CyberSagacity

EXECUTIVE & TECHNICAL BRIEF

Why application security is broken.

For industry conferences, boards, CISOs, and AppSec leaders. The evidence is uniform — across Gartner, Verizon, CISA, Forrester, and Ponemon — that application security is failing at scale.

PUBLISHED
2026

AUDIENCE
CISO · Board · Conference · AppSec

FORMAT
Executive Brief

EXECUTIVE OVERVIEW

A widening gap between the defects we ship and the attacks we face.

Software now sits at the center of every digital operation. Yet the mechanisms meant to secure it have failed to keep pace with modern development, AI-generated code, expanding attack surfaces, and the accelerating tempo of exploitation.

The evidence is uniform across Gartner, Verizon, CISA, Forrester, Ponemon, and independent security labs: **application security is failing at scale.** Organizations ship software with known weaknesses, lack the analytics to distinguish real risk from noise, and watch attackers exploit the same classes of defects they have exploited for decades.

This brief consolidates the most authoritative findings across the industry to demonstrate why a fundamental rethinking of application security — grounded in **accurate data, statistical risk modeling, and business-aligned intelligence** — is now urgently required.

THE EVIDENCE IS OVERWHELMING

Software quality is in decline. Breaches are becoming the norm.

Software Quality Is in Decline

90%+

Of software contains defects. More than 50% contains serious vulnerabilities.

GARTNER, 2025 · SOFTWARE QUALITY & TECHNICAL DEBT RESEARCH

Development velocity, microservices proliferation, and DevOps automation have dramatically increased the number of releases — **but not the quality of what is released**. Organizations lack meaningful visibility into defect accuracy, overlap across tools, or the true risk of what they deploy.

Breaches Are Becoming the Norm

67%

Of organizations suffered at least one application-layer breach in the last 12 months.

VERACODE, STATE OF SOFTWARE SECURITY 2025

Attackers exploit application weaknesses because they remain **the most direct path to sensitive data, business logic, and authentication flaws.**

KNOWN VULNERABILITIES STILL DRIVE THE MAJORITY OF BREACHES

Not a lack of tooling.
A lack of accuracy, prioritization, and actionable intelligence.

60%

Of breach victims were compromised through a known, unpatched vulnerability.

PONEMON INSTITUTE & SERVICENOW · VULNERABILITY RESPONSE REPORT

62%

Of breached organizations were unaware they were vulnerable prior to the incident.

PONEMON INSTITUTE

This demonstrates not a lack of tooling, but a lack of accuracy, prioritization, and actionable intelligence.

ATTACKERS ARE EXPLOITING THE SAME DEFECTS — BUT FASTER

These are not zero-day mysteries. They are decades-old defect classes.

Recycled Vulnerabilities Remain the Primary Attack Vector

56%

Of external attacks leverage known application vulnerabilities.

FORRESTER · STATE OF APPLICATION SECURITY 2025

Adversaries do not need novel exploits — just **scalable automation against well-understood weaknesses**.

CISA CONFIRMS

"Most software vulnerabilities are not unknown, unique, or novel. They fall into well-known classes of defects identified for decades."

— Jen Easterly, CISA Director, foreword to Verizon DBIR 2024

Despite industry knowledge, organizations continue to introduce the same categories of defects — SQL injection, XSS, insecure deserialization, broken access control, API misconfigurations, and more.

AI-GENERATED CODE IS EXPANDING THE ATTACK SURFACE

AI now writes production code.
It also writes insecure code at industrial scale.

AI Writes a Meaningful Portion of Production Code

25%+

Of all new code at Google is written by AI.

JACK KELLY, FORBES 2024

~30%

Of Microsoft's code is generated by AI.

JORDAN NOVET, CNBC 2024

AI Introduces Defects at Industrial Scale

48%

Of AI-generated code contained at least one insecure pattern or vulnerability.

CSET · CYBERSECURITY RISKS OF AI-GENERATED CODE, NOV 2024

Generative models produce syntactically correct but **semantically insecure patterns** — accelerating defect creation faster than traditional AppSec tools can detect or evaluate.

APPSEC TOOLS CANNOT KEEP UP

AppSec has become a data problem — not a tool problem.

Tool Accuracy Is Poor and Unverified

SAST, DAST, MAST, SCA, and IAST tools disagree on nearly everything:

- Minimal overlap (**<1–5%**) in detected defects across tools.
- High false-positive and false-negative rates.
- No standardized accuracy benchmarks.
- No financial or compliance context.
- No unified statistical understanding of risk.

> **This creates noise — not intelligence.**

AppSec Has Become a Data Problem

Organizations now operate:

- **Thousands** of applications.
- **Tens of thousands** of defects.
- **Dozens** of tools and outputs.
- **Countless** inconsistent severity labels.

The problem is no longer detection — it is **correction, prioritization, and risk quantification**.

THE CONSEQUENCE

A system that cannot protect itself.

The industry's inability to:

- Correct and normalize tool outputs.
- Identify false positives and false negatives.
- Understand true defect severity.
- Link vulnerabilities to business and compliance impact.
- Quantify financial exposure.
- Prioritize remediation based on real risk.

...has created an environment in which **software is released with defects, exploited quickly, and increasingly targeted** through automated and AI-assisted adversarial tools.

> **This is why application security is broken — and why a new approach, rooted in statistically validated accuracy, risk modeling, and business-aligned intelligence, is required.**

CyberSagacity provides the foundation for that approach.