

The TAG logo consists of the letters "TAG" in a bold, white, sans-serif font, centered within a dark blue rectangular box.

TAG

ANALYST REPORT

OVERVIEW OF THE REACH SECURITY NETWORK SECURITY ASSURANCE (NSA) OFFERING

DR. EDWARD AMOROSO,
CEO, TAG
RESEARCH PROFESSOR, NYU



Reach

OVERVIEW OF THE REACH SECURITY NETWORK SECURITY ASSURANCE (NSA) OFFERING

DR. EDWARD AMOROSO, CEO, TAG,
RESEARCH PROFESSOR, NYU

Today, every infrastructure change, application deployment, cloud migration, or business integration introduces the possibility that network security controls will drift away from their intended state. For example, over time, firewall rules accumulate, temporary exceptions become permanent, duplicate policies emerge, obsolete objects remain active, and overly permissive access paths quietly develop throughout the enterprise.

To illustrate the point, recent research from Reach Security suggests that firewalls are the single most common source of configuration-related breaches, with 42% of security professionals reporting such incidents. Similarly, Reach observes a multitude of drift alerts each day from their customer base, alerting security teams that some network security control, usually a firewall rule, has been altered or misaligned.

A problem, however, is that in the absence of alerts, firewalls and enterprise networks would appear to be functioning normally, and yet collectively, such problems create one of the largest hidden attack surfaces inside modern organizations. This is only made more challenging as autonomous agents emerge that can locate or create attack paths that were previously unknown or ignored.

In fact, we believe that AI-powered attackers are now demonstrating the ability to continuously analyze exposed configurations, identify policy weaknesses, correlate misconfigurations into complete attack paths, and rapidly exploit opportunities before defenders recognize that drift has occurred. This shifts network security from a periodic governance exercise into a continuous assurance problem.

To address the problem, the new Reach Network Security Assurance (NSA) offering is designed to continuously identify, validate, prioritize, and remediate network security weaknesses before adversaries, whether human or non-human, can capitalize on them. Below we outline the risks that Reach NSA addresses, and we provide an overview of the platform and our assessment of the market prospects.

NETWORK SECURITY CONFIGURATION DRIFT IN THE AI ERA

Common examples of the drift problem include firewall exceptions becoming permanent, legacy applications leaving behind unused rules that nobody feels comfortable removing, and cloud deployments creating inconsistent security controls across different environments. As these types of changes accumulate over months and years, an enterprise network can and will increasingly diverge from its original security architecture.

The resulting network, in our experience, typically contains three categories of hidden weakness. The first category consists of stale security, access, or other policy-based rules that continue allowing communication for systems, applications, or business processes that no longer exist. These unnecessary rules expand the available attack surface without providing operational value – so this is an obvious risk.

The second category includes shadowed rules that have effectively become invisible because they are superseded by broader policies elsewhere in the rule base. While administrators often assume these rules continue enforcing security policy, they may actually provide no protection whatsoever while simultaneously complicating policy management. This is not always an easy condition to detect, so this situation arises more often than one might expect.

The third and perhaps most dangerous category involves overly permissive rules that authorize substantially broader access than originally intended. These policies frequently emerge from operational urgency, troubleshooting exercises, or business requests requiring rapid deployment. Once implemented, however, they often remain indefinitely, quietly creating lateral movement opportunities that sophisticated attackers can exploit.

Individually, these issues may appear relatively minor, but collectively, they produce hidden pathways across enterprise environments that AI-powered offensive platforms can discover almost instantly. Rather than searching randomly for vulnerabilities, autonomous attackers will increasingly analyze policy relationships, identify unintended trust boundaries, map reachable assets, and calculate optimal attack paths using machine-speed reasoning.

REACH NETWORK SECURITY ASSURANCE (NSA)

The Reach NSA solution approaches the challenges discussed above by shifting organizations from periodic network security assessment toward continuous network security assurance. For example, rather than treating firewall management as an administrative function, the platform continuously evaluates whether deployed network controls continue enforcing the organization's intended security posture.

One might view the NSA offering as part of a logical progression from the earliest manual approaches to firewall and network policy administration, through early platforms that introduced automation such as from Tufin, Firemon, and AlgoSec, and now achieving a full next-generation approach designed to handle configuration drift in the context of modern AI-enabled threats.



Figure 1. Evolution of Network Security Policy Management to Reach NSA

The architecture continuously examines security controls to identify policy drift, redundant rules, unused objects, compliance deviations, excessive permissions, and configuration inconsistencies across heterogeneous environments. Rather than just generating reports, the platform correlates findings into operational risk, allowing security teams to distinguish cosmetic issues from weaknesses that materially increase attack exposure.

Once such findings have been presented, the requirement becomes remediation. Reach maps each weakness to the relevant enforcement point and provides step-by-step guidance for correcting the misconfiguration. This might include removing unnecessary permissions, adjusting overly permissive access, eliminating unused or redundant rules, or restoring intended policy enforcement.

Where appropriate, these steps can also be automated according to the customer's operational and change management preferences, helping teams reduce exposure without turning remediation into another manual governance exercise.

One valuable aspect of the Reach approach is its emphasis on continuous assurance rather than static compliance. The platform continuously monitors for change, identifies configuration drift, prioritizes high-impact improvements, and supports safe remediation workflows. Such continuous lifecycle transforms network security management into an ongoing operational discipline instead of an occasional audit exercise.

Reach also extends beyond firewall rule analysis by leveraging AI intelligence across multiple security domains. Cybersecurity domain-specific AI and deterministic models evaluate misconfigurations, unused controls, compliance gaps, rule weaknesses, policy optimizations, and broader asset protection issues. By correlating network controls with enterprise assets and context, the platform enables security teams to understand whether rules are working.

Reach also emphasizes integrated remediation to safely remove unnecessary permissions, optimize security controls, eliminate policy drift, and improve overall network posture. This closed-loop operating model reduces the window during which new weaknesses remain available for exploitation. The practical objective is to discover and correct hidden network weaknesses before autonomous attackers discover them first.

TAG PERSPECTIVE

Exposure management has tended to focus on identifying vulnerabilities or external attack surface exposure. Less attention has been directed toward the policy drift that accumulates inside enterprise networks. We believe that as offensive AI becomes capable of continuously reasoning about enterprise network configurations, attackers will increasingly target misconfigurations rather than software vulnerabilities alone.

In many environments, exploiting an unnecessary firewall exception, an overly broad access policy, or an unintended trust relationship has proven to be substantially easier than exploiting a software flaw. This reality elevates the importance of continuously validating network policy correctness, especially as enterprise networks begin to sprawl across hybrid cloud and software-as-a-service (SaaS) environments.

Reach is well positioned here with its focus on continuous assurance, AI-assisted policy analysis, configuration drift detection, integrated remediation, and posture persistence. We are encouraged by the company's emphasis on operationalizing assurance rather than expanded reporting. Security teams will require platforms that actively maintain secure configurations instead of just documenting when those configurations have degraded.

From a broader market perspective, we also believe Reach NSA will complement adjacent disciplines such as CTEM and emerging AI-driven security operations. Organizations will thus increasingly expect these capabilities to function together as components of a unified continuous assurance architecture rather than as isolated point products – and this plays directly into the Reach NSA focus area.

Overall, we see Reach NSA as addressing a problem whose importance will continue to increase as AI compresses both attack timelines and defender response windows. Organizations that continuously identify and remediate policy drift will enjoy a meaningful defensive advantage over those relying on periodic reviews. We will watch carefully as this process unfolds and how Reach approaches the market with its NSA offering.

ABOUT TAG

Recognized by Fast Company, TAG is a trusted next generation research and advisory company that utilizes an AI-powered SaaS platform to deliver on-demand insights, guidance, and recommendations to enterprise teams, government agencies, and commercial vendors in cybersecurity and artificial intelligence.

Copyright © 2026 TAG Infosphere, Inc. This report may not be reproduced, distributed, or shared without TAG Infosphere's written permission. The material in this report is comprised of the opinions of the TAG Infosphere analysts and is not to be interpreted as consisting of factual assertions. All warranties regarding the correctness, usefulness, accuracy, or completeness of this report are disclaimed herein.