PAW 2026 : Déployer des Privileged Access Workstations en Entreprise

> Déployer des PAW en 2026 : architecture, image durcissée, flux réseau, intégration Tiering AD et Entra ID. Protégez les accès admin avec des postes dédiés.

En 2026, les comptes administrateurs restent la cible prioritaire des attaquants qui cherchent à compromettre un système d'information. Pourtant, une réalité embarrassante demeure dans la plupart des organisations françaises : les administrateurs système gèrent leurs tâches privilégiées depuis le même poste que celui qu'ils utilisent pour naviguer sur le web, consulter leurs emails ou ouvrir des pièces jointes. Cette pratique transforme chaque poste d'administrateur en vecteur d'attaque potentiel, capable de compromettre l'ensemble du Tier 0 en quelques minutes. Les Privileged Access Workstations — PAW en abrégé — constituent la réponse architecturale à ce risque. Issus du programme Microsoft Privileged Access Management (PAM), les PAW sont des postes de travail physiques ou virtuels dédiés exclusivement aux opérations d'administration sensibles. Isolés du réseau bureautique, dépourvus de navigateur grand public, d'email et de logiciels non maîtrisés, ils reposent sur le principe *Clean Source* : toute décision ou action d'administration doit provenir d'un système aussi digne de confiance que la ressource cible. Dans un contexte où les groupes APT ciblent activement les infrastructures françaises (rapports ANSSI 2025-2026), où NIS 2 impose une gouvernance des accès privilégiés, et où les ransomwares s'attaquent systématiquement aux comptes à hauts privilèges avant de chiffrer, déployer des PAW n'est plus optionnel pour les RSSI et DSI qui souhaitent réduire leur surface d'attaque de manière structurelle. Ce guide détaille l'architecture, la construction de l'image, l'intégration avec le Tiering Model Active Directory et Entra ID, ainsi que les cas terrain en entreprise française.

📋 EN BREF

IAM ET GESTION DES IDENTITÉS

PAW 2026 : Privileged Access Workstations — Guide Complet

Le principe Clean Source : fondation architecturale des PAW

Le principe *Clean Source* (source propre) est la règle absolue sur laquelle repose toute l'architecture PAW. Il stipule que **toute dépendance de sécurité doit être aussi digne de confiance que l'objet sécurisé lui-même**. En d'autres termes : si vous administrez un contrôleur de domaine Active Directory (actif le plus critique d'un SI), le poste depuis lequel vous vous connectez doit être au moins aussi bien protégé que ce contrôleur de domaine.

> ⚡ **Retour terrain**
>
> Dans les projets IAM, le cas le plus fréquent que je rencontre est celui des comptes de service sans propriétaire identifié — créés pour un projet terminé ou un prestataire parti, et jamais supprimés. Pour une banque régionale, l'inventaire a identifié 134 comptes de service sans propriétaire actif, dont 23 avaient des droits administrateurs locaux sur des serveurs de production. La désactivation progressive de ces comptes sur 6 semaines n'a déclenché aucune anomalie applicative.

Prenons des exemples concrets qui illustrent les violations du principe Clean Source :

Violation classique : Un administrateur se connecte au DC depuis son poste bureautique Windows 11 standard. Ce poste a accès à Internet, reçoit des emails, exécute Teams. Si ce poste est compromis (phishing, drive-by download), l'attaquant dispose immédiatement de credentials Tier 0 en mémoire via un dump LSASS. Le DC est compromis sans qu'aucune protection sur le DC lui-même n'ait été contournée.

Violation subtile : Un admin utilise un jump server (bastion) accessible depuis n'importe quel poste du réseau. Si n'importe quel poste peut atteindre le bastion, la chaîne de confiance est brisée : le bastion est Tier 0, mais les postes sources sont Tier 2.

Application correcte : L'admin dispose d'un PAW physique dédié, isolé réseau, depuis lequel il accède au DC. Ce PAW est géré exclusivement depuis des outils d'administration dédiés (Intune/SCCM isolé). La chaîne de confiance est homogène de bout en bout.

Ce principe s'applique également aux outils de gestion des PAW eux-mêmes : le serveur WSUS qui pousse les mises à jour des PAW, le serveur SCCM qui gère les images, le serveur de journalisation qui collecte les logs — tous doivent être dans le périmètre Tier 0 ou au moins cloisonnés avec des droits d'accès stricts depuis les PAW uniquement.

Architecture PAW : trois profils selon le contexte

La Microsoft Privileged Access Architecture définit trois profils de PAW adaptés à différents contextes organisationnels. Le choix du profil dépend du niveau de risque de l'environnement, du budget et des contraintes opérationnelles.

Profil 1 — Hardware PAW (matériel physique dédié)

Il s'agit du profil de référence pour les accès Tier 0. Un ordinateur portable ou fixe dédié exclusivement à l'administration, physiquement distinct du poste bureautique de l'administrateur. Aucune donnée personnelle, aucun accès Internet direct, aucune connexion à des partages réseau bureautiques.

Caractéristiques : Windows 11 Enterprise ou Server 2025 Core, TPM 2.0 obligatoire, BitLocker activé (TPM+PIN), Secure Boot, pas de ports USB actifs hors clavier/souris (BIOS lockdown), FIDO2 comme seule méthode MFA autorisée.

Usage : Administration des contrôleurs de domaine, gestion des GPO critiques, accès à Azure AD/Entra avec droits Global Admin ou Privileged Role Administrator, gestion des certificats PKI.

Profil 2 — VM PAW sur hyperviseur durci

Une machine virtuelle dédiée à l'administration, hébergée sur un hyperviseur lui-même durci et isolé, distinct des hyperviseurs de production bureautique. Ce profil convient aux équipes qui souhaitent réduire les coûts matériels tout en maintenant un niveau d'isolation acceptable pour le Tier 1.

Caractéristiques : Hyperviseur dédié (Hyper-V Server 2025 ou ESXi hardened), réseau VM PAW séparé via VLAN dédié, pas de connexion aux réseaux bureautiques dans la configuration réseau de la VM, snapshots interdits en production (risque de roll-back de credentials), intégration Credential Guard activé dans la VM.

Usage : Administration de serveurs d'infrastructure (DNS, PKI, SCCM), gestion des partages fichiers critiques, administration des hyperviseurs de production depuis une VM PAW sur un hyperviseur de management dédié.

Profil 3 — PAW Cloud (Azure Virtual Desktop / Windows 365)

Pour les environnements hybrides ou full-cloud, une session de bureau virtuel Azure dédiée à l'administration, accessible uniquement depuis des postes physiques conformes via Conditional Access Policy Entra ID. Ce profil s'applique particulièrement aux missions de consulting ou aux organisations ayant peu d'infrastructure on-premises.

Caractéristiques : Azure Virtual Desktop (AVD) ou Windows 365 Enterprise, Entra Conditional Access avec filtre sur le nom du device (compliant + PAW tag), MFA FIDO2 obligatoire, session non persistante (profils FSLogix en lecture seule), Private Endpoints pour éviter le transit Internet.

Usage : Administration Entra ID, Azure subscriptions, gestion des politiques Intune, accès aux portails Azure avec droits élevés.

Comparaison des trois profils PAW

Critère	Hardware PAW	VM PAW	PAW Cloud
Isolation physique	Maximale	Partielle (hyperviseur)	Logique (AVD)
Coût matériel	Élevé (2 postes/admin)	Modéré	Faible (licence AVD)
Niveau Tiering recommandé	Tier 0 exclusif	Tier 0 / Tier 1	Tier 1 / Cloud
Compatibilité NIS 2 ANSSI	Oui (recommandé)	Oui (si hyperviseur dédié)	Conditionnel
Gestion MDM/Intune	Enrôlement dédié isolé	Tenant MDM séparé	Natif Azure
Risque de contamination croisée	Très faible	Faible (si VLAN correct)	Dépend du Conditional Access

Ce que protège un PAW : le périmètre d'isolation

Un PAW n'est pas simplement un poste avec un antivirus supplémentaire. C'est une architecture d'isolation multicouche qui élimine les vecteurs d'attaque les plus exploités contre les comptes administrateurs.

Isolation réseau stricte

Le PAW est connecté à un VLAN dédié (ex. VLAN 10 — PAW Management). Les règles de pare-feu autorisent uniquement :

PAW → Contrôleurs de domaine (TCP 389/636/3268, TCP 445, TCP 135 RPC)

PAW → Serveurs gérés sur les ports d'administration (WMI, PowerShell Remoting TCP 5985/5986, RDP TCP 3389 restreint aux PAW sources)

PAW → Serveurs de mise à jour internes (WSUS dédié)

PAW → SIEM/syslog (UDP 514 / TCP 6514)

Les flux suivants sont **bloqués en sortie** depuis le VLAN PAW :

PAW → Internet (HTTP/HTTPS) — navigation web interdite

PAW → Postes utilisateurs bureautiques (VLAN bureautique)

PAW → Serveurs de messagerie (SMTP, IMAP, Exchange)

PAW → Partages réseau bureautiques (DFS, serveurs de fichiers non-Tier)

Restrictions applicatives

Aucun navigateur grand public (Chrome, Firefox, Edge en mode standard) n'est installé sur un PAW. Si l'accès à un portail web d'administration est requis (Azure Portal, console ESXi), un profil Edge Application Guard peut être envisagé avec une liste blanche d'URL stricte via AppLocker.

Le client de messagerie (Outlook, Thunderbird) est absent. Les communications doivent transiter par le poste bureautique standard, physiquement distinct. Cette contrainte est souvent la principale résistance des administrateurs lors de la mise en place des PAW : elle est non négociable pour garantir l'intégrité du poste.

Technologies de protection activées

Credential Guard : Isolement LSA via VBS (Virtualization-Based Security), protection des credentials NTLM/Kerberos contre le dump mémoire (Mimikatz, ProcDump). Voir notre guide Credential Guard Windows Server 2025.

AppLocker / WDAC : Politique d'autorisation par liste blanche, seuls les exécutables signés par des éditeurs approuvés peuvent s'exécuter. Bloque les outils d'attaque non signés, les scripts téléchargés, les macros malveillantes.

BitLocker TPM+PIN : Chiffrement intégral du disque, le PIN est obligatoire au démarrage (pas de boot automatique), protection contre l'extraction physique du disque.

Windows Defender Application Control (WDAC) : En complément ou remplacement d'AppLocker sur Windows 11 22H2+, WDAC offre une politique noyau (kernel-level) plus robuste contre les contournements utilisateur.

Secure Boot + UEFI lockdown : Empêche le boot depuis un support externe, protège contre les bootkits.

Construction de l'image PAW : étapes et outils

La construction d'une image PAW robuste suit un processus rigoureux, inspiré du CIS Benchmark Windows 11 (niveau 2) et des recommandations ANSSI pour les postes d'administration.

Base OS

Utilisez Windows 11 Enterprise (23H2 minimum en 2026) ou Windows Server 2025 en mode Desktop Experience si des outils serveur sont requis. Partez d'une image ISO officielle Microsoft VLSC, vérifiez le hash SHA-256 avant déploiement. N'utilisez jamais une image provenant d'une source tierce.

La liste des logiciels présents sur un PAW doit être aussi courte que possible :

Inclus : RSAT (Remote Server Administration Tools), PowerShell 7+, Windows Admin Center, outils d'administration spécifiques signés (console MMC, Active Directory Users & Computers, etc.)

Exclus : Office suite complète (Word, Excel — si nécessaire, utiliser une version très restreinte sans macros), navigateur grand public, client Teams/Slack, client email, Adobe Acrobat Reader (substituer par le lecteur Edge PDF uniquement pour documents internes)

Durcissement CIS Benchmark niveau 2

Appliquez le CIS Benchmark Windows 11 niveau 2 via GPO ou script PowerShell DSC. Les paramètres clés pour les PAW :

Désactivation des protocoles réseaux legacy (LLMNR, NetBIOS, WPAD)

SMB signing obligatoire en client et serveur

NTLMv1 désactivé, NTLMv2 session security forcée

Kerberos AES-256 uniquement (RC4 désactivé)

LSA protection activée (RunAsPPL=1 dans la registry)

Audit renforcé : logon/logoff, account management, process creation avec command line logging

Configuration AppLocker

La politique AppLocker d'un PAW suit une approche liste blanche stricte. Créez des règles basées sur l'éditeur (Publisher rules) plutôt que sur le hash (trop rigide pour les mises à jour) :

```
 # Vérifier l'état de Credential Guard sur le PAW
Get-CimInstance -Namespace "root\Microsoft\Windows\DeviceGuard" `
    -ClassName "Win32_DeviceGuard" |
    Select SecurityServicesRunning, VirtualizationBasedSecurityStatus
# SecurityServicesRunning : 1 = Credential Guard actif
# VirtualizationBasedSecurityStatus : 2 = VBS activé et en cours d'exécution

# Vérifier la politique AppLocker effective
Get-AppLockerPolicy -Effective | Format-List

# Exporter la politique AppLocker pour audit
Get-AppLockerPolicy -Effective -Xml | Out-File C:\PAW-AppLocker-Policy.xml

# Tester si un exécutable serait bloqué par AppLocker
Test-AppLockerPolicy -Path "C:\Users\admin\Downloads\tool.exe" `
    -User "CORP\tier0-admin01"
```

Structure OU et GPO dédiées

Les PAW doivent être dans une OU dédiée, protégée, avec une GPO de durcissement appliquée uniquement à ces machines. Cette OU doit être dans l'arborescence Tier 0 de votre Tiering Model Active Directory.

```
 # Créer l'OU dédiée PAW dans la structure Tier 0
New-ADOrganizationalUnit -Name "PAW" `
    -Path "OU=Tier0,DC=corp,DC=fr" `
    -ProtectedFromAccidentalDeletion $true `
    -Description "Privileged Access Workstations - Tier 0 exclusif"

# Vérifier que l'OU est bien protégée contre la suppression accidentelle
Get-ADOrganizationalUnit -Identity "OU=PAW,OU=Tier0,DC=corp,DC=fr" |
    Select ProtectedFromAccidentalDeletion, DistinguishedName
```

Flux réseau PAW : règles pare-feu détaillées

La politique de flux réseau des PAW est le point le plus critique à valider lors d'un audit. Voici les règles pare-feu à implémenter au niveau du firewall réseau (PfSense, Fortinet, Cisco ASA) ET au niveau du Windows Firewall local sur chaque PAW (via GPO).

Flux autorisés depuis le VLAN PAW (10.0.10.0/24 dans cet exemple)

Source	Destination	Port / Protocole	Usage
VLAN PAW	DC Tier 0	TCP 389, 636, 3268, 3269	LDAP / LDAPS / GC
VLAN PAW	DC Tier 0	TCP 445, UDP 88	SMB, Kerberos
VLAN PAW	DC Tier 0	TCP 135, 49152-65535	RPC dynamique
VLAN PAW	Serveurs Tier 1	TCP 5985, 5986	PowerShell Remoting (WinRM)
VLAN PAW	Serveurs Tier 1	TCP 3389 (restreint PAW)	RDP administration uniquement
VLAN PAW	WSUS dédié PAW	TCP 8530 / 8531	Mises à jour isolées
VLAN PAW	SIEM / Syslog	TCP 6514 (TLS)	Journalisation centralisée

Flux bloqués (règles DENY explicites)

Source	Destination	Justification
VLAN PAW	Internet (0.0.0.0/0)	Pas de navigation web, pas de téléchargement
VLAN PAW	VLAN bureautique	Isolation totale des postes utilisateurs
VLAN bureautique	VLAN PAW	Les postes bureautiques ne doivent pas atteindre les PAW
VLAN PAW	Serveurs de messagerie	Pas d'email sur le PAW
VLAN PAW	Serveurs fichiers bureautiques	Pas d'accès aux partages utilisateurs

Intégration avec le Tiering Model Active Directory

Les PAW s'intègrent directement dans le modèle de Tiering Active Directory et en constituent le bras armé côté postes d'administration. Sans PAW, le Tiering Model reste théorique : les GPO de restriction de logon peuvent être contournées si les postes d'administration ne sont pas eux-mêmes cloisonnés.

Tier 0 — Contrôle de l'identité

Le PAW Tier 0 (Hardware PAW physique) est réservé à l'administration des actifs les plus critiques : contrôleurs de domaine Active Directory, autorité de certification PKI racine, serveurs ADFS, infrastructure Entra ID Connect (anciennement AAD Connect). Les comptes utilisés depuis un PAW Tier 0 ne doivent jamais se connecter à un poste Tier 1 ou Tier 2.

La GPO de restriction de logon appliquée aux DC doit refléter cette contrainte : seuls les membres du groupe `Tier0-Admins` peuvent se connecter localement ou via les services réseau sur les DC, et uniquement depuis des machines membres de l'OU PAW Tier 0.

```
 # GPO : Restriction de logon sur les DC - User Rights Assignment
# "Permettre l'ouverture de session locale" = Tier0-Admins uniquement
# "Permettre l'ouverture de session via les Services Bureau à Distance" = Vide (RDP bloqué)
# "Refuser l'ouverture de session locale" = Tier1-Admins, Tier2-Admins, Domain Users

# Vérifier la politique de logon effective sur un DC
Invoke-Command -ComputerName DC01.corp.fr -ScriptBlock {
    secedit /export /cfg C:\temp\secpolicy.cfg /quiet
    Get-Content C:\temp\secpolicy.cfg | Select-String -Pattern "SeInteractiveLogonRight|SeDenyInt
}
```

Tier 1 — Serveurs d'entreprise

Les PAW Tier 1 (VM PAW sur hyperviseur dédié) administrent les serveurs d'application, les serveurs de fichiers, les hyperviseurs de production. Les administrateurs Tier 1 ne peuvent pas utiliser leurs outils Tier 1 pour accéder aux DC (restriction réseau + GPO logon).

Tier 2 — Postes utilisateurs

L'administration des postes utilisateurs depuis un PAW Tier 2 est rarement mise en place en pratique (coût/bénéfice), mais recommandée dans les environnements à haute sensibilité. En pratique, les organisations démarrent par le Tier 0 et Tier 1.

Restriction de logon bidirectionnelle

Le principe de restriction de logon est bidirectionnel dans le Tiering Model :

Les comptes Tier 0 ne peuvent pas se loguer sur des machines Tier 1 ou Tier 2 (GPO "Refuser l'ouverture de session locale" sur OU Tier 1/Tier 2)

Les comptes Tier 1 ne peuvent pas se loguer sur les DC Tier 0 (GPO sur OU DC)

Les PAW Tier 0 ne peuvent pas être utilisés par des comptes Tier 1 ou Tier 2 (GPO sur OU PAW Tier 0)

PAW et Entra ID / MFA : l'intégration cloud

Les environnements hybrides (Active Directory on-premises + Entra ID) nécessitent une stratégie PAW étendue au plan cloud. Les accès aux portails Azure, aux consoles Microsoft 365 Administration, aux APIs Graph depuis des comptes Global Admin doivent impérativement provenir de PAW, que l'accès soit on-premises ou cloud.

Jointure du PAW à Entra ID

Selon l'architecture :

Hybrid Join : Le PAW est joint à Active Directory ET à Entra ID. Permet d'utiliser les Conditional Access Policies Entra basées sur la conformité Intune ET les GPO Active Directory. Recommandé pour les environnements hybrides.

Entra ID Join only : Pour les PAW Cloud (AVD), jointure directe à Entra ID, gestion via Intune uniquement, sans dépendance AD on-premises.

Conditional Access Policy dédiée aux PAW

Une politique Conditional Access spécifique aux PAW doit être créée dans Entra ID pour que les comptes admin hautement privilégiés (Global Admin, Privileged Role Administrator, Security Administrator) ne puissent s'authentifier aux services Microsoft qu'depuis des appareils identifiés comme PAW.

Configuration de la politique :

Utilisateurs ciblés : Groupe `sg-paw-tier0-admins` contenant uniquement les comptes admin Tier 0

Applications ciblées : Azure Management (797f4846-ba00-4fd7-ba43-dac1f8f63013), Microsoft Graph, portails d'administration

Condition appareil : Filtre sur attributs device — `device.extensionAttribute1 -eq "PAW"` (tag appliqué lors de l'enrôlement)

Contrôle d'accès : MFA obligatoire (FIDO2 Security Key uniquement — pas de SMS, pas d'authenticator app)

Résultat : Un compte Global Admin ne peut s'authentifier à Azure Portal que depuis un appareil tagué PAW avec une clé FIDO2 physique

FIDO2 comme seule méthode MFA autorisée sur les PAW

L'utilisation d'une clé de sécurité physique FIDO2 (YubiKey 5 Series, Feitian, etc.) est la méthode MFA recommandée pour les comptes admin accédant depuis les PAW. Contrairement à l'authenticator mobile :

La clé FIDO2 ne peut pas être phishée (protocole lié à l'origine)

Elle ne dépend pas d'un smartphone (qui peut être compromis séparément)

Elle peut être mise en escrow et stockée dans un coffre-fort pour les accès d'urgence (break-glass)

Voir notre article sur le Just-In-Time Access pour l'intégration avec Entra PIM (Privileged Identity Management) depuis un PAW.

Gestion des PAW : MDM, mises à jour et gouvernance

La gestion des PAW elle-même doit respecter le principe Clean Source : les outils de gestion des PAW doivent être aussi protégés que les PAW qu'ils gèrent.

Enrôlement MDM isolé

Si vous utilisez Microsoft Intune pour gérer les PAW, créez un **tenant Intune dédié** (ou a minima un groupe d'enrôlement séparé) pour les PAW, distinct du tenant Intune bureautique. Les politiques Intune PAW sont :

Profile de configuration Credential Guard activé (VBS)

Profile BitLocker (TPM+PIN, récupération via tenant admin uniquement)

Profile Windows Defender Application Control (politique WDAC)

Script PowerShell de vérification de conformité post-déploiement

Restriction des applications autorisées (liste blanche via Intune)

Mises à jour isolées via WSUS dédié

Les PAW ne peuvent pas accéder à Windows Update directement (flux Internet bloqué). Les mises à jour transitent par un serveur WSUS (ou Intune via Private Endpoints) dédié, situé dans le VLAN Management. Ce serveur WSUS doit lui-même être dans le périmètre Tier 0 ou Tier 1 sécurisé.

Processus de mise à jour recommandé :

Téléchargement et validation des mises à jour sur le WSUS PAW (isolé)

Test sur un PAW de qualification avant déploiement en production

Déploiement en fenêtre de maintenance planifiée

Vérification post-déploiement : Credential Guard toujours actif, AppLocker policy non altérée

Gestion des mots de passe administrateurs locaux

Chaque PAW dispose d'un compte administrateur local dont le mot de passe doit être géré par Microsoft LAPS (Local Administrator Password Solution). LAPS génère un mot de passe unique par machine, stocké dans Active Directory (ou Entra ID pour Windows LAPS 2023+), accessible uniquement aux membres du groupe PAW-LAPS-Readers. Cela empêche les mouvements latéraux via un mot de passe local partagé entre tous les PAW.

Surveillance et audit des PAW

La surveillance des PAW combine des alertes sur les comportements anormaux (connexion admin depuis un non-PAW) et une journalisation exhaustive des actions d'administration.

Détection des connexions admin depuis des non-PAW

L'événement Windows **Event ID 4624** (Logon Success) avec Logon Type 3 (réseau) ou Type 10 (RemoteInteractive/RDP) vers un DC ou serveur Tier 0 provenant d'une IP hors VLAN PAW est une alerte critique. Elle indique qu'un compte privilégié s'authentifie depuis un poste non-PAW, violation directe du principe Clean Source.

```
 # Identifier les connexions non-PAW vers les DC (Event 4624 Type 10 et 3)
# À exécuter sur les DC ou depuis un SIEM collectant les logs Security
Get-WinEvent -FilterHashtable @{
    LogName = 'Security'
    Id      = 4624
} | Where-Object {
    # Type 10 = RemoteInteractive (RDP), Type 3 = Network
    ($_.Message -match "Logon Type:\s+10" -or $_.Message -match "Logon Type:\s+3") -and
    # Source IP hors plage VLAN PAW (adapter selon votre plan d'adressage)
    $_.Message -notmatch "10\.0\.10\." -and
    # Exclure les comptes machines et SYSTEM
    $_.Properties[5].Value -notmatch "\$$" -and
    $_.Properties[5].Value -ne "SYSTEM"
} | Select-Object TimeCreated,
    @{N='User';       E={$_.Properties[5].Value}},
    @{N='Domain';     E={$_.Properties[6].Value}},
    @{N='SourceIP';   E={$_.Properties[18].Value}},
    @{N='LogonType';  E={$_.Properties[8].Value}} |
    Format-Table -AutoSize
```

Intégration SIEM

Les événements suivants doivent être collectés depuis les PAW et envoyés au SIEM en temps réel :

Event 4624/4634 : Logon/Logoff — qui se connecte sur le PAW

Event 4688 : Process creation avec command line — quels processus sont lancés

Event 4698/4702 : Scheduled task created/modified — persistance potentielle

Event 4719 : System audit policy changed — tentative de contournement de l'audit

Event 8004 (AppLocker) : Exécutable bloqué par AppLocker — tentative d'exécution non autorisée

Dans votre SIEM (Splunk, Microsoft Sentinel, Elastic SIEM), créez des règles de corrélation :

Alerte si un compte membre de `Tier0-Admins` génère un Event 4624 Type 2 (interactif) sur un poste hors OU PAW

Alerte si un PAW (par son hostname) génère du trafic vers Internet (détection via logs firewall)

Alerte si AppLocker bloque plus de 3 exécutables en 10 minutes sur un PAW (tentative d'exploitation)

Cas terrain France : PME, ETI et grandes entreprises

Le déploiement des PAW se décline différemment selon la taille de l'organisation. Voici des retours d'expérience de missions de conseil à Paris et Lyon.

PME / ETI avec 5 à 10 administrateurs

Pour une PME ou ETI française de 200 à 1000 collaborateurs, le déploiement PAW complet (Hardware PAW Tier 0, VM PAW Tier 1) peut sembler disproportionné. En pratique, le bon compromis consiste à :

Déployer des Hardware PAW uniquement pour les 2-3 admins AD/Domaine (Tier 0) — coût : 2 000 à 3 000 € HT par poste

Utiliser des VM PAW sur un mini-hyperviseur dédié (NUC Intel Pro ou equivalent) pour les admins serveurs Tier 1

Commencer par sécuriser les flux réseau (VLAN PAW) avant d'investir dans l'image durcissée complète

Référence normative applicable : la PSSI ANSSI recommande explicitement l'isolement des postes d'administration dans son guide "Recommandations relatives à l'administration sécurisée des SI" (ANSSI-PA-022). Dans le cadre NIS 2, les entités importantes doivent pouvoir justifier de contrôles équivalents.

Grandes entreprises CAC40

Dans les groupes CAC40 et ETI sensibles (secteur bancaire, énergie, défense), les PAW s'intègrent dans une architecture de sécurité complète :

WALLIX Bastion : Enregistrement de sessions, audit des commandes, gestion des accès privilégiés (PAM). Le WALLIX Bastion est accessible depuis les PAW uniquement, pas depuis les postes bureautiques. Les cibles (DC, serveurs) sont accessibles via le bastion, les PAW se connectent au bastion qui proxifie les sessions. WALLIX et PAW sont complémentaires : le PAW protège le point d'entrée, le bastion enregistre et contrôle les sessions.

CyberArk PAM : Solution concurrente à WALLIX, très répandue dans les grands comptes. CyberArk EPV (Enterprise Password Vault) stocke les credentials des comptes de service et admin, les PAW récupèrent les mots de passe via l'API CyberArk avec authentification MFA. Couplage PAW + CyberArk = zéro connaissance du mot de passe par l'administrateur humain.

Thales / Atos : Dans certains contextes OTAN ou défense nationale, les PAW sont des postes homologués CC EAL4+ avec des distributions Windows durcies maison.

Intégration WALLIX Bastion + PAW : architecture recommandée

L'architecture PAW + WALLIX est de loin la plus répandue en France pour les ETI et grandes entreprises :

L'administrateur s'assied devant son Hardware PAW (ou active sa VM PAW)

Il s'authentifie sur le PAW avec son PIN + FIDO2

Il ouvre le client WALLIX (ou le portail HTTPS WALLIX accessible uniquement depuis le VLAN PAW)

Il s'authentifie à WALLIX avec son compte AD Tier 0 + MFA

WALLIX lui présente les cibles autorisées (DC, serveurs Tier 1) selon ses droits

La session RDP ou SSH est proxifiée et enregistrée par WALLIX

Les credentials des comptes de service sont injectés par WALLIX sans que l'admin les connaisse

Ce modèle permet un audit complet (vidéo de session, logs de commandes), une rotation automatique des mots de passe, et une révocation immédiate d'accès en cas d'incident sans changer les mots de passe manuellement.

Checklist déploiement PAW

À RETENIR

Checklist PAW — Déploiement opérationnel

Phase 1 — Prérequis et conception

[ ] Inventaire des comptes administrateurs par niveau Tier (0/1/2)

[ ] Définition du plan d'adressage VLAN PAW séparé

[ ] Sélection du profil PAW (Hardware / VM / Cloud) par Tier

[ ] Décision matérielle validée (TPM 2.0, Secure Boot, UEFI lockdown)

[ ] Validation du budget et planning de déploiement

Phase 2 — Construction de l'image

[ ] Image Windows 11 Enterprise 23H2+ depuis source officielle VLSC

[ ] Application CIS Benchmark Windows 11 niveau 2

[ ] Credential Guard activé et vérifié (SecurityServicesRunning=1)

[ ] BitLocker TPM+PIN configuré et clé de récupération en escrow

[ ] AppLocker/WDAC : politique liste blanche déployée et testée

[ ] Suppression logiciels non nécessaires (navigateur grand public, email, Office non sécurisé)

[ ] LSA RunAsPPL activé (registry HKLM\SYSTEM\CurrentControlSet\Control\Lsa\RunAsPPL=1)

[ ] RSAT et outils d'administration installés et signés

Phase 3 — Infrastructure réseau

[ ] VLAN PAW créé et isolé sur les équipements réseau

[ ] Règles firewall : PAW → DC et serveurs gérés uniquement

[ ] Règles firewall : bloquer PAW → Internet et PAW → VLAN bureautique

[ ] WSUS dédié PAW configuré et accessible uniquement depuis VLAN PAW

Phase 4 — Intégration AD et Entra ID

[ ] OU PAW créée dans structure Tier 0, protégée contre suppression accidentelle

[ ] GPO de durcissement PAW appliquée (logon restriction, audit renforcé)

[ ] Groupes de sécurité Tier0-Admins, PAW-LAPS-Readers créés

[ ] LAPS déployé sur tous les PAW (voir guide LAPS)

[ ] Entra ID : PAW enrôlés dans tenant dédié ou groupe Intune dédié

[ ] Conditional Access Policy : comptes Tier 0 → PAW uniquement + FIDO2

Phase 5 — Surveillance et audit

[ ] Collecte logs Security (4624, 4688, 4719, 8004) vers SIEM

[ ] Alerte SIEM : connexion compte Tier 0 depuis non-PAW

[ ] Alerte firewall : trafic sortant depuis VLAN PAW vers Internet

[ ] Revue mensuelle des accès aux PAW et des exceptions AppLocker

[ ] Test semestriel de l'isolation réseau (scan depuis VLAN bureautique vers VLAN PAW)

PAW en 2026 : tendances et évolutions

L'architecture PAW évolue pour répondre aux nouvelles contraintes des environnements hybrides et cloud-first. En 2026, plusieurs tendances marquent le déploiement des PAW en entreprise française :

PAW-as-a-Service via Windows 365 Frontline : Microsoft propose des sessions Windows 365 dédiées à l'administration, avec Conditional Access enforced nativement. Adapté aux organisations sans infrastructure on-premises.

Intégration Microsoft Copilot for Security depuis PAW : Les RSSI utilisent Copilot for Security (basé sur GPT-4) pour l'analyse de logs et la réponse aux incidents. Les accès à cette plateforme doivent être soumis aux mêmes contraintes PAW que tout autre outil d'administration cloud.

PAW et Zero Trust Network Access (ZTNA) : Remplacement progressif des VPN traditionnels par du ZTNA (Zscaler Private Access, Netskope) pour les accès distants. Les PAW s'authentifient via ZTNA avec un certificat machine client, éliminant le VPN comme vecteur d'attaque potentiel.

Certification CSPN ANSSI des solutions PAM : WALLIX PAM et CyberArk disposent de certifications CSPN (Certification de Sécurité de Premier Niveau) ANSSI, facilitant leur intégration dans les architectures PAW pour les OIV et OSE soumis à la directive NIS 2.

La sécurisation des infrastructures Active Directory passe inévitablement par des PAW correctement déployés. En 2026, face à la sophistication croissante des attaques (techniques DCOM, pass-the-ticket, golden ticket), le PAW reste la première ligne de défense opérationnelle pour protéger les accès admin contre la compromission initiale.

FAQ — Privileged Access Workstations

Un PAW doit-il être physique ou peut-il être une VM ?

Les deux approches sont valides, mais le niveau d'isolation diffère. Un Hardware PAW physique offre la protection maximale car il élimine le risque d'une compromission de l'hyperviseur (escape de VM). Pour le Tier 0 (contrôleurs de domaine, PKI, Entra Global Admin), un PAW physique est recommandé. Pour le Tier 1 (serveurs d'application, infrastructure), une VM PAW sur un hyperviseur dédié et durci est acceptable, à condition que cet hyperviseur lui-même soit dans un périmètre sécurisé, géré uniquement depuis le VLAN PAW, et que les snapshots soient désactivés en production pour éviter les roll-backs de credentials.

Comment gérer les mises à jour d'un PAW isolé d'Internet ?

Les mises à jour d'un PAW isolé transitent par un serveur WSUS (Windows Server Update Services) interne, situé dans un VLAN sécurisé accessible uniquement depuis le VLAN PAW. Ce WSUS télécharge les mises à jour Microsoft depuis Internet (flux sortant autorisé uniquement

pour le WSUS), les valide, puis les pousse vers les PAW via le VLAN Management. Pour les organisations utilisant Intune, les mises à jour peuvent transiter via Private Endpoints Azure, sans que les PAW n'aient d'accès Internet direct. Une fenêtre de maintenance mensuelle avec validation post-déploiement (vérification Credential Guard, AppLocker) est recommandée.

Un admin peut-il utiliser son PAW pour des tâches courantes (email, navigation) ?

Non, et c'est la règle la plus difficile à faire accepter opérationnellement. Un PAW est un outil monotâche : administration uniquement. L'administrateur dispose de deux postes : son poste bureautique standard pour email, navigation, Teams, et son PAW pour les tâches d'administration. Tolérer l'usage bureautique sur le PAW détruit immédiatement l'isolation recherchée. En pratique, les organisations les mieux avancées configurent le PAW pour n'afficher que les outils d'administration au lancement de session, sans accès au bureau Windows standard, réduisant la tentation d'utilisation détournée.

PAW et Bastion (WALLIX/CyberArk) sont-ils complémentaires ou redondants ?

Complémentaires, sans aucun doute. Ils opèrent sur des couches différentes. Le PAW sécurise la source : le poste depuis lequel l'administrateur travaille. Le Bastion sécurise le transit et l'enregistrement des sessions vers les cibles (DC, serveurs). Sans PAW, un attaquant qui compromet le poste de l'admin peut rebondir vers le Bastion avec les credentials de l'admin. Sans Bastion, les sessions d'administration ne sont pas enregistrées ni auditées. La combinaison PAW + Bastion + PIM (Privileged Identity Management) constitue l'architecture PAM complète recommandée par l'ANSSI pour les OIV et OSE.

Quel budget prévoir pour déployer des PAW en PME ?

Pour une PME française avec 5 administrateurs (2 Tier 0, 3 Tier 1), le budget de déploiement initial est de l'ordre de 15 000 à 25 000 € HT, incluant : Hardware PAW physiques Tier 0 (2 postes × 2 500 € = 5 000 €), mini-hyperviseur dédié Tier 1 (3 000 à 5 000 €), licences Windows

11 Enterprise (500 à 800 €/poste), intégration VLAN et règles firewall (2 à 5 jours de consulting, 1 500 à 2 500 €/jour à Paris). Les coûts récurrents sont faibles : maintenance WSUS, renouvellement des clés FIDO2 (30 à 80 €/clé). Pour les grandes entreprises avec WALLIX ou CyberArk, les licences PAM représentent 50 000 à 200 000 €/an selon le nombre de comptes gérés. ROI : un incident de compromission AD coûte en moyenne 2 à 5 M€ en France selon le CESIN ; les PAW réduisent drastiquement ce risque.

Sources

ANSSI CERT-FR — Publications et alertes

MITRE ATT&CK — Framework des techniques d'attaque

CISA — Advisories de cybersécurité

