Livre blanc commercial

La sécurité en tant que stratégie : intégrer la protection à votre infrastructure

Repenser la sécurité dans un contexte de menaces en constante évolution

Face à la transformation numérique qui remodèle l'entreprise, sa protection doit elle aussi évoluer. Pour se protéger, les responsables informatiques doivent réévaluer leur infrastructure en se demandant non seulement si elle est sécurisée aujourd'hui, mais aussi si elle est capable d'affronter l'avenir.

Dans le même temps, un changement plus vaste est en cours. Dans des environnements de données plus complexes et distribués, l'infrastructure doit évoluer pour soutenir l'innovation, mais aussi pour fournir un socle qui l'accélère et la protège. Dans ce contexte, la sécurité ne se limite pas à la défense. Elle devient une capacité stratégique qui permet aux organisations de se transformer en toute confiance.

En réalité, une grande partie des infrastructures actuelles n'ont pas été conçues pour le mode de fonctionnement actuel des entreprises. Les micrologiciels ne sont pas toujours mis à jour. Les outils de surveillance sont incapables d'atteindre les environnements distants ou edge. De plus, les menaces évoluent à un rythme que les systèmes existants ne peuvent pas suivre. Des risques d'altération lors de la mise hors service aux vulnérabilités cryptographiques introduites par l'informatique quantique, la sécurité des infrastructures est confrontée à de nouvelles pressions.

Un changement crucial dans votre approche peut assurer la réussite future de votre organisation. Abandonnez la défense traditionnelle au profit d'une protection intégrée. La sécurité doit être intégrée à votre socle, ancrée dans le silicium, renforcée tout au long du cycle de vie et réactive aux menaces en temps réel. En déployant une infrastructure adéquate, les organisations peuvent évoluer plus rapidement, réduire les risques opérationnels et se concentrer sur l'essentiel : accélérer un avenir centré sur les données.

Dans cet article, nous explorerons les raisons pour lesquelles la sécurité des infrastructures est devenue une priorité stratégique. Nous verrons également comment remodeler la protection au niveau architectural pour renforcer la résilience, l'innovation et le degré de préparation des organisations tournées vers l'avenir.

Les inconvénients de l'infrastructure héritée

Les environnements d'entreprise actuels sont dynamiques, distribués et gourmands en données. Les déploiements hybrides et edge constituent la norme, et les charges de travail doivent se déplacer rapidement sur un large éventail d'emplacements et de cas d'utilisation.

Travailler dans ces environnements exige une infrastructure capable de fournir une télémétrie en temps réel, de prendre en charge une visibilité à distance cohérente et de réagir automatiquement aux dérives de politique ou aux anomalies du micrologiciel. Mais ce n'est là qu'une partie de l'équation. Les menaces (en particulier au niveau du micrologiciel) évoluent trop rapidement pour être traitées manuellement, sans compter le renforcement des réglementations. NIST, ISO, SEC, RGPD : la conformité dépend désormais de la capacité à appliquer des contrôles au niveau du matériel et à maintenir une visibilité sur l'ensemble de la stack d'infrastructure.

Les systèmes hérités n'ont pas été conçus pour ce niveau de complexité. Les systèmes anciens disposent rarement des fonctionnalités de protection intégrée, d'automatisation et d'intégrité cryptographique nécessaires pour protéger les actifs distants ou répondre aux attentes modernes en matière de sécurité et de conformité. Dans de nombreux cas, les patchs du micrologiciel ne sont pas appliqués, la mise hors service ne fait l'objet d'aucun suivi et l'application des politiques échoue dans les environnements distribués.

Les lacunes des systèmes hérités s'agrandissent :

— **Un micrologiciel non pris en charge** ne peut pas recevoir de correctifs ou de mises à jour, entraînant des vulnérabilités persistantes.

— **Un matériel obsolète** ne dispose pas de protections cryptographiques ou de processus de démarrage sécurisé.

— **Une mise hors service non sécurisée** risque d'exposer des données sensibles ou d'entraîner une réutilisation des appareils à des fins malveillantes.

Quelques indicateurs clés peuvent révéler que votre infrastructure vous met en danger :

À quoi ressemblent les menaces d'aujourd'hui ?

— Implantations de micrologiciels ciblant les actifs edge non gérés

— Informatique quantique faisant sauter le chiffrement traditionnel

— Oublis de correctifs entraînant des vulnérabilités zero-day

— Risques d'altération lors de la mise hors service du serveur

Trois signes qu'il est temps de réévaluer votre infrastructure

1. Vos opérations s'étendent jusqu'à l'edge, mais pas vos outils de surveillance.

Les sites distants, les filiales et les actifs distribués se situent souvent en dehors de la visibilité centralisée. Lorsque le micrologiciel n'est pas mis à jour régulièrement, les risques s'accumulent silencieusement. Les emplacements edge sont particulièrement vulnérables aux altérations physiques et aux dérives de politique, car les équipes informatiques ne peuvent pas toujours être sur place pour détecter les problèmes à un stade précoce.

2. Vos protections s'appliquent au moment de l'exécution.

Si votre infrastructure ne vérifie la sécurité qu'au démarrage ou pendant le fonctionnement, il est peut-être déjà trop tard. La dérive du micrologiciel, l'altération et les mises à jour fantômes peuvent toutes échapper aux défenses traditionnelles. Les attaques modernes ciblent les racines du micrologiciel et du matériel que les protections traditionnelles appliquées au niveau du système d'exploitation sont incapables de voir. Si l'architecture est laissée sans protection, vous risquez de ne pas détecter une violation avant d'en subir les conséquences.

3. Votre matériel a plus d'une ou deux générations de retard.

Le matériel hérité peut ne pas prendre en charge les outils de gestion, l'automatisation des politiques ou la cryptographie résistante aux attaques quantiques nécessaires dans les environnements actuels. Les équipes informatiques constatent de plus en plus que les infrastructures vieillissantes deviennent incompatibles avec la sécurité proactive. Cette situation limite les capacités d'automatisation, d'analyse et de conformité lorsqu'elles sont nécessaires.

Pour se prémunir contre ces risques, les équipes informatiques ont besoin d'une infrastructure conçue pour la résilience dès le premier jour.

Protéger chaque phase du cycle de vie du serveur

Face à des menaces de plus en plus sophistiquées, la protection des charges de travail implique de protéger l'ensemble du cycle de vie du serveur : validation de la chaîne logistique, authentification du micrologiciel, surveillance de l'exécution et mise hors service sécurisée.

La sécurité doit commencer avant même l'installation du serveur et se terminer à la toute fin de la mise hors service.

Les modèles hérités ont tendance à traiter la sécurité comme un point de contrôle, en vérifiant l'identité au démarrage ou en recherchant des anomalies au moment de l'exécution. Néanmoins, ces défenses ponctuelles exposent l'infrastructure lors des phases critiques du cycle de vie. Les attaquants exploitent davantage les failles introduites au préalable, notamment via l'altération pendant le transport, et ultérieurement, par exemple en cas de suppression inadéquate des données en fin de vie.

Une approche englobant le cycle de vie de la sécurité de l'infrastructure devient essentielle pour réduire les risques dans les environnements distribués actuels. Aussi, il convient de sélectionner une infrastructure :

— **Fondée sur la confiance :** authentification au niveau matériel intégrée au niveau du silicium

— **Actualisable :** validation cryptographique du micrologiciel tout au long du cycle de vie, empêchant ainsi le redéploiement ou les mises à jour fantômes

— **Sécurisée jusqu'au bout :** outils de mise hors service sécurisés qui effacent les données, vérifient la suppression et génèrent des rapports vérifiables

Grâce aux protections intégrées à la plateforme, l'infrastructure devient plus résiliente et moins dépendante des interventions réactives.

Cette approche prend en compte les points faibles de plus en plus ciblés par les attaquants, et garantit aux organisations que leur infrastructure reste sécurisée du début à la fin.

À quoi ressemble la sécurité du cycle de vie dans la pratique ?

— **Approvisionnement :** vérifier l'intégrité du micrologiciel avant l'arrivée du matériel pour éviter toute altération dans la chaîne logistique ou pendant l'expédition

— **Provisionnement :** automatiser le démarrage sécurisé et appliquer les politiques de sécurité dès le départ

— **Exploitation :** surveiller en permanence les dérives du micrologiciel, les modifications non autorisées ou les anomalies

— **Mise hors service :** effacer les données de manière cryptographique et confirmer leur suppression avec des rapports vérifiables

La visibilité et le contrôle réduisent les risques cachés

Pour que la sécurité soit gérable (notamment dans les environnements distribués), elle ne doit pas seulement être puissante, elle doit aussi être claire. Les équipes informatiques ont besoin d'informations en temps réel sur la configuration de l'infrastructure, les écarts par rapport à la politique et les lacunes potentielles existantes, avant que ces dernières ne soient exploitées.

Sans cette visibilité cohérente, les menaces peuvent se dissimuler dans des micrologiciels obsolètes ou des actifs mal configurés, en particulier dans les emplacements hybrides et edge. Le suivi manuel et la surveillance cloisonnée ne suffisent plus à assurer la sécurité des infrastructures modernes.

C'est pourquoi une approche plus poussée de la visibilité et du contrôle est en train d'émerger. Les responsables informatiques recherchent des outils pour :

— Signaler les micrologiciels obsolètes et détecter les versions non conformes en temps réel

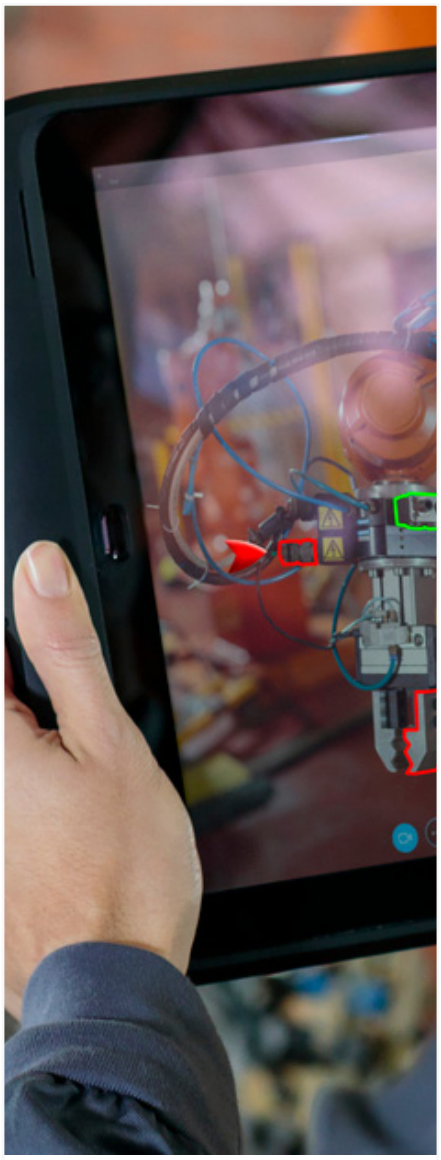
— Automatiser l'application des politiques sur l'ensemble des parcs de serveurs

— Prendre en charge l'accès à distance pour une sécurité cohérente à l'edge

— Protéger les opérations sensibles grâce à une isolation matérielle

— Se préparer aux menaces futures grâce à un chiffrement résistant aux technologies quantiques

Ensemble, ces fonctionnalités contribuent à combler les lacunes et à réduire les risques cachés sans alourdir le fardeau opérationnel.



L'importance de la visibilité dans les environnements complexes

Lorsque l'infrastructure comprend des datacenters sur site, des plateformes cloud et des sites distants, une visibilité limitée augmente le risque d'oublis de mises à jour ou de correctifs incohérents, qui sont des points d'entrée courants pour les attaquants. Les outils proposant une télémétrie intégrée, des tableaux de bord centralisés et une application automatisée des politiques aident les équipes informatiques à obtenir une vue plus complète de leur environnement et à réduire de manière proactive l'exposition aux menaces en constante évolution.

La sécurité intégrée stimule l'innovation

Une sécurité intégrée discrètement en arrière-plan fait bien plus que réduire les risques. Elle peut aider les organisations à évoluer plus rapidement, à prendre des décisions plus éclairées et à libérer des ressources pour se concentrer sur l'avenir.

Face à des menaces plus complexes et à des environnements plus distribués, la protection intégrée permet aux équipes informatiques de passer d'une stratégie de défense basée sur l'exécution à une protection continue basée sur le cycle de vie, qui évolue avec l'infrastructure. Au lieu de se démener pour patcher des micrologiciels obsolètes ou corriger les erreurs de configuration, les équipes peuvent se concentrer sur l'ajustement des performances, les projets innovants et les améliorations de l'architecture à long terme.

Avantages de la protection intégrée

— Moins de cycles de patchs urgents
— Risque de temps d'arrêt réduit
— Préparation facilitée pour les audits
— Déploiement plus rapide avec moins d'erreurs de configuration
— Focalisation des équipes sur les projets stratégiques

La sécurité intégrée évite les problèmes et accélère le potentiel. En consacrant moins de temps à la conformité, aux audits et à la gestion des correctifs, les équipes peuvent réinvestir dans des projets de transformation, des initiatives de données et des fonctionnalités pérennes qui font avancer l'entreprise.

HPE intègre la protection de la puce jusqu'au cloud

Une fois les exigences de sécurité de l'infrastructure prises en compte, l'étape suivante consiste à évaluer les performances des différentes plateformes. HPE propose une approche différenciée, offrant une protection du silicium au cloud via les serveurs HPE ProLiant Compute Gen12 et HPE Integrated Lights-Out (iLO). La sécurité étant intégrée à chaque niveau de la stack et à chaque étape du cycle de vie, les organisations peuvent réduire les risques sans ralentir leur transformation.

Avec HPE ProLiant Compute Gen12 et HPE iLO 7, les clients bénéficient de plusieurs avantages :

Silicon Root of Trust de HPE : micrologiciel directement lié au matériel pour établir l'authenticité dès le départ

Automatisation du cycle de vie guidée par l'IA : la gestion intelligente de l'infrastructure détecte les anomalies, applique les politiques et rationalise les mises à jour dans l'ensemble de l'environnement

Visibilité centralisée : tableaux de bord en temps réel et vues de conformité pour les audits

Contrôle de l'edge au cœur : gestion à distance sécurisée pour les opérations hybrides et distribuées

Enclave sécurisée intégrée : la seule enclave intégrée au serveur du secteur isole les opérations critiques au niveau du matériel, offrant ainsi une protection renforcée contre les menaces au niveau du micrologiciel

Préparation quantique : protections cryptographiques conçues pour répondre aux normes futures

Mise hors service sécurisée : outils intégrés pour effacer les données de manière cryptographique et vérifier leur retrait

Tableau 1. Tableau comparatif des architectures

Domaine	Approche traditionnelle	Approche intégrée HPE
Sécurité de la chaîne logistique	Processus dépendant du fournisseur	Usine de confiance avec validation cryptographique
Protection du micrologiciel	Validation de l'exécution uniquement	Silicon Root of Trust avec micrologiciel immuable
Gestion à distance	Outils manuels, politiques variées	HPE iLO 7 avec contrôle centralisé des politiques
Visibilité du cycle de vie	Journaux incomplets, outils cloisonnés	Tableau de bord de bout en bout et vue sur la conformité
Mise hors service sécurisée	Effacement manuel, lacunes des audits	Outils d'effacement sécurisé intégrés avec vérification
Préparation quantique	Non traitée	Cryptographie post-quantique intégrée dès le matériel

Questions à poser lors de votre prochaine évaluation

— La plateforme prend-elle en charge l'intégrité complète du cycle de vie du micrologiciel ?

— Peut-elle automatiser l'application des politiques dans les environnements hybrides ?

— Est-elle équipée pour la cryptographie post-quantique ?

— À quel point son architecture d'accès et de gestion à distance est-elle robuste ?

Structurer l'appel d'offres

Incluez des critères d'évaluation allant au-delà des protections au moment de l'exécution. Demandez aux fournisseurs comment ils gèrent l'intégrité du cycle de vie du micrologiciel, la préparation quantique et le provisionnement sécurisé. Objectif : une sécurité prête pour l'avenir qui commence au niveau du silicium et s'étend à l'ensemble de l'architecture.

Protégez votre avenir avec une infrastructure résiliente et prête pour l'avenir

Nous sommes à l'aube d'une nouvelle ère commerciale. L'intégration de l'IA, les opérations hybrides, les obligations de conformité accrues et l'augmentation des menaces pesant sur les micrologiciels redéfinissent l'infrastructure sécurisée. Les organisations prêtes pour l'avenir ont besoin d'une architecture résiliente par nature et sécurisée par défaut.

La sécurité moderne nécessite plus qu'une simple protection des processus d'exécution. Elle exige une approche du cycle de vie qui commence par une chaîne logistique fiable, inclut une validation continue du micrologiciel et prend en charge la mise hors service sécurisée en fin de vie. Face à des environnements informatiques plus distribués et à des menaces plus sophistiquées, les organisations ont besoin de défenses intégrées qui comblent les lacunes de visibilité, réduisent le nombre de tâches manuelles et aident les équipes à se concentrer sur l'innovation et les objectifs à long terme.

Les serveurs HPE ProLiant Compute Gen12 avec HPE iLO 7 offrent une protection non pas « ajoutée », mais véritablement intégrée. De la Silicon Root of Trust de HPE à l'architecture d'enclave sécurisée, ces solutions intègrent des protections qui s'adaptent à votre infrastructure et réduisent la complexité de la stack.

Avec HPE à vos côtés, vous pouvez :

— Moderniser en toute sécurité les environnements hybrides et edge

— Réduire les risques opérationnels et de conformité grâce à une protection intégrée

— Libérer des ressources informatiques pour l'innovation et la croissance à long terme

Les risques du statu quo

L'infrastructure héritée peut sembler plus abordable au premier abord. Cependant, celle-ci cache des coûts qui s'accumulent rapidement : correctifs manuels, audits ratés, réaction face aux violations ou encore temps d'arrêt. Investir dans une infrastructure sécurisée et basée sur le cycle de vie transforme la protection en un avantage stratégique. Grâce à des innovations telles que la gestion pilotée par l'IA et la seule enclave sécurisée intégrée du secteur, HPE aide les organisations à se moderniser en toute confiance et à préparer leur avenir.

En savoir plus

HPE.com/iLO

HPE.com/ProLiant

Visiter HPE.com

Live Chat

a50013491FRE

HEWLETT PACKARD ENTERPRISE

hpe.com