PREVENT THE ULTIMATE NIGHTMARE

www.skyportsystems.com

Overview

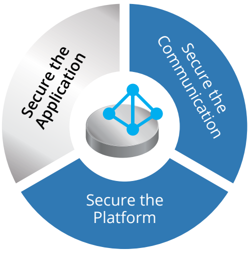
Your organization probably uses Microsoft Active Directory — 90% of enterprises do so. Unfortunately, Active Directory has known issues related to credential hijacking. In 2015, over 75% of all records that were compromised were the result of data breaches involving the loss or theft of a privileged credential. Attackers use stolen administrative access for weeks without detection resulting in breach costs in the millions.

Administrative credentials can be stolen by any compromised system accessed by an administrator. Administrative workstations that cache credentials and are vulnerable to phishing and website malware. Services involved in domain controller management, patching and backup are themselves subject to vulnerabilities that can become attacks against domain controllers.

Skyport Systems is the first company founded to deliver purpose-built secure infrastructure for critical applications and computing environments. Skyport's award-winning SkySecure platform protects your Active Directory infrastructure with our unique rearchitectiure of the x86 hardware and software stack into a turnkey, trusted system with embedded security.

Microsoft has recently published detailed guidelines for securing privileged access and mitigating credential theft. SkySecure makes it feasible for enterprises of any size to implement Microsoft's advanced recommendations, such as building a dedicated management domain, enforcing separation between authoritative and untrusted systems, and ensuring the applications run on trustworthy infrastructure.

SkySecure Safeguards Active Directory



Organizations have expertise managing their user policies in Active Directory, but often encounter challenges securing Active Directory hosts themselves and have an even harder time verifying the job is done. SkySecure automates and verifies that appropriate microsegmentation rules are in place on an appliance to secure communications only between trusted hosts. The platform is secure by default it is immune to malware and rootkits. In addition, SkySecure simplifies the adoption of advanced Microsoft security safeguards that have proven effective in the Fortune 500.

Who Has Access to Privileged Credentials?

- Assigned domain admins
- Anyone with access to VCenter Server
- Anyone with access to server hardware
- Anyone with access to the management network
- Anyone with access to the backups of the DC
- Anyone who can send an email that Is opened on the admin workstation

SKYPORT
SYSTEMS

TURNKEY SECURITY FOR ACTIVE DIRECTORY

Creating the secured buffer zones between authority systems and high-risk systems such as workstations and servers that might be directly exposed to attackers is challenging and the resulting arrangement nearly impossible to maintain as requirements and administrative staff change. SkySecure does the automatically, in a comprehensive-but-comprehensible way that cannot be bypassed and requires no software agents or redesign of the network.

- A pre-assembled system with always-on security that deploys in under an hour
- Predefined security templates for Active Directory components to speed deployment and reduce configuration errors
- Microsegmentation between participating servers in the same tier, such as only allowing web access to WindowsUpdate and Activation services
- A forensic trail of all administrative and operational activity is stored for the lifetime of the system

CLEAN SOURCE INFRASTRUCTURE

It can be challenging to verify that malware and rootkits are not present on a system, especially when attacks target the operating system, BIOS, and the hardware. A verified clean source is necessary to assure the application environment is not compromised. SkySecure management service continuously revalidates the integrity of infrastructure's hardware and software, The SkySecure platform automatically performs many of the verification and audit functions that normally must be pulled together from several different systems.

- Secure boot and with persistent malware and rootkit prevention
- Management and maintenance of cryptographic libraries, reporting functions, BIOS and firmware updates, and all common low-level infrastructure attack vectors
- Golden master and booted image verification
- Audit trails for all provisioning and operational activity to provide ongoing validation of best practices and complacence requirements

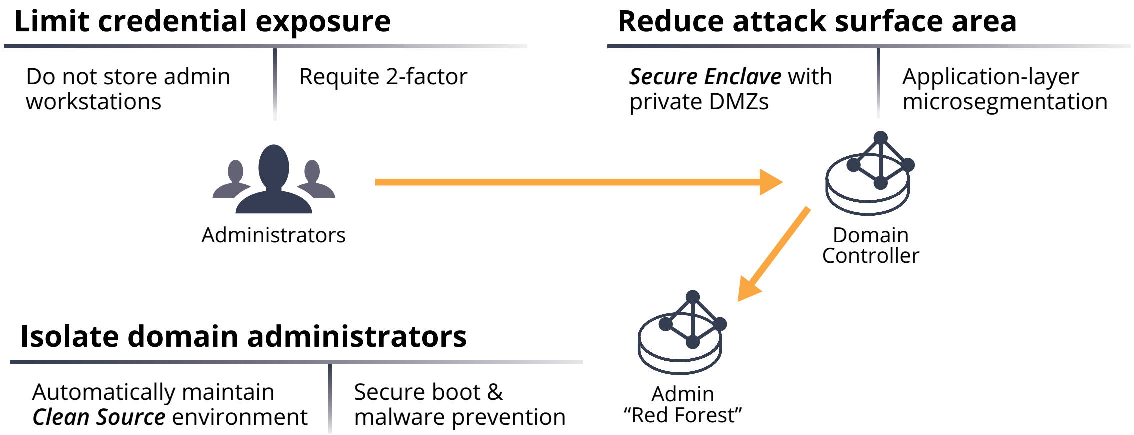
REDUCE CREDENTIAL EXPOSURE

In many Active Directory deployments, privileged credentials are widely shared across trusted and untrusted systems alike, increasing opportunities for theft. SkySecure reduces credential sprawl and detects fraudulent logins.

- Two-factor TLS-encrypted browser-based remote administrative console that does not expose domain administrative Kerberos tickets
- Hardware-based secure credential store based on TPM
- Kerberos ticket inspection to detect and deny fraudulent administrator logins, golden ticket attacks, and unacceptable use of older NTLM protocol versions

Where to Start?

You can incrementally deploy Active Directory components, such as production domain controllers and certificate authorities, on SkySecure using predefined security templates. Alternatively, you can develop an approach to implement Microsoft's security guidelines, working with Skyport and our professional service partners. The first step is to contact us at www.skyportsystems.com and we will identify the best path forward to a secure Active Directory environment for your organization.


Limit credential exposure
Do not store admin workstations
Requite 2-factor
Reduce attack surface area
Secure Enclave with private DMZs
Application-layer microsegmentation
Administrators
Domain Controller
Isolate domain administrators
Automatically maintain *Clean Source* environment
Secure boot & malware prevention
Admin "Red Forest"

Spotlight: Red Forest and Ascent Solutions

SECURE ACTIVE DIRECTORY ADMINISTRATIVE SYSTEMS WITH A RED FOREST

The cornerstone of a secure Active Directory environment is a dedicated administrative management domain (also known as a Red Forest*). A Red Forest architecture provides the strongest protection by isolating the administrative systems and credentials from the production environment to prevent attacks from untrusted systems.

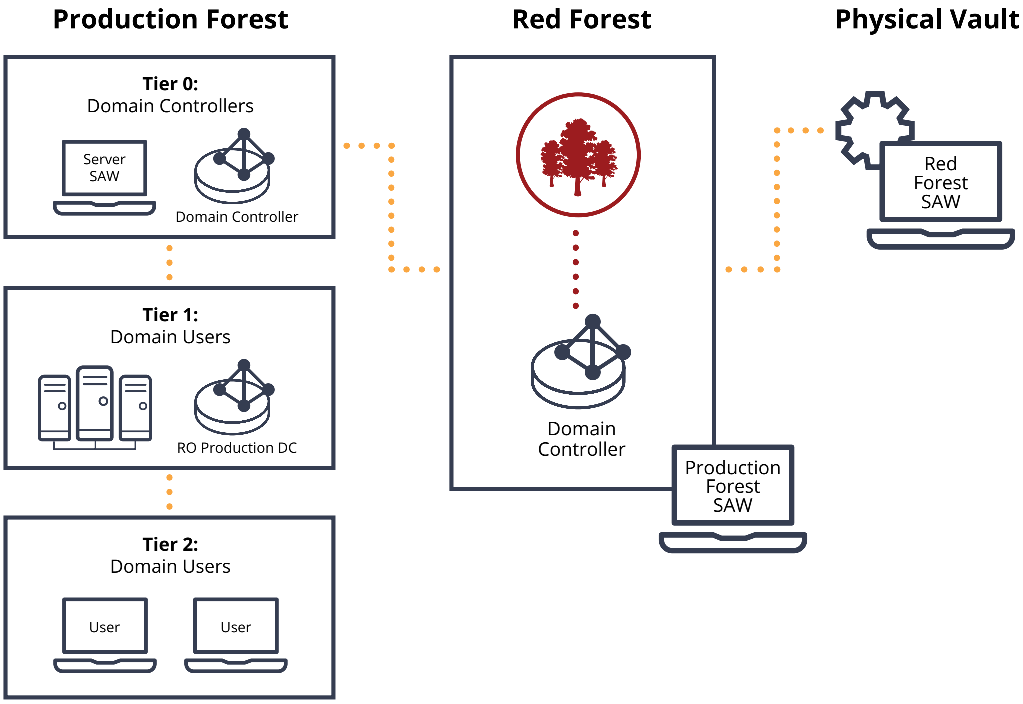
Until now, implementing a Red Forest was only feasible for large enterprises due to the complexity and expense of the process. Now Ascent Solutions and Skyport Systems have developed a solution that enables organizations of any size to adopt and significantly reduce the risks to their Active Directory environment.

- Limit Active Directory administrative exposure
- Restrict logons and credential exposure
- Provide assurance of the production forest without the complexity and cost of a rebuild
- Allow only authorized people and workstations to conduct administrative activities

Ascent Solutions: Deploy Quickly and with Confidence

Skyport has partnered with Ascent Solutions, a professional services provider with extensive experience with securing Microsoft Active Directory for customers big and small. Together we deliver solutions for Active Directory forests, cloud access authentication services in the DMZ, and a turnkey branch office solution. The packages are inclusive of the hardware, software, and services expertise needed to easily, effectively, and rapidly secure your Active Directory implementation in any environment.

To learn more about how Skyport can secure your Active Directory environment, visit us at www.skyportsystems.com.



* Microsoft guidance on ESAE: https://technet.microsoft.com/en-US/library/mt631193.aspx#ESAE_BM

SKYPORT
SYSTEMS

©2016 Skyport Systems, Inc