Réduire les risques pour la sécurité des réseaux de data center en temps réel, sans perturbation

Le coût des vulnérabilités au sein de l'infrastructure stratégique des data centers

Les data centers, qui alimentent les systèmes de back-end et d'inférence d'IA, sont indispensables dans les entreprises modernes. Cependant, leur rôle stratégique augmente également les risques. Une CVE non corrigée ou une attaque de type « zero-day » peut entraîner des pertes financières, nuire à la réputation de l'entreprise et provoquer des interruptions de service.

Dans le paysage des menaces actuel, ce « délai de correction » constitue une vulnérabilité critique. Alors que les hackers n'ont besoin que de quelques heures pour exploiter une CVE, les équipes de défense mettent souvent plusieurs semaines, voire plusieurs mois, à tester et à déployer les correctifs dans les environnements de production.

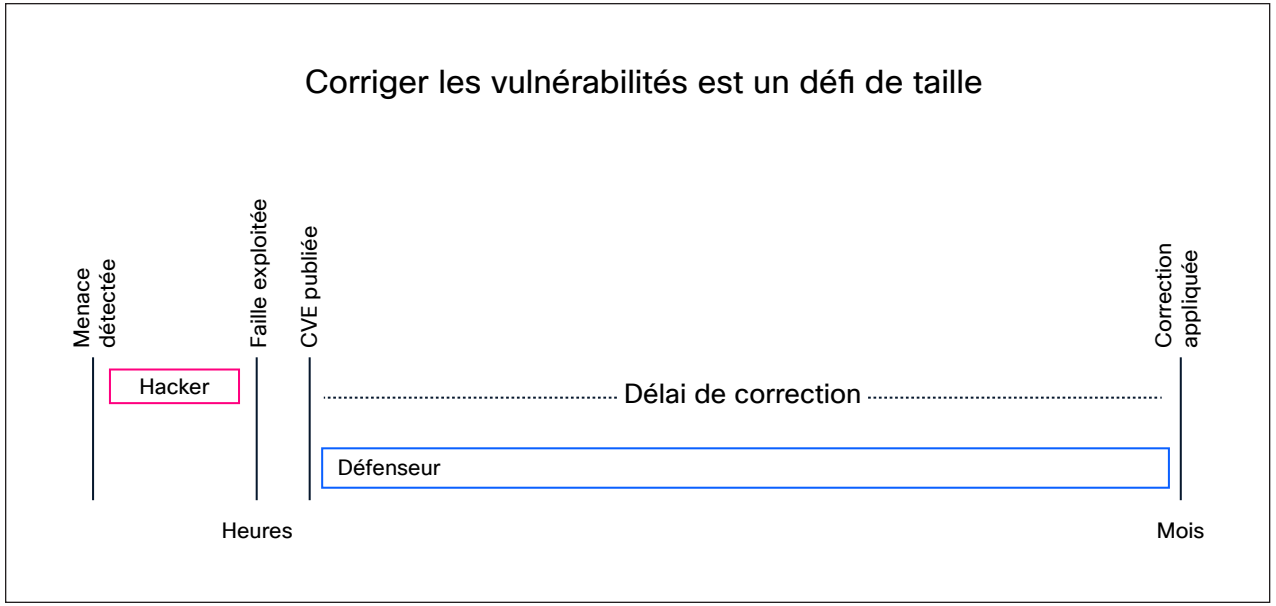

Figure 1. La correction des vulnérabilités est un défi de taille

Cisco® Live Protect change la donne en assurant une protection immédiate contre les vulnérabilités pour les commutateurs Cisco Nexus®, ce qui permet de bloquer les attaques sans interrompre le fonctionnement du réseau. Exploiter une infrastructure de data center exige une sécurité constante et une disponibilité élevée. Les méthodes classiques d'application de correctifs aux CVE entraînent souvent des perturbations et des interruptions de service. Cisco Live Protect pour les commutateurs de la gamme N9000 met en place des mécanismes de défense en temps réel afin de corriger instantanément les vulnérabilités et de garantir une protection continue ainsi que la stabilité de l'infrastructure, sans opération de maintenance ni mise à niveau d'urgence.

Les atouts de Cisco Live Protect

L'application de correctifs classiques implique des fenêtres de maintenance, des redémarrages et d'éventuelles interruptions de service. Cisco Live Protect propose une approche révolutionnaire de la sécurité :

- **Aucune interruption :** appliquez des politiques de sécurité aux systèmes en production, sans redémarrer les commutateurs.
- **Protection immédiate :** protégez les vulnérabilités dès qu'une menace est détectée, bien avant qu'une mise à niveau PSIRT standard ne soit planifiée.
- **Revalidation continue :** assurez la sécurité grâce à la visibilité eBPF.
- **Efficacité opérationnelle :** les SMU de sécurité (protections) sont supprimées une fois la mise à niveau complète du bundle PSIRT appliquée.

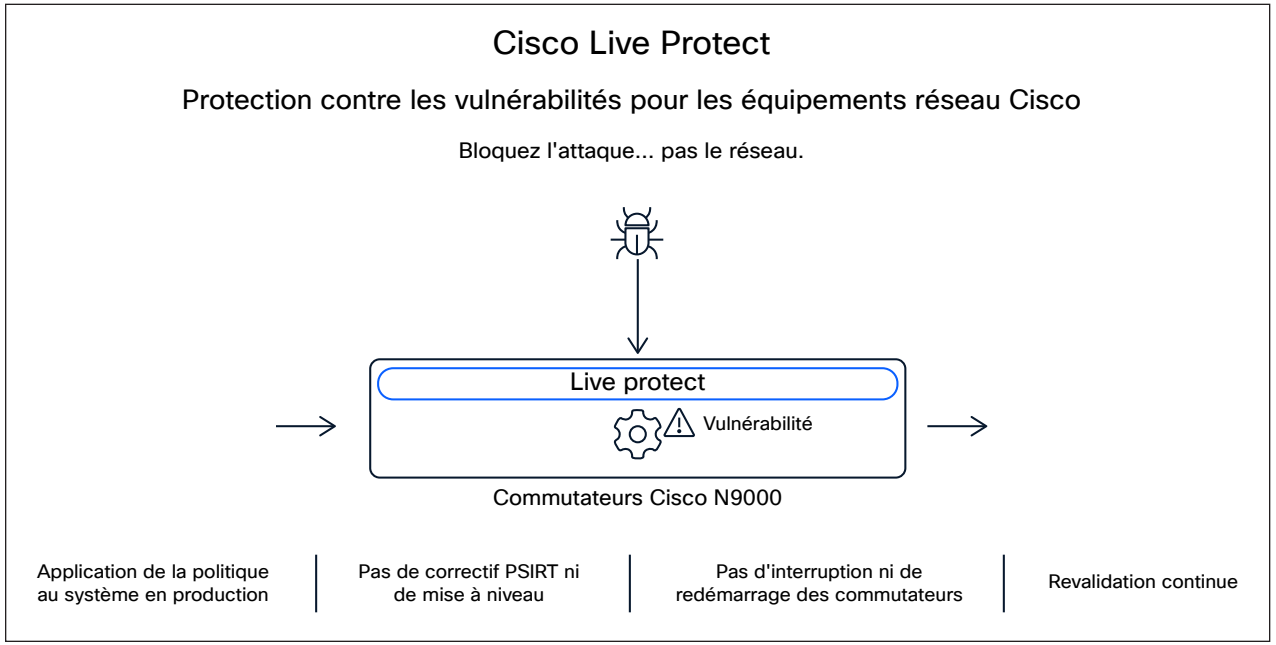

Figure 2. Live Protect

Une innovation optimisée par eBPF

Cisco est le premier fournisseur à proposer un agent Tetragon professionnel directement intégré à Cisco NX-OS à partir de la version 10.6(1)F. En s'appuyant sur la technologie eBPF (extended Berkeley Packet Filter), Live Protect offre une visibilité approfondie et des mécanismes d'application des règles au niveau du noyau pour :

- la prévention des élévations de privilèges ;
- la protection du plan de contrôle ;
- la sécurité des API et de la CLI ;
- la surveillance des opérations d'E/S sur les fichiers.

Plateformes prises en charge

Live Protect est disponible pour les clients Nexus disposant d'une **licence Essentials ou supérieure**.

Plateformes prises en charge (Cisco NX-OS 10.6(2)F) :

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

Fonctionnement

Cisco Live Protect s'appuie sur la technologie avancée eBPF pour assurer la sécurité en temps réel des équipements réseau du data center. La configuration est flexible et permet une gestion des équipements individuellement via l'interface de ligne de commande ou les API de Cisco NX-OS, ou une automatisation complète de l'ensemble de l'infrastructure réseau du data center grâce aux pipelines CI/CD. Nexus Dashboard centralise l'orchestration, en offrant une visibilité instantanée sur les équipements touchés par des CVE, en automatisant le déploiement des mécanismes de défense et en surveillant en continu leur efficacité.

Composants

- **Cisco Live Protect :** assure une protection au niveau du noyau des équipements réseau grâce à la technologie eBPF.
- **Tetragon Agent :** compile les mécanismes de protection compensatoires contre les CVE en stratégies eBPF prêtes à être déployées.
- **Nexus Dashboard :** cette console centralisée assure l'orchestration, la visibilité et la surveillance de l'ensemble des commutateurs Cisco Nexus.

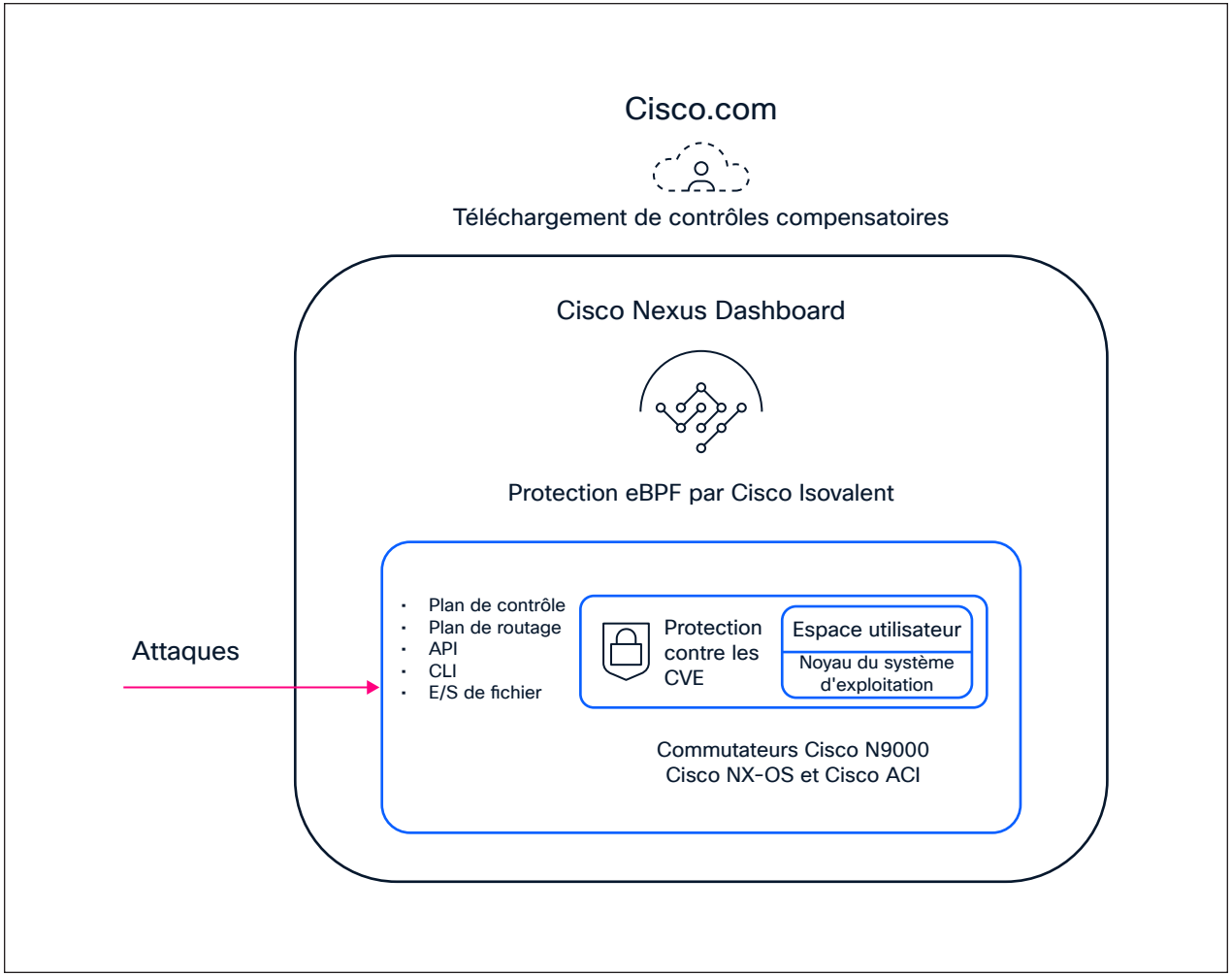

Figure 3 : Live Protect et la correction des CVE pour les commutateurs de la gamme Cisco N9000

- **Outils d'intégration :** assurent la prise en charge des API, de la CLI et des pipelines CI/CD pour une automatisation et une gestion fluides.

Live Protect simplifie les mises à niveau et assure une correction continue des vulnérabilités dans les environnements Cisco NX-OS et Cisco ACI®, afin de garantir une sécurité et des performances ininterrompues dans l'ensemble de votre système, depuis le cœur de l'infrastructure.

Apprenez-en plus

Protégez votre data center avec Cisco Live Protect pour bénéficier d'une sécurité automatisée en temps réel, sans interruption.

Pour en savoir plus, consultez notre blog Cisco Live Protect ou contactez dès aujourd'hui votre conseiller Cisco.

Ressources

Page web de Cisco Live Protect

Découvrez Cisco Live Protect à l'œuvre dans une vidéo

Notes de version de Cisco NX-OS.

Cas d'usage

Secteur	Principaux cas d'usage de Cisco Nexus et Live Protect
Services financiers	· Correction des CVE en temps réel · Protection contre les attaques de type « zero-day » · Réduction des interruptions de service des applications stratégiques · Amélioration de la conformité et de la préparation aux audits
Santé	· Protection des données sensibles des patients · Correction des CVE en temps réel · Disponibilité continue des systèmes de santé · Conformité (par exemple, loi HIPAA)
Commerce et e-commerce	· Sécurisation des paiements et des données clients · Réduction des interruptions de service pendant les périodes de forte activité · Protection en temps réel contre les CVE et les attaques de type « zero-day » · Conformité à la norme PCI DSS
Administrations et secteur public	· Orchestration centralisée de la sécurité · Réponse aux menaces de type « zero-day » · Conformité aux réglementations · Protection des informations sensibles et garantie de la continuité des services publics
Télécommunications	· Protection contre les menaces avancées (par exemple, les attaques DDoS) · Maintien de performances réseau ininterrompues · Automatisation des opérations de sécurité · Gestion centralisée des politiques
Eau et énergie	· Protection des systèmes de contrôle stratégiques · Correction en temps réel des CVE et des attaques de type « zero-day » · Conformité aux réglementations · Maintien de la résilience et de la disponibilité
Enseignement et recherche	· Protection de la propriété intellectuelle et des données sensibles · Accès continu aux ressources numériques · Réponse aux menaces en temps réel · Automatisation des opérations de sécurité
Production industrielle	· Sécurisation des environnements OT et IT · Correction des vulnérabilités en temps réel · Protection de la propriété intellectuelle · Garantie de la continuité des activités

C22-5771857-00 02/26