Privilege Assurance: Technical Specifications Guide

Limit the potential damage of a cyber attack

Lock Down you Active Directory

Attackers know that Active Directory accounts are attractive targets. Compromising Active Directory accounts gives malicious actors access to your key network assets that can be difficult to detect. And those attacks can cost your organization time, money, and your reputation.

Active Directory is critical control infrastructure for most organizations. QOMPLX's Privilege Assurance solution helps identify weaknesses in your Active Directory environment, spotlight accounts that pose a risk to your organization, and identify concentrated pockets of privileges that malicious actors will seek to exploit.

Our Approach and Methodology

QOMPLX's Privilege Assurance software analyzes Active Directory data to identify security risks associated with privileged user accounts, stale or outdated user accounts and machines, weaknesses in policy, and other risks. To fulfill this purpose, Privilege Assurance extracts and processes Active Directory data.

Privilege Assurance (PA) monitors the configurations of Active Directory by issuing a series of Lightweight Directory Access Protocol (LDAP) queries. It may also connect to individual machines using the Server Message Block (SMB) protocol to collect user session information and local administrator metadata, if a company opts to include SMB-based data collection. SMB sessions provide visibility into local admin accounts and the computers to which they have active sessions.

Data Collected:

- Active Directory configuration parameters including Domains, Trusts, Organizational Units (OUs), and Group Policy Objects (GPOs)
- User profile settings in Active Directory, such as User ID, Display Name, and Email Address
- Log on activity and account configuration parameters
- IP addresses of systems
- User account rights and other Access Control Entries (ACEs)
- Computers joined to Active Directory, including parameters such as OS and last logonKerberos principal names (e.g. a workstation user or a network server)
- Active Directory group configurations and members
- Hygiene-related attributes such as stale accounts, old password accounts, and admin accounts without password expiration

- Computer-based attributes such as sessions and local admin settings

Analytics:

Privilege Assurance offers the following analytics:

- Active Directory domain and forest trusts
- User account and group creation and changes
- Excessive non-admin user permissions
- Sale and abandoned Active Directory accounts
- Pathways to attacker objectives

Privilege Assurance installs in minutes and analyzes data in QOMPLX's secure cloud, eliminating the need to process on-premises, or purchase equipment for analytics processing. QOMPLX also offers a full set of managed services and professional Advisory services for customers that require additional support to ensure success with securing and modernizing Active Directory.

Ready to learn more about *QOMPLX's Privilege Assurance solution*? Contact us today.

+1 (703) 995-4199 | info@QOMPLX.com | www.QOMPLX.com

Why QOMPLX®

QOMPLX makes it faster and easier for organizations to integrate all of the disparate data sources across the enterprise into a unified analytics infrastructure to make better decisions. This broader analytics infrastructure is provided through QOMPLX:OS, an enterprise operating system that powers QOMPLX's decision platforms in cybersecurity, insurance underwriting, and quantitative finance. Headquartered in Reston, VA, QOMPLX, Inc. also has offices in New York and London. More information about QOMPLX can be found at https://www.qomplx.com/.