SafeBreach

# Key Findings from the 2026 SafeBreach State of the Breach Report

We analyzed the results of millions of real-world attack simulations from 2025 to see where enterprise security programs stand against today's most pressing threats.

Here's a breakdown of the key insights and actionable takeaways that can help you build resilience in 2026.

2026 STATE OF THE BREACH

## The AI race is on—and AI infostealers are winning

**94.3%** BLOCK RATE

**AI spyware** shows extremely strong prevention due to the mature detection capabilities for surveillance-style behaviors.

**78.4%** BLOCK RATE

**AI malware** was blocked moderately well, suggesting machine-generated payloads are still within reach of defenses.

**36.1%** BLOCK RATE

**AI infostealers** remain the most dangerous exposure point, with the lowest blockage rates and the highest enterprise risk

### Prepare for AI-Driven Unpredictability

Ensure you're not relying too heavily on EDRs to stop AI-generated payloads and focus efforts on strengthening identity and data pathways.

2026 STATE OF THE BREACH

## Network inspection & DLP controls are having all the fun

**58.8** MILLION

The number of malicious actions blocked by network inspection, the number one control by volume.

**9x** IMPACT

The protective effect of network inspection controls over endpoint, despite smaller deployment and budget.

**53%** BLOCK RATE

The block rate of endpoint controls, compared to 70% for DLP and 65% for network inspection.

### Don't Rely Only on EDR

Balance your stack with strong network inspection and DLP controls, which deliver an outsized impact over endpoint alone.

2026 STATE OF THE BREACH

## We've mastered the noisy payload

**85%** BLOCK RATE

Enterprises showed high prevention rates against high-noise, payload-centric ransomware families like Medusa.

### Branch Out

If you're confident in your general ransomware readiness, ensure you have the same level of protection across all environments, including cloud, container, and SaaS.

2026 STATE OF THE BREACH

## Stealth & identity continue to evade

**27%** MISS RATE

Sophisticated, identity-driven campaigns—like Russian GRU tradecraft—are bypassing defenses via credential abuse and Living-off-the-Land (LOTL) techniques.

### Expand Visibility

Assess your exposure to credential theft, session hijacking, and lateral movement. Dive into data flows and potential exfiltration paths.

2026 STATE OF THE BREACH

## Lateral movement is the decisive battleground

**60%**

The number of enterprise organizations that exposed harvestable credentials during testing, providing zero-effort privilege escalation for attackers.

### Harden Identity

Reduce cached secrets in the Windows Registry and persistent plain-text passwords. Ensure multi-factor authentication (MFA), identity access management (IAM), and segmentation policies are enforced consistently.

2026 STATE OF THE BREACH

## Centralized architectures are leading the way

**85.2%** BLOCK RATE

Industries with centralized, cloud-heavy architectures perform better across the board, even against low-noise techniques.

**64.3%** BLOCK RATE

Sprawling IT/OT environments and endpoint-heavy strategies face high exposure regardless of tool count.

### Modernize & Reduce Fragmentation

Prioritize simplification of distributed environments, strengthen governance models that centralize control ownership, and reduce reliance on endpoint-only strategies.

2026 STATE OF THE BREACH

## Resilience is a continuous practice, not a milestone

Organizations that treat security as an operational loop saw rapid, measurable improvement across all threat categories.


### Incorporate Exposure Validation

Partner with an **adversarial exposure validation expert** to continuously validate, prioritize, and reduce your most critical exposures.

**READ THE FULL REPORT AT**
www.safebreach.com/white-papers/safebreach-2026-state-of-the-breach-report/