Enigma Networks

The New Era of AI-Fueled Cybercrime:

Why Traditional Perimeter Defenses and Periodic Penetration Tests are No Longer Enough

Executive Summary

For years, enterprise cybersecurity has been built on the assumption that the perimeter could be hardened enough to keep attackers out. Today however, most breaches begin not with a technical exploit, but with stolen or abused credentials – allowing attackers to simply log in. Once inside, they exploit a dangerous blind spot: limited visibility and control over the internal network.

This blind spot is now under direct assault from AI-powered adversaries. They are leveraging artificial intelligence to automate reconnaissance, privilege escalation, lateral movement, and data exfiltration – all while blending into normal activity. **Traditional perimeter-based defenses, rules-based SIEMs, and periodic pen tests can no longer keep up.**

Verizon's 2024 Data Breach Investigations Report shows that stolen credentials and phishing remain the #1 cause of breaches. IBM's latest Cost of a Data Breach Report found average detection times still exceed 200 days – more than enough time for attackers to cause serious damage undetected.

Zero Trust for Internal Networks (ZTNX) extends Zero Trust principles beyond the perimeter, continuously learning normal behaviors, monitoring every connection, and detecting anomalies in real time. Enigma AI™ is the first platform purpose-built for ZTNX, delivering agentless, at-scale visibility and control inside the network. For organizations facing the accelerating pace of AI-driven attacks, ZTNX is no longer optional – it's mission critical.

1. The Dangerous Blind Spot in Cybersecurity

Every enterprise has a perimeter defense strategy. But once traffic crosses the firewall, most organizations lose deep visibility into what's happening between devices, workloads, and cloud instances. Visibility is sparse an many organizations rely on logs and alerts designed for compliance rather than real-time detection. An alarming 96% of lateral movement behavior goes undetected by SIEMs and endpoint tools – the most commonly used types of cybersecurity solutions – and 70-80% of successful cyberattacks exploit this blind spot (Gigamon).

The result? Entire segments of your environment, from IoT devices to third-party systems, operate without meaningful inspection. This is exactly where attackers operate, often for months, without raising alarms.

Case in point: In the SolarWinds incident, attackers infiltrated trusted network segments for months, using legitimate accounts and carefully planned lateral movement to avoid triggering alerts. This wasn't a perimeter failure, it was an internal visibility failure.

2. “Logging In” is the #1 Attack Vector

Verizon’s DBIR shows stolen credentials and phishing cause over 60% of breaches and remains the top cause of breaches globally. AI is now supercharging these attacks with automation and hyper-personalization at unprecedented scale. Phishing volume alone has surged 4,151% since the release of ChatGPT in 2022 (SlashNext).

The result isn’t just more attacks; it’s more effective ones. As of March 2025, AI-driven phishing was found to be 24% more effective than even the most elite human red teams (Hoxhunt), and materially more effective than average phishing attempts in the wild. What once required seasoned operators can now be mass-produced: while one human might hand-craft ten phishing lures in a day, AI can generate 10,000 in seconds, each as persuasive as the human-written versions.

And sometimes, it’s not even that technical. In the 2023 Clorox breach, hackers linked to Scattered Spider simply called the help desk and tricked staff into resetting passwords and MFA. Once inside they operated for weeks without detection.

3. AI-Powered Attacks Move Silently

Artificial intelligence is changing the threat landscape in ways defenders have never faced. Once inside the network, attackers now employ:

- **Behavioral mimicry:** AI can learn and replicate the normal patterns of a target user, making detection far harder.
- **Real-time evasion:** Polymorphic malware adapts on the fly to bypass endpoint and perimeter defenses.
- **Automated reconnaissance:** AI can map internal networks, find high-value targets, and identify the weakest path to them in seconds.
- **Throttled and timed activities:** spacing out moves over weeks to avoid triggering “burst” or “spike” alerts.

These capabilities compress the kill chain from weeks to hours or less while keeping attacker dwell times in the hundreds of days. Without continuous baselining and anomaly detection inside the network, their activity is indistinguishable from routine operations.

4. It’s Not Just About Ransomware Anymore

While ransomware gets the headlines, the most damaging cybercrimes today have diversified well beyond encrypting data for ransom. Common attack objectives now include:

- **Data exfiltration** for IP theft is rampant in sectors like pharma and manufacturing. Proprietary R&D and trial results fetch high black-market prices.
- **Business Email Compromise (BEC)** exploits trusted channels to redirect payments or manipulate deals. The FBI’s IC3 report shows $3.1 billion in losses in 2023 alone.
- **Supply chain compromises** leverage third-party software updates or integrations to deliver malicious payloads at scale.
- **Corporate espionage** involves long-term stealth operations designed to exfiltrate sensitive trade secrets without disruption.

Example: In one stark example of pharmaceutical cyber espionage which occurred over several years (Operation CuckooBees), Chinese threat group APT41 exfiltrated formulas, trial data, and research documentation, bypassing encryption entirely. In cases like these, attackers quietly departed with **decades of R&D work**—not ransom demands—underscoring how devastating these breaches can be.

5. Why Pen Testing is Not Enough

Penetration testing is valuable but can't replicate the persistence or adaptability of real-world adversaries:

- **Point-in-time limitation:** A pen test captures a snapshot, while attackers operate continuously.
- **Scope restrictions:** Many pen tests exclude insider threat scenarios or assume a purely external starting point.
- **Lack of stealth simulation:** Real attackers may dwell for months, carefully avoiding noisy actions.

Reality: Pen testing can lead to a false sense of security. Passing a pen test may mean you can stop an opportunistic external exploit but says little about whether you could detect a compromised service account slowly harvesting data over 90 days. As The Hacker News highlights, "the security control that 'passed' in the test may very well fail when it really matters, two weeks later."

6. The Urgency of Zero Trust for Internal Networks

Zero Trust has become mainstream but most implementations stop at identity and edge access controls. Internal traffic remains largely trusted by default, contradicting Zero Trust's core principle: *"Never trust, always verify."* **Key drivers of urgency include:**

- **The quickly shifting nature of breaches:** AI-driven attackers can alter tactics, tools, and behaviors within minutes, dynamically adjusting to evade detection and exploit newly discovered weaknesses. A breach's footprint can change multiple times a day—making point-in-time controls obsolete before they can be updated.
- **Collapse of the perimeter:** Hybrid and cloud environments, remote work, and BYOD have dissolved traditional boundaries. The internal network is now fully exposed to compromised credentials, supply chain vulnerabilities, and insider threats.
- **Increasing regulatory pressure:** Frameworks like CISA Zero Trust Maturity Model, PCI DSS 4.0, HIPAA, and NIST 800-207 emphasize internal visibility, segmentation, and continuous monitoring – not just perimeter security.
- **The speed-to-impact gap:** Once attackers gain internal access, the window before damage is done is shrinking – making continuous monitoring, segmentation enforcement, and anomaly detection critical.

While many Zero Trust implementations stop at identity controls or network access, ZTNX enforces Zero Trust principles deep inside the network – treating every east-west interaction as untrusted by default and continuously verifying behavior in real time.

7. How Enigma AI Delivers ZTNX

Enigma AI is the first and only platform built specifically to deliver ZTNX at scale:

- **Agentless deployment:** Immediate visibility across all subnets without endpoint installations.
- **Continuous asset discovery:** Identifies every device, workload, and shadow asset.
- **Full east-west visibility:** Monitors all internal communications and detects anomalies in real time.
- **AI-driven baselining:** Learns normal behaviors to flag policy violations, credential misuse, or s uspicious movements.
- **Seamless integration:** Works alongside IAM, ZTNA, and SOAR tools to orchestrate automated response.

Conclusion:

The nature of cybercrime is changing faster than most organizations can adapt. AI is amplifying attackers' ability to operate inside your network without detection, and the old perimeter-first mindset is no longer enough.

Zero Trust for Internal Networks is the next frontier of enterprise defense and Enigma AI is leading the way. The question for security leaders is no longer if they need ZTNX, but how soon they can deploy it.

Enigma Networks® is proud to lead the ZTNX movement. To learn more or see the platform in action, visit **getenigma.ai** or request a demo today.

Enigma Networks