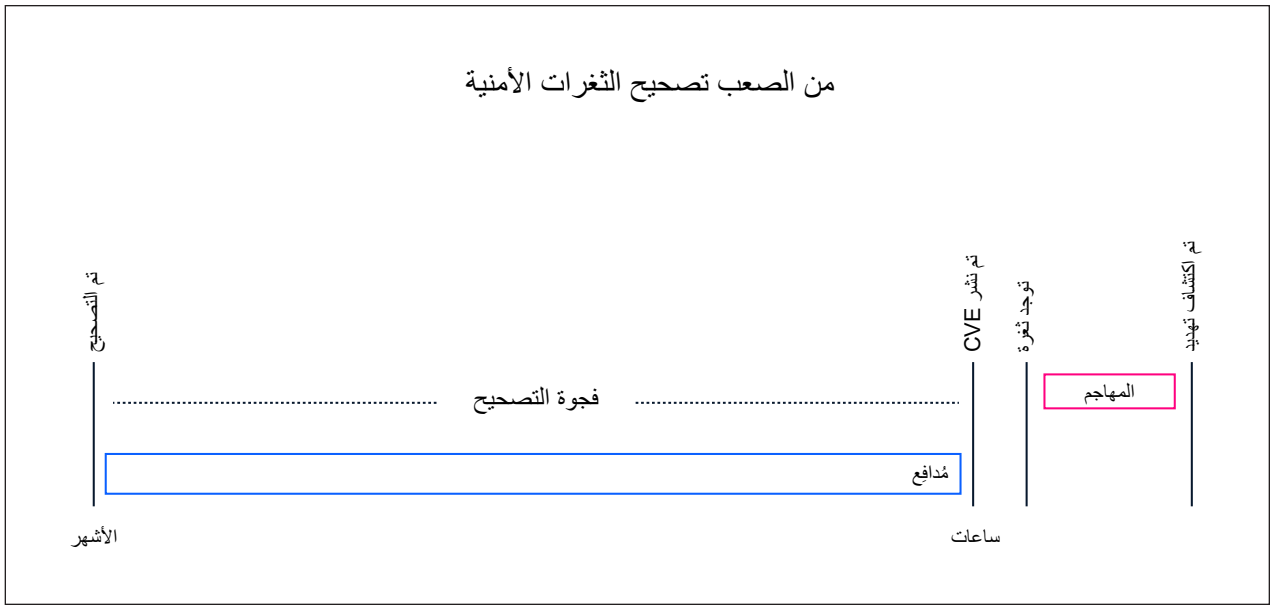
تعزيز أمن شبكات مراكز البيانات والحد من المخاطر دون انقطاع للخدمة وفي الوقت الفعلي

تكلفة الثغرات الأمنية في البنية التحتية الحيوية لمراكز البيانات

تُعد مراكز البيانات التي تدعم الأنظمة الخلفية وأنظمة الاستنتاج الخاصة بالذكاء الاصطناعي ركيزة حيوية للأعمال الحديثة. ومع ذلك، فإن دورهم الحيوي يزيد أيضًا من المخاطر. يمكن أن تؤدي ثغرة أمنية (CVE) لم يتم إصلاحها أو هجوم 0-day إلى خسائر مالية، وإلحاق الضرر بالسمعة، وتعطيل الخدمات.

في ظل مشهد التهديدات الراهن، تُعد "فجوة التصحيح" هذه ثغرة أمنية بالغة الخطورة. في حين لا يستغرق المهاجمون سوى بضع ساعات لاستغلال ثغرة أمنية (CVE)، غالبًا ما يحتاج المدافعون إلى أسابيع أو حتى أشهر لاختبار وتطبيق التصحيحات الأمنية في بيئات التشغيل الفعلية.



الشكل 1. يُعد تصحيح الثغرات الأمنية تحديًا

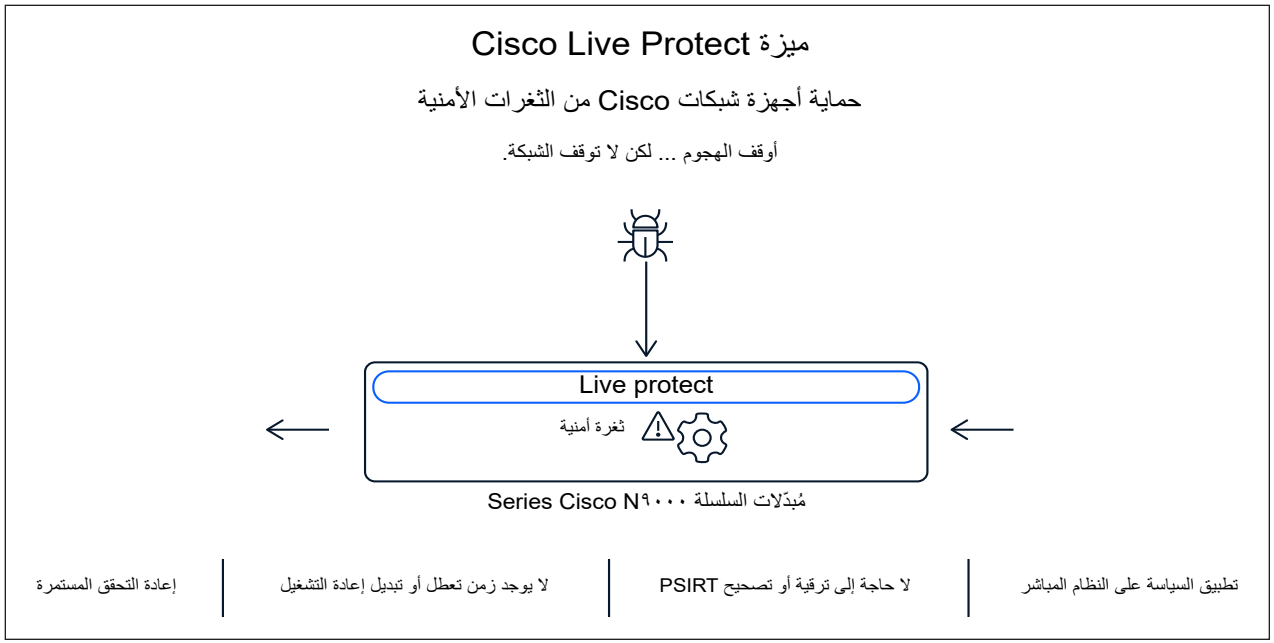
تُحدث خدمة Cisco® Live Protect نقلة نوعية من خلال توفير حماية فورية ضد الثغرات الأمنية لمبدلات Cisco Nexus®، مما يتيح لك صد الهجمات دون الحاجة إلى إيقاف عمل الشبكة. تتطلب صيانة البنية التحتية لمركز البيانات أمانًا متسقًا ووقت تشغيل موثوقًا. غالبًا ما تتسبب عمليات تصحيح الثغرات الأمنية التقليدية في حدوث اضطرابات وزمن تعطل. توفر خدمة Cisco Live Protect لمبدلات سلسلة N9000 دروعًا تعمل في الوقت الفعلي للحد من الثغرات الأمنية فورًا، مما يضمن استمرارية الحماية والاستقرار دون الحاجة إلى صيانة طارئة أو ترقيات عاجلة.

حقوق الطبع والنشر © لعام 2026 لصالح Cisco و/أو الشركات التابعة لها. جميع الحقوق محفوظة.

لماذا ميزة Cisco Live Protect؟

تتطلب عمليات التحديث التقليدية فترات صيانة وإعادة تشغيل واحتمالية توقف النظام عن العمل. تقدم Cisco Live Protect نهجًا ثوريًا للأمان:

- **انعدام زمن التعطل:** تتطبيق سياسات الأمان على الأنظمة قيد التشغيل دون الحاجة إلى إعادة تشغيل المبدّل.
- **حماية فورية:** قم بحماية الثغرات الأمنية فور اكتشاف التهديد، وقبل وقت طويل من موعد الترقية القياسية التي تُجريها فرق الاستجابة للحوادث الأمنية للمنتجات (PSIRT).
- **إعادة التحقق المستمرة:** حافظ على وضعية أمنية محكمة بفضل قابلية الملاحظة الأمنية المدعومة بتقنية eBPF.
- **الكفاءة التشغيلية:** تتم إزالة وحدات التحديث الأمني (SMUs) بمجرد تطبيق ترقية شاملة لحزمة PSIRT.



الشكل 2. Live Protect

ابتكار مدعوم بتقنية eBPF

تُعد Cisco أول من يطرح في السوق وكيل Tetragon بمستوى مؤسسي مدمج مباشرةً في نظام التشغيل Cisco NX-OS، وذلك بدءًا من الإصدار 10.6(1)F. من خلال الاستفادة من تقنية eBPF (Extended Berkeley Packet Filter))، توفر ميزة Live Protect رؤيةً متعمقةً وآليات إنفاذ على مستوى النواة (Kernel) من أجل:

- الوقاية من تصعيد الامتيازات
- حماية مستوى التحكم
- أمان واجهة برمجة التطبيقات (API) وواجهة سطر الأوامر (CLI)
- مراقبة عمليات الإدخال والإخراج للملفات

الأنظمة الأساسية المدعومة

تتوفر Live Protection لعملاء Nexus الذين لديهم **ترخيص Essentials أو أعلى**.

دعم المنصة (Cisco NX-OS 10.6(2)F):

- منصات Cisco N9300 وN9200 الثابتة (ذاكرة وصول عشوائي بسعة 24 جيجابايت أو أكثر)
- مبدّلات Cisco N9300 الذكية
- مبدّلات السلسلة Cisco N9400 Series

حقوق الطبع والنشر © لعام 2026 لصالح Cisco و/أو الشركات التابعة لها. جميع الحقوق محفوظة.

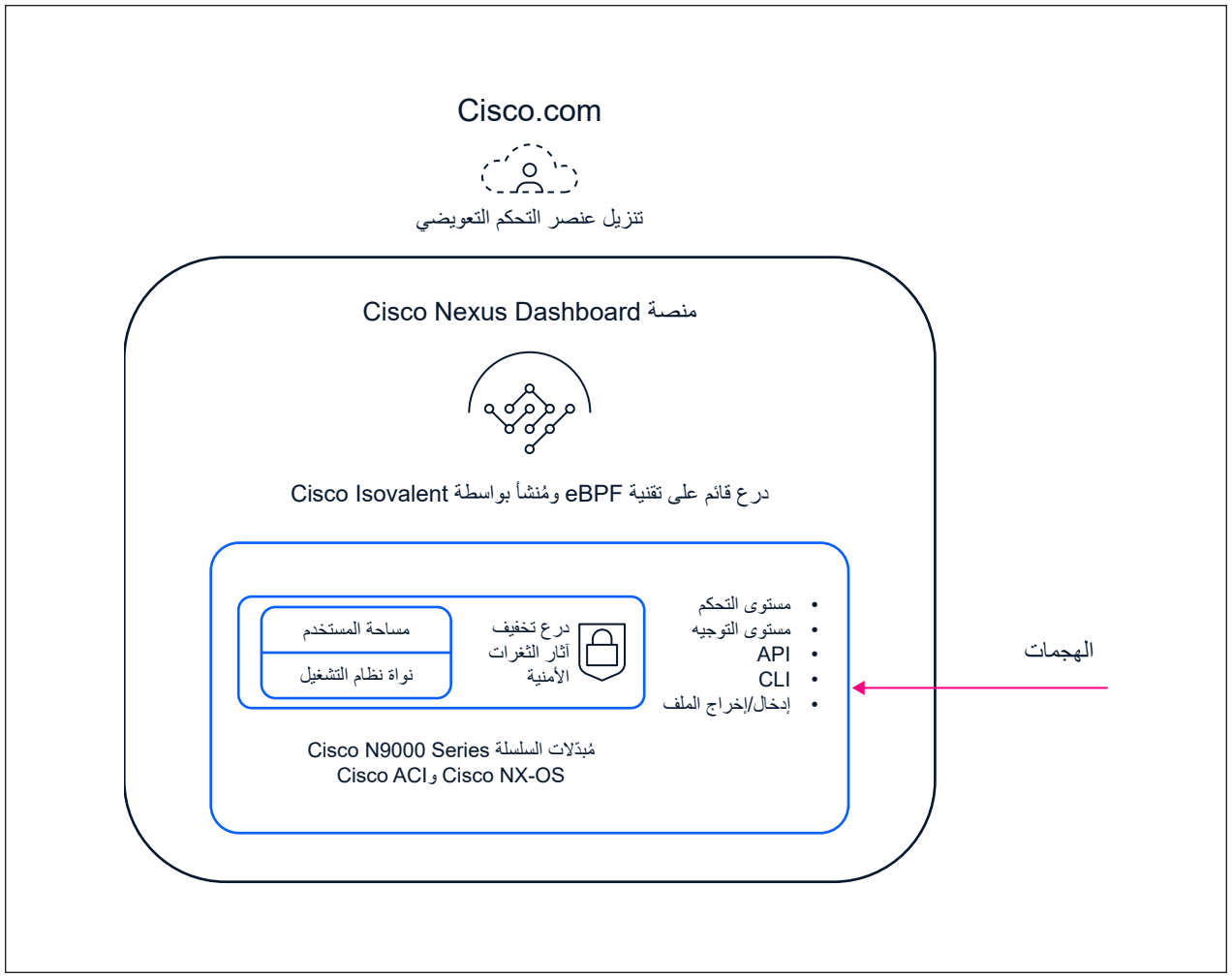
طريقة العمل

تستخدم Cisco Live Protect تقنية eBPF المتقدمة لتوفير حماية أمنية فورية لأجهزة الشبكة في مراكز البيانات. يتميز التكوين بالمرونة، مما يسمح بالإدارة على الأجهزة الفردية من خلال واجهة سطر الأوامر Cisco NX-OS أو واجهة برمجة التطبيقات، من أجل التشغيل الآلي الكامل عبر بنية مركز البيانات الخاص بك من خلال خطوط أنابيب CI/CD. توفر منصة Nexus Dashboard إمكانية التنسيق المركزي، مما يتيح رؤية فورية للأجهزة المتأثرة بثغرات CVE، وأتمتة نشر دروع الحماية، والمراقبة المستمرة لفعاليتها.

المكوّنات

- **Cisco Live Protection:** توفر حماية على مستوى النواة على أجهزة الشبكة باستخدام تقنية eBPF.
- **وكيل Tetragon:** يجمع ضوابط التعويض الخاصة بثغرات CVE في سياسات eBPF قابلة للنشر
- **Nexus Dashboard:** وحدة تحكم مركزية للتنسيق والرؤية والمراقبة عبر جميع مبدلات Cisco Nexus
- **أدوات الدمج:** دعم واجهات برمجة التطبيقات (APIs) وواجهة سطر الأوامر (CLI) ومسار التكامل المستمر/التسليم المستمر (CI/CD) لأتمتة وإدارة سلسة

تضمن ميزة "Live Protect" سلاسة عمليات الترقية والمعالجة المستمرة للثغرات الأمنية في بيئات Cisco NX-OS وCisco ACI®، مما يحافظ على استمرارية الأمان والأداء بدءًا من صميم البنية التحتية ووصولاً إلى النظام بأكمله.



الشكل 3. ميزة Live Protect وتخفيف مخاطر الثغرات الأمنية (CVE) لمبدّلات Cisco N9000 Series

معرفة المزيد

احمِ مركز بياناتك باستخدام Cisco Live Protect للحصول على حماية أمنية آلية وفورية، وضمان عدم توقف الخدمة نهائيًا.

تعرّف على المزيد على **مدونة Cisco Live Protect** الخاصة بنا أو تواصل مع ممثل Cisco الذي اليوم.

الموارد

صفحة ويب Cisco Live Protect

شاهد Cisco Live Protect أثناء العمل عبر الفيديو

ملاحظات إصدار Cisco NX-OS.

حالات الاستخدام

المجال	حالات الاستخدام الرئيسية لـ Cisco Nexus وLive Protect
الخدمات المالية	• تخفيف آثار ثغرات CVE في الوقت الفعلي • الحماية من هجمات Zero-day • تقليل زمن التعطل عن العمل للتطبيقات الحيوية • تعزيز الامتثال والجاهزية للتدقيق
الرعاية الصحية	• حماية بيانات المرضى الحساسة • تخفيف آثار ثغرات CVE في الوقت الفعلي • التوافر المستمر لأنظمة الرعاية الصحية • الامتثال (على سبيل المثال، HIPAA)
البيع بالتجزئة والتجارة الإلكترونية	• تأمين المدفوعات وبيانات العملاء • تقليل وقت التعطل عن العمل خلال فترات الذروة • حماية فورية ضد ثغرات CVE وهجمات zero-day • الامتثال لمعايير PCI DSS
الحكومة والقطاع العام	• التنظيم الأمني المركزي • الاستجابة لتهديدات zero-day • الامتثال التنظيمي • حماية المعلومات الحساسة وضمان استمرارية عمل الخدمات العامة
الاتصالات ومقدمو الخدمات	• الدفاع ضد التهديدات المتقدمة (على سبيل المثال، DDoS) • الحفاظ على أداء الشبكة دون انقطاع • عمليات أمنية مؤتمتة • إدارة السياسة المركزية
الطاقة والمرافق	• تأمين أنظمة التحكم الحيوية • التصدي الفوري لثغرات CVE وهجمات zero-day • الامتثال التنظيمي • الحفاظ على المرونة واستمرارية التشغيل
التعليم والبحث	• حماية الملكية الفكرية والبيانات الحساسة • الوصول المستمر إلى الموارد الرقمية • الاستجابة للتهديدات في الوقت الفعلي • عمليات أمنية مؤتمتة
التصنيع	• بيئات التشغيل الآمنة وتكنولوجيا المعلومات • الحد من الثغرات الأمنية في الوقت الفعلي • حماية الملكية الفكرية • ضمان استمرارية التشغيل

26/02 00-5771857-1110R)