AYI NEDJIMI Consultants

Zero Trust Architecture : Implémentation Complète et

Catégorie : Techniques de Hacking Lecture : 15 min Publié le : 08/03/2026 Auteur : Ayi NEDJIMI

Guide complet Zero Trust Architecture : principes NIST SP 800-207, piliers identité/device/réseau/application/données, modèles SDP/BeyondCorp/ZTNA.

Avertissement : Les techniques présentées dans cet article sont destinées exclusivement à des fins éducatives et de tests autorisés. Toute utilisation malveillante est illégale et contraire à l'éthique professionnelle.

2.1 Les sept tenets du Zero Trust

Le NIST (National Institute of Standards and Technology) a publié en août 2020 le document de référence **SP 800-207 "Zero Trust Architecture"**, qui définit sept principes fondamentaux (tenets). Ces principes constituent la boussole de toute implémentation Zero Trust : Guide complet Zero Trust Architecture : principes NIST SP 800-207, piliers identité/device/réseau/application/données, modèles SDP/BeyondCorp/ZTNA. Les techniques offensives évoluent rapidement : zero trust architecture implementation fait partie des compétences essentielles que tout pentester et red teamer doit maîtriser pour mener des missions réalistes. Nous abordons notamment : 8. métriques de maturité zero trust, 9. quick wins et pièges à éviter et 10. checklist zero trust -- évaluation de votre posture. Les professionnels y trouveront des recommandations actionnables, des commandes prêtes à l'emploi et des stratégies de mise en œuvre adaptées aux environnements d'entreprise.

Tenet 1 -- Toutes les sources de données et services de calcul sont considérés comme des ressources. Cela inclut les serveurs, les postes de travail, les devices IoT, les applications SaaS, les API, les bases de données. Le scope est total : aucune catégorie de ressource n'échappe au modèle Zero Trust.

Tenet 2 -- Toutes les communications sont sécurisées indépendamment de la localisation réseau. Un flux entre deux serveurs dans le même datacenter doit être chiffré et authentifié avec la même rigueur qu'un flux traversant Internet. Le réseau interne n'est pas un facteur de confiance. Ce principe justifie le chiffrement systématique (mTLS, IPsec) et l'abandon des protocoles en clair (HTTP, LDAP sans TLS, SMBv1).

Tenet 3 -- L'accès aux ressources individuelles est accordé session par session. Chaque requête d'accès est évaluée indépendamment. Un accès accordé à 9h00 peut être révoqué à 9h05 si le contexte change (risque détecté, terminal non conforme, localisation suspecte). Ce principe impose l'évaluation continue, pas seulement à l'authentification initiale.

Tenet 4 -- L'accès aux ressources est déterminé par une politique dynamique. La décision d'accès intègre de multiples signaux : identité du sujet (utilisateur, service), attributs du terminal (patch level, présence d'un agent EDR), attributs comportementaux (horaires habituels, geolocalization), et sensibilité de la ressource demandée. C'est le coeur du **Policy Decision Point (PDP)**.

Tenet 5 -- L'entreprise surveille et mesure l'intégrité et la posture de sécurité de tous les actifs. Aucun appareil n'obtient un statut de confiance permanent. La conformité est réévaluée en continu : un poste qui ne reçoit plus ses mises à jour ou dont l'antivirus est désactivé voit ses droits d'accès immédiatement restreints.

Tenet 6 -- L'authentification et l'autorisation sont dynamiques et strictement appliquées avant l'accès. L'authentification doit être forte (multi-facteurs, résistante au phishing), l'autorisation doit suivre le principe du moindre privilège, et les deux sont réévalués en permanence via des mécanismes comme le Continuous Access Evaluation (CAE).

Tenet 7 -- L'entreprise collecte un maximum d'informations sur l'état actuel du réseau et des communications pour améliorer sa posture de sécurité. La visibilité totale est un prérequis. Sans télémétrie exhaustive -- logs d'authentification, flux réseau, activité des endpoints, comportement des utilisateurs -- le Zero Trust est aveugle. Ce principe justifie l'investissement dans les solutions EDR/XDR, le SIEM, et les outils de Network Detection and Response (NDR).

2.2 Au-delà du NIST : le modèle CISA Zero Trust Maturity

La CISA (Cybersecurity and Infrastructure Security Agency) a enrichi le cadre NIST avec un **modèle de maturité Zero Trust** publié en 2023, qui définit cinq piliers (Identity, Devices, Networks, Applications & Workloads, Data) et quatre niveaux de maturité (Traditional, Initial, Advanced, Optimal). Ce modèle fournit une feuille de route concrète pour évaluer sa progression et prioriser les investissements.

Le modèle CISA ajoute trois capacités transversales : la **visibilité et analytique** (telemetry, SIEM, UEBA), l'**automatisation et orchestration** (SOAR, policy-as-code), et la **gouvernance** (ownership des données, classification, politiques d'accès). Ces capacités transversales sont le ciment qui relie les cinq piliers.

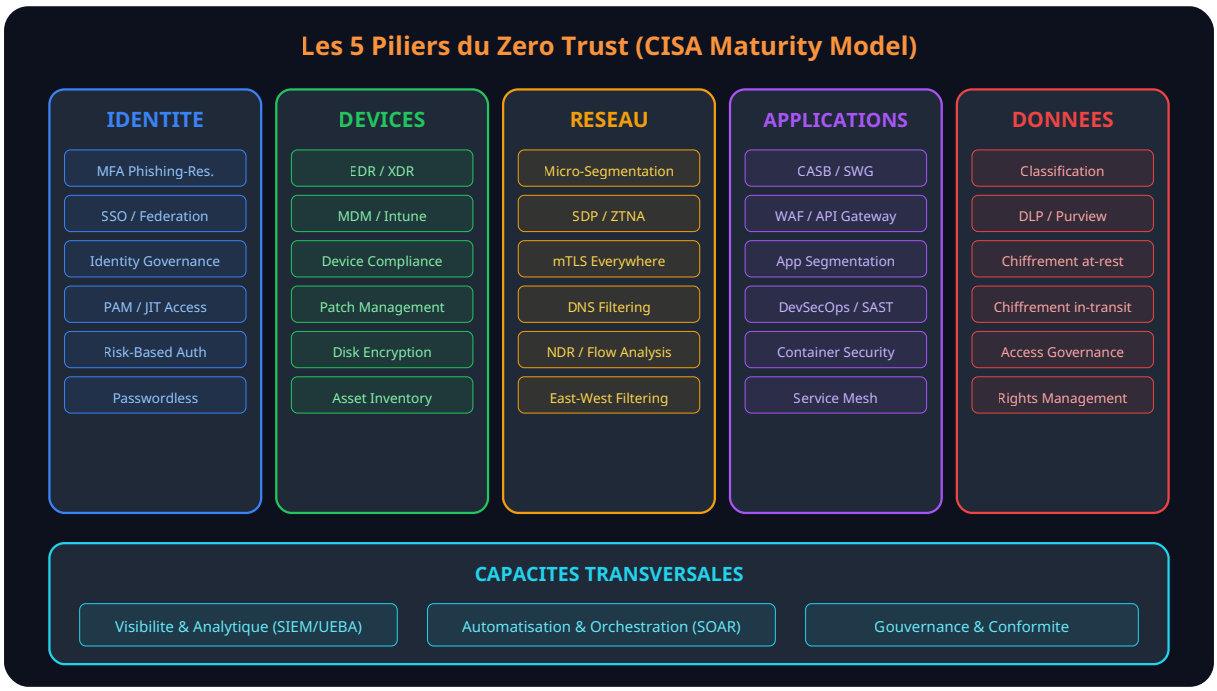

Figure 1 -- Les 5 piliers du Zero Trust et les capacités transversales (modèle CISA)

Cas concret
L'exploitation de la vulnérabilité MOVEit (CVE-2023-34362) par le groupe Cl0p a compromis plus de 2 500 organisations dans le monde en juin 2023. Cette attaque par injection SQL sur un logiciel de transfert de fichiers a démontré l'impact dévastateur d'une seule vulnérabilité zero-day dans un produit largement déployé.

Software-Defined Perimeter (SDP) / ZTNA : Le SDP rend les ressources **invisibles** au réseau. Contrairement au VPN qui accorde l'accès à un segment réseau entier, le SDP (ou ZTNA -- Zero Trust Network Access) n'expose que l'application spécifique à laquelle l'utilisateur est autorisé, après vérification de son identité et de la posture de son terminal. L'attaquant qui scanne le réseau ne voit rien : les ports sont fermés, les services masqués derrière un broker d'accès.

East-West traffic monitoring : Le trafic latéral (est-ouest) entre serveurs représente souvent 80 % du trafic total dans un datacenter. Les firewalls périmétrique ne le voient pas. Les solutions NDR (Network Detection and Response) et les agents de micro-segmentation apportent la visibilité nécessaire pour détecter les flux anormaux, les scans internes et les tentatives de mouvement latéral.

3.4 Pilier 4 : Applications et Workloads

Les applications sont les vecteurs par lesquels les utilisateurs accèdent aux données. Le pilier Application exige que chaque application soit **sécurisée dès la conception (secure by design), surveillée en production, et protégée contre les attaques applicatives**.

Application-level access control : L'accès aux applications doit être médié par un proxy d'accès (CASB pour le SaaS, application proxy pour les applications internes) qui vérifie l'identité, la posture du device et les politiques d'accès avant d'autoriser la connexion. Ce proxy peut également inspecter le contenu (DLP), limiter les actions (read-only pour les terminaux non gérés) et journaliser les activités.

Sécurité des API : Les API sont omniprésentes (microservices, intégrations SaaS, applications mobiles) et constituent une surface d'attaque massive. Le Zero Trust appliqué aux API inclut l'authentification mutuelle (mTLS), l'autorisation par scopes OAuth (principe du moindre privilège sur les permissions API), le rate limiting, et la validation des schémas. Consultez notre article sur les attaques API GraphQL et REST pour comprendre les menaces.

Sécurité des conteneurs et du service mesh : Dans les environnements Kubernetes, le service mesh (Istio, Linkerd) implémente le Zero Trust au niveau des microservices : mTLS automatique entre tous les pods, politiques d'autorisation fine (quel service peut appeler quel service), et observabilité des flux. Cela complète les contrôles RBAC Kubernetes et les network policies.

3.5 Pilier 5 : Données -- l'objectif ultime

Les données sont la **raison d'être de toute la stratégie Zero Trust**. L'identité, le device, le réseau et les applications ne sont que des moyens pour protéger l'actif le plus précieux : les données. Le pilier Data exige la classification, le chiffrement, le contrôle d'accès granulaire et la prévention des fuites.

Classification des données : Avant de protéger les données, il faut savoir quelles données existent, où elles résident et quelle est leur sensibilité. La classification (Public, Interne, Confidentiel, Très Confidentiel) peut être automatisée par des outils comme Microsoft Purview Information Protection qui scannent les repositories et appliquent des labels basés sur le contenu (numéros de carte bancaire, données personnelles, propriété intellectuelle).

Data Loss Prevention (DLP) : Les politiques DLP empêchent l'exfiltration de données sensibles via tous les canaux : email, upload cloud, copie USB, impression. L'intégration du DLP avec le Conditional Access permet des contrôles contextuels : un document "Confidentiel" peut être ouvert depuis un terminal géré mais pas téléchargé depuis un terminal personnel.

Chiffrement et Rights Management : Le chiffrement at-rest et in-transit est un minimum. Le Rights Management (Azure Information Protection, Vera) va plus loin en associant des droits d'utilisation au document lui-même : interdiction de copier, d'imprimer, de transférer, avec révocation possible à tout moment. Le document reste protégé même s'il quitte le périmètre de l'entreprise.

ZTNA 1.0 (endpoint-initiated) : L'agent sur le terminal initie la connexion vers un broker cloud qui vérifie l'identité et la posture, puis établit un tunnel vers l'application cible. Exemples : Zscaler Private Access (ZPA), Palo Alto Prisma Access. L'avantage est que le broker masque complètement l'application de l'Internet. L'inconvénient est la dépendance à un agent installé sur le terminal.

ZTNA 2.0 (service-initiated) : Pas d'agent requis côté client. Un connecteur léger est déployé devant l'application dans le réseau de l'entreprise et établit un tunnel sortant vers le broker cloud. L'utilisateur accède via un navigateur, le broker vérifie l'identité et redirige vers le connecteur. Exemples : Cloudflare Access, Azure AD Application Proxy. Idéal pour les scénarios BYOD et les accès tiers (prestataires, partenaires).

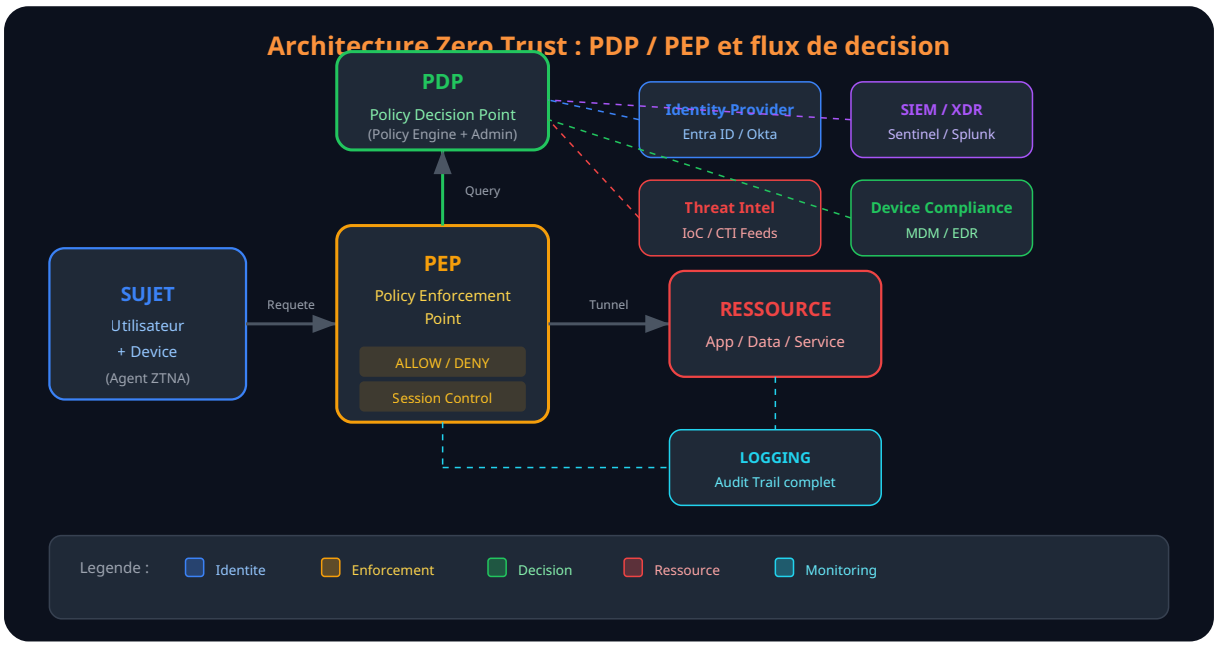

Figure 2 -- Architecture Zero Trust : composants PDP/PEP, sources de données et flux de décision

Les IdP les plus utilisés dans les déploiements Zero Trust incluent **Microsoft Entra ID** (avec Conditional Access et Identity Protection), **Okta** (avec Adaptive MFA et FastPass), **Ping Identity** et **Keycloak** (open source). La consolidation des identités dans un IdP unique (ou fédéré) est un prérequis : si certains utilisateurs s'authentifient via un mécanisme hors du périmètre de l'IdP, ils échappent aux contrôles Zero Trust. Pour comprendre les risques d'attaque sur les IdP, consultez notre article dédié aux attaques sur les Identity Providers.

5.3 SIEM et analytics -- la visibilité totale

Le SIEM (Security Information and Event Management) est l'infrastructure de visibilité du Zero Trust. Il collecte, corrèle et analyse les logs de tous les composants -- IdP, EDR, firewall, proxy, applications, DNS -- pour détecter les comportements anormaux et alimenter le PDP en signaux de risque.

Un SIEM moderne intègre des capacités d'**UEBA (User and Entity Behavior Analytics)** qui établissent une baseline comportementale pour chaque utilisateur et entité. Les déviations (connexion à une heure inhabituelle, accès à des ressources jamais utilisées, volume de données transférées anormal) génèrent des alertes de risque qui peuvent automatiquement déclencher une réévaluation des accès via le PDP. Microsoft Sentinel, Splunk, Elastic Security et Google Chronicle sont les leaders du marché.

5.4 Micro-segmentation -- isoler pour protéger

La micro-segmentation est l'implémentation réseau du principe du moindre privilège. Elle crée des frontières de sécurité autour de chaque workload individuel, limitant les communications aux seuls flux nécessaires. L'implémentation se fait à plusieurs niveaux :

Niveau	Technologie	Granularité	Cas d'usage
Réseau (L3/L4)	VLAN, ACL, Firewall	Sous-réseau	Segmentation grossière entre zones (DMZ, LAN, serveurs)
Host-based	Illumio, Guardicore	Workload	Isolation par serveur/VM, policies basées sur les labels
Container	Network Policies K8s, Calico	Pod	Isolation entre microservices dans un cluster
Service Mesh	Istio, Linkerd	Service	mTLS automatique, AuthorizationPolicy
Application (L7)	WAF, API Gateway	Endpoint API	Filtrage par méthode HTTP, payload, headers

Recommandation : commencez par la visibilité
Avant de déployer des politiques de micro-segmentation en mode enforcement, déployez les agents en **mode observabilité** pendant au minimum 30 jours. Cartographiez les flux réels entre vos workloads. Identifiez les dépendances non documentées. Créez vos policies basées sur les flux observés, pas sur les flux théoriques. Un déploiement en mode enforcement sans cette phase de découverte **causera des incidents de production**.

La troisième phase s'attaque au réseau. C'est la phase la plus complexe techniquement, mais aussi la plus impactante pour limiter le mouvement latéral :

- **Cartographier tous les flux réseau** : déployer les agents de micro-segmentation en mode observabilité. Identifier les dépendances applicatives, les flux legacy, les communications non documentées.
- **Déployer le ZTNA** en remplacement du VPN traditionnel. Commencer par les applications les moins critiques pour valider le modèle, puis migrer progressivement les applications sensibles.
- **Implémenter la micro-segmentation** : créer des policies basées sur les flux observés. Déployer en mode monitor (alert-only) pendant 30 jours minimum, puis activer l'enforcement graduellement, environnement par environnement.
- **Chiffrer les communications internes** : déployer mTLS pour les flux applicatifs critiques. Dans les environnements Kubernetes, activer le service mesh avec mTLS automatique.
- **Déployer le DNS filtering** et le Network Detection and Response (NDR) pour la visibilité sur les flux est-ouest et la détection des communications avec les C2.

Attention : risque de disruption de la production
La micro-segmentation est le contrôle Zero Trust qui présente le plus de risque opérationnel. Un flux bloqué par erreur peut provoquer une panne applicative. Le mode observabilité préalable, les exceptions temporaires, les runbooks de rollback et les circuits d'escalade sont **indispensables**. Ne jamais déployer en enforcement un vendredi soir.

6.4 Phase 4 : Data-centric security (mois 12-18)

La quatrième phase place les données au centre de la stratégie. C'est la maturité maximale du modèle Zero Trust :

- **Classifier les données** : déployer une solution de classification automatique (Microsoft Purview, Varonis, BigID) qui scanne les repositories de données et applique des labels de sensibilité basés sur le contenu.
- **Implémenter le DLP** : définir des politiques de prévention des fuites de données sur tous les canaux (email, cloud storage, endpoints, web). Intégrer le DLP avec le Conditional Access pour des contrôles contextuels.
- **Déployer le Rights Management** : protéger les documents sensibles avec des droits persistants (interdiction de copier, transférer, imprimer) qui suivent le document même en dehors de l'entreprise.
- **Implémenter le Data Access Governance** : revues d'accès aux données, principe du moindre privilège sur les partages de fichiers, bases de données et applications. Éliminer les accès "everyone" et les permissions héritées excessives.
- **Automatiser la réponse** : intégrer les alertes DLP, classification et anomalies d'accès aux données dans le SOAR pour des réponses automatiques (révocation d'accès, quarantaine du fichier, notification au SOC).

Avantages par rapport au VPN : pas de backhauling du trafic via le datacenter central (performance), pas de surface d'attaque réseau (les App Connectors n'ont pas d'adresse IP routable), segmentation applicative native (l'utilisateur n'accède qu'aux applications autorisées, pas au réseau entier).

7.4 Zoom : Illumio -- micro-segmentation sans agent réseau

Illumio adopte une approche **host-based** de la micro-segmentation. Plutôt que de modifier l'infrastructure réseau (VLAN, firewall), Illumio déploie un agent léger (VEN -- Virtual Enforcement Node) sur chaque workload (serveur physique, VM, conteneur) qui programme les règles du firewall local de l'OS (iptables sous Linux, Windows Firewall sous Windows).

Le processus se déroule en trois étapes :

1. **Illumination :** Les agents collectent les flux réseau réels et les remontent vers la console Illumio qui génère une **carte de dépendances applicatives** en temps réel. Cette carte montre qui communique avec qui, sur quels ports, avec quel volume.
2. **Labeling :** Chaque workload est identifié par des **labels multi-dimensionnels** (Role: web-server, App: e-commerce, Env: production, Loc: paris-dc1) plutôt que par des adresses IP. Les politiques sont écrites en termes de labels, ce qui les rend indépendantes de l'infrastructure réseau.
3. **Enforcement :** Les politiques sont compilées en règles de firewall local et poussées aux agents. Le mode "visibility-only" génère des alertes sans bloquer ; le mode "enforcement" bloque les flux non autorisés.

8. Métriques de maturité Zero Trust

8.1 Le Zero Trust Maturity Model

Mesurer la progression Zero Trust est essentiel pour justifier les investissements et identifier les lacunes. Voici un framework de métriques aligné sur le modèle CISA :

Figure 3 -- Les 4 niveaux de maturité Zero Trust et leurs caractéristiques

8.2 KPIs opérationnels du Zero Trust

Au-delà du modèle de maturité global, voici les KPIs opérationnels à suivre pour mesurer l'efficacité de votre déploiement Zero Trust :

KPI	Cible	Mesure
Couverture MFA	100 %	% d'authentifications avec MFA / total authentifications
MFA phishing-resistant (admins)	100 %	% d'admins utilisant FIDO2/WHfB
Terminaux conformes	>95 %	% de devices compliant dans Intune/MDM
Couverture EDR	100 %	% d'endpoints avec agent EDR actif
Comptes à privilèges en JIT	100 %	% de rôles admin activés via PIM/PAM
Legacy auth blocked	100 %	% de protocoles legacy bloqués
Micro-segmentation coverage	>80 %	% de workloads critiques avec policies enforcées
MTTD (Mean Time to Detect)	<1h	Temps moyen de détection d'un incident
MTTR (Mean Time to Respond)	<4h	Temps moyen de réponse à un incident
Données classifiées	>90 %	% de données avec label de sensibilité

9. Quick wins et pièges à éviter

9.1 Les 10 quick wins Zero Trust

Ces actions peuvent être mises en oeuvre rapidement et offrent un retour sur investissement immédiat :

1. **Activer le MFA pour tous les comptes**, en commençant par les administrateurs. Utiliser les Authentication Strengths pour exiger du MFA phishing-resistant sur les comptes critiques.
2. **Bloquer les protocoles d'authentification legacy** (IMAP, POP3, SMTP Auth) via une politique Conditional Access. Ces protocoles ne supportent pas le MFA et sont le vecteur principal du password spraying.
3. **Implémenter des break-glass accounts** : deux comptes d'urgence avec des mots de passe longs (40+ caractères), stockés dans un coffre physique, exclus du Conditional Access, avec monitoring en temps réel de leur utilisation.
4. **Activer Identity Protection** (ou équivalent) : les politiques risk-based détectent les credentials compromis, les connexions impossibles et les patterns d'attaque en temps réel.
5. **Déployer le Continuous Access Evaluation (CAE)** : révocation quasi instantanée des tokens quand le compte est compromis, plutôt que d'attendre l'expiration (60-90 minutes).
6. **Supprimer les accès admin permanents** : migrer vers le JIT (Just-in-Time) via PIM/PAM. Un Global Admin permanent est un ticket d'or pour l'attaquant qui compromet ce compte.
7. **Bloquer les pays non autorisés** : une politique CA qui bloque les connexions depuis les pays où l'organisation n'a aucune activité élimine une grande partie du bruit d'attaque.
8. **Inventorier les applications et les consentements OAuth** : identifier les applications tierces avec des permissions excessives (Mail.ReadWrite, Files.ReadWrite.All) et révoquer les consentements suspects. Voir notre article sur la sécurité OAuth.
9. **Activer les alertes sur les événements critiques** : création de nouveaux admins, modification des politiques CA, connexion des break-glass accounts, nouveaux consentements d'application.
10. **Documenter et tester les procédures de break-glass** : les comptes d'urgence doivent être testés trimestriellement et leur accès audité en continu.

9.2 Les pièges courants du Zero Trust

- **"Zero Trust washing" :** acheter un produit labellisé "Zero Trust" et considérer que la transformation est terminée. Le Zero Trust est une stratégie, pas un produit. Un ZTNA seul sans gestion des identités, sans device compliance et sans micro-segmentation n'est qu'un VPN amélioré.
- **Ignorer l'expérience utilisateur :** des contrôles trop stricts (MFA à chaque requête, blocage systématique des terminaux personnels) provoquent des contournements par les utilisateurs (shadow IT, partage de credentials). L'équilibre sécurité/productivité est critique.
- **Sous-estimer l'inventaire :** vous ne pouvez pas protéger ce que vous ne connaissez pas. Un inventaire incomplet des identités, des devices et des applications crée des angles morts que l'attaquant exploitera.

- **Big-bang deployment :** déployer le Zero Trust en une seule phase massive garantit des incidents de production et un rejet par les utilisateurs. L'approche progressive (4 phases sur 12-18 mois) est la seule viable.
- **Négliger le réseau legacy :** les protocoles comme NTLM, Kerberos sans protection, SMBv1 ou LLMNR créent des chemins de contournement du Zero Trust. Le durcissement du réseau legacy est indispensable en parallèle du déploiement Zero Trust.

Pour approfondir ce sujet, consultez notre outil open-source advanced-nmap-scanner qui facilite l'automatisation des scans réseau avancés.

10. Checklist Zero Trust -- évaluation de votre posture

Utilisez cette checklist pour évaluer votre niveau de maturité Zero Trust actuel et identifier les chantiers prioritaires :

Pilier Identité

- MFA activé pour 100 % des utilisateurs (pas d'exception)
- MFA phishing-resistant (FIDO2/passkeys) pour tous les administrateurs
- Protocoles d'authentification legacy bloqués
- Conditional Access (ou équivalent) déployé avec politiques risk-based
- PAM/PIM déployé -- aucun accès admin permanent
- Revues d'accès trimestrielles automatisées
- SSO consolidé via un IdP unique
- Break-glass accounts configurés, testés et monitorés

Pilier Devices

- MDM/UEM déployé sur 100 % des terminaux gérés
- Politiques de conformité device actives (chiffrement, patch, AV)
- EDR/XDR déployé sur tous les endpoints
- Conformité device intégrée dans les décisions d'accès (Conditional Access)
- Stratégie BYOD définie et implémentée
- Patch management automatisé avec SLA de conformité

Pilier Réseau

- ZTNA déployé en remplacement (ou complément) du VPN
- Micro-segmentation des workloads critiques
- Chiffrement mTLS pour les flux applicatifs internes
- DNS filtering et NDR pour la détection des anomalies réseau
- Trafic est-ouest monitoré et filtré
- Protocoles legacy réseau désactivés (LLMNR, NBT-NS, WPAD)

Pilier Applications

- CASB déployé pour la visibilité et le contrôle des applications SaaS
- WAF/API Gateway pour les applications web et API exposées
- DevSecOps : SAST/DAST intégrés dans le pipeline CI/CD

- Service mesh avec mTLS pour les architectures microservices
- Inventaire et contrôle des consentements OAuth

Pilier Données

- Classification automatique des données (labels de sensibilité)
- DLP déployé sur email, cloud storage et endpoints
- Chiffrement at-rest et in-transit systématique
- Rights Management pour les documents sensibles
- Revues d'accès aux données et suppression des permissions excessives

Capacités transversales

- SIEM déployé avec logs de tous les composants Zero Trust
- UEBA pour la détection comportementale
- SOAR pour l'automatisation de la réponse
- Métriques ZT suivies et reportées mensuellement
- Tests red team / purple team réguliers pour valider l'efficacité

Sources et références : MITRE ATT&CK · OWASP Testing Guide

Questions frequentes

Comment mettre en place Zero Trust Architecture dans un environnement de production ?

La mise en place de Zero Trust Architecture en production necessite une planification rigoureuse, incluant l'evaluation des prerequis techniques, la definition d'une architecture cible, des tests de validation approfondis et un plan de deploiement progressif avec des points de controle a chaque etape.

Pourquoi Zero Trust Architecture est-il essentiel pour la securite des systemes d'information ?

Zero Trust Architecture constitue un element fondamental de la securite des systemes d'information car il permet de reduire significativement la surface d'attaque, d'ameliorer la detection des menaces et de renforcer la posture globale de securite de l'organisation face aux cybermenaces actuelles.

Cette technique Zero Trust Architecture : Implémentation Complète et est-elle utilisable dans un pentest autorisé ?

Oui, à condition d'avoir une lettre de mission signée définissant le périmètre, les horaires et les techniques autorisées. Documentez chaque action et restez dans le scope défini.

Articles connexes

Techniques de Hacking
Mouvement Latéral : Techniques, Détection et Prévention

PtH, PtT, RDP hijacking, pivoting et contre-mesures
Microsoft 365
Sécuriser Entra ID : Conditional Access, MFA et Bonnes Pratiques
Configuration avancée du PDP Microsoft
Identité & Attaques
Attaques sur les Identity Providers (Okta, Entra, Keycloak)
Golden SAML, token theft, session hijacking
Authentification
Contournement FIDO2 et Passkeys
Limites du phishing-resistant MFA
Défense & Détection
Évasion EDR/XDR : Techniques et Contre-mesures
Comprendre les capacités et limites de l'EDR
Cloud & Containers
Kubernetes Offensif : RBAC et Sécurité
Zero Trust appliqué aux environnements K8s

Références et ressources externes

- NIST SP 800-207 -- Zero Trust Architecture -- Document de référence (2020)
- CISA Zero Trust Maturity Model -- Modèle de maturité avec 5 piliers
- Google BeyondCorp Papers -- Articles académiques sur l'implémentation BeyondCorp
- MITRE ATT&CK Enterprise Matrix -- Cartographie des techniques d'attaque
- Forrester -- The Definition of Modern Zero Trust -- Analyse Forrester du concept ZT

> Points clés à retenir
>
> - 8. Métriques de maturité Zero Trust
> - 9. Quick wins et pièges à éviter
> - 10. Checklist Zero Trust -- évaluation de votre posture
> - Questions frequentes

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr