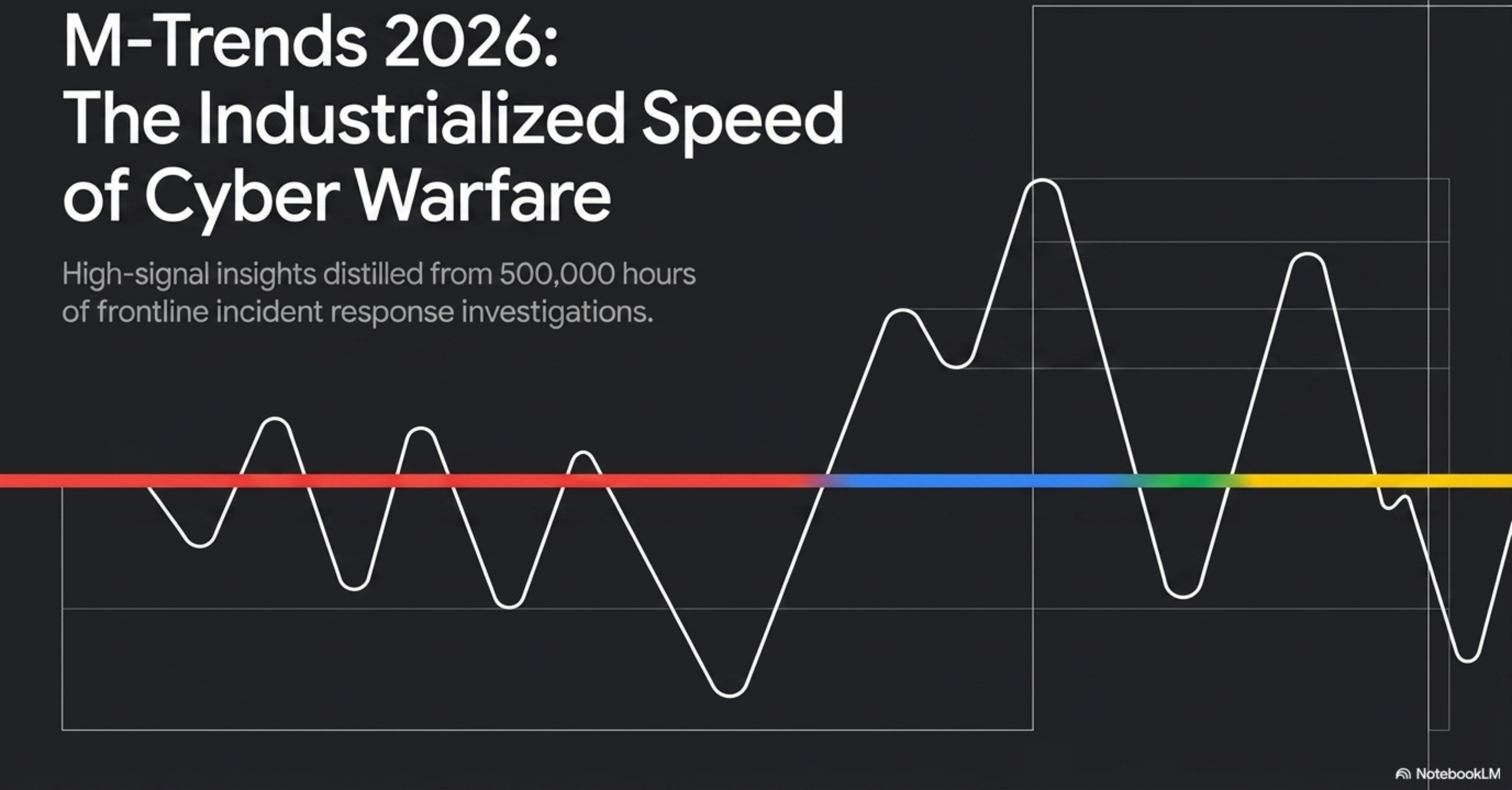
M-Trends 2026: The Industrialized Speed of Cyber Warfare

High-signal insights distilled from 500,000 hours of frontline incident response investigations.



The Paradigm Shift

The threat landscape has industrialized. Attackers are moving faster, hiding deeper, and targeting the very infrastructure designed to save you.

22 Seconds

The Collapsed Hand-off: The median time from an initial network breach to an attacker handing off access to a secondary ransomware group.

-7 Days

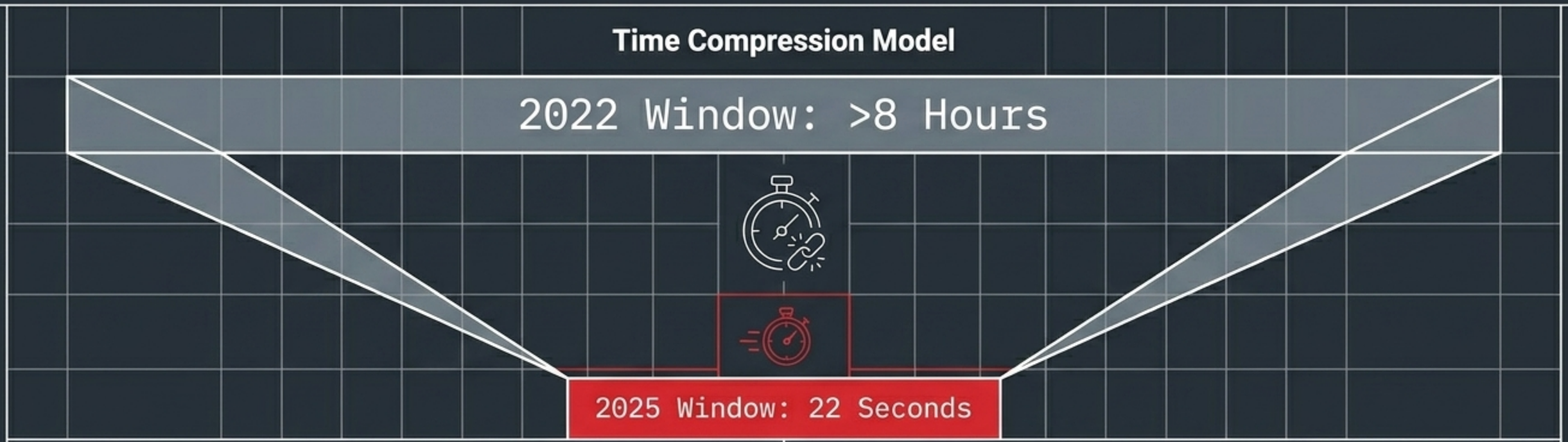
Negative Exploit Time: Attackers are routinely weaponizing vulnerabilities a full week before vendors release security patches.

Infrastructure Targeted

Recovery Denial: Ransomware groups are systematically hunting backups and virtualization layers (ESXi, vSphere) to deny the ability to recover.

The Death of the Detection Window

Insight: In 2022, security teams had over 8 hours to intercept an initial access breach before the hand-off to a secondary group. In 2025, that window collapsed to 22 seconds.



A minor alert today is a catastrophic compromise in **22 seconds.**
Relying on manual detection is fighting last decade's war.

The Division of Labor: Pre-Staged Payloads

Attackers no longer wait to sell access on dark web forums; they pre-stage tools so the ransomware operator is fully equipped the moment they log in.

The Old Way

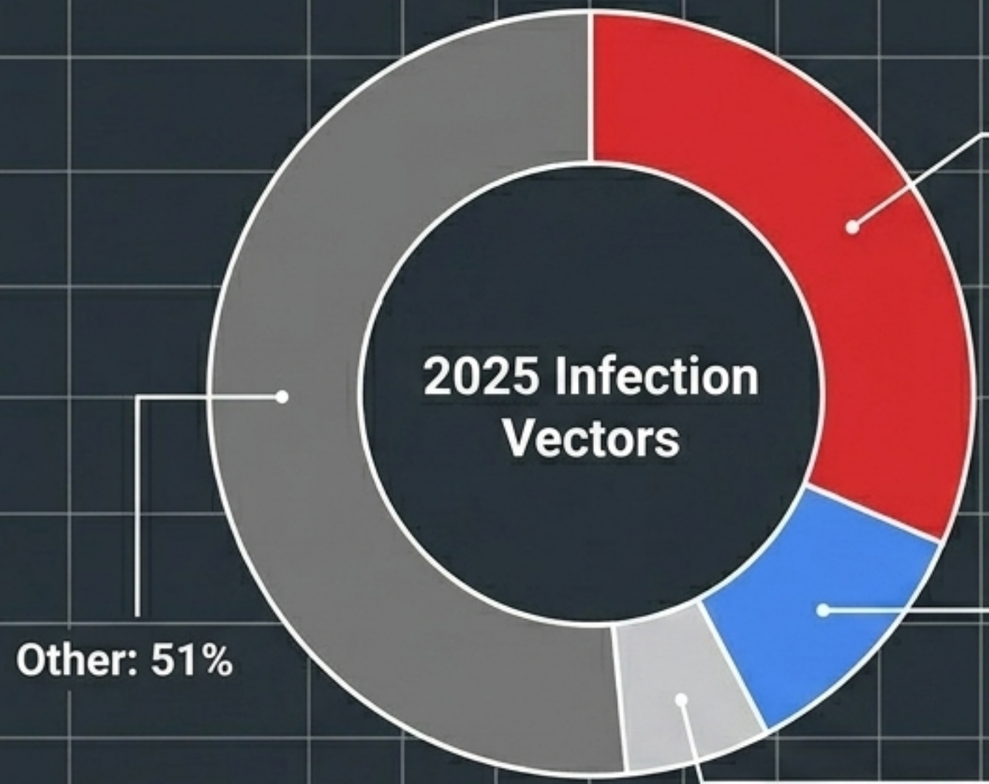
- Initial Access Broker
- Post ‘For Sale’ on Dark Web Forum
- Wait for Buyer

The 2025 Division of Labor

- Initial Access Partner (e.g., UNC1543)
- Seamless direct delivery
- Secondary Group (e.g., RansomHub)
- Actioned in 70 minutes
- Immediate Ransomware Execution

Documented cases show threat groups delivering secondary malware a mere 70 minutes after initial infection.

Initial Access Vector Shift: The Rise of Vishing



Exploits: 32%
(Leading vector for 6th consecutive year)

Voice Phishing (Vishing): 11%
(Surging past email)

Email Phishing: 6%
(Sustained decline)

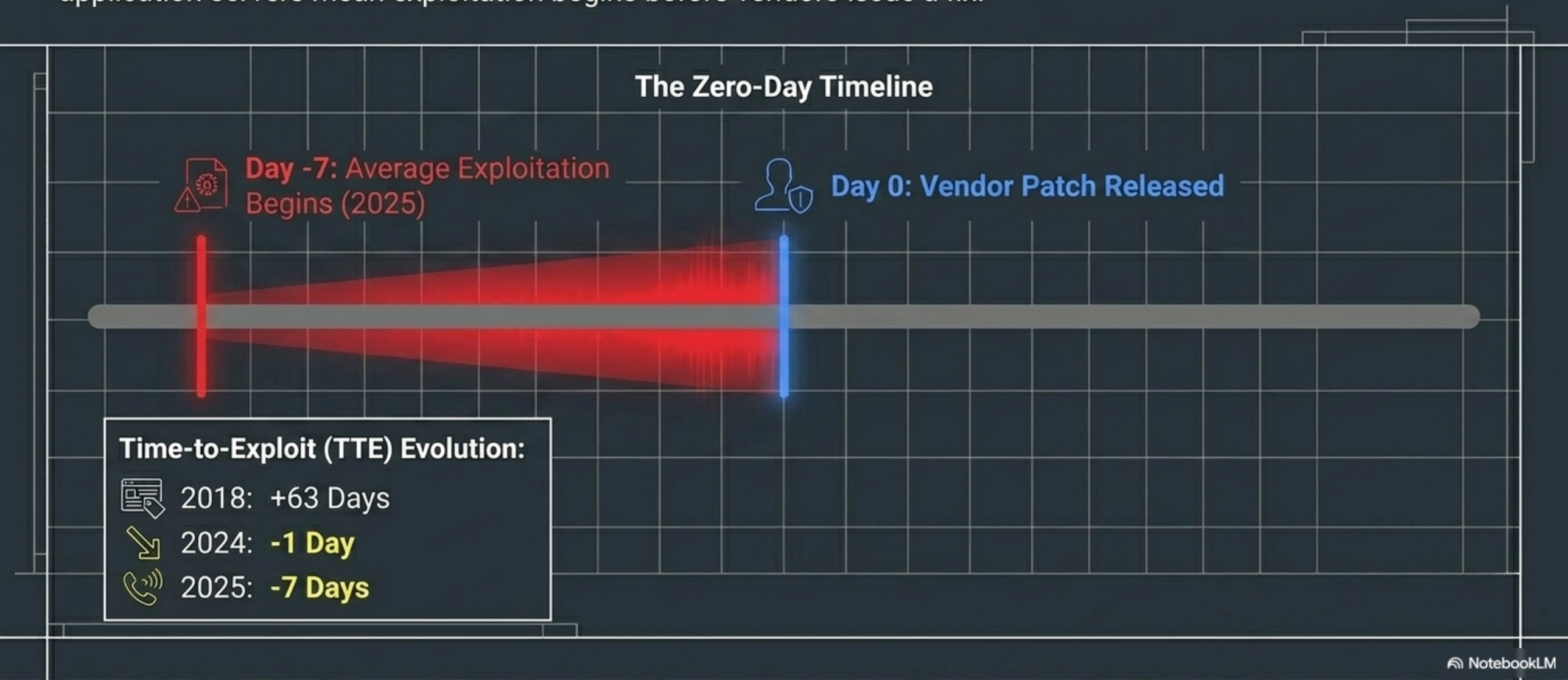
Interactive Social Engineering

Threat clusters (like **UNC3944 / Scattered Spider**) are calling IT helpdesks, sounding stressed, and impersonating employees to request **MFA bypass** codes codes.

Highly interactive **voice attacks** easily bypass automated email filters, requiring human-centric defensive strategies.

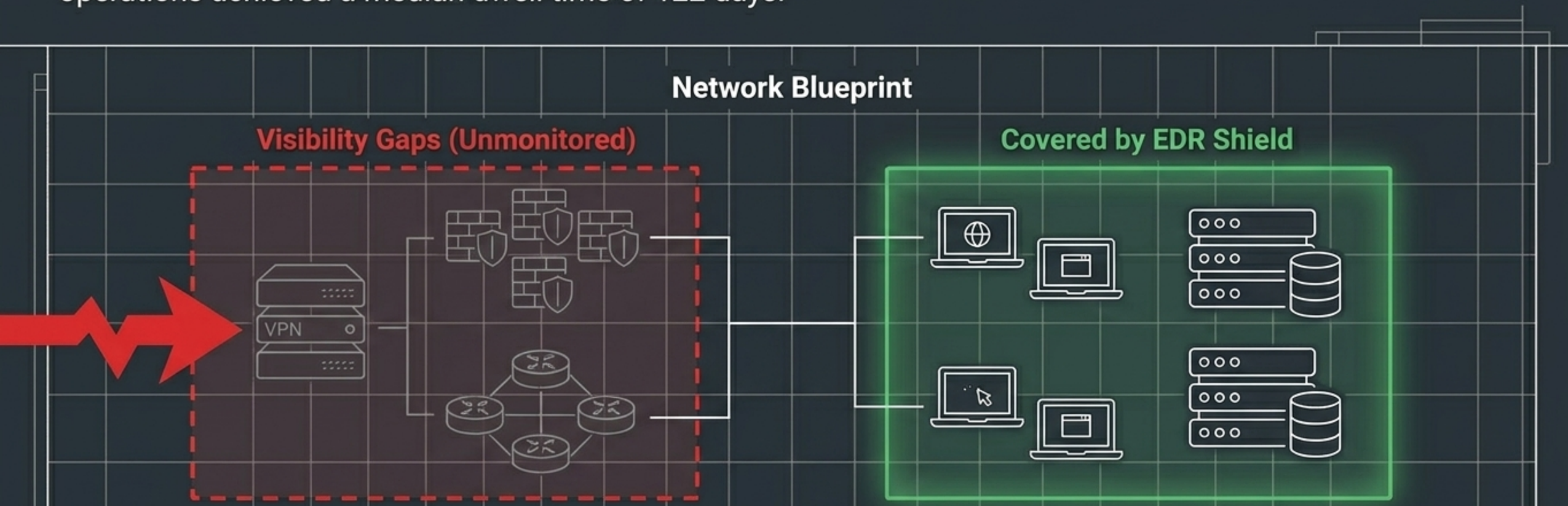
The Negative Patching Window

You cannot patch what doesn’t have a patch yet. Zero-day exploits against enterprise application servers mean exploitation begins before vendors issue a fix.



Hiding in the Blind Spots: Edge Infrastructure

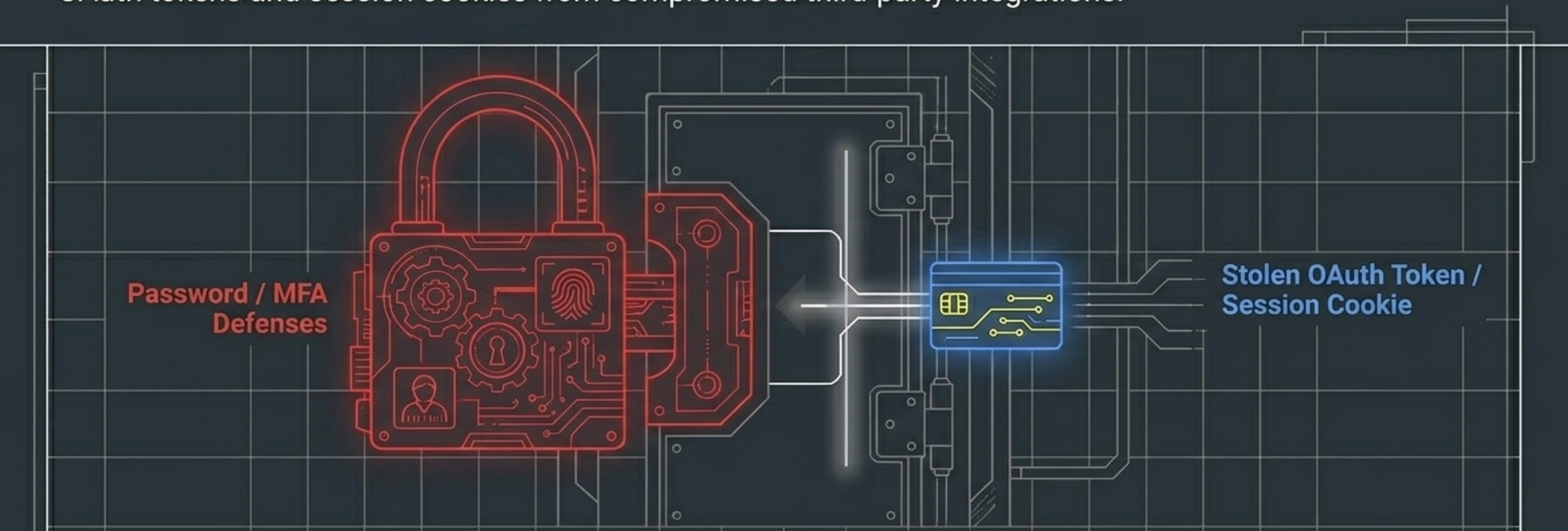
Global median dwell time rose to 14 days in 2025. Espionage & DPRK IT worker operations achieved a median dwell time of 122 days.



Attackers use lightweight malware (e.g., BRICKSTORM) to establish long-term persistence on proprietary edge appliances that cannot run standard Endpoint Detection and Response (EDR) software.

SaaS & The Identity Perimeter

Attackers are no longer just guessing passwords; they are harvesting long-lived OAuth tokens and session cookies from compromised third-party integrations.



These tokens remain valid post-logout, allowing threat actors to seamlessly pivot into downstream customer environments and execute large-scale data theft without triggering MFA alerts.

Ransomware's New Goal: Recovery Denial

Groups like REDBIKE (Akira) and AGENDA (Qilin) aren't just locking files; they hunt down and destroy emergency access and backups before deploying encryption.

The Ransomware Evolution Matrix

	Traditional Ransomware	Modern Recovery Denial
Focus	Extortion via disruption	Forcing payment via total destruction
Targets	User files, basic endpoints	Identity services, backup infrastructure, virtualization layers
Action	Dual-threat encryption and data theft	Exploiting AD CS templates for permanent admin, wiping cloud backups
Defense	Restore from daily connected backups	Immutable, air-gapped recovery environments

Attacks Moving Down the Stack

Advanced adversaries bypass guest operating systems entirely. Encrypting hypervisor datastores at the root level locks every virtual machine on a host simultaneously.

The AI Reality Check: Accelerator, Not Mastermind

The Expectation

Fully autonomous AI systems initiating end-to-end breaches and acting as independent masterminds.

The 2026 Reality

AI acts as a force multiplier for existing tactics. Real-world applications include:

- **PROMPTFLUX**: Malware querying **LLMs** mid-execution to rewrite its own source code and evade signatures.

- **QUIETVAULT**: Credential stealers using **AI command-line tools** to hunt for developer tokens.

- **Social Engineering**: LLMs shifting mass generic emails to hyper-personalized, rapport-building **vishing scripts**.

The Defensive Bright Spot: Internal Detection

52%

of intrusions were detected internally by the victim organization in 2025 (up from 43% in 2024).

The data proves that expanding internal visibility and telemetry works.

When organizations detect breaches internally using their own tools, the median dwell time drops to just 10 days.

Synthesis: The Defensive Paradigm Shift

The Defensive Posture Matrix			
	Dimension	Legacy Mindset	M-Trends 2026 Mandate
	**Visibility**	From: Relying solely on Endpoint Detection (EDR) →	To: Forwarding Edge Device and Hypervisor logs to a centralized SIEM
	**Identity**	From: Passwords & basic SMS MFA →	To: Continuous identity verification and restricted third-party App consent
	**Resilience**	From: Network-connected daily backups →	To: Immutable, air-gapped recovery environments decoupled from primary AD

The 3-Step Immediate Action Plan

1. Isolate Tier-0 & Backups

Remove hypervisors and backup infrastructure from the primary corporate domain. Enforce dedicated out-of-band management.

2. Expand Visibility to the Edge

Audit all uncatalogued VPNs, routers, and edge appliances. Forward their administrative logs to long-term storage to close blind spots.

3. Train Helpdesks on Vishing

Shift security awareness beyond the email inbox. Train IT support to require out-of-band verification for MFA resets and password changes.

Proactive Containment is the Only Option.

Closer collaboration between cybercriminal partners has collapsed the window for defense. You have 22 seconds.

Google Cloud

For more information, visit **cloud.google.com**.

If your organization suspects a cyber incident,
or you are experiencing a security breach, **please contact Mandiant for Incident Response Assistance**.