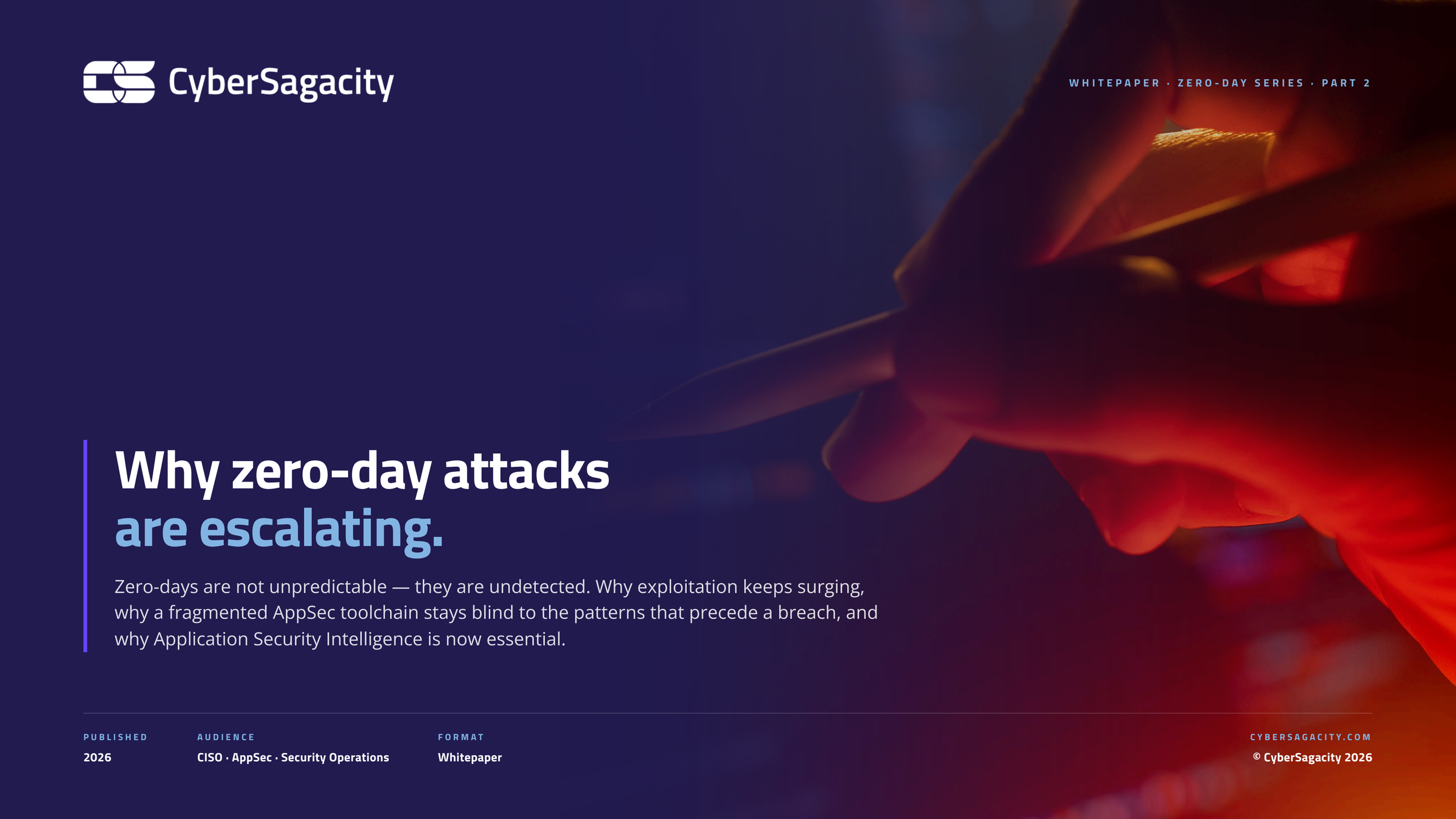
CyberSagacity



Why zero-day attacks are escalating.

Zero-days are not unpredictable — they are undetected. Why exploitation keeps surging, why a fragmented AppSec toolchain stays blind to the patterns that precede a breach, and why Application Security Intelligence is now essential.

PUBLISHED
2026

AUDIENCE
CISO · AppSec · Security Operations

FORMAT
Whitepaper

EXECUTIVE SUMMARY

Zero-days are not unpredictable. They are undetected.

Over the past three years, the volume, speed, and sophistication of zero-day exploitation have surged — attackers now weaponize new vulnerabilities within days.

Despite billions invested in SAST, DAST, SCA, MAST, IAST, ASPM, and PenTesting, today's AppSec ecosystem remains fragmented, noisy, and blind to the patterns of failure that precede zero-day breaches. Legacy tools chase known signatures — not the systemic code weaknesses and statistical indicators that point to future exposure.

CyberSagacity eliminates that blind spot — applying actuarial-grade analytics to reveal the defect patterns attackers later turn into zero-days.

UNDERSTANDING ZERO-DAY ATTACKS

A flaw the vendor doesn't yet know exists — exploited on day zero.

No patch, no update, no signature exists to prevent exploitation. Zero-days are not magic — they exploit **structural weaknesses** (improper access control, insecure deserialization, injection paths, sandbox escapes, input-trust failures) that AST tools frequently misclassify or miss.

01
Unknown to vendors
No patch is available — defenders have no fix to deploy.

02
Unknown to scanners
No signature or rule exists to detect the flaw.

03
Unknown to security teams
No risk treatment plan covers an unseen threat.

04
Unknown in codebases
The underlying defect patterns go unrecognized.

CyberSagacity solves this by identifying the predictive precursors to those vulnerabilities.

THE NEW NORMAL · A STEADY & RISING WAVE

Zero-day exploitation is persistent, industrialized, and accelerating.

2025 · SURGING AGAIN

+46%

Exploitation up in early 2025 vs. prior periods — 30+ zero-days already on CISA's KEV list, with 2024 Ivanti VPN flaws exploding into mass exploitation.

2024 · ELEVATED & SUSTAINED

75

Vulnerabilities exploited as zero-days — nearly double 2020. 44% targeted enterprise infrastructure: security tools, VPNs, and firewalls.

2023 · ALL-TIME PEAK

97

Zero-day exploits — the highest number ever recorded, driven largely by state-sponsored groups.

> **The baseline keeps rising. Each year resets the “new normal” higher than the last.**

HOW ZERO-DAY ATTACKS HAPPEN · 2023–2025

Recent zero-days — and the AppSec failures that let them through.

CVE-2024-21887 · CVE-2023-46805

Ivanti Connect Secure / Policy Secure

Chained VPN-appliance flaws bypassed authentication and executed remote code — 2,000+ devices compromised across government, telecom, and healthcare.

AST GAP Only partial visibility into embedded VPN codebases; missed correlations.

CYBERSAGACITY Anomaly detection flags abnormal auth flows; recognizes high-risk RCE-chain constructs.

CVE-2025-21297

Microsoft Office RTF Code Execution

A malicious RTF document executed arbitrary code with minimal user interaction — fueling phishing, lateral movement, and credential theft.

AST GAP Weaknesses appear as “low severity” or are dismissed as legacy code.

CYBERSAGACITY Reclassifies low-severity flaws by actuarial exploit likelihood from historical data.

CVE-2025-53690

Sitecore ViewState Deserialization RCE

Insecure ViewState deserialization via an exposed machine key led to full system compromise and lateral movement.

AST GAP Tools rarely correlate insecure config + deserialization as compounded risk.

CYBERSAGACITY Identifies exploit chains (config → deserialization → RCE) with multi-factor risk ranking.

CVE-2023-34362

MOVEit Transfer SQL Injection

A zero-day SQL injection drove one of the largest global data-extortion attacks — hundreds of organizations compromised.

AST GAP False negatives and inconsistent classification hid the real severity.

CYBERSAGACITY Corrects miscategorized input-handling flaws; detects statistical precursors to injection.

WHY ZERO-DAY ATTACKS ARE INCREASING

Four forces are driving the surge — and the toolchain is one of them.

Attackers weaponize faster

A **5-day median** from disclosure to exploitation. *(Mandiant)*

Security tools are the target

Nearly **half** of 2024 zero-days hit VPNs, firewalls, and gateways — turning defenses into entry points.

The black market professionalized

Exploits now sell for **millions** — funding research teams, broker networks, and state-sponsored investment.

The toolchain is fragmented

Multiple SAST, DAST, SCA, API scanners, and PenTests — and **no two agree** on severity, accuracy, coverage, or confidence.

CyberSagacity eliminates this fragmentation — exposing the real risk signals hiding inside inconsistent AST outputs.

WHY TRADITIONAL AST TOOLS FAIL AGAINST ZERO-DAYS

Five systemic failures against the unknown.

01

Signatures can't see the unknown

AST tools rely on pattern libraries. Zero-days exploit patterns that aren't in the library.

02

False positives bury weak signals

Up to **97%** of “critical” findings are false positives — hiding the anomalies that precede zero-days.

03

False negatives leave blind spots

Tools miss **40–60%** of real vulnerabilities in large codebases.

04

No cross-tool correlation

Overlapping vulnerabilities across tools are almost never reconciled — making exploit patterns invisible.

05

No financial or business context

Zero-day risks are business risks. Traditional tools cannot quantify impact or prioritize by outcome.

HOW CYBERSAGACITY PROTECTS AGAINST ZERO-DAY ATTACKS

The first AppSec intelligence system built to anticipate zero-days.

A

Correct the data

Every defect from every tool is corrected, normalized, and classified statistically — so you see the real vulnerabilities, not the contradictions and mislabels.

B

Reveal hidden patterns

Actuarial models built on **35M+ defects** surface weak semantic patterns, risk-magnifying defect chains, and coverage gaps — exposing future exploit vectors first.

C

Quantify the risk

Defect clusters become probabilistic exploit likelihood, financial exposure, data-loss and regulatory consequence, and remediation ROI — business decision intelligence.

D

Improve posture continuously

Ongoing normalization, correlation, updated scoring, enterprise dashboards, and compliance mapping (NIST, PCI, CMMC, HIPAA) — a continuous intelligence loop.

Zero-day defense stops being reactive — and becomes a continuous intelligence loop.

HOW CYBERSAGACITY WOULD HAVE PREVENTED RECENT ZERO-DAYS

Same events.
A different outcome.

Zero-Day Event	Traditional AST Failure	What CyberSagacity Would Have Identified
Ivanti VPN RCE	Tools failed to correlate auth bypass + path traversal.	Pattern cluster flagged as a high-likelihood exploit chain.
Microsoft RTF RCE	Legacy code weaknesses mislabeled as low risk.	Historical patterns show elevated exploitability.
Sitecore Deserialization RCE	No correlation between config exposure + deserialization risk.	Links config exposure directly to RCE patterns.
MOVEit SQL Injection	Core input-validation gaps hidden by false negatives.	Statistical analysis detects exploit-prone input flows.
Barracuda ESG Backdoor	Tools missed the persistence mechanisms.	Identifies anomalous behavior signatures.

PREPARING FOR ZERO-DAY ATTACKS

Zero-day defense becomes predictive, measurable, achievable.

- **Adopt evidence-based AppSec** — risk must be quantified, not assumed.
- **Replace signature thinking with predictive models** — historical defect data reveals tomorrow's exploit vectors.
- **Continuously normalize and correlate** all AST outputs — fragmented tooling means fragmented visibility.
- **Prioritize by business and financial impact** — not every “high” matters, and not every “low” is safe.
- **Validate compliance against real exploitability** — zero-days frequently target compliance gaps.

CONCLUSION

Zero-days are a structural consequence of fragmented workflows, inconsistent severity scoring, incomplete coverage, and the absence of true defect intelligence. Organizations need more than scanners — they need insight.

With CyberSagacity, zero-day defense becomes predictive, actionable, measurable, and achievable.