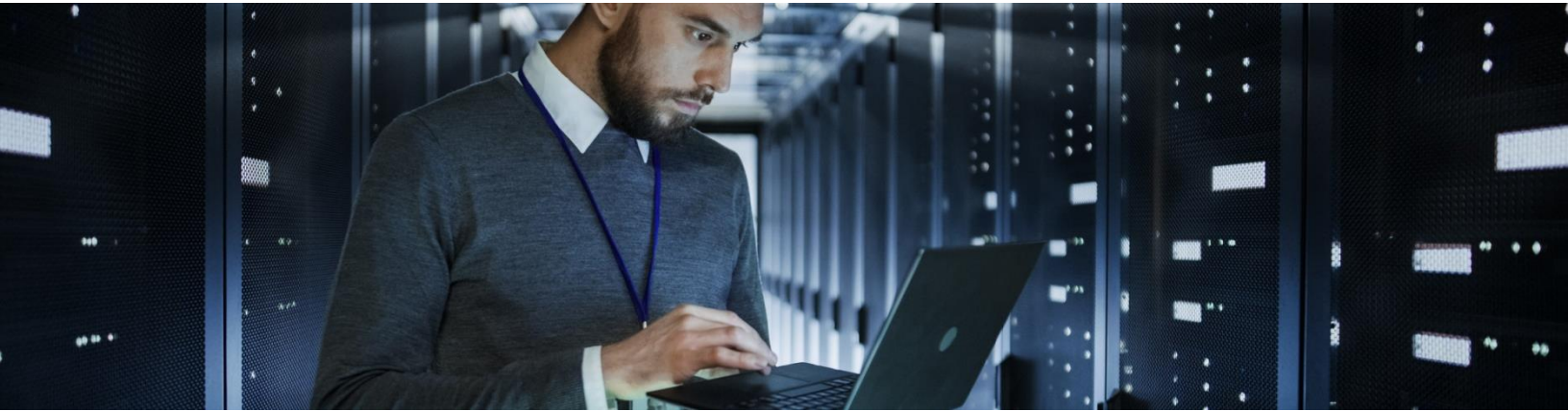# Active Directory Security Checklist

As the foundation of an organization's cyber security, Active Directory is an extremely high-value organizational asset and its adequate protection and security are paramount to business today.

Active Directory Security Checklist

The following 10-item checklist is intended to help organizations worldwide adequately assess and maintain the security of their foundational Active Directory (AD) deployments –

❑ Ensure that all stakeholders in the organization have a clear understanding of the paramount importance of AD security and that there exists a clear chain of accountability for AD security

❑ Ensure that your AD's logical (i.e. forest, domain and trust relationship) structure is sound

❑ Ensure that all domain controllers (DCs) have adequate physical, system and network security

❑ Ensure that all AD configuration data (e.g. Schema, Replication, FSMOs, Backups etc.) is secure

❑ Ensure that all privileged users in AD i.e. all accounts that possess Domain-admin equivalent privileged access in AD are accurately identified, and their number reduced to a bare minimum

❑ Ensure that access for all non-critical identity and access management functions/admin tasks (e.g. password resets) is provisioned/delegated in AD based on the principle of least privilege

❑ Ensure that all AD admins/privileged users have dedicated high-security alt accounts and admin workstations that are as secure as DCs, and that all tools used by them are highly trustworthy

❑ Ensure that you have complete, accurate privileged access visibility into AD at all times

❑ Ensure that auditing mechanisms are in place to capture enactment of all sensitive activity and that threat intelligence capabilities are in place to actively detect malicious activity against AD

❑ Ensure that AD management, breach-detection, incident-response and disaster-recovery plans are in place and that security assessments and privileged access audits are performed routinely