JSOC IT Launches AUTOPSY — Security Verification Platform That Runs the Investigation Before the Breach

READY™ replaces self-reported security posture with API-verified findings — the average org scores 20–35 points lower than it claims.

WASHINGTON, DC, UNITED STATES, March 13, 2026 /EINPresswire.com/ -- JSOC IT Launches AUTOPSY — The Security Verification Platform That Runs the Investigation Before the Breach, Not After It Introduces READY™, the flagship API-verified assessment that replaces self-reported security posture with evidence-based findings — and reveals the average organization scores 20–35 points lower than it claims

> Every breach ends with an autopsy. We built AUTOPSY to run it first."
>
> *Tawfiq Momin*

JSOC IT, the cybersecurity firm known for embedded Forward Deployed Engineering engagements across regulated industries, today announced the launch of AUTOPSY — a new security verification platform that investigates an organization's security stack via live API integrations before a breach occurs, rather than after one forces the conversation.

The platform's flagship product, READY™, is the first commercially available security assessment to replace self-reported questionnaires with API-verified telemetry across an organization's entire security stack — including endpoint detection, identity and access management, backup and recovery, vulnerability management, and more than 24 integrated security platforms.

The launch introduces a new category in cybersecurity: Security Verification — the discipline of proving what a security program actually does, rather than documenting what it claims to do.

"The cybersecurity industry has been running on an honor system. Organizations report their security posture, check the boxes, earn the certificates — and everyone moves on until a breach forces the autopsy. We built AUTOPSY to run that investigation first. READY™ is the verdict it delivers. Most organizations find out they're not as ready as they thought — and now they find out before it matters."
— Sam Sawalhi, Founder, JSOC IT

THE READINESS GAP

JSOC IT's assessment data reveals a consistent and alarming pattern across regulated organizations: the gap between self-reported security posture and API-verified security reality averages 20 to 35 percentage points. The firm calls this the Readiness Gap — the difference between what a CISO believes about their environment and what AUTOPSY verifies is actually true.

In a representative READY™ engagement with a mid-market financial services firm, AUTOPSY surfaced findings that had been invisible to the organization's existing tools, last audit, and GRC platform:
Silent EDR coverage failure: 23% of endpoints had sensor failures generating no alerts — deployed on paper, blind in practice
MFA exclusions on internet-facing systems: Four legacy finance applications were excluded from MFA enforcement — all with direct internet exposure
Untested backup infrastructure: The last verified full-restore test was 14 months prior; current backups had never been validated in production
Dormant privileged accounts: 34 inactive admin accounts remained active, including credentials belonging to three former employees
None of these findings appeared in the organization's self-reported security assessment. All of them would have been available to an attacker. The firm's self-reported score was 87. Their READY™ verified score: 61.

THE AUTOPSY PLATFORM
AUTOPSY connects to an organization's security stack via live API integrations across five major security frameworks simultaneously: NIST CSF 2.0, CIS Controls v8, SOC 2, ISO 27001:2022, and MITRE ATT&CK. The platform's 24 current integrations span endpoint, identity, cloud, vulnerability management, backup, and threat intelligence, with 40+ integrations planned through Q3 2026.
AUTOPSY is delivered through a three-phase engagement model:
Phase 1 — The AUTOPSY: Full READY™ assessment across all 15 security domains. API-verified findings. Readiness Gap quantified. Forensic report delivered.
Phase 2 — The Rebuild: JSOC IT Forward Deployed Engineers are embedded with the client to remediate every finding surfaced by the AUTOPSY — tool by tool, control by control.
Phase 3 — Always On: Continuous API-verified monitoring ensures the organization's verified posture is maintained — not assumed — in perpetuity.

"Deployed is not the same as defended. Every organization we've worked with had security tools. What they didn't have was verified proof that those tools were working — especially at 2 AM on a Saturday when response times are 5.6x slower and nobody is watching. AUTOPSY is the 2 AM Test™ for your entire security stack."
— Sam Sawalhi, Founder, JSOC IT

AVAILABILITY
AUTOPSY is available immediately for regulated organizations in financial services, healthcare,

and professional services with 200–2,500 employees. The READY™ assessment is available as a standalone engagement or as part of the full three-phase Resilience Program. MSP and MSSP partnership inquiries are also being accepted.

For more information or to schedule a READY™ assessment: ready.jsocit.com

ABOUT JSOC IT
JSOC IT is a cybersecurity firm specializing in security verification, Forward Deployed Engineering, and continuous resilience for regulated organizations. The company's AUTOPSY platform connects to an organization's security stack via live API integrations to verify real security posture against claimed posture — replacing self-reported assumptions with evidence-based findings. JSOC IT serves clients in financial services, healthcare, and professional services across the United States. For more information, visit ready.jsocit.com.

MEDIA CONTACT
Briana Siegel
Media JSOC IT
press@jsocit.com
www.jsocit.com
ready.jsocit.com

Briana Siegel
JSOC IT, Inc
+1 202-839-4440
email us here
Visit us on social media:
LinkedIn
