Active Directory holds the “keys to the kingdom,” and if not safeguarded properly, it will compromise your entire security infrastructure. Purple Knight is a free Active Directory security assessment tool built and managed by an elite group of Microsoft identity experts.

Active Directory Security Report Card
Pre- and Post-Attack Security Indicators
Prioritized, Actionable Guidance
Community-Driven Threat Models
MITRE ATT&CK Correlation

Spot weaknesses in Active Directory before attackers do.

Attackers take advantage of weak Active Directory configurations to identify attack paths, access privileged credentials, and get a foothold into target networks. Purple Knight queries your Active Directory environment and performs a comprehensive set of tests against the most common and effective attack vectors to uncover risky configurations and security vulnerabilities. You receive prioritized, corrective guidance to close gaps before they get exploited by attackers.

Minimize your attack surface and stay ahead of ever-evolving threats.

To lockdown Active Directory, you must think like an attacker. Purple Knight maps pre- and post-attack security indicators to the MITRE ATT&CK framework, offering an overall risk score along with the likelihood of compromise and specific remediation steps. You can proactively harden your Active Directory against new adversary tactics and techniques with built-in threat modeling, which is constantly updated by a team of security experts.
Take back the keys to your kingdom.

The hard truth is that Active Directory is a soft target for attackers attempting to steal credentials and deploy ransomware across your network. But securing Active Directory is difficult given its constant flux, the sheer number of settings, and the increasingly sophisticated threat landscape. And with easy access to powerful hacking tools, even small-time criminals can be just as dangerous as sophisticated nation-state adversaries. Purple Knight is on a mission to help organizations combat the deluge of escalating attacks targeting Active Directory. Regardless of company size or industry, we believe that security programs must be empowered to safely challenge their defenses, find weak spots, and take immediate action.
Semperis is the pioneer of identity-driven cyber resilience for cross-cloud and hybrid environments. The company provides cyber preparedness, incident response, and disaster recovery solutions for enterprise directory services—the keys to the kingdom. Semperis' patented technology for Microsoft Active Directory protects over 40 million identities from cyberattacks, data breaches, and operational errors. Semperis is headquartered in New Jersey and operates internationally, with its research and development team distributed between San Francisco and Tel Aviv.

Semperis hosts the award-winning Hybrid Identity Protection conference. The company has received the highest level of industry accolades; most recently being ranked the fourth fastest-growing company in the tri-state area and 35th overall in Deloitte's 2020 Technology Fast 500™. Semperis is accredited by Microsoft and recognized by Gartner.