The Risks with Service Accounts

anetac

Service accounts are privileged, non-human accounts that are commonly used for automated tasks or for allowing applications to interact with other systems. Due to their often elevated privilege access to sensitive data and software pervasiveness, service accounts are more vulnerable and constitute a critical attack surface that needs to be managed. Service accounts are hard to detect and map making them a prime vector for attackers.

HYGIENE	SECURITY
Password Neglect - Service account passwords are often hard coded, easily discoverable, can be non-complex, and rarely changed. Changing them without understanding the internal dependency landscape risks impact on critical applications.	**Lateral Movement -** Threat actors frequently employ lateral movement tactics during cyberattacks and compromised service accounts are a way for cyber criminals to move undetected across an organization's environment.
Dormant or Unknown Service Accounts - Service accounts without visibility, proper account management and configuration, can lead to increased attack surface risk.	**High Privileges** - Service accounts, especially privileged ones, often hold admin-level access to sensitive data and systems, making them tempting attack targets.
NTLM - Migrating from NTLM requires visibility of the service account landscape in order to map usage and dependencies on AD accounts before remediating them.	**Incident Response** - The effort to quickly identify affected service accounts and analyze logs after an active directory attack can take days and tie up valuable resources.
Shared-use Service Accounts - Security hygiene is negatively impacted and opens up risk when human accounts are being used in scripts and behaving like non-human service accounts.	**Compliance Risks**: To mitigate compliance risks with regulations and standards such as HIPAA, PCI DSS, SOX, and GDPR, organizations must establish policies and procedures for managing service accounts which are often manual activity and usage reviews which are labor intensive, costly, and immediately outdated.
Service Account Sprawl - Organizations generate high volumes of service accounts which are difficult to identify, configure, and monitor creating a highly vulnerable internal attack surface.	**Blast Radius** - Poor visibility into service accounts creates issues identifying the actual impact radius of anomalous and suspicious human and nonhuman account behavior.

Anetac helps uncover blind spots with dynamic visualization of service account chains.