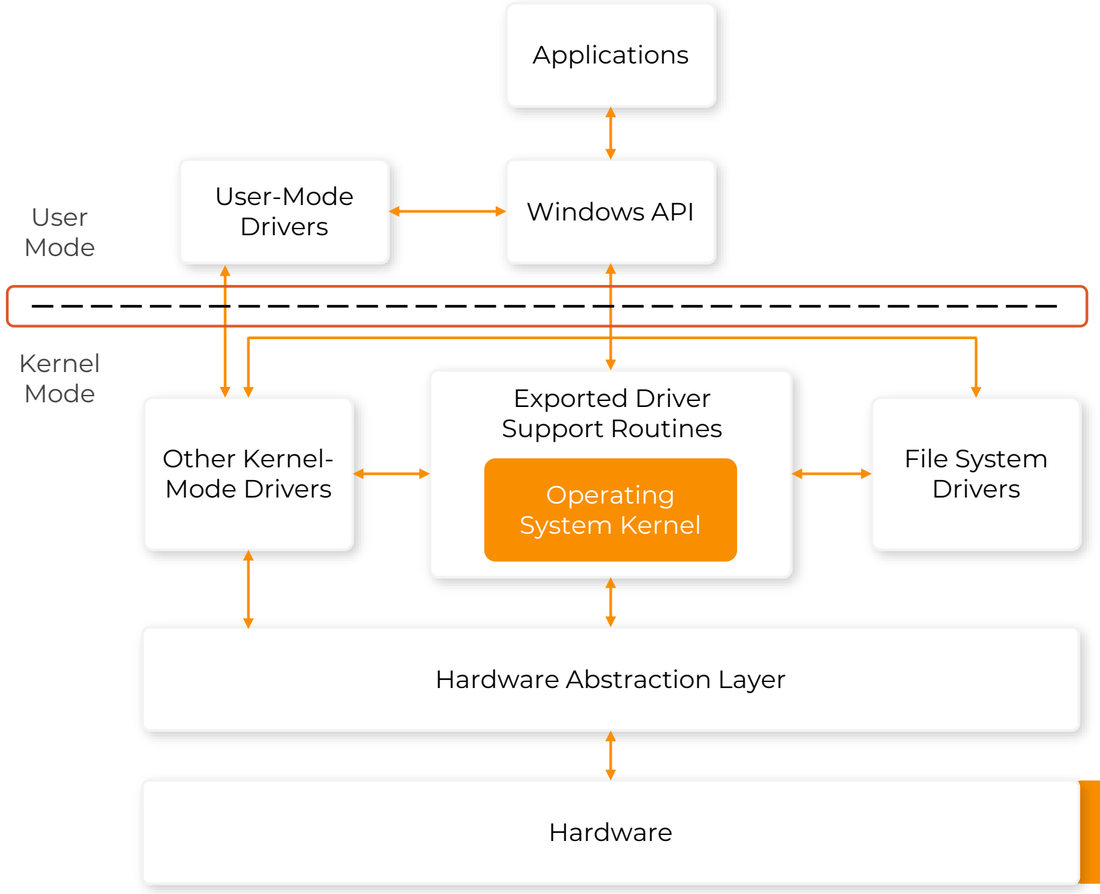
1. Suspension of Services
2. Ransomware
3. Patient Data Exfiltration
4. Initial Access
5. Malicious Access to Medical Devices
6. Lack of Visibility
7. Lateral Movement

What Happens When The EDR is Bypassed?

Blind spots persist
in **XDR and MDR**
since they depend on
visibility provided by EDRs,
they are **equally susceptible**
to evasion.



Defense Bypass: The Overlooked Flaw Undermining Cyber Defenses



EDR

Monitoring Technique	Bypassed?
Kernel Callbacks	Yes
ETW Kernel	Yes
ETW Userland	Yes
AMSI	Yes
System	Yes

Monitoring at this level gives you the full truth about the network

Network Interface Card

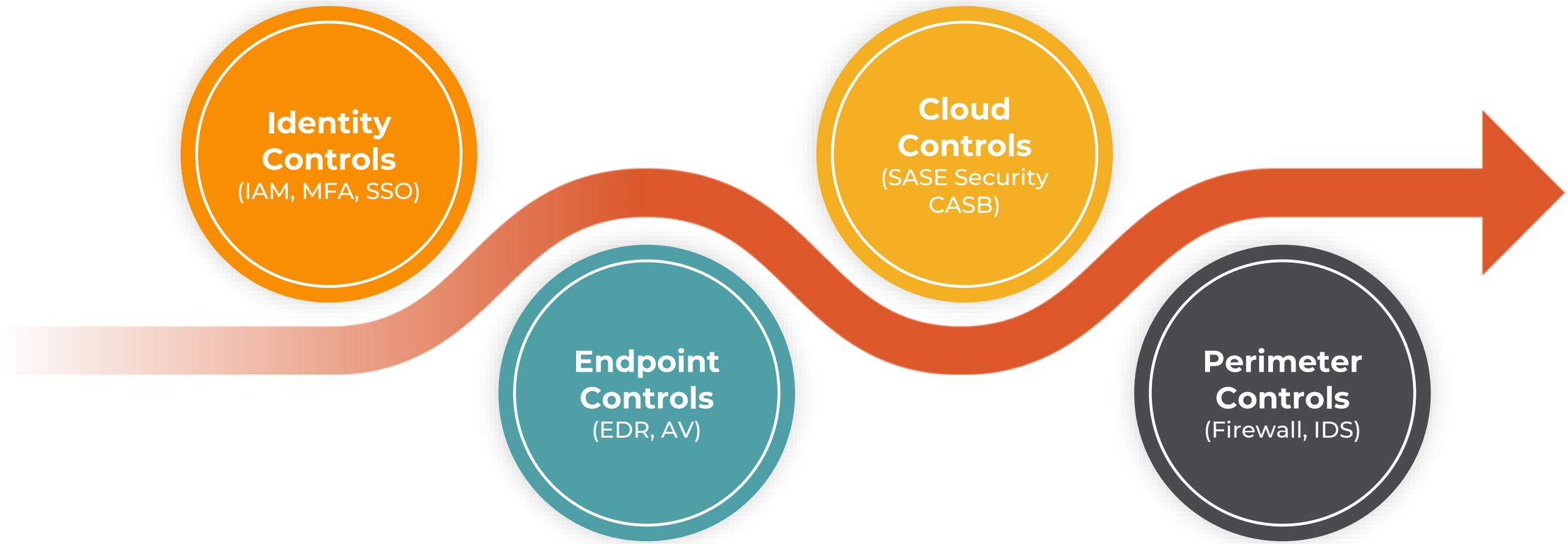
Attack In | Phishing, Malware Dropper, Etc

Attack Out | Lateral movement, C&C, Exfiltration, Etc

LUMU

Fragmented Defenses, Fragmented Visibility

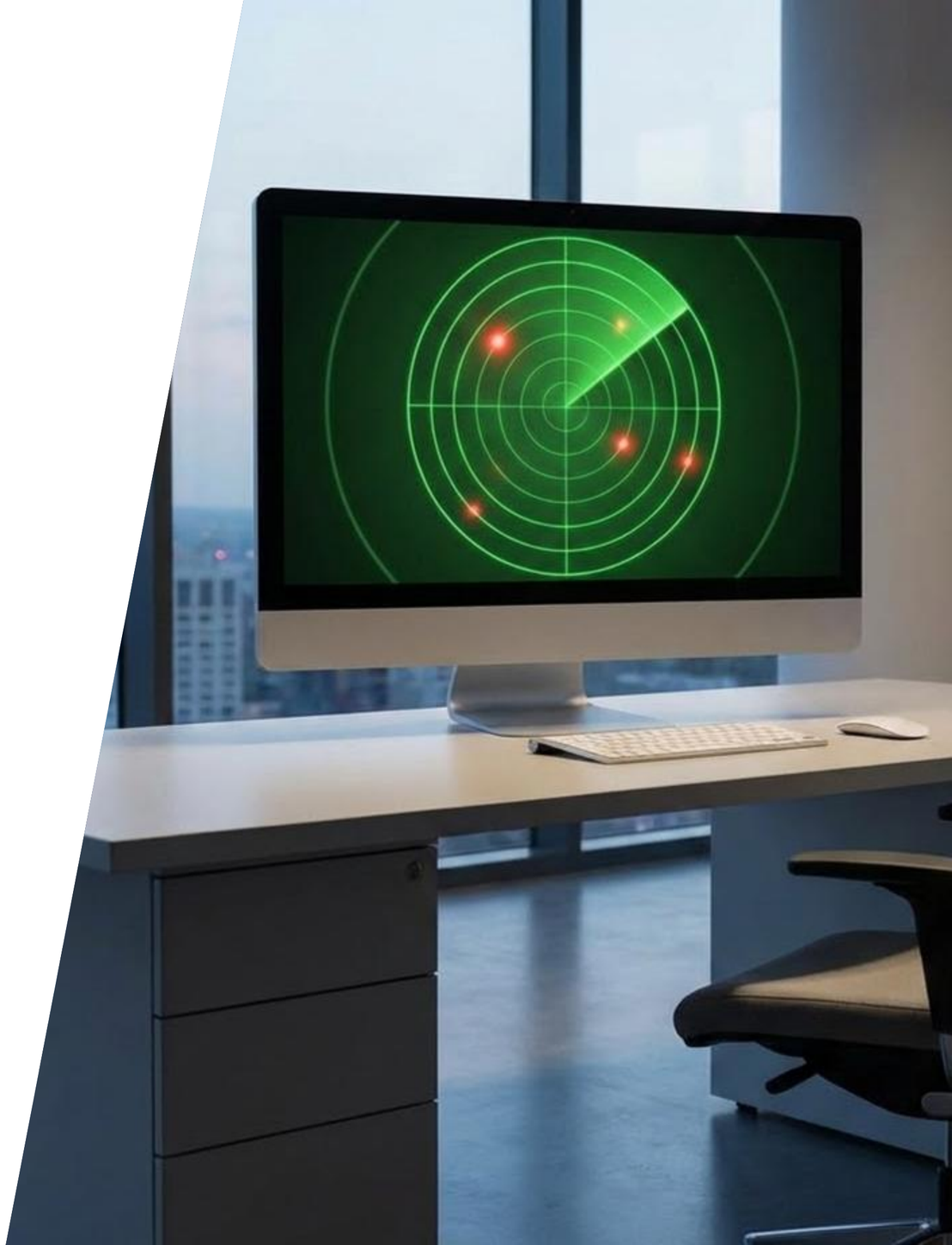
Attackers Leverage Blindspots to Bypass Existing Solutions



LUMU

The Security Cat-and-Mouse Game

- Persistent Adversaries
- Adaptive Defenses
- Strategic Foresight



LUMU

Windows EDR Evasion:
API Hooks and Syscalls

- **Hooking Evasion**

Malware unhooks APIs or loads clean versions of system DLLs (e.g., ntdll.dll) to bypass EDR's inline API hooks and monitoring routines.

- **Direct & Indirect Syscalls**

Instead of standard API calls, advanced malware issues direct syscalls or jumps into legit memory locations to mask behavior and avoid detection.

- **AMSI & ETW Bypasses**

By patching functions like AmsiScanBuffer and EtwEventWrite at runtime, malware disables script scanning and event tracing for stealth execution.

LUMU

Process Injection & Memory Residency

- **Classic Injection Methods**

Attackers load signed but vulnerable drivers to gain kernel access and disable security controls undetected, e.g., with tools like AuKill.

- **Advanced Techniques**

Innovations like thread pool injection (e.g., Pool Party) avoid typical detection paths and leverage trusted system mechanics.

- **Staying In Memory**

To remain stealthy, malware avoids disk access, uses sleep masks, encrypts memory, and periodically bounces memory regions.

LUMU

Kernel-Level & Driver-Based Evasion

- **BYOVD Attacks**

Techniques like process hollowing, doppelgänging, and reflective DLL loading allow malware to blend into legitimate processes.

- **Callback Tampering**

Kernel-mode rootkits remove or patch monitoring callbacks like PsSetCreateProcessNotifyRoutine to blind EDR systems to events.

- **EDR Self-Defense Limits**

Even hardened EDR solutions can be bypassed if attackers disable protections from the kernel level using privilege escalation or exploits.

Linux and macOS Evasion Techniques

- **Linux: Rootkits & LD_PRELOAD**

Attackers use shared libraries like Symbiote and rootkits to inject into and hide within legitimate Linux processes.

- **macOS: Reflective Injection**

macOS malware uses Objective-C swizzling, AppleScript abuse, and Mach-O reflection to inject code without disk traces.

- **Living Off the Land**

Both platforms see attackers misuse built-in tools—bash, cron, AppleScript—for stealthy operations that bypass EDR.

LUMU

Top EDR Bypass Tools & Techniques

- AuKill & AvNeutralizer: Kernel EDR killers
- EDRKillShifter: Script-based disabling
- Safe Mode Ransomware Deployment
- Reflective DLL/Mach-O Loaders
- Living-off-the-Land (LOLBins)

Insiders & Blind Spots in Security

- Insiders can exploit trust and bypass technical controls
- EDRs focus on external malware and anomalies, not policy violations
- Real-World Examples include AT&T unlocking scandal and bank fraud using check cashing overrides

Key Lessons for Defenders

- Assume Breach Mentality
- Layered Defense is Essential
- Monitor Beyond Alerts

How will you enhance your defense strategy?

EDR evasion is not just theoretical, it’s happening daily. Prepare your teams, strengthen your tools, **and assume breach. Stay proactive.**

LUMU

Thank you

www.lumu.io

Open Your Free Account Today