Active Directory Hardening Services

Overview

Securing Active Directory (AD) privileged access is critical to ensuring the overall security of an environment. If an adversary can move laterally, elevate permissions, and achieve Domain Admin access, they can achieve total control of your network. We take a practical approach to hardening AD against these risks. Our approach considers the additive security benefits of each step versus the cost to implement and the long-term cost to operate the added controls.

There are five major phases of an AD hardening roadmap.

Lateral Movement Prevention

1. Preventing lateral movement between systems is a critical preventative control. Local administrative access to client computers and member servers should be limited to a credential that is unique to each system. This control can be achieved with Microsoft LAPS. Ravenswood's LAPS deployment approach addresses technical components and the business process changes necessary to have a successful deployment.

Credential Tiering

2. Credential tiering isolates privileged credentials from higher risk systems. By implementing isolation, the risk of credential theft and privilege escalation is significantly reduced. Tiering is often implemented by beginning with the most privileged credentials in AD – Domain Admins. Future phases may address isolation of privileged access to member servers and client computers.

Privileged Access Workstations (PAWs)

3. Privileged Access Workstations (PAWs) provide a known-good, clean keyboard for performing privileged or sensitive tasks. PAWs isolate sensitive accounts and processes from the risk of a potentially compromised workstation by ensuring that the PAW is built from clean media and prevented from accessing threat vectors such as the Internet. This approach protects (but does not prevent) from threats such as credential theft, keyboard logging, application vulnerabilities, etc.

Just-in-Time Access

4. Using a new, secured administrative forest, just-in-time (JIT) privileged access is provided to administrators following a multi-factor authentication (MFA) challenge. JIT access automatically expires after a predetermined period of time. After access expires, the administrator must request access again and complete another MFA challenge. Time-limited access potentially mitigates common attack vectors such as pass-the-hash and pass-the-ticket.

Administrative Forests

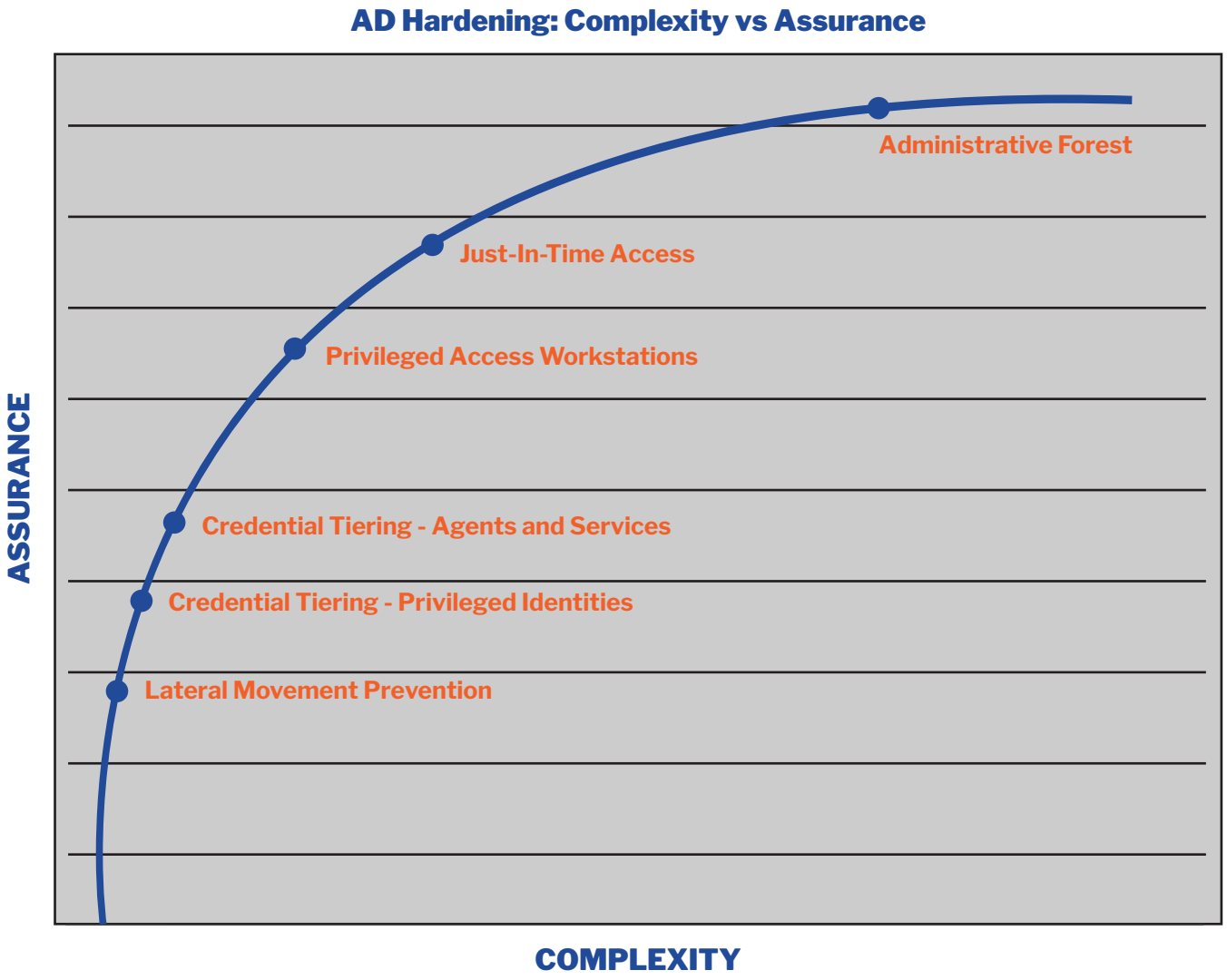
5. Administrative forests (sometimes called a red forest) are isolated instances of AD that house privileged credentials such as Domain Admins. By isolating privileged credentials, an attacker must bypass significant sets of security controls to elevate their access. Implementing these controls in a production AD forest that may have been compromised in the past is often not possible or recommended.

155 N WACKER DRIVE, SUITE 4250 CHICAGO, IL 60606
info@ravenswoodtechnology.com
www.ravenswoodtechnology.com

RAVENSWOOD
TECHNOLOGY GROUP

Active Directory Hardening Maturity Model

Hardening Active Directory (AD) and protecting privileged credentials is a complex undertaking. While a perfect world of complete protection is desirable, the reality is that operational cost and complexity of each step of the journey must be considered. Our view on the assurance each step provides versus the complexity of implementing and maintaining that step is captured in this chart.



155 N WACKER DRIVE, SUITE 4250 CHICAGO, IL 60606
www.ravenswoodtechnology.com

RAVENSWOOD
TECHNOLOGY GROUP