QOMPLX Privilege Assurance for Azure Active Directory

Protect your hybrid environments with real-time security monitoring and recommendations from QOMPLX Privilege Assurance (PA) for Azure Active Directory (AD):

- **Improve security against Identity-based attacks:** QOMPLX Privilege Assurance for Azure AD introduces new security recommendations that help protect against identity-based attacks, which are among the most common and dangerous cyber threats. By identifying and addressing vulnerabilities, these new PA extensions help organizations enhance the security of their Azure AD environment, reducing the risk of unauthorized access, data breaches, and other security incidents.

- **Fast streamlined configuration:** Easy set up in just a few clicks allows organizations to deploy and use QOMPLX Privilege Assurance for Azure AD, as a convenient and accessible option for all sizes of organizations. Read-only permissions to Azure tenant needed. No agents, scripts, or extensive permissions required.

- **Protect identities across on-premises and cloud environments:** Combined QOMPLX Privilege Assurance and the new Privilege Assurance for Azure AD enables organizations to protect identities across both cloud and on-premises environments. This allows organizations to extend their security policies to hybrid environments and ensure that their users' identities are protected anywhere. By offering this seamless security coverage, QOMPLX provides a comprehensive solution for protecting identities in a modern, distributed IT environment.

Privilege Assurance (PA) for Azure Active Directory (AD)

Privilege Assurance for Azure AD are designed to highlight configuration and operations deficiencies and risks that can result in or facilitate lateral movement or Azure tenant compromise. Key capabilities added in the Azure AD Extension include:

- Azure Active Directory specific data collector
- Security recommendations and information

The ability to audit privileges on any given object inside an Azure tenant and subscriptions, enumerate dangerous privileges, and make changes before being abused inside Azure AD complements existing on premise AD support. Some additional items listed here also apply to only Azure AD and O365-enabled clients.

Data collection

Privilege Assurance has been extended to collect data from Azure Active Directory tenants. In just a few clicks and read-only permissions PA for Azure AD highlights security misconfigurations on:

- Azure Tenants
- Azure Users
- Azure Groups
- Azure Applications
- Azure Service Principals
- Azure Roles
- Azure Devices
- Azure Permissions
- Azure API Permissions

As with Active Directory Privilege Assurance all the data is available for you to explore on your own in addition to our analytics and recommendations.

Security recommendations and information

QOMPLX Privilege Assurance for Azure AD focuses on highlighting dangerous identity related risks including monitoring guest user access and MFA coverage across accounts. Additionally, Privilege Assurance for Azure AD checks for common backdooring techniques widely published and easily implemented by attackers.

> QOMPLX Privilege Assurance for Azure AD focuses on access control, authorization policies, and permissions management, multi-factor authentication (MFA) requirements, guest user access, and security policies and configurations.

1. **Access control, authorization policies, and permissions management:**
   This category of security checks focuses on ensuring that access to organizational data and systems is tightly controlled and properly authorized. It involves managing permissions for users, groups, and service accounts, and identifying and removing excessive privileges that could lead to data breaches or unauthorized access.

2. **Multi-factor authentication (MFA) requirements:**
   This category of security checks emphasizes the importance of multi-factor authentication in protecting organizational data and systems from unauthorized access. It involves enforcing MFA requirements for all accounts, especially those with administrative roles or elevated privileges, and blocking legacy sign-ins that do not support MFA. By implementing MFA, organizations can greatly reduce the risk of unauthorized access and data breaches.

3. **Guest user access:**
   This category of security checks focuses on managing guest user access to organizational data and systems. It involves ensuring that guest users are only granted access to the resources they need to do their job, and that their access is closely monitored to prevent data exfiltration or other unauthorized activities. This category also includes ensuring that guest users are unable to invite other guests, as this can lead to uncontrolled access and data breaches.

4. **Security policies and configurations:**
   This category of security checks focuses on ensuring that appropriate policies and configurations are in place to protect organizational data and systems. It involves implementing security default policies and restricting user consent for applications to prevent unauthorized access and data breaches. By implementing and enforcing appropriate policies and configurations, organizations can greatly reduce the risk of data breaches and protect sensitive information from unauthorized access.

Ready to learn more about QOMPLX? Contact us today.

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

Why QOMPLX®

QOMPLX harnesses data to provide unified visibility into cyber risks and trust in identity. QOMPLX solutions reduce cyber risk and attack surfaces by mapping exposures and performing real-time detection of attacks. This approach increases network observability by closing the largest remaining gaps in cybersecurity: identity verification, cross-tool data fusion, and data interoperability. QOMPLX defends some of the world's most renowned brands by re-establishing trust for client organizations, assuring authentication, and enabling confident security decisions.

For more information, visit qomplx.com and follow us @QOMPLX.