CSPM LP BUILD

Asset: cloud-discovery-exposure-management-EN

ENGLISH

**Every CISO Wants to Know: Where’s the Risk? CDEM Reveals All.**

**Identify rogue assets and reduce risk with Prisma Cloud**

**Is Your Cloud Asset Inventory 100% Accurate?**

It's hard enough to gain visibility and control over managed assets in a cloud environment. But companies also have many shadow cloud assets outside the view of security that are exposed to the internet, giving attackers ample opportunity to exploit weaknesses — before security teams are aware they even exist.

The solution? **Cloud discovery and exposure management.**

Choose wisely, and you can secure your unknown and known cloud assets with a single asset inventory. Our guide to cloud discovery and exposure management explains how. Highlights:

* Where a CDEM delivers the biggest value.
* Identifying rogue cloud and shadow instances you're not tracking.
* Using an outside-looking-in view to compare data with CSPM for a comprehensive survey of exposures.
* Onboarding unmanaged assets, remediating exposure and strengthening cloud security posture for thorough compliance and governance.

Get the details, learn how to use CDEM to find, evaluate and remediate the risks of rogue assets, and take a giant leap forward in enterprise cloud security.

By submitting this form, I understand my personal data will be processed in accordance with [Palo Alto Networks Privacy Policy](https://www.paloaltonetworks.com/legal-notices/privacy) and [Terms of Use](https://www.paloaltonetworks.com/legal-notices/terms-of-use).

<Download>

Asset: cloud-discovery-exposure-management-FR

FRENCH

**À la question que tous les RSSI se posent : quels sont les risques ? Une seule réponse : le CDEM.**

**Identifiez les ressources non autorisées pour réduire votre surface de risque avec Prisma Cloud**

**Votre inventaire des ressources cloud est-il vraiment complet ?**

Assurer une visibilité et un contrôle sur les ressources gérées d’un environnement cloud est une chose. Reprendre la main sur les nombreuses instances de Shadow Cloud passant sous les radars et exposées à Internet en est une autre. D’autant que ces vulnérabilités représentent une véritable aubaine pour les cybercriminels, qui les exploitent avant même que les équipes de sécurité n’en découvrent l’existence.

La solution ? Un **outil CDEM** (Cloud Discovery and Exposure Management).

Choisir la bonne solution CDEM, c'est dresser un inventaire complet de toutes vos ressources cloud connues et inconnues. Notre livre blanc vous dit tout :

* Principaux avantages d’une solution CDEM
* Identification du Shadow Cloud et des instances cloud non autorisées et non gérées
* Vue extérieure de vos environnements cloud pour comparer les données au CSPM et détecter toutes les ressources exposées
* Intégration des ressources non gérées, réduction de la surface d'exposition et renforcement de la posture de sécurité cloud pour une conformité et une gouvernance strictes

Découvrez comment un outil CDEM vous aide à identifier, évaluer et corriger les risques associés aux ressources non autorisées. Vous améliorerez ainsi considérablement la sécurité cloud de votre entreprise.

En soumettant ce formulaire, vous acceptez de fait nos [conditions d'utilisation](https://www.paloaltonetworks.com/legal/terms-of-use.html). Consultez notre [déclaration de confidentialité](https://www.paloaltonetworks.fr/privacy).

<Telecharger>

Asset: cloud-discovery-exposure-management-DE

GERMAN – this needs to be set up as a double opt in for Germany.

**Jeder CISO will wissen, wo Gefahren lauern. CDEM deckt sie auf.**

**Prisma Cloud identifiziert riskante Assets und bannt Gefahren**

**Haben Sie ein zu 100 % korrektes Verzeichnis Ihrer Cloud-Ressourcen?**

In Cloud-Umgebungen ist es schwierig genug, alle verwalteten Assets im Auge und unter Kontrolle zu behalten. In den meisten Unternehmen werden jedoch zusätzlich zahlreiche cloudbasierte Schattenressourcen genutzt, über die die Sicherheitsteams keinen Überblick haben. Diese Assets sind über das Internet zugänglich und bieten Angreifern daher verlockende Gelegenheiten, Schwachstellen auszunutzen – bevor den Sicherheitsteams bewusst wird, dass es sie gibt.

Die Lösung? **Cloud Discovery and Exposure Management (CDEM).**

Wenn Sie die richtige Wahl treffen, können Sie sowohl die Ihnen unbekannten als auch die bekannten Cloud-Assets mit einem einzigen Ressourcenverzeichnis schützen. In unserem Leitfaden zu Cloud Discovery and Exposure Management erfahren Sie, wie. Highlights:

* Wo CDEM den größten Mehrwert bietet.
* Wie Sie nicht konforme Cloud- und Schatten-IT-Instanzen identifizieren, die nicht überwacht werden.
* Wie Sie die Perspektive eines Außenstehenden nutzen und mit den Daten Ihres CSPM vergleichen, um eine umfassende Übersicht über alle potenziellen Einfallstore zu erstellen.
* Wie Sie nicht verwaltete Assets in Ihre Infrastruktur eingliedern, Sicherheitslücken schließen, das Cloud-Sicherheitsniveau anheben und damit zu vorbildlicher Compliance und Governance beitragen.

Informieren Sie sich ausführlich darüber, wie Sie CDEM zur Bewertung und Behebung der mit nicht konformen Assets verbundenen Risiken nutzen und damit die Sicherheit der Cloud-Umgebungen Ihres Unternehmens erheblich verbessern können.

Mit dem Absenden dieses Formulars erklären Sie sich mit unseren [Geschäftsbedingungen](https://www.paloaltonetworks.com/legal/terms-of-use.html) einverstanden. Unsere [Datenschutzerklärung](https://www.paloaltonetworks.de/privacy) anzeigen.

<Jetzt herunterladen>