TAG

ANALYST REPORT

STRENGTHENING FEDERAL IDENTITY SECURITY WITH SEMPERIS PURPLE KNIGHT

DR. EDWARD AMOROSO
CHIEF EXECUTIVE OFFICER, TAG,
RESEARCH PROFESSOR, NYU

Strengthening Federal Identity Security with Semperis Purple Knight

By Ed Amoroso

Version 1.0
March 29, 2026

Introduction
In my ongoing work at TAG supporting U.S. federal agencies, I continue to see a persistent and somewhat uncomfortable problem – namely, that *identity* remains the most frequently exploited attack surface element in government networks. This would be a manageable situation if deployed identity security solutions were fully effective, but my observation is that too often, they simply are not.

Let's dig into this issue to see what can be done (and please recognize that enterprise teams also exhibit this problem).

First off, the mismatch between threat and defense for identity is particularly evident in hybrid environments, where agencies must manage a complex mix of on-premises Active Directory, cloud-based identity services such as Entra ID, and third-party identity providers like Okta.

Despite years of investment in Zero Trust initiatives and compliance-driven security programs, many federal teams still lack a simple and effective way to assess their identity posture across this distributed environment. It's not just budget challenges, but more a lack- at last to date – of great options.

This is precisely where Semperis Purple Knight looks to provide meaningful value. Designed as a free, low-risk assessment tool, it enables these federal teams to scan their hybrid identity infrastructure for vulnerabilities and misconfigurations without introducing operational friction. Its appeal is straightforward. That is, there is no cost (yes, you read that correctly) and I would venture to guess that you will see immediate actionable insight.

Purple Knight has now reached more than 65,000 downloads globally (wow!), and its assessment engine evaluates over 210 indicators of exposure and compromise. These checks are aligned with frameworks such as MITRE ATT&CK, ensuring that findings are relevant and grounded in real-world adversary behavior.

Importantly, all analysis is conducted locally within the agency's environment, which eliminates concerns around sensitive data leaving federal systems. We all know that this is a critical and challenging requirement for government adoption.

Another compelling aspect of Purple Knight is the baseline insight it provides. Data from recent assessments shows that government agencies tend to begin with scores that are pretty bad. This is no criticism, but rather as a reflection of the complexity of hybrid identity environments. Over time, incremental configuration drift, legacy settings, and inconsistent policy enforcement create gaps that are difficult to detect without purpose-built tooling.

By establishing a baseline score, Purple Knight gives federal teams a starting point for measurable improvement. The tool includes built-in remediation guidance that prioritizes high-impact issues, allowing teams to focus their efforts where it matters most. Organizations that follow this guidance have demonstrated average score improvements of approximately 21 points, with some achieving gains as high as 61 points.

Purple Knight's support for Microsoft GCC High environments is also a useful factor. This capability, currently in beta, addresses a long-standing gap for federal agencies operating in highly regulated cloud environments. It would appear that teams can use Purple Knight to generate a unified security posture score that spans both on-premises Active Directory and GCC High Entra ID.

It is worth noting that Purple Knight is also the only free identity security assessment tool recommended by name in the Five Eyes Alliance advisory on detecting and mitigating Active Directory compromises. This endorsement, including from organizations such as National Security Agency (NSA) and Cybersecurity and Infrastructure Security Agency (CISA), signals a high degree of confidence in both the methodology and the practical utility of the tool.

From a broader perspective, Purple Knight aligns with federal Zero Trust directives. These mandates emphasize continuous assessment, least privilege enforcement, and rapid remediation of vulnerabilities. By providing an accessible mechanism to identify identity-related weaknesses and track improvement over time, Purple Knight serves as a pragmatic entry point for agencies seeking to operationalize these principles.

In any event, Purple Knight seems like a no-brainer from my perspective, and I would hope that identity teams across all federal agencies take note – and act soon.

Let me know what you think.