GUIDE TANIUM

Gestion des endpoints nouvelle génération

Ce guide sert d'introduction à la gestion des endpoints, fournissant une vue d'ensemble de base aux professionnels de l'informatique et de la cybersécurité de tous niveaux. Les prochaines sections traitent des enjeux liés à la gestion des endpoints pour de nombreuses entreprises, puis approfondissent les piliers d'une stratégie efficace et les spécificités de l'approche proposée par Tanium.

Pourquoi toutes les organisations ont besoin de garantir la sécurité des endpoints

Le coût de la cybercriminalité a explosé ces dernières années, les organisations générant de plus grandes quantités de données et devenant de plus en plus dépendantes de leurs environnements numériques. D'après IBM, le coût global d'une violation de données s'élève aujourd'hui à 4,88 millions de dollars, ce qui représente une augmentation annuelle de 10 % et constitue un record historique.[1]

Lorsqu'ils ciblent une entreprise, les acteurs malveillants prennent généralement la voie de la moindre résistance. Les attaques par ingénierie sociale ou hameçonnage visant un utilisateur final sont souvent plus rapides que les tentatives d'intrusion à travers les couches de défense réseau. Les endpoints offrent un accès facile aux bases de données et aux comptes précieux, c'est pourquoi les organisations se doivent de faire des efforts supplémentaires en vue de garantir leur sécurité.

Les attaques informatiques contre les grandes organisations attirent l'attention des médias, mais ce sont surtout les PME qui en sont les principales victimes. Ces organisations ont tendance à avoir des budgets informatiques plus petits et une capacité limitée de surveillance et de remédiation des menaces.

Protéger efficacement les endpoints, c'est permettre à toute organisation, petite ou grande, de minimiser les risques d'attaque, de préserver la confidentialité des données et d'assurer la disponibilité des systèmes.

Une stratégie robuste de sécurité des endpoints peut entraîner les avantages suivants :

Prévention de la perte de données

En améliorant la sécurité des terminaux, les outils spécialisés permettent aux entreprises de mieux protéger leurs données critiques, comme les informations sensibles et la propriété intellectuelle, comme les fuites accidentelles, les malwares ou les attaques par ransomware.

Renforcement de la cyber-défense

En fournissant aux équipes les informations clés pour sécuriser les endpoints, identifier les menaces et y répondre sans délai, les entreprises minimisent à la fois les risques d'attaque et les dommages associés.

Garantie de la continuité des activités

Autre avantage significatif de la sécurité des endpoints : elle protège les endpoints contre les attaques qui pourraient perturber les utilisateurs finaux et les opérations. Si les efforts en matière de sécurité des terminaux portent leurs fruits, les utilisateurs peuvent utiliser leurs appareils sans se soucier des cybermenaces, des attaques de ransomware ni d'autres risques potentiels.

Réduction des coûts de sécurité

De nombreuses organisations attendent d'avoir été victimes d'un incident pour investir dans la cybersécurité. Par conséquent, ils doivent dépenser davantage pour corriger les problèmes et se couvrir contre les menaces. Selon un rapport d'IBM, les entreprises ayant largement recours à l'IA et à l'automatisation en cybersécurité économisent en moyenne 2,22 millions de dollars par rapport à celles qui n'en font pas usage.

Les cinq composants clés de la sécurité des endpoints

Une stratégie complète de sécurité des endpoints doit comprendre au moins cinq composants : découverte, gestion, surveillance, remédiation et automatisation.

1. **Découverte :** Pour protéger efficacement les endpoints, les administrateurs de sécurité doivent savoir qu'ils existent. C'est pourquoi chaque stratégie de sécurité des endpoints doit commencer par l'identification de tous vos endpoints. À ce stade, on procède à une exploration du réseau pour repérer les actifs non maîtrisés, que les équipes de sécurité peuvent soit bloquer, soit intégrer dans leur périmètre de contrôle.

2. **Gestion :** Une fois tous vos terminaux identifiés, leur gestion continue devient plus simple et plus efficace. La gestion des endpoints est essentielle pour soutenir des mesures de sécurité proactives. Assurer la sécurité des endpoints grâce à des correctifs réguliers, des mises à jour, des déploiements logiciels efficaces et des configurations conformes aux standards constitue une barrière solide contre toute tentative d'intrusion.

3. **Surveillance :** Après avoir identifié et contrôlé tous les endpoints, l'étape suivante consiste à établir une surveillance des performances en temps réel. Grâce à la surveillance en temps réel, les administrateurs peuvent identifier plus facilement les activités malveillantes, les violations des politiques de sécurité et d'autres opportunités d'optimiser, et ainsi d'éviter les risques.

4. **Remédiation :** En cas de menace, les organisations doivent pouvoir isoler rapidement les terminaux pour éviter la propagation de malwares ou d'autres processus actifs facilitant l'accès non autorisé à d'autres appareils.

5. **Automatisation :** L'automatisation n'est peut-être pas une fonction traditionnelle de la protection des endpoints, mais elle joue désormais un rôle central dans les stratégies de défense avancées contre les cyber-attaques L'automatisation facilite des opérations clés : détection des nouveaux endpoints sur le réseau, application homogène des politiques de sécurité, réponse en temps réel aux attaques, et remédiation autonome des incidents.

Conseils pour améliorer la sécurité des endpoints

Actifs 24h/24, les endpoints connectés sont répartis sur de vastes zones géographiques et soumis à des normes de sécurité et de contrôle hétérogènes. Compte tenu de cela, la seule façon d'assurer la sécurité des endpoints est de traiter tous les endpoints comme des menaces de sécurité et d'adopter une politique de gestion « toujours active » avec une surveillance, une mise à jour et des correctifs continus. Cette approche peut réduire la surface de menace et l'impact des incidents de cybersécurité.

Les stratégies suivantes sont essentielles pour améliorer la sécurité des endpoints :

Cartographier l'environnement informatique

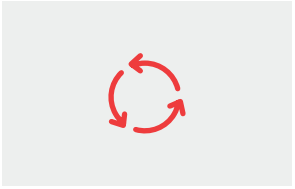
IBM a constaté qu'une violation sur trois impliquait des données « fantômes », qui existent en dehors du périmètre informatique.[6] Les DSI et RSSI doivent avoir une visibilité en temps réel sur l'ensemble des appareils connectés au réseau : leur nombre, leur emplacement, leur propriétaire et leur niveau de mise à jour et de sécurité.

Simplifier l'environnement

Les technologies obsolètes représentent un point d'entrée privilégié pour les cybercriminels, souvent faute de mises à jour ou parce qu'elles ne sont plus activement surveillées. Pour garantir la sécurité des systèmes, les décideurs IT doivent adopter de bonnes pratiques en matière d'hygiène numérique, notamment en éliminant les technologies dépassées.

Éliminer les silos

De nombreuses organisations peinent à gérer des actifs IT répartis dans des silos numériques distincts, chacun piloté par ses propres responsables. La croissance des entreprises ne fait qu'amplifier cette problématique. Mettre fin aux silos et encourager la collaboration entre IT et sécurité renforce la réactivité face aux menaces et améliore la gestion des incidents.



Composants clés de la gestion des endpoints et de la sécurité

La forte homogénéité des outils sur le marché de la gestion des endpoints rend la sélection d'une solution pertinente particulièrement complexe. Cependant, toutes les plateformes n'offrent pas les mêmes outils et fonctionnalités. Comprendre ce qu'il faut rechercher dans une solution de gestion des endpoints vous fera gagner du temps et vous garantira une couverture complète.

Gestion des stocks d'actifs

Les appareils inconnus peuvent constituer une menace directe pour le réseau d'une entreprise. Pour cette raison, le parcours vers une gestion des endpoints efficace commence par l'identification des actifs et l'inventaire.

La gestion des stocks d'actifs implique la découverte, le catalogage et le suivi de tout le matériel et des logiciels au sein d'un réseau d'entreprise. Cela permet aux organisations de détecter plus facilement les vulnérabilités et menaces potentielles.

La gestion des stocks d'actifs doit être un processus continu, avec une analyse et des rapports en temps réel.

Gestion de la configuration

> **Les erreurs de configuration figurent actuellement dans le Top 10 OWASP, l'une des principales références en matière de vulnérabilités pour les professionnels de la cybersécurité.[2]**

Les organisations commettent fréquemment des erreurs de configuration, par manque de temps ou de ressources pour suivre les changements requis.

La gestion de la configuration se concentre sur la définition, l'application et la mise en œuvre de l'état souhaité d'un système sur les systèmes informatiques, les serveurs et les logiciels. Il s'agit aussi d'assurer la maîtrise des systèmes d'information pour renforcer la sécurité et limiter les menaces.

La plupart des systèmes de configuration traditionnels ont été conçus pour des environnements anciens, avant l'ère du cloud, et des infrastructures sur site. Les entreprises d'aujourd'hui ont besoin d'architectures modernes capables d'analyser en permanence les environnements d'endpoints pour détecter les erreurs de configuration ou les conflits de politiques susceptibles d'entraîner des violations.

Déploiement

> **Un logiciel peut offrir une excellente expérience utilisateur, tout en représentant un véritable défi opérationnel pour les équipes IT qui doivent l'administrer à grande échelle.**

Le recours à une solution de gestion des terminaux légère mais puissante permet d'automatiser et d'accélérer la gestion des logiciels à travers toute l'entreprise. La plateforme doit permettre de déployer facilement des ensembles d'applications vers des cibles flexibles, telles que des groupes d'utilisateurs, des sites géographiques ou des services.

Réponse aux incidents

D'après le dernier indice de préparation à la cybersécurité publié par Cisco, les organisations sont de plus en plus exposées aux ransomwares, au vol d'identifiants, aux attaques sur la chaîne d'approvisionnement, à l'ingénierie sociale et au cryptojacking. De plus, **11 % des entreprises prévoient que les cyberattaques liées à l'IA fassent partie des trois principaux risques au cours de l'année à venir.**[3]

Alors que les cybermenaces ne cessent de s'intensifier, les organisations doivent rechercher des moyens de réduire le temps moyen de résolution des incidents de sécurité (MTTR) lorsqu'ils se produisent. L'une des meilleures approches consiste à s'appuyer sur une plateforme de gestion des terminaux dotée de capacités avancées de réponse aux incidents, telles que la détection des menaces en temps réel et l'intégration avec des outils SIEM et EDR. Ce type de fonctionnalité peut aider à passer rapidement de la détection des incidents à la remédiation, et à réduire l'impact d'une attaque.

Gestion des correctifs

> **Le nombre total de vulnérabilités et d'expositions publiées (CVE) devrait augmenter de 25 % cette année, pour un total de 34 888, soit environ 2 900 par mois.**[4]

Le suivi et la correction des vulnérabilités sont nécessaires pour protéger les endpoints et prévenir les incidents de cybersécurité. Il est essentiel de disposer d'une plateforme de gestion des endpoints capable de détecter, de distribuer et d'appliquer automatiquement des mises à jour aux logiciels, systèmes d'exploitation, applications, etc. Cette approche favorise une gestion plus efficace, tout en s'assurant que chaque système bénéficie des correctifs en temps voulu.

Risque et conformité

Aujourd'hui, toutes les organisations doivent assurer la protection des donnéees sensibles contre les acteurs malveillants. En outre, elles doivent rester conformes en respectant les règles régissant l'utilisation des informations et des ressources informatiques. Ces objectifs ne peuvent être atteints que si les organisations ont une visibilité constante sur l'emplacement de leurs données.

Pour gérer les risques et la conformité, les organisations doivent avoir une connaissance complète de tous les endpoints réseau. En outre, elles ont besoin d'alertes en temps réel pour détecter le moment où des appareils ou des utilisateurs non autorisés tentent d'accéder à des ressources privées.

Comment l'automatisation transforme la gestion des endpoints

La plupart des environnements informatiques sont désormais très dynamiques et de plus en plus complexes. Dans le même temps, les services informatiques du monde entier sont confrontés à une pénurie croissante de personnel. **De fait, d'ici 2026, la pénurie mondiale de personnel aura un impact sur 90 % des organisations dans le monde.**[5] Cela signifie que les équipes informatiques et de sécurité sont souvent tenues de relever des défis complexes en matière d'endpoints pour résoudre de nouveaux problèmes opérationnels ou de menaces de sécurité avec une compréhension incomplète de l'impact potentiel et avec un manque d'alignement ou d'expertise nécessaire dans les environnements informatiques qu'elles sont chargées de protéger.

Avec des demandes croissantes et des moyens limités, les systèmes de gestion des endpoints traditionnels, qui manquent d'intelligence intégrée et d'automatisation, montrent leurs limites. Avec des équipes déjà sous pression et des budgets qui n'évoluent pas au rythme des besoins des environnements IT modernes, les équipes IT et sécurité doivent impérativement gagner en efficacité en automatisant les tâches répétitives et chronophages du quotidien.

Les principaux enjeux résolus grâce à la gestion automatisée des endpoints

1. **Complexité croissante :** Les services informatiques sont submergés par le nombre croissant d'endpoints, de systèmes d'exploitation et d'applications. Les systèmes de gestion autonome des endpoints aident à éliminer les charges de gestion et permettent aux organisations de faire plus avec moins.

2. **Menaces croissantes :** L'intensification des cybermenaces exige des mises à jour plus réactives, une gestion rigoureuse des configurations et une synchronisation étroite avec les fournisseurs pour réduire la surface d'exposition. L'automatisation des endpoints permet aux équipes de traiter les vulnérabilités avec plus de rapidité et de précision afin d'éviter les goulots d'étranglement en matière de sécurité.

3. **Workflows manuels :** Le développement et la maintenance de l'automatisation pour les tâches administratives courantes et l'application de politiques et de configurations standards prennent du temps et nécessitent une intégration entre plusieurs outils. La gestion des endpoints automatisée rationalise les tâches administratives.

4. **Risque lié à l'automatisation :** Les systèmes autonomes présentent des risques lorsqu'ils sont mis en œuvre sans contrôles stricts ni normalisation pour garantir la cohérence, la fiabilité et la résilience. Un accès continu à des données en temps réel permet aux équipes de rendre l'automatisation plus fiable, même dans des contextes très changeants, limitant ainsi les problèmes techniques, les interruptions de service et les failles de sécurité.

5. **Goulets d'étranglement en matière de développement :** L'automatisation de workflows impliquant plusieurs solutions ponctuelles peut s'avérer instable et lente, en raison de l'incompatibilité des architectures d'API, des formats de données et des protocoles utilisés. Cette hétérogénéité ralentit fortement le travail des développeurs lorsqu'il s'agit de concevoir des automatisations fiables.

6. **Visibilité limitée :** La fragmentation des solutions métiers limite la visibilité, le contrôle et le suivi granulaires, notamment en raison des silos de données et des processus manuels, ce qui freine le recours à l'automatisation. Pour mettre en œuvre l'automatisation en toute confiance et démontrer le retour sur investissement à la direction, les opérateurs ont besoin d'une gouvernance transparente et de workflows contrôlables pour garantir et signaler les résultats positifs. Cela devient possible grâce à une plateforme robuste d'automatisation des endpoints.

Comment choisir une solution de gestion des endpoints

Les fonctionnalités et les composants ne sont qu'une partie de l'équation lors de la sélection d'une plateforme de gestion des endpoints. Il est également important de prendre en compte le type de solution de gestion des endpoints correspondant le mieux aux besoins et aux objectifs futurs de votre organisation.

De fait, il existe aujourd'hui plusieurs types de plateformes de gestion des endpoints sur le marché offrant différents niveaux de visibilité et de contrôle. Nous allons ici passer en revue certains outils de gestion des endpoints fréquemment utilisés, en comparant clairement leurs bénéfices et leurs faiblesses.

Comparaison des types courants d'outils de gestion des endpoints

Endpoint detection and response (EDR)

Les outils EDR sont conçus pour détecter les menaces connues dans un environnement. L'EDR consiste souvent en des systèmes de suivi des endpoints, recourant à l'heuristique pour repérer les comportements suspects.

Bien que les outils EDR soient utiles pour identifier les menaces entrantes, ils souffrent de certaines limitations. Par exemple, les outils EDR ne peuvent voir que certains types de menaces connues. Par conséquent, les systèmes EDR peuvent créer des angles morts où les acteurs malveillants peuvent se cacher. Pour économiser la bande passante et l'espace disque, les systèmes EDR limitent les types d'activités enregistrées ainsi que la période durant laquelle les données sont archivées.

Avantages d'une solution EDR

- Détecte automatiquement les menaces entrantes
- Peut détecter les anomalies à l'aide d'une analyse comportementale
- S'intègre à des outils de sécurité tiers tels que SIEM

Inconvénients d'une solution EDR

- Assure uniquement le suivi des menaces connues
- Dispose de capacités limitées pour la tenue des registres
- Produit souvent des faux positifs

Détection et réponse étendues (XDR)

Les plateformes XDR utilisent des techniques IA telles que l'apprentissage automatique pour détecter, hiérarchiser et atténuer les menaces entrantes.

En plus d'extraire des données des endpoints, les plateformes XDR recueillent également des informations à partir d'autres outils de sécurité tels que les plateformes SIEM et les solutions de sécurité réseau. Une plateforme XDR surveille l'activité de plusieurs sources pour détecter les problèmes et alerter les professionnels de la cybersécurité.

Avantages d'une plateforme XDR

- Fournit une surveillance complète
- Consolide les données de sécurité de plusieurs endpoints et systèmes
- Réduit le temps de neutralisation des menaces

Inconvénients d'une plateforme XDR

- Peut être complexe à configurer et à interpréter
- Coûteuse à mettre en œuvre et à maintenir
- Nécessite une intégration profonde avec d'autres outils de sécurité

Plateformes de protection des endpoints (EPP)

Les EPP offrent principalement une surveillance, un contrôle et une gestion centralisés de l'activité antivirus. Les organisations utilisent des EPP pour surveiller et gérer les logiciels antivirus sur des endpoints distribués et générer des rapports de sécurité. En plus d'offrir une protection antivirus, certaines plateformes utilisent des technologies telles que l'apprentissage automatique et les passerelles de messagerie pour détecter les anomalies et filtrer le contenu malveillant.

L'un des points faibles des solutions EPP est leur vision limitée aux terminaux et leur manque d'interopérabilité avec d'autres outils de cybersécurité. Par conséquent, les EPP offrent des avantages limités aux équipes de cybersécurité.

Avantages d'une plateforme EPP

- Améliore l'efficacité des antivirus tout en étendant leur champ d'action
- Certaines plateformes sont basées sur le cloud
- Peut aider à limiter les attaques d'ingénierie sociale

Inconvénients d'une plateforme EPP

- Ne s'intègre pas toujours aux autres outils de sécurité
- Peut être complexe
- Offre une détection et une réponse limitées aux menaces

Gestion unifiée des endpoints (UEM)

L'UEM permet aux organisations de gérer les endpoints à partir d'une console unique basée sur le cloud. Cela garantit une gestion fluide et réactive des endpoints, de la mise à jour à la sécurisation. De plus, l'UEM réduit les coûts en consolidant les outils et en rationalisant les processus de gestion.

L'UEM est passée de la gestion des appareils mobiles (MDM) à la gestion de la mobilité d'entreprise (EMM). L'UEM étend les capacités MDM et EMM à d'autres types d'appareils, et permet de surveiller et de contrôler différents systèmes d'exploitation sur des sites distribués.

Avantages de l'UEM

- Offre une surveillance complète des performances
- Réduit la complexité
- Aide à la configuration, aux mises à jour et à l'application des politiques

Inconvénients de l'UEM

- Les solutions UEM traditionnelles manquent de capacités d'automatisation
- Les plateformes UEM ont tendance à manquer de capacités de sécurité avancées
- Peuvent être très gourmand en ressources et nécessiter des ressources informatiques et de stockage importantes

Gestion convergée des endpoints (XEM)

La gestion convergée des endpoints (XEM) réunit les opérations de sécurité et la gestion informatique pour aider à contrôler les environnements informatiques et de sécurité complexes.

Grâce à une interface centralisée, cette solution regroupe les données et outils des endpoints, facilitant la gestion et la prise de décision pour les équipes IT et sécurité.

Avantages

- Centralise la gestion et la sécurité des endpoints
- Automatise les tâches de routine comme les mises à jour et la gestion des correctifs
- Fournit une visibilité en temps réel sur les endpoints

Inconvénients

- Nécessite des experts qualifiés et une formation
- Peut être difficile à mettre en œuvre et à gérer
- Les équipes peinent souvent à tirer pleinement parti de leur potentiel

L'approche de Tanium en matière de gestion des endpoints

De nombreuses organisations gèrent encore les endpoints à l'aide d'outils obsolètes avec des architectures de hub-and-spoke traditionnelles, où chaque hub (ou serveur) doit se connecter à un serveur central et à plusieurs endpoints (spokes). Ces systèmes sont réputés pour leur inefficacité et peinent généralement à dépasser quelques dizaines de milliers d'endpoints, ce qui entraîne des communications lentes, des problèmes de performance, des retards de correctifs et des failles de sécurité.

Grâce à son architecture exclusive en chaîne linéaire, Tanium permet aux terminaux de se relier automatiquement à leurs pairs à proximité, formant une chaîne sécurisée à faible latence, idéale pour une gestion rapide et fiable.

Cette architecture permet une visibilité et un contrôle en temps réel sur chaque endpoint distribué, permettant ainsi aux organisations de découvrir rapidement les actifs, de gérer les inventaires et de résoudre les problèmes de performance. Avec Tanium, les équipes de sécurité et en charge des opérations peuvent déployer automatiquement des correctifs, disposer d'une visibilité réseau approfondie et réduire leur surface de menace globale.

Pourquoi utiliser Tanium Platform pour la gestion des endpoints ?

Dans 9 cas sur 10, une vulnérabilité est exploitée entre 40 et 60 jours après avoir été identifiée. Or, il faut en moyenne entre 60 et 150 jours pour déployer un patch, ce qui donne aux menaces une marge de manœuvre considérable.

> Tanium Platform aide à combler cette lacune en automatisant les mises à jour, en réduisant l'exposition et en renforçant les défenses du réseau.

Voici quelques-unes des façons dont les équipes de sécurité et en charge des opérations peuvent utiliser Tanium :

Réduisez les cyber-risques et les charges de travail administratives grâce à une solution de correctifs évolutive et hautement efficace qui garantit un taux de réussite de 99 %.	Boostez l'efficacité en automatisant entièrement l'application de correctifs et les déploiements de logiciels.	Accélérez jusqu'à 8 fois le provisionnement des endpoints, réduisant ainsi le coût d'imageage et de réimageage des systèmes.	Installez les logiciels en toute sécurité à grande échelle, en gagnant un temps précieux grâce à une galerie d'applications d'entreprise pré-packagée.
Éliminez les silos avec des rapports unifiés sur Windows, Mac et Linux, à partir d'une vue unifiée.	Réaffectez les coûts logiciels des équipements non utilisés.	Obtenez des informations instantanées sur l'environnement réseau global grâce à des données à jour.	TANIUM

Pleins feux sur l'intégration : Microsoft et Tanium

Tanium s'intègre à plusieurs produits Microsoft leaders, notamment CoPilot for Security, Defender for Endpoint, Sentinel, Entra ID et Intune. Grâce aux données instantanées de Tanium, associées aux capacités avancées d'intelligence et d'analyse des menaces de Microsoft, les opérations IT gagnent en efficacité et robustesse à grande échelle. Tanium a obtenu le prix 2024 Microsoft Partner of the Year Award dans la catégorie Innovation des fournisseurs de logiciels indépendants (Independent Software Vendor, ISV) et a été nommé finaliste dans les catégories Microsoft Commercial Marketplace pour les régions Global et Amériques.

> « En utilisant une approche de pointe avec Tanium et Microsoft, nous avons rendu l'orchestration et l'automatisation plus transparentes. »

Dane Thomas
Head of Global Security Engineering, JLL

Pleins feux sur l'intégration : ServiceNow et Tanium

L'intégration étroite de Tanium avec la plateforme d'automatisation intelligente de ServiceNow permet aux organisations d'atteindre une visibilité totale sur leurs actifs, de diminuer les risques et d'améliorer l'expérience des agents, des employés et des clients. Tanium peut se combiner avec ServiceNow pour créer une CMDB complète et précise, répondre aux risques de vulnérabilité et améliorer la conformité globale.

Gartner déclare que « la gestion autonome des endpoints (AEM) représente l'avancée la plus significative en matière de gestion des endpoints depuis plus d'une décennie » dans le rapport 2025 Innovation Insights : Autonomous Endpoint Management, Gartner.

Pour prendre en charge l'AEM Tanium, nous développons plusieurs technologies fondamentales conçues pour être utilisées individuellement par les utilisateurs Tanium ou combinées dans des workflows sur Tanium Platform.

Intelligence cloud en temps réel

Tanium AEM repose sur une intelligence cloud en temps réel qui analyse instantanément les tendances, l'impact et les modèles d'utilisation sur des millions d'endpoints. La solution utilise un système unique de traitement de flux multi-modèles à l'échelle du cloud qui combine divers modèles analytiques et d'IA pour obtenir les informations requises. Tanium AEM affine continuellement ces informations en fonction de l'évolution des conditions et des technologies informatiques.

Tanium Automate

Tanium Automate rationalise l'automatisation des tâches informatiques et de sécurité avec des données en temps réel. La solution permet aux utilisateurs d'automatiser rapidement des tâches complexes en remplaçant les étapes manuelles par des solutions simples no-code ou low-code pour :

- créer des playbooks low-code ou no-code pour les opérations courantes et les tâches de sécurité ;
- permettre à différents niveaux de compétences de créer une automatisation efficace ;
- définir des critères pour chaque étape avant de poursuivre ;
- maintenir une visibilité complète des actions avec les journaux d'audit, le statut en temps réel et la planification ;
- exécuter les scénarios Automate à l'aide d'API Tanium via des outils tels que ServiceNow ou les solutions de sécurité Microsoft ;

Scores de confiance

Les scores de confiance Tanium regroupent des données mondiales en temps réel pour vous aider à évaluer la sécurité et la fiabilité des actions et modifications que vous souhaitez effectuer dans votre environnement.

Real-Time Cloud Intelligence de Tanium analyse les tendances sur de nombreux endpoints, y compris le déploiement de logiciels et de correctifs, pour générer le score de confiance, fournissant ainsi un aperçu précis de l'impact potentiel de vos actions.

Cela vous aide à comprendre la probabilité de réussite lorsque vous envisagez d'apporter des changements à votre environnement et vous permet de hiérarchiser les tâches et de prendre des mesures décisives. Les scores de confiance fournissent les avantages suivants.

- **Précision des données :** Les scores de confiance Tanium évitent les conjectures en fournissant des informations claires et réelles basées sur les résultats des actions précédemment exécutées sur de nombreux endpoints.
- **Prise de décision optimisée :** Offre une base solide pour la prise de décision en fournissant des informations précises et fiables concernant le succès prévu pour une action.
- **Analyse liée aux pairs :** Aide les utilisateurs à évaluer l'impact potentiel des actions de déploiement en s'appuyant sur le contexte unique d'autres environnements.
- **Technologie en attente de brevet :** Utilise une technologie unique et exclusive pour analyser les enregistrements décrivant la réussite et les problèmes des actions de déploiement, ce qui permet de calculer avec précision le score de confiance pour votre environnement.

Modèles de déploiement et anneaux

Lorsqu'il est nécessaire de modifier à grande échelle les endpoints, Tanium AEM exploite les modèles et anneaux de déploiement pour aider à réduire les perturbations en mettant en œuvre des changements alignés sur le flux opérationnel de l'organisation. Cette approche facilite des déploiements par étapes, assurant un contrôle optimal et une exécution répétée avec succès.

Grâce aux modèles et anneaux de déploiement, les organisations peuvent :

- 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 uniforme ;
- créer des plans de déploiement personnalisés adaptés aux différents niveaux de tolérance des risques ;

> **« 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

Les organisations adoptant la gestion autonome des endpoints doivent s'attendre à de nombreux avantages issus d'un environnement plus sécurisé, résilient et conforme.

Résilience opérationnelle

Grâce à une visibilité immédiate sur l'impact des changements et à une approche par phases basée sur des données en temps réel, les équipes informatiques peuvent déployer plus sereinement et limiter les perturbations coûteuses.

Sécurité renforcée et mieux maîtrisée

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

Réduction des coûts de support informatique

En automatisant la résolution des problèmes sur les endpoints, on réduit la surcharge des équipes de support et on limite les interruptions qui nuisent à la productivité des employés.

Garantir la conformité

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

Gestion informatique évolutive

En déléguant les tâches routinières à l'automatisation, les équipes peuvent se concentrer sur des projets à forte valeur ajoutée qui stimulent le développement.

Agilité informatique accrue

Les processus automatisés et les données en temps réel permettent aux services informatiques de s'adapter rapidement et de répondre à des besoins opérationnels en constante évolution.

La gestion des endpoints peut paraître complexe, notamment pour les entreprises distribuées dont l'environnement IT ne cesse de croître. Cependant, obtenir une visibilité et un contrôle en temps réel sur les endpoints est essentiel pour prévenir les incidents de sécurité, limiter la dispersion des ressources IT et réduire les coûts. Et cela est à la portée de toute organisation, quel que soit son budget ou son niveau d'expertise.

Tanium aide les organisations de tous les secteurs à moderniser leurs opérations et à faire l'expérience de la nouvelle génération de gestion autonome des endpoints. Avec Tanium, elles peuvent instantanément exécuter des changements à grande échelle avec plus de rapidité, de confiance et de précision.

Programmez une démo personnalisée en direct pour découvrir comment Tanium peut résoudre les défis de gestion des endpoints de votre organisation.

1 https://www.ibm.com/reports/data-breach
2 https://owasp.org/Top10/
3 https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2024/m03/cybersecurity-readiness-index-2024.html
4 https://www.helpnetsecurity.com/2024/02/26/cve-count-rise-2024/
5 https://www.cio.com/article/2108474/it-staff-shortages-damage-the-bottom-line-idc-report.html

TANIUM

Le pouvoir de la certitude.™

Rendez-nous visite sur www.tanium.fr et suivez-nous sur LinkedIn et X.