Top 10 Actions to Protect Active Directory from Attacks

Most Fortune 1000 companies use Active Directory or Azure AD—and AD is involved in ~90% of cyberattacks. How can you protect your organization?

semperis

1

Follow identity best practices

Privileged access is a prime target. Protect it! Remove inactive users and computers and regularly update service account passwords.

semperis

2

Secure inter-forest trusts

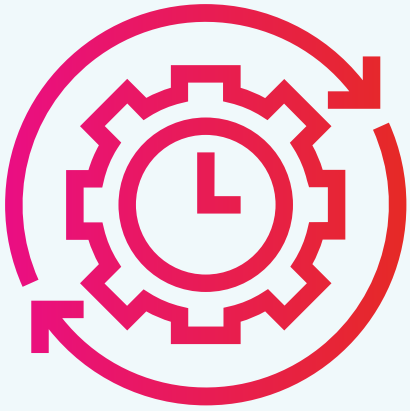
Who do you trust? Use SID filtering or selective authentication across forests, especially after a merger or acquisition.

semperis

3

Plan for secure, speedy backup and recovery

Backup every domain, especially the root + at least two DCs per domain, using supported methods. Keep and test offline backups to avoid re-infection.



semperis

4

Enhance Kerberos security

Eliminate unconstrained delegation. Remove SPNs assigned to admin accounts and annually reset the KRBTGT account in each domain.

semperis

5

Deter lateral movement

Make it difficult to jump from PC to PC. Implement the Local Administrators Password System and restrict Local Administrators group membership.

semperis

6

Minimize privileged user and group membership

Use “least privilege” principles to limit privileged users and groups both in AD and on PCs, remove admin permissions granted to service accounts, and monitor for permission changes on AdminSDHolder.

semperis

7

Lock down dependencies

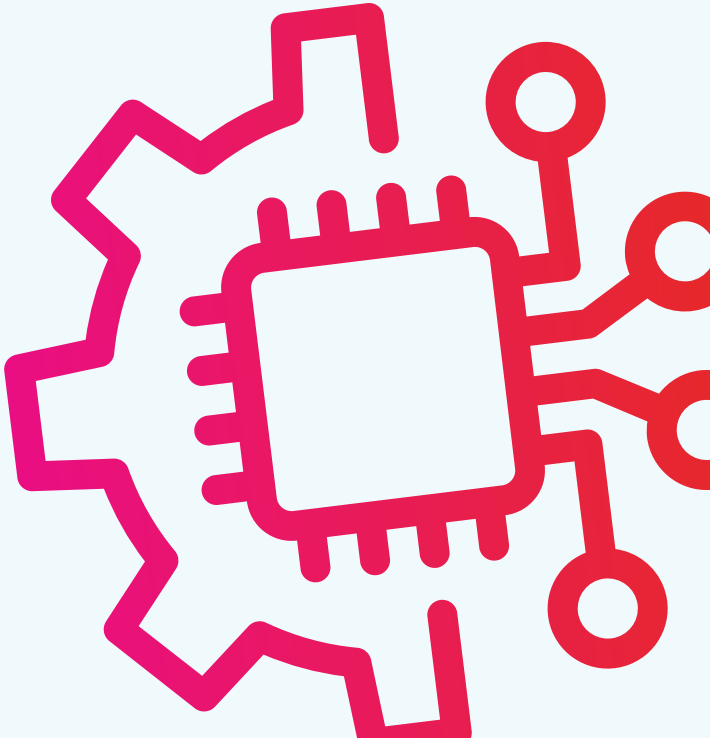
Limit hypervisor admin privileges and restrict DIT access. Evaluate management tools and services with elevated access, including PAM tool permissions.

semperis

8

Harden domain controllers

Remove unnecessary server roles and agents. Disable the Print Spooler service on all DCs and consider using Server Core.

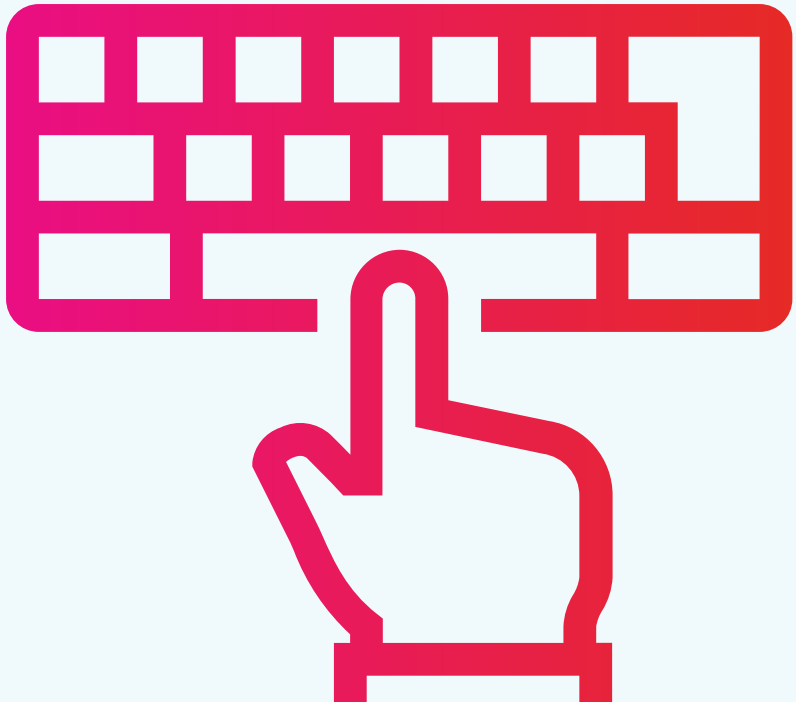


semperis

Restrict privileged access

9

Deploy a tiered administrative model with separate named admin accounts and privileged access workstations, just-in-time access, and break-glass accounts.



semperis

10

Monitor for unusual activity

Implement a SIEM with UEBA capabilities. Monitor privileged groups for membership changes and watch for ACL changes to sensitive objects.

semperis