# 3 KEYS TO SECURING YOUR ACTIVE DIRECTORY

www.skyportsystems.com

## Upgrade Active Directory to a Secure First-Class Application

Microsoft's Active Directory is used by over 90% of the organizations in the world to manage access to nearly every piece of the IT infrastructure — users, data, applications, computers, storage, and the network. In 2015, 75% of all breaches involved the loss or theft or privileged credentials, which demonstrates the importance of improving Active Directory and credential security. However, most Active Directory systems were stood up over a decade ago and have not been updated to address the modern day threat landscape. Attacks consistently compromise vulnerable environments from a single insecure workstation in a few hours.

Microsoft recently published guidelines for safeguarding Active Directory and securing privileged access that have proven effective in many large enterprises[1]. They detail advanced practices such as implementing segmentation between AD forests based on trust zones, locking down administrative workstations and access, building trustworthy clean source servers, and whitelisting all communications. Unfortunately, fully adopting the guidelines is too costly and complex for most organizations, so improving the security of the AD environment is only done by large enterprises.

Skyport Systems provides the quickest and most assured way to regain control over your Active Directory environment by providing a secure enclave to host your production domain controllers and other authoritative systems. Skyport's award-winning SkySecure makes it easy for you to comply with Microsoft's advanced guidance. You can finally treat AD as a first-class application by:

- Safeguarding AD from attacks with specialized protections that defend against today's threats
- Empowering a single team to own the application, platform, and controls to securely operate AD
- Isolating the administrative domain to protect privileged credentials and systems

SkySecure can be deployed incrementally with measurable protections each step of the way. A project to protect your environment can usually be accomplished within a few months and will not disrupt your current production environment or architecture.

1 https://technet.microsoft.com/en-us/library/Microsoft

Secure Computing Environment

Isolation and Protection for Active Directory

Single Point of Administration

SKYPORT SYSTEMS

## Comply with Microsoft's Guidance

Microsoft's guidance for securing privileged access and Active Directory is a thoughtful approach to protect administrative credentials and authoritative systems from determined adversaries, however many fundamental steps have traditionally been insurmountable for most organizations to reach. SkySecure is a unique platform that makes it feasible to complete the journey to modernize. Specific examples are called out in the comparative table below.

| Microsoft Guidance | Current Approach without SkySecure | How SkySecure Helps |
|---|---|---|
| **Enforce Communication Whitelisting**<br>Only allow communications between the domain controller to approved systems and applications | Implement access control with group policy objects or host-based firewalls.<br><br>**Challenges:**<br>• Determining the set of restrictive rules to implement that do not break the environment<br>• Managing, maintaining and troubleshooting the rules over time<br>• Preventing malware from bypassing the controls | *SkySecure* wraps each AD component in a compartment that lets you:<br>• Easily determine and enforce whitelist communication policies, such as only allow communications to authoritative patch, configuration and domain service systems<br>• Block domain controllers from web browsing, reaching the internet, or communicating with untrusted systems<br>• Easily make changes to the policy and audit the configuration<br>• Audit all communications for each component for the lifetime of SkySecure<br>• Prove the security controls cannot, and are not, being bypassed |
| **Implement Privileged Admin Workstations (PAW/SAW)**<br>Use dedicated domain administration workstations or use jump servers to enforce RDP session restrictions and enforce two-factor authentication | Hardened admin workstations with endpoint security products<br><br>**Challenges:**<br>• Admin workstations are too easy to identify and compromise<br>• It isn't viable to use dedicated workstations or jump hosts<br>• May not have implemented twofactor authentication | *SkySecure* enables administrators to:<br>• Obtain secure graphical console access remotely, without caching privileged credentials on administrator workstations<br>• Use an easy-to-deploy virtual PAW/SAW that can restrict RDP access and prevent malware on administrative workstation from infecting domain controllers<br>• Guarantee two-factor authentication is always used to access privileged systems |
| **Build an Isolated Forest for Active Directory Administrators**<br>Isolate domain admin servers and workstations from the production domain | There is no isolated administrative forest<br><br>**Challenges:**<br>• Little security against privilege escalation attacks<br>• It is difficult to build an admin forest | *SkySecure* enables you to implement a turnkey administration forest, (a Red Forest,) that:<br>• Isolates privileged systems and credentials from the production environment with a one-way trust model<br>• Uses pre-configured system and security settings to streamline deployment<br>• Can be deployed rapidly without changing your network or application environment |

## Where to Start?

Pick your path. Most start securing production domain controllers by deploying them incrementally on SkySecure. But you can choose to implement a secure approach for administrative access with virtual PAWs/SAWs or to build an isolated *Red Forest* to protect privileged credentials.

**Visit us at www.skyportsystems.com to learn more.**

SKYPORT SYSTEMS