Atténuez les risques liés à la sécurité du réseau de centre de données sans interruption en temps réel

Le coût des vulnérabilités dans les infrastructures critiques de centre de données

Les centres de données, qui alimentent les systèmes dorsaux et d'inférence d'IA, sont essentiels aux entreprises modernes. Cependant, leur rôle critique accroît également les risques. Une attaque de CVE ou du jour zéro non corrigée peut entraîner des pertes financières, une atteinte à la réputation et des perturbations des services.

Dans le cadre des menaces actuel, cette « correction des lacunes » constitue une vulnérabilité critique. Alors que les agresseurs ne prennent que quelques heures à exploiter une CVE, les défenseurs mettent souvent des semaines ou même des mois, à tester et à déployer des correctifs dans les environnements de production.

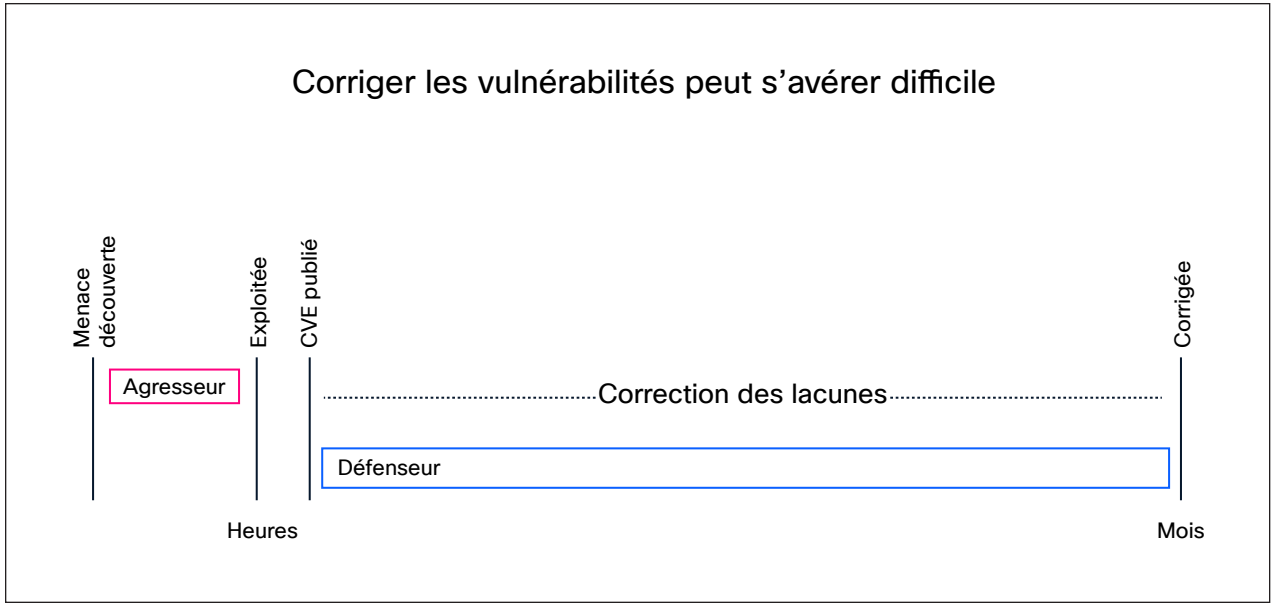

Figure 1. Corriger les vulnérabilités peut s'avérer difficile

Cisco® Live Protect change la donne en fournissant une protection immédiate contre les vulnérabilités des commutateurs Cisco Nexus®, vous permettant ainsi de contrer les attaques sans arrêter votre réseau. Le maintien des infrastructures de centres de données nécessite une sécurité constante et une disponibilité fiable. Les correctifs de CVE traditionnels entraînent souvent des perturbations et des temps d'arrêt. Cisco Live Protect pour les commutateurs de la série N9000 offre des boucliers en temps réel pour atténuer instantanément les vulnérabilités, assurant ainsi une protection et une stabilité en continu, sans maintenance ni mises à niveau urgentes.

Pourquoi Cisco Live Protect?

Les correctifs traditionnels nécessitent des fenêtres de maintenance, des redémarrages et des temps d'arrêt potentiels. Cisco Live Protect offre une approche révolutionnaire en matière de sécurité :

- **Aucun temps d'arrêt :** appliquez les politiques de sécurité aux systèmes opérationnels sans redémarrer le commutateur.
- **Protection immédiate :** bloquez les vulnérabilités dès qu'une menace est découverte, bien avant qu'une mise à niveau standard de l'équipe PSIRT ne soit prévue.
- **Revalidation en continu :** maintenez une posture sécurisée grâce à une observabilité en matière de sécurité optimisée par eBPF.
- **Efficacité opérationnelle :** les SMU (boucliers) de sécurité sont retirés une fois qu'une mise à niveau complète de l'équipe PSIRT est appliquée.

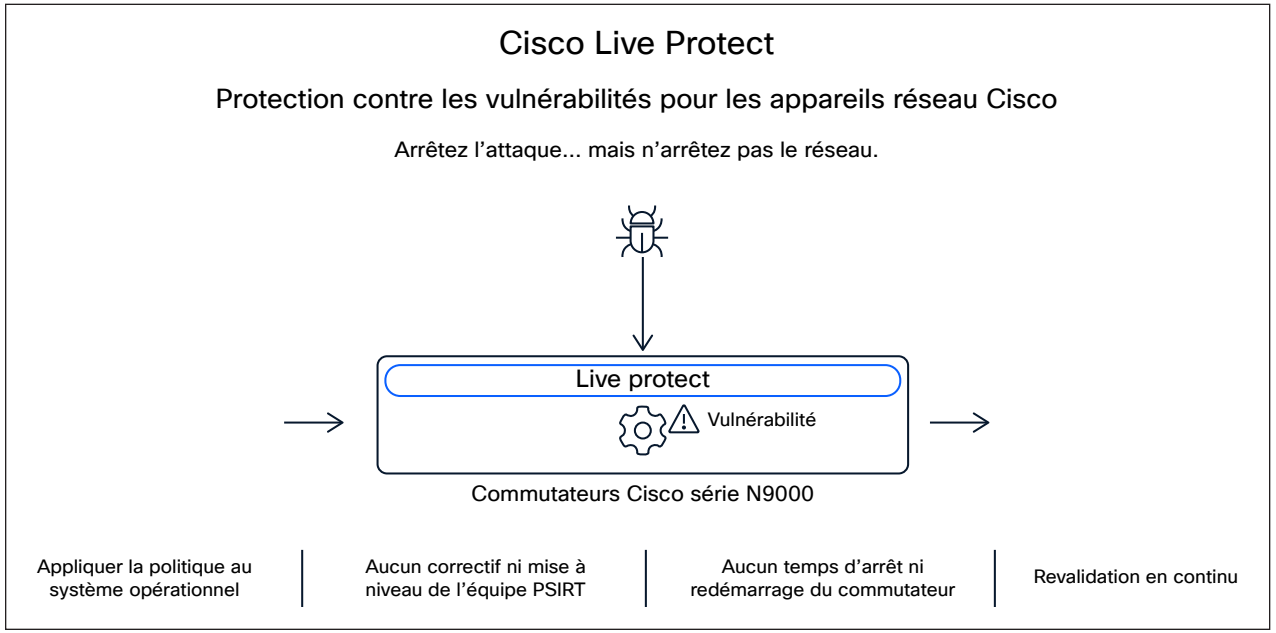

Figure 2. Live Protect

L'innovation alimentée par eBPF

Cisco est le premier à commercialiser un agent Tetragon de niveau entreprise intégré directement à Cisco NX-OS à partir de la version 10.6(1)F. En s'appuyant sur eBPF (extended Berkeley Packet Filter), Live Protect offre une visibilité et une application approfondies au niveau du noyau pour :

- la prévention de l'escalade des privilèges
- la protection du plan de commande
- la sécurité des API et des CLI
- la surveillance des E/S de fichiers

Plateformes prises en charge

Live Protect est offert aux clients Nexus disposant d'une **licence Essentials ou ultérieure**.

Soutien de la plateforme (Cisco NX-OS 10.6(2)F) :

- Plateformes fixes Cisco N9300 et N9200 (≥24 Go de mémoire vive)
- Commutateurs intelligents Cisco N9300
- Commutateurs Cisco série N9400

Fonctionnement

Cisco Live Protect utilise la technologie eBPF avancée pour offrir une sécurité en temps réel aux appareils des réseaux des centres de données. La configuration est flexible, ce qui permet la gestion sur les appareils individuels à l'aide de Cisco NX-OS CLI ou API, pour une automatisation complète de l'ensemble de votre structure de centre de données avec des pipelines CI/CD. Grâce à une orchestration centralisée, Nexus Dashboard offre une visibilité immédiate sur les appareils touchés par les CVE, automatise le déploiement des boucliers de sécurité et supervise continuellement leur efficacité.

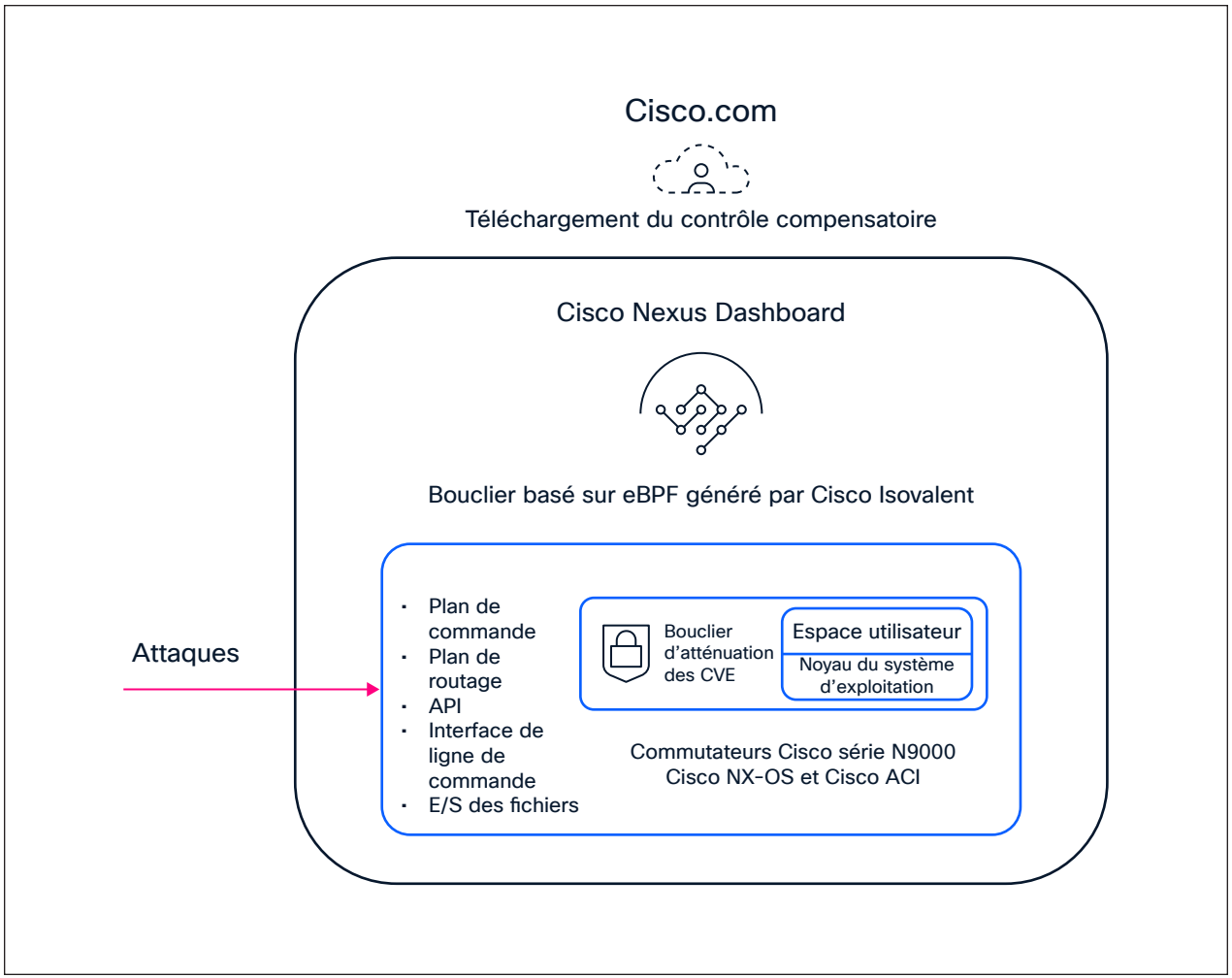

Figure 3. Live Protect et atténuation des CVE pour les commutateurs Cisco N9000

Composants

- **Cisco Live Protect :** offre une protection au niveau du noyau des appareils réseau à l'aide de la technologie eBPF
- **Agent Tetragon :** compile les contrôles compensatoires de CVE dans les politiques eBPF déployables
- **Nexus Dashboard :** console centralisée pour l'orchestration, la visibilité et la supervision de tous les commutateurs Cisco Nexus
- **Outils d'intégration :** prise en charge des API, CLI et pipelines CI/CD pour une automatisation et une gestion faciles

Live Protect garantit des mises à niveau faciles et une réduction en continu des vulnérabilités dans les environnements Cisco NX-OS et Cisco ACI®, garantissant ainsi une sécurité et des performances ininterrompues à partir de l'infrastructure centrale du réseau dans l'ensemble de votre système.

En savoir plus

Protégez votre centre de données avec Cisco Live Protect pour une sécurité automatisée en temps réel et sans temps d'arrêt.

Pour en savoir plus, consultez le blogue Cisco Live Protect ou communiquez avec votre représentant Cisco dès aujourd'hui.

Ressources

Page Web Cisco Live Protect

Voir Cisco Live Protect à l'œuvre avec vidéo

Notes de version de Cisco NX-OS.

Scénarios d'utilisation

Secteur	Principaux scénarios pour Cisco Nexus et Live Protect
Services financiers	· Atténuation des CVE en temps réel · Protection contre les attaques du jour zéro · Réduction des temps d'arrêt pour les applications essentielles · Amélioration de la conformité et de la préparation à l'audit
Soins de santé	· Protection des données sensibles des patients · Atténuation des CVE en temps réel · Disponibilité en continu des systèmes de santé · Conformité (p. ex., HIPAA)
Commerce de détail et commerce électronique	· Sécurisation des paiements et des données des clients · Réduction des temps d'arrêt pendant les périodes de pointe · Protection en temps réel contre les CVE et le jour zéro · Conformité avec PCI DSS
Secteur public et gouvernemental	· Orchestration centralisée de la sécurité · Intervention contre les menaces au jour zéro · Exigence réglementaire · Protection des renseignements sensibles et assurance de la disponibilité des services publics
Fournisseurs de services et de télécommunication	· Défense contre les menaces avancées (p. ex., déni de service distribué) · Maintien d'un rendement ininterrompu du réseau · Opérations de sécurité automatisées · Gestion des politiques centralisée
Énergie et services publics	· Sécurisation des systèmes de contrôle critiques · Atténuation en temps réel des attaques CVE et du jour zéro · Exigence réglementaire · Maintien de la résilience et de la disponibilité
Éducation et recherche	· Protection de la propriété intellectuelle et des données sensibles · Accès en continu aux ressources numériques · Intervention contre les menaces en temps réel · Opérations de sécurité automatisées
Secteur manufacturier	· Environnements des TO et des TI sécurisés · Atténuation des vulnérabilités en temps réel · Protection de la propriété intellectuelle · Assurance d'une continuité opérationnelle

C22-5771857-00 2026-02