Silverfort

Silverfort für Active Directory: Identity-Security-Lücken schließen und laterale Bewegung eindämmen

Für mehr als 90 % der Unternehmen ist Active Directory (AD) nach wie vor das Rückgrat von Authentifizierung und Zugriff. Doch jahrelanger Gruppenwildwuchs, Akquisitionen und uneinheitliche Praktiken haben in den meisten AD-Umgebungen eine massive Identitäts-Altlast hinterlassen. Veraltete Konfigurationen, überprivilegierte Berechtigungen, Schattenadministratoren und unverwaltete Konten sind Schwachstellen, die Angreifer gezielt ausnutzen. Mit der Einführung von hybriden Identitätsmodellen überträgt sich diese gewachsene Komplexität auch auf Cloud-IdPs und vergrößert die Angriffsfläche zusätzlich.

Ohne einen proaktiven Ansatz für Active Directory bleiben Unternehmen mit dauerhaften Herausforderungen konfrontiert:

- **Fehlende Transparenz über alle AD-Konten – ob Benutzer-, Service oder Shared Accounts** – schafft Blind Spots, die Angreifer gezielt nutzen, um sich lateral zu bewegen und Privilegien auszuweiten
- **Abhängigkeit von Legacy-Protokollen und Fehlkonfigurationen** (z.B. Kerberos-to-NTLM-fallbacks, Nutzung von **NTLMv1/NTLMv2**) sowie fehlende native MFA-Unterstützung lassen kritische On-Prem-Ressourcen und Legacy-Anwendungen ungeschützt zurück
- **Gewachsene Identitäts-Altlasten** wie veraltete Konten, Schattenadministratoren, langlebige Secrets und unklare Zuständigkeiten erhöhen Lizenzkosten, verursachen Audit-Probleme und bergen versteckte Risiken
- **Fragmentierte Kontrollen**, die für Provisionierung statt für Live-Authentifizierung ausgelegt sind, hinterlassen Lücken zwischen Erkennung und Durchsetzung und begrenzen die Reaktionsfähigkeit in Echtzeit

So schließt Silverfort Identity-Security-Lücken in AD

Die Silverfort Identity-Security-Plattform beseitigt Blind Spots in AD durch Echtzeit-Transparenz, Kontrolle und Schutz – weit über die Möglichkeiten herkömmlicher Tools hinaus:

- **Sehen Sie alle AD-Authentifizierungen in Echtzeit.** Überwachen Sie **Kerberos, NTLM und LDAP** über Benutzer, Service Accounts, Geräte und Server hinweg; Erkennen Sie Kerberos-denied-to-NTLM-fallbacks und andere riskanten Authentifizierungsmuster in Echtzeit.
- **Verbessern Sie AD-Hygiene im großen Maßstab.** Klassifizieren Sie automatisch alle Konten – einschließlich Benutzer-, Service, Shared und Admin-Accounts –, um **Schattenadministratoren, veraltete Benutzer und unverwaltete Identitäten** aufzudecken. Zeigen Sie auf, wo sich Service Accounts tatsächlich authentifizieren, um klare Zuständigkeiten zu etablieren und Risiken sicher zu beheben.

- **Setzen Sie adaptive Sicherheitskontrollen in Echtzeit durch.** Blockieren Sie riskante Zugriffe sofort oder sichern Sie diese umgehend mit **MFA** ab. Setzen Sie **Virtual-Fencing-Richtlinien ein**, um Service Accounts und privilegierte Konten so einzuschränken, dass sie sich ausschließlich zwischen genehmigten Quellen und Zielen authentifizieren können.
- **Modernisieren Sie Authentifizierungsprotokolle ohne Unterbrechung.** Identifizieren Sie, wo Kerberos Legacy-Authentifizierung ersetzen kann, priorisieren Sie die **Abschaffung von NTLMv1 u**nd setzen Sie **richtlinienbasierte Kontrollen für NTLMv2** durch – für mehr Protokollsicherheit ohne Infrastrukturänderungen.

So funktioniert es

Schritt 1: Gewinnen Sie End-to-End-Transparenz über AD-Authentifizierungen

Silverfort integriert sich direkt in die bestehende Unternehmensumgebung und überwacht kontinuierlich jede AD-Authentifizierung (Kerberos, NTLM, LDAP) sowie alle zugehörigen Aktivitäten über Benutzerkonten, Service Accounts und Legacy-Protokolle hinweg – ohne Auswirkungen auf die Performance. Erkennen Sie sofort Kerberos-denied-to-NTLM-Fallbacks und fehlkonfigurierte SPNs.

Schritt 2: Identifizieren Sie Risiken und verbessern Sie die Identity-Security-Lage

Durch die Analyse von AD-Authentifizierungsaktivitäten deckt Silverfort Identitätsrisiken wie Schattenadministratoren, veraltete Benutzer und unverwaltete Service Accounts auf und ermöglicht es Security Teams, kritische Sicherheitslücken zu schließen.

Schritt 3: Setzen Sie adaptive Schutzmaßnahmen und Least Privilege durch

Auf Basis vollständiger Transparenz erweitert Silverfort den MFA-Schutz sowie granulare, zugriffsbasierte Kontrollen auf AD-Ressourcen und Legacy-Systeme – einschließlich Service Accounts und privilegierter Benutzer –, um laterale Bewegungen und Privilegieneskalation in Echtzeit zu verhindern.

Die wichtigsten Vorteile

Reduzieren Sie das Risiko von Ransomware-Angriffen und lateraler Bewegung

Stoppen Sie Angreifer proaktiv dabei, AD Blind Spots zur Privilegieneskalation oder zur Verbreitung von Ransomware auszunutzen.

Vereinfachen Sie den Betrieb Ihrer Identity Security

Erweitern Sie MFA- und Least-Privilege-Kontrollen nahtlos auf AD- und Legacy-Systeme und reduzieren Sie so Komplexität und operativen Aufwand.

Reduzieren Sie Kosten und beschleunigen Sie Audits

Identifizieren und beseitigen Sie veraltete Konten, Schattenadministratoren und ungenutzte Service Accounts, um Lizenzkosten zu senken und Compliance-Reports zu vereinfachen.

Stärken Sie Ihre Compliance-Bereitschaft

Erweitern Sie Sicherheitskontrollen auf alle AD-Identitäten und -Ressourcen – mit vollständiger Transparenz und privilegiertem Zugriffsschutz, um Compliance-Anforderungen zu erfüllen.

Über Silverfort

Silverfort sichert jede Dimension der Identität – Mensch oder Maschine, Cloud und On-Prem. Wir bieten End-to-End-Identitätsschutz, der sich einfach implementieren lässt, ohne Geschäftsabläufe zu stören – für bessere Sicherheitsergebnisse bei weniger Aufwand. Entdecken Sie jede Identität, analysieren Sie Risiken und setzen Sie Schutzmaßnahmen direkt durch, um laterale Bewegung, Ransomware und andere identitätsbasierte Bedrohungen zu stoppen.