WideField Security Awarded Two U.S. Patents for Foundational Identity Threat Detection and Posture Management Technology

Patents cover live session graph analysis and meta session stitching - core innovations powering dynamic identity defense for the agentic AI era

WideField Security

SANTA CLARA, CA, UNITED STATES, June 2, 2026 /EINPresswire.com/ -- WideField Security Inc., the leading identity visibility, threat detection and response company, today announced that the United States Patent and Trademark Office has granted the company two patents covering its foundational approach to identity threat detection and identity security posture management.

U.S. Patent No. 12,592,942, titled "Session Analysis for Identity Threat Detection and Identity Security Posture Management," and U.S. Patent No. 12,592,943, titled "Session Analysis for Identity Posture Management and Security," were both issued March 31, 2026.

"Identity has become the new perimeter, and that perimeter is no longer a moment in time," said Abhay Kulkarni, co-founder and CEO of WideField Security. "It is a continuous, living surface that spans humans, AI agents and machine identities operating across hundreds of applications. These patents validate the architectural bet we made from day one. Static, login-centric defenses cannot stop today's session hijacking, token theft and AI agent misuse. You need a live, dynamic view of identity in use, and that is exactly what our platform delivers."

U.S. Patent No. 12,592,942 describes WideField's live session graph technology. The system ingests continuous telemetry signals from identity-adjacent sources, including Secure Access Service Edge, Endpoint Detection and Response, Identity and Access Management and cloud applications and constructs a graph of nodes and edges representing users, devices, applications, sessions and third-party app tokens.

When analysis surfaces a security event, the platform enforces remediation policies ranging from revoking sessions and access tokens to disabling federated logins and quarantining downstream applications.

U.S. Patent No. 12,592,943 describes WideField's meta session stitching technology. Because a single user journey is fragmented across many distributed sessions and entities such as an Okta SSO session, downstream Salesforce and GitHub session, an OAuth-connected third-party app and the underlying device - no single log tells the full story. The patented method correlates these fragmented signals into a unified signal hierarchy, reconstructs the full session underlying each meta session, determines whether that session's posture is healthy, potentially compromised or compromised, and enforces security policy based on that determination.

Together, the patents protect WideField's methods for ingesting telemetry across SaaS, cloud, on-premises, IAM, EDR, MDM and SASE sources; constructing live session graphs and stitched meta sessions of every AI agent, non-human and human identity; and enforcing remediation policies in real time when identity risk is detected.

For two decades, identity security was treated as a checkpoint problem. A user logged in, multi-factor authentication fired, single sign-on issued a token, and access was assumed to be safe until the next login. That model is collapsing under converging pressure.

Application sessions now last days or weeks rather than minutes, meaning a single stolen token can provide an attacker prolonged, undetected access. Approximately 80% of breaches now involve the abuse of valid credentials or session tokens rather than software exploits. And the rise of Agentic AI has introduced a new class of identity, AI agents, copilots and autonomous workflows that act on behalf of users, hold their own credentials, chain calls across SaaS APIs and operate continuously without human supervision. These non-human identities outnumber human identities in many enterprises today and cannot be governed by login-time controls alone.

"What makes these innovations powerful is the hierarchy of signals we correlate and the dynamic posture we maintain on every active session," said Kartik Kumar, co-founder and CTO of WideField Security and lead inventor on both patents. "We can stitch together an IAM login event with downstream application activity, EDR malware detections, SASE network anomalies and OAuth grants to a third-party AI agent; all into one composite view of an identity in motion. That is what makes detection of session hijacking, third-party token abuse and rogue agent behavior possible at machine speed."

About WideField Security:

WideField Security modernizes identity security for the AI era. The company's platform connects the identity fabric across SaaS, cloud and on-premises environments to deliver real-time visibility,

threat detection and response across AI agents, human identities and non-human identities. By protecting identity at rest, in motion and in use, WideField helps enterprises eliminate the root causes of identity-led breaches rather than treating their symptoms. Learn more at www.widefield.ai.

Sonia Awan
Outbloom Public Relations
soniaawan@outbloompr.net
Visit us on social media:
LinkedIn
