Tanium Autonomous Endpoint Management (AEM)

Permettre aux organisations d'atténuer efficacement les risques tout en assurant la résilience opérationnelle

SOLUTION BRIEF

Grâce à sa plateforme en temps réel, Tanium AEM exploite de manière sûre et évolutive les informations en temps réel de tous les endpoints gérés dans le cloud Tanium pour recommander et automatiser les modifications sur les endpoints au sein de l'environnement d'un client. Elle permet aux équipes informatiques et de sécurité d'adapter les opérations efficacement et en toute confiance, tout en améliorant la posture de sécurité de l'environnement.

La fréquence accrue des mises à jour du système d'exploitation et des logiciels des fournisseurs, la dérive continue de la configuration sur les endpoints et l'exploitation plus rapide des vulnérabilités par les assaillants rendent difficile pour les équipes informatiques et de sécurité le suivi du rythme et le maintien d'une position sécurisée, résiliente et conforme.

1. L'augmentation des cyberattaques impose un déploiement plus rapide des correctifs, une meilleure conformité de la configuration des appareils et un alignement plus étroit avec les cycles de vie des fournisseurs pour réduire les vulnérabilités.
2. Les équipes informatiques et de sécurité sont surchargées par une maintenance constante de l'environnement, et doivent entreprendre des changements au niveau des endpoints avec une visibilité et une compréhension limitées de l'impact en aval, créant ainsi des risques opérationnels.
3. L'automatisation est intrinsèquement complexe, sa mise en place demande des experts hautement qualifiés et, sans données en temps réel pour l'informer de la durée d'exécution, elle peut fonctionner de manière peu fiable et provoquer des perturbations.

Tanium Autonomous Endpoint Management (AEM) est la prochaine évolution de la plateforme Converged Endpoint Management de Tanium. Tanium AEM débloque une valeur commerciale significative à travers la suite complète de solutions de Tanium, y compris la découverte et l'inventaire des actifs, la gestion des vulnérabilités, la gestion des endpoints, la réponse aux incidents et l'expérience numérique des employés. Tanium AEM exploite les capacités d'IA/ML intégrées à la plateforme pour favoriser une prise de décision plus rapide et de meilleure qualité, ainsi que des résultats commerciaux significatifs pour les clients.

Tanium AEM offre une augmentation significative de l'efficacité opérationnelle grâce à l'automatisation des tâches de routine qui permet aux ressources de se concentrer sur les initiatives de croissance, sans compromettre la sécurité, les performances ou la disponibilité. En outre, grâce à une automatisation fiable et évolutive, AEM améliore la posture de sécurité des clients et accélère l'atténuation des risques en gérant les vulnérabilités et les incidents de manière proactive.

En tirant parti des données en temps réel et de l'analyse des changements sur les endpoints mondiaux gérés dans le cloud, Tanium AEM formule des recommandations et automatise les changements de manière sûre et fiable, garantissant ainsi la santé opérationnelle, tout en réduisant les risques informatiques pour l'entreprise et en améliorant la sécurité de l'environnement informatique.

90 %

La probabilité qu'une vulnérabilité soit exploitée atteint 90 % entre 40 et 60 jours après la découverte

Kenna Security

3x

L'exploitation des vulnérabilités a été multipliée par près de3 (180 %) en 2023

Verizon

93 %

93 % des responsables informatiques indiquent que le manque de compétences du personnel a un impact sur les efforts d'automatisation

CompTIA

Cas d'utilisation de Tanium AEM

Améliorer la disponibilité informatique en évitant les perturbations lors du déploiement des modifications au niveau des endpoints

AEM fournit un score de confiance et des règles d'automatisation ainsi que des logiciels disponibles via la galerie Tanium Deploy. Le score de confiance fournit un contexte en temps réel sur la sécurité d'une mise à jour dans l'environnement du client, sur la base des succès obtenus dans l'univers des endpoints cloud Tanium. Les modifications peuvent ensuite être gérées via des anneaux de déploiement de Tanium AEM qui changent de phase pour s'adapter à la cadence de l'entreprise.

Identifier de manière proactive les risques et les éléments opérationnels pour améliorer la santé opérationnelle et la sécurité de l'environnement

Tanium Guide évalue et analyse globalement l'environnement informatique dynamique d'un client en temps réel pour guider les opérateurs : il leur fournit des recommandations qui les orientent en toute confiance vers la meilleure action à entreprendre et le changement à apporter à leurs endpoints.

Par exemple :

1. Identifier les endpoints dont les signatures Microsoft Defender for Endpoint sont obsolètes et fournir un scénario pour y remédier
2. Identifier les endpoints avec des scores de risque accrus au-delà d'un seuil spécifique

Mettre à l'échelle les opérations informatiques et de sécurité de manière rentable

Tanium Automate peut être utilisé pour capturer l'expertise des opérateurs dans des scénarios réutilisables et reproductibles, avec peu ou pas de code. Ces scénarios peuvent combiner les tâches informatiques et de sécurité de l'ensemble de la plateforme Tanium.

Par exemple :

1. Analyser l'utilisation des logiciels sur tous les endpoints et utilisation de données en temps réel pour identifier les licences les moins utilisées. Informer les utilisateurs que la suppression des logiciels inutilisés est planifiée
2. Les serveurs de correctifs qui sont membres d'un cluster de manière à garantir une haute disponibilité sont maintenus pendant le processus de bout en bout.

Réduire le temps nécessaire pour remédier aux vulnérabilités logicielles avec un impact moindre sur l'entreprise

Le workflow Visibilité de la remédiation passe directement des résultats de conformité au processus de correction pour corriger les vulnérabilités afin d'améliorer la collaboration entre les équipes de sécurité et les équipes des opérations informatiques. Ensemble, ils réduisent les risques sur un ensemble unifié de données, de rapports en temps réel et de flux de travail simplifiés.

Identifier et corriger de manière proactive les risques Zero Day

Tanium Guardian publie la recherche Zero Day qui produit des rapports dynamiques et des conseils sur les situations où l'environnement informatique d'un client est exposé à des problèmes Zero Day. Tanium Guardian fonctionne avec Tanium AEM pour fournir des conseils proactifs sur les implications de la remédiation sur les endpoints afin que le personnel des opérations informatiques et de sécurité puisse évaluer intelligemment l'impact Zero Day sur les opérations commerciales.

Répondre instantanément à toute question concernant les endpoints

Tanium Ask utilise la puissance de l'IA générative pour permettre à tous, de la direction générale aux opérateurs, de poser des questions sur les endpoints qui éclairent les décisions opérationnelles ou commerciales. En utilisant la visibilité en temps réel de Tanium, Tanium Ask fournit à ses utilisateurs des réponses instantanées qui reflètent l'état actuel de leur environnement.

Par exemple :

1. Quel est le temps moyen pour appliquer un correctif à mes appareils ?
2. Y a-t-il aujourd'hui des serveurs qui rencontrent des problèmes de performance ?
3. Quels sont les endpoints qui n'ont pas utilisé Adobe Photoshop ?
4. Quels sont les endpoints auxquels il manque les correctifs critiques qui ont été publiés il y a plus de 30 jours ?

Bases de la plateforme Tanium AEM

Tanium AEM peut analyser instantanément les tendances de sensors, l'impact des changements et les modèles d'utilisation des utilisateurs sur des millions de endpoints afin de générer une intelligence cloud en temps réel qui informe les fonctions autonomes de Tanium.

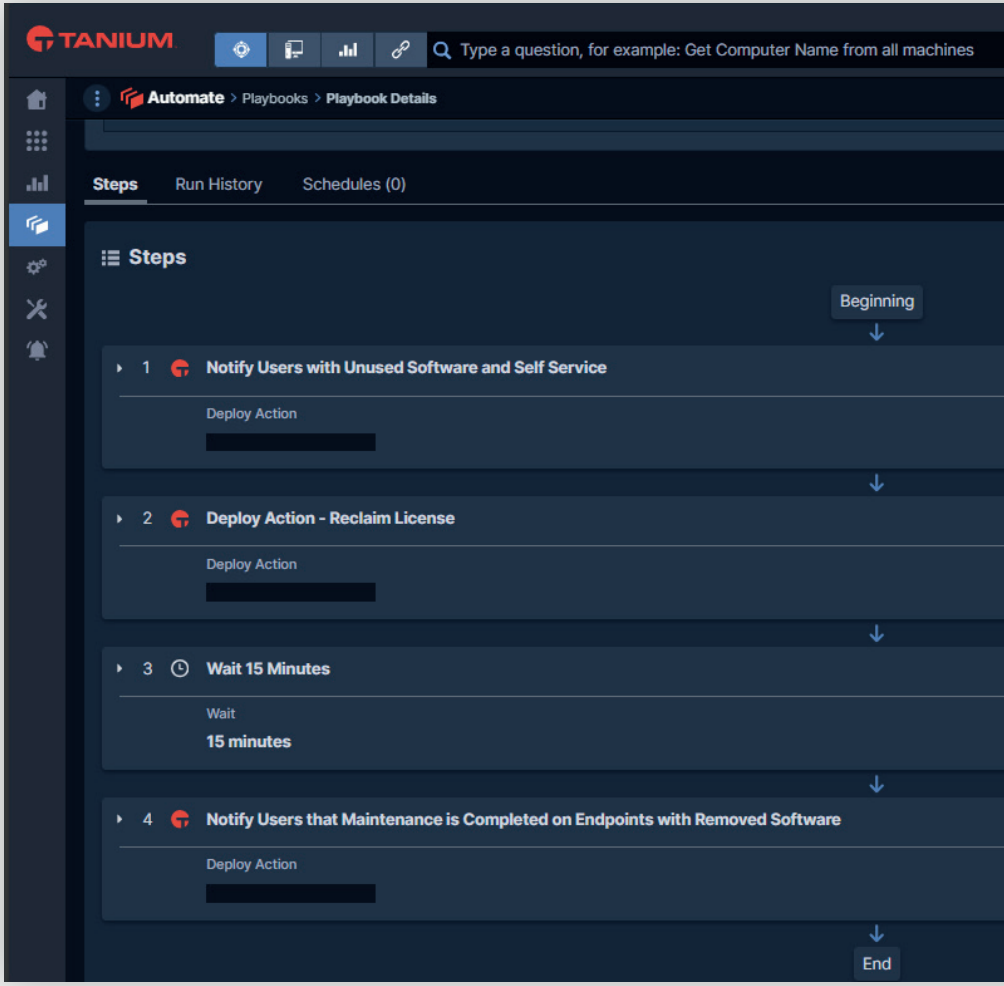
- Tanium utilise une architecture de traitement de flux multi-modèles spéciale à l'échelle du cloud qui peut mélanger différents modèles analytiques et d'IA en fonction des informations nécessaires
- Tanium AEM continue d'améliorer et d'ajuster les idées grâce à l'utilisation de l'intelligence cloud en temps réel, qui s'appuie sur l'évolution des conditions et des technologies informatiques

Étant donné que l'intelligence cloud en temps réel ne s'appuie pas sur l'expérience utilisateur, nous devons utiliser des images qui véhiculent ce concept.

Tanium Automate simplifie l'orchestration et l'automatisation des tâches informatiques et de sécurité, grâce à des données en temps réel et à sa facilité d'action.

Grâce à Tanium Automate, les opérateurs automatisent les tâches complexes à grande vitesse et à grande échelle en remplaçant les processus manuels par une orchestration et une automatisation faciles à implémenter, avec peu ou pas de code.

- Créer des scénarios avec peu ou pas de code pour automatiser les opérations courantes et les tâches de sécurité
- Permettre à un large éventail d'auteurs à différents niveaux de compétences techniques de créer une automatisation puissante
- Définir les critères d'entrée, de sortie et de réussite pour chaque étape avant de passer à la suivante
- Maintenir une visibilité complète des actions, grâce notamment aux journaux d'audit historiques, au statut actuel du manuel et aux calendriers futurs
- Utilisez les API Tanium pour exécuter les scénarios Automate via des outils tels que ServiceNow ou les solutions de sécurité Microsoft

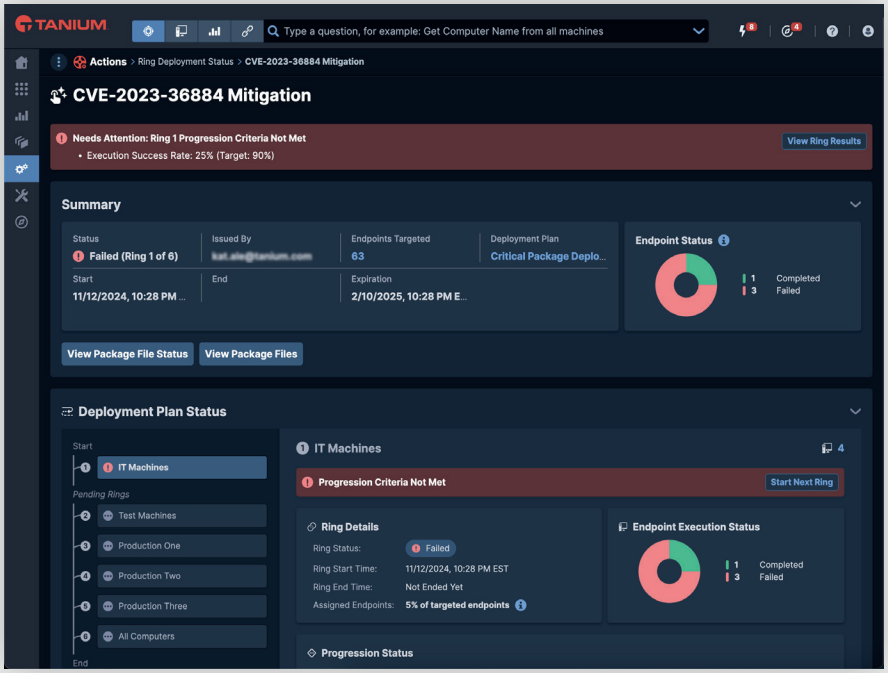


Tanium Automate

Les modèles de déploiement et les anneaux minimisent les perturbations en déployant des changements correspondant au rythme de l'entreprise.

Lorsque des modifications à grande échelle des endpoints sont nécessaires, les modèles de déploiement et les anneaux permettent d'éliminer progressivement les déploiements, en s'assurant qu'ils sont bien gérés et reproductibles.

- Configurer les critères de progression en tirant parti des données en temps réel pour déployer en toute sécurité des changements entre les anneaux
- Tirer parti des plans de déploiement réutilisables pour apporter des changements de manière cohérente
- Créer des plans de déploiement personnalisés adaptés aux différents niveaux de tolérance des risques

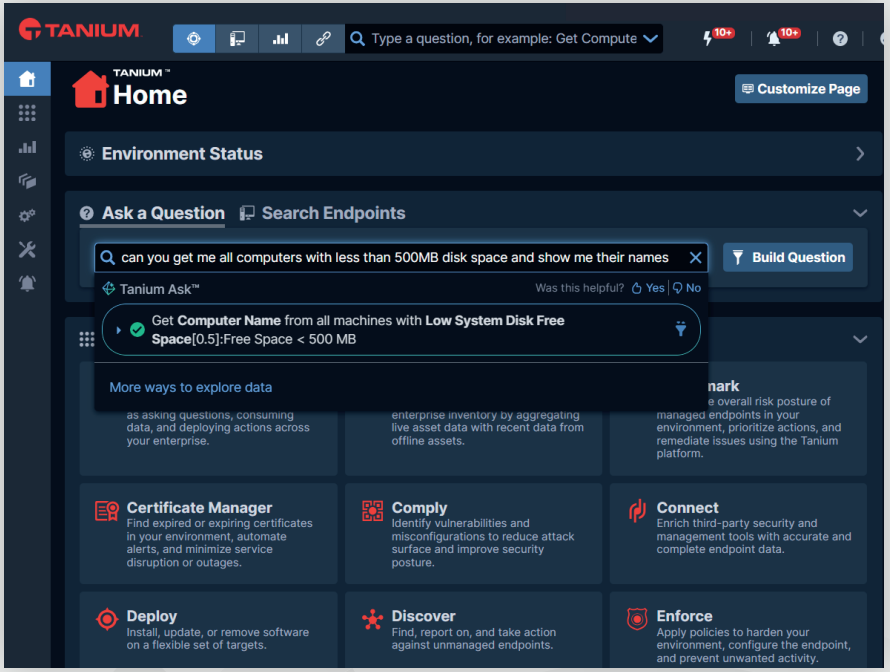


Modèles et anneaux de déploiement

Tanium Ask permet à toute l'équipe d'obtenir des réponses aux questions les plus complexes en matière d'informatique et de sécurité.

Tanium Ask tire parti de l'IA reposant sur les Large Language Models (LLM) pour s'assurer que les opérateurs Tanium à tous les niveaux peuvent poser une question sur leur environnement informatique et obtenir une réponse en utilisant des données en temps réel, quelle que soit la complexité de la question.

- Les opérateurs peuvent poser des questions en langage naturel, en toute simplicité :
  « Quel est le temps moyen pour appliquer un correctif à mes appareils ? »
  « Y a-t-il des serveurs qui rencontrent des problèmes de performance aujourd'hui ? »
  « Quels endpoints ont utilisé Adobe Photoshop ? »
- Affinez davantage vos invites Tanium Ask avec Question Builder de Tanium
- Obtenez des réponses aux questions en temps réel, quelle que soit l'échelle de l'environnement
- Enregistrez vos questions Tanium Ask préférées pour les utiliser à l'avenir



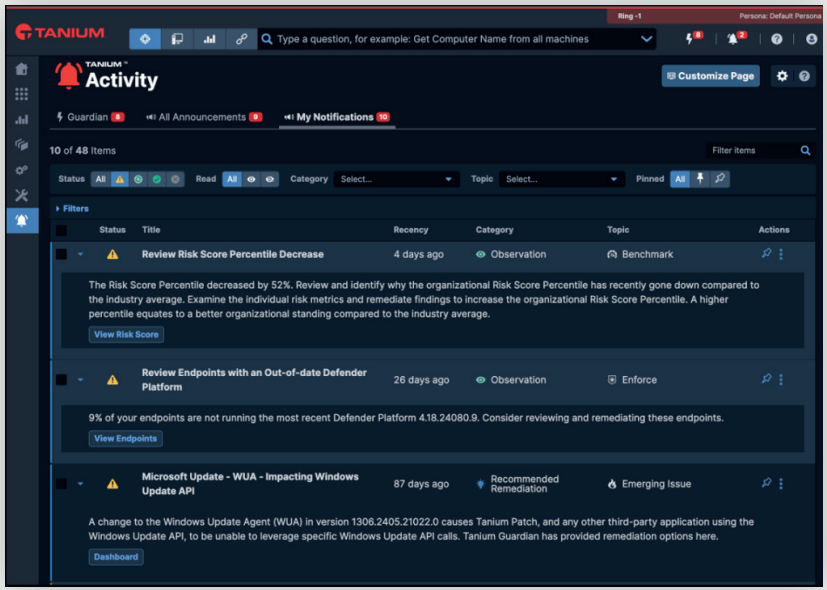
Tanium Ask™

Contrôles autonomes de Tanium AEM

Tanium Guide hiérarchise les tâches des services informatiques et des services de sécurité, ce qui leur permet de prendre les meilleures mesures possibles sur les endpoints.

L'utilisation de l'intelligence cloud en temps réel comme base de Tanium Guide tire parti des benchmarks et de l'analyse en temps réel des environnements informatiques dynamiques mondiaux pour fournir des recommandations opportunes et entièrement exploitables afin de s'assurer que les opérateurs se concentrent toujours sur la mise en œuvre des changements permettant d'améliorer au mieux l'environnement.

- Passer des recommandations de Tanium Guide aux workflows pour implémenter les modifications nécessaires
- Tirer parti des notifications d'observation environnementale pour relier les opérateurs aux workflows d'enquête
- Identifier rapidement les problèmes potentiels sans passer au crible les rapports et les données volumineuses
- Réduire considérablement la probabilité de négliger des questions critiques ou urgentes

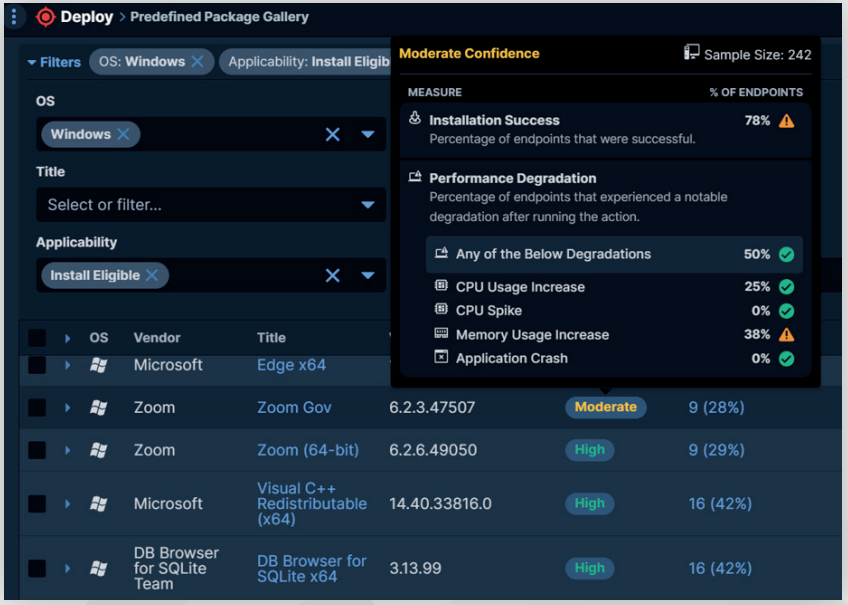


Tanium Guide

Tanium Adaptive Actions permet aux équipes informatiques de réduire considérablement les temps de réponse et de remédiation sur les endpoints critiques.

Les recommandations de Tanium Guide sont liées au composant Adaptive Actions : ce scénario d'automatisation permet l'implémentation de la recommandation elle-même. Les actions adaptatives peuvent s'exécuter sans intervention de l'opérateur, mais peut être entièrement personnalisé et contrôlé selon les besoins.

- Les scores de confiance indiquent la probabilité de réussite d'une action et que celle-ci produise le résultat souhaité
- Déployer des changements dans l'environnement en utilisant une approche progressive, celle des anneaux, pour contenir les problèmes et réduire les risques
- Planifier la progression du déploiement de l'anneau en fonction de critères de réussite préconfigurés
- Garder les humains dans la boucle si nécessaire à des fins de visibilité, de gouvernance et de contrôle

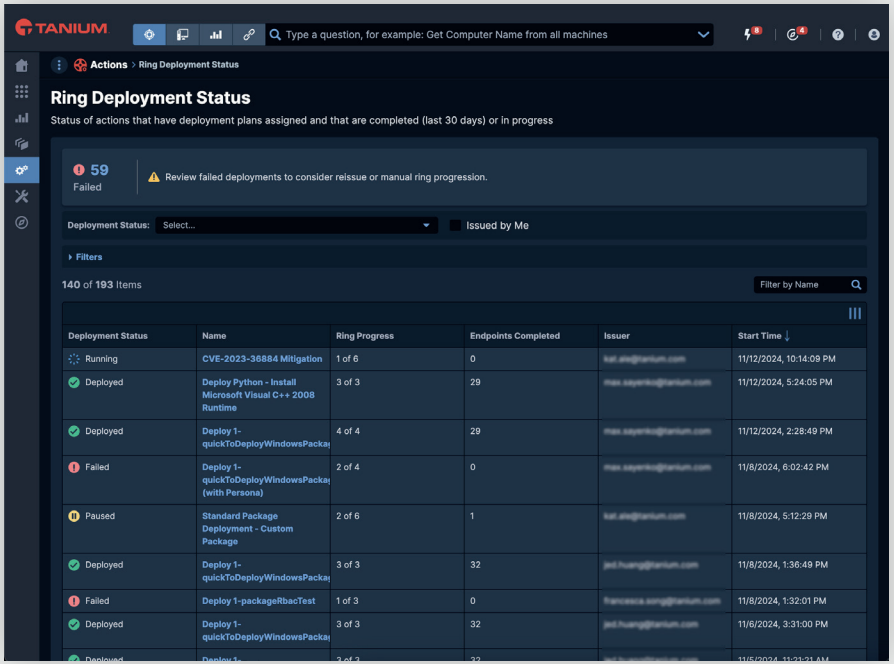


Tanium Adaptive Actions

Tanium Action Oversight offre aux opérateurs un contrôle total avec une gouvernance sur tous les aspects des fonctions autonomes de Tanium.

Tanium AEM donne la priorité à la sécurité. Chaque système est lié au composant de gouvernance centralisée, Tanium Action Oversight. Il offre visibilité, remédiation et contrôle au bon niveau de détail.

- Tenir un registre complet des activités autonomes, notamment des actions passées, en cours ou programmées
- Bénéficier d'une visibilité et d'un contrôle complets sur toutes les activités autonomes en cours (par ex., arrêt ou annulation de la progression)
- Les opérateurs peuvent inspecter l'activité autonome à différents niveaux de granularité, ce qui facilite les activités de diagnostic et de planification
- En cas de problème, une suite complète de fonctions est disponible pour isoler et corriger rapidement et facilement les problèmes selon les besoins

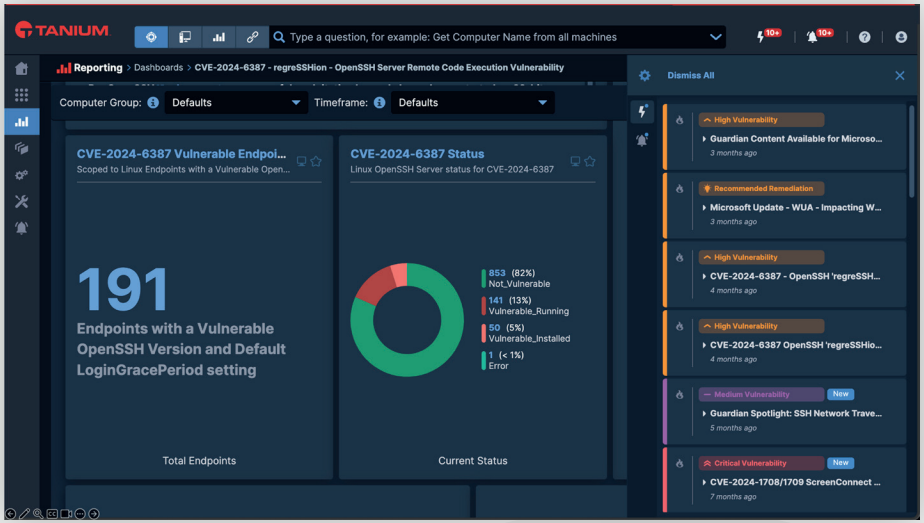


Surveillance des actions de Tanium

Tanium Guardian fournit des alertes, des informations et des remédiations pour répondre rapidement et efficacement aux vulnérabilités zero-day critiques.

En combinant l'analyse globale des endpoints en temps réel et l'intelligence humaine, Tanium Guardian fonctionne comme une voie express spéciale pour les problèmes zero-day ou critiques. Guardian combine rapports, tableaux de bord, analyses et automatisation pour permettre aux opérateurs de résoudre les problèmes avant qu'ils ne perturbent les opérations commerciales.

- Obtenir une visibilité instantanée sur les problèmes critiques et de haute gravité sur vos endpoints qui pourraient exposer votre environnement à des attaques et des exploits
- Profiter d'atténuations et d'automatisations efficaces, ce qui vous permet de prendre immédiatement le contrôle des problèmes émergents
- Corriger les problèmes en toute confiance uniquement sur les endpoints affectés à l'aide de technologies de contrôle autonome telles que les scores de confiance, les actions adaptatives ou les anneaux



Tanium Guardian

« Je recommande vivement d'utiliser Tanium Automate, en particulier aux équipes de sécurité très occupées qui tentent de gagner du temps sur les tâches manuelles et répétitives comme l'application de correctifs. Automate simplifie considérablement l'orchestration de la sécurité et vous permet de gagner d'innombrables heures pour vous concentrer sur le travail de fond ».

David Anderson
Responsable de l'automatisation des correctifs et de la remédiation des vulnérabilités, VFC

Avantages de Tanium AEM

Tanium AEM révolutionne les processus de prise de décision et d'exécution des équipes informatiques et de sécurité, garantissant des changements sûrs et fiables dans leur environnement, à la fois à l'échelle et en temps réel.

Résilience opérationnelle

En déployant des changements à l'aide d'informations issues de l'analyse en temps réel des changements apportés aux endpoints à l'échelle mondiale, combinées à des anneaux de déploiement et à une visibilité sur l'impact en temps réel des changements, les équipes informatiques peuvent éviter des perturbations coûteuses qui ont un impact sur l'activité et la productivité.

Conformité assurée

La surveillance continue, l'analyse comparative du secteur et les contrôles de conformité automatisés garantissent que l'organisation répond aux exigences réglementaires, réduisant ainsi le risque d'amendes et de problèmes juridiques.

Position de sécurité améliorée

L'identification, la hiérarchisation et la remédiation proactives des cyber-risques liés aux vulnérabilités et aux dérives de configuration aident à protéger l'organisation contre les cyber-menaces, en protégeant les données sensibles et en maintenant la confiance des clients.

Mise à l'échelle de l'informatique et de la sécurité

L'automatisation des tâches de routine permet au personnel de se concentrer sur des initiatives stratégiques qui stimulent la croissance de l'entreprise, optimisant ainsi l'utilisation des ressources humaines.

Réduire les coûts de support informatique

La résolution automatique de plusieurs problèmes liés aux endpoints réduit les frais généraux de support informatique et de sécurité, ce qui peut perturber et entraver la productivité des employés.

Agilité informatique accrue

Les processus automatisés et les données en temps réel permettent aux directions informatiques de s'adapter rapidement et de répondre aux besoins commerciaux en constante évolution.

Faire toute la différence

Tanium AEM est une solution révolutionnaire qui établit la norme sur la manière dont une plateforme convergée en temps réel doit fournir une automatisation sûre et fiable pour gérer et sécuriser l'infrastructure informatique. AEM offre à vos équipes d'exploitation et de sécurité informatique les atouts suivants :

- Plateforme convergée offrant visibilité, contrôle et remédiation pour divers besoins en matière d'opérations informatiques et de sécurité
- Observations prioritaires et exploitables à partir de millions de points de données
- Analyse des données en temps réel pour des informations instantanées
- Analyse détaillée de la réussite probable d'une action
- Exécution en toute confiance des changements dans les grands domaines informatiques en temps réel
- Exécution d'une action progressive pour la réduction des risques
- Gouvernance et contrôle lors de toute activité autonome
- Amélioration de l'efficacité opérationnelle grâce à une orientation stratégique

DEMANDEZ VOTRE DÉMO AUJOURD'HUI

Contactez un membre de notre équipe pour voir Tanium à l'œuvre.

Essayer Tanium AEM maintenant →

© Tanium 2025