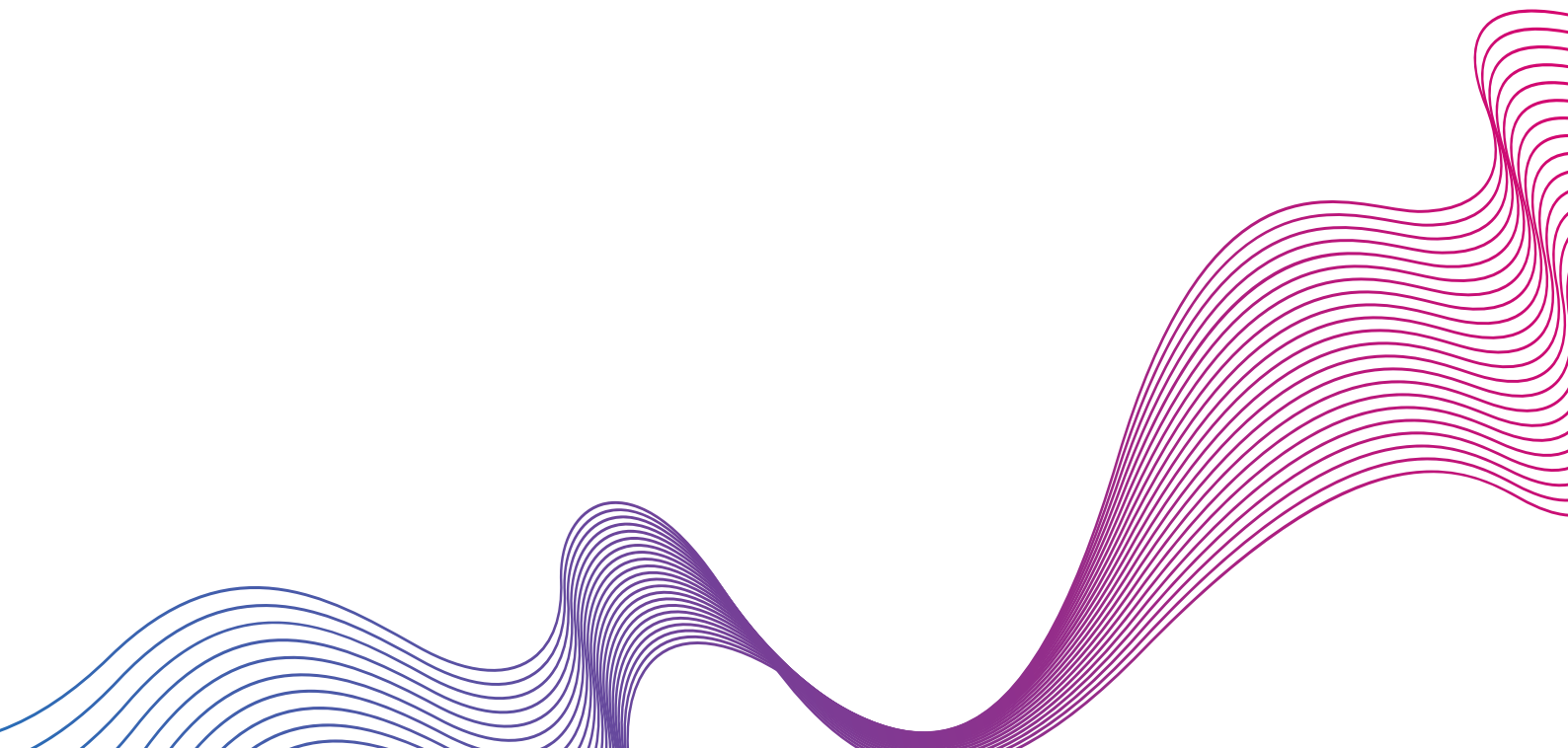


5 impératifs

pour une architecture
de sécurité adaptative

TABLE DE MATIÈRES

Introduction	1
Qu'est-ce qu'une architecture de sécurité adaptative ?	2
Composants d'une architecture de sécurité adaptative	3
Les quatre étapes de l'architecture de sécurité adaptative de Gartner	4
Objectifs d'une ASA	5
Les challenges rencontrés par les organisations et comment les surmonter avec une ASA	6
Déterminer ce qui doit être protégé	8
5 éléments clés à prendre en compte lors de la mise en œuvre d'une ASA	9
Mise en œuvre d'une ASA avec l'aide d'AD360	12
15 capacités essentielles IAM recommandées par Gartner dans AD360	13



INTRODUCTION

LE MONDE DE LA CYBERSÉCURITÉ ÉVOLUE RAPIDEMENT.

De nouveaux défis apparaissent alors que les anciennes méthodes de protection des réseaux et des données ne suffisent plus. Le paysage des menaces évolue chaque minute, et les adversaires deviennent chaque jour plus sophistiqués. Les équipes de sécurité informatique ne peuvent plus se concentrer sur la surveillance des seuls terminaux, mais doivent adopter une approche plus intégrée et proactive de la sécurité pour rester efficaces dans les années à venir.

L'architecture de sécurité adaptative (ASA) a gagné en popularité ces dernières années à mesure que la nécessité d'une nouvelle approche de la cybersécurité devenait plus évidente. Dans cet e-book, nous allons découvrir ce qu'est une ASA et pourquoi vous devriez envisager de la mettre en œuvre dans le cadre de votre stratégie de défense à l'avenir.

QU'EST-CE QU'UNE ARCHITECTURE DE SÉCURITÉ ADAPTATIVE ?

ASA est un modèle de sécurité qui met l'accent sur la nécessité d'une évolution constante de la sécurité pour faire face à l'évolution des menaces.

Il est conçu pour être flexible et adaptable afin de pouvoir répondre rapidement aux nouvelles menaces dès leur apparition. Une ASA s'appuie sur une variété de contrôles de sécurité, tels que des pare-feu, des systèmes de détection et de prévention des intrusions et des logiciels anti-malware. Elle implique un certain nombre de mesures proactives, telles que des audits de sécurité réguliers et des évaluations de vulnérabilité.

L'ASA permet une surveillance en temps réel et des réponses rapides aux problèmes de sécurité, garantissant ainsi que les organisations offrent à leurs clients et employés une tranquillité d'esprit en matière de protection des données.

De nombreuses équipes de sécurité informatique se concentrent sur la prévention des cyberattaques et ont tendance à adopter la mentalité de réponse aux incidents au lieu de la mentalité de réponse continue qu'une ASA favorise. Quelle est la différence entre la réponse aux incidents et la réponse continue ? Les deux se ressemblent, mais il existe en fait des distinctions essentielles.

Voici un aperçu de chacune d'elles :

- ✔ La réponse aux incidents est généralement initiée en réponse à un événement ou une menace spécifique. Il s'agit d'une approche plus réactive qui est adoptée lorsque quelque chose s'est déjà produite. L'objectif est de limiter les dégâts et de minimiser l'impact de l'incident.
- ✔ La réponse continue est une approche proactive adoptée sur une base permanente. Il s'agit de surveiller constamment vos systèmes et d'être prêt à répondre aux incidents avant qu'ils ne se produisent. L'objectif est d'empêcher les incidents de se produire en premier lieu, ou du moins de minimiser leur impact s'ils se produisent.

De nombreuses organisations doivent passer de la réponse aux incidents à la réponse continue. Grâce à cette évolution, les systèmes de défense de la sécurité peuvent anticiper et surveiller les menaces existantes et potentielles, fournir un retour d'information en temps réel et ajuster rapidement les politiques de sécurité existantes pour sécuriser les réseaux d'une organisation. Bien que ces actions soient toujours nécessaires, les équipes de sécurité devraient adopter des plates-formes de sécurité adaptatives, capables de s'adapter aux menaces émergentes et d'employer des défenses et des mécanismes de réponse dynamiques. Les stratégies de cyberattaque devenant de plus en plus sophistiquées grâce à l'automatisation et à d'autres tactiques, les organisations doivent adapter leurs méthodes pour y faire face.

COMPOSANTS D'UNE ARCHITECTURE DE SÉCURITÉ ADAPTATIVE

Il y a quatre composants clés de
architecture de sécurité adaptative



Visibilité

La capacité de voir ce qui se passe dans le réseau et d'identifier les menaces potentielles. Cela peut se faire grâce à des outils comme la surveillance du réseau et les systèmes de détection des tentatives d'intrusion.



Automatisation

La capacité de prendre des mesures sur la base des informations fournies par le composant de renseignement. Il peut s'agir de bloquer automatiquement les adresses IP connues pour être associées à des attaques ou de placer en quarantaine les fichiers contenant des logiciels malveillants.



Intelligence

La capacité de comprendre ce que les données des outils de visibilité nous indiquent. Cela nécessite des analystes capables d'interpréter les données et de déterminer ce qu'elles signifient en termes de menaces pour la sécurité.



Réponse

La capacité à réagir rapidement aux incidents lorsqu'ils se produisent. Cela implique de disposer d'un plan pour faire face à une attaque et d'être capable d'exécuter ce plan rapidement et efficacement.

LES QUATRE ÉTAPES DE L'ARCHITECTURE DE SÉCURITÉ ADAPTATIVE DE GARTNER

L'architecture de sécurité adaptative de Gartner est un cadre que les organisations peuvent utiliser pour concevoir et mettre en œuvre leurs stratégies de sécurité. Ce cadre repose sur le principe de la "défense en profondeur", une stratégie de sécurité qui s'appuie sur de nombreuses mesures de sécurité pour protéger les actifs d'une organisation contre les cyberattaques. L'architecture de sécurité adaptative de Gartner met l'accent sur la rapidité et l'agilité et est conçue pour fournir aux organisations une approche flexible et évolutive de la sécurité.

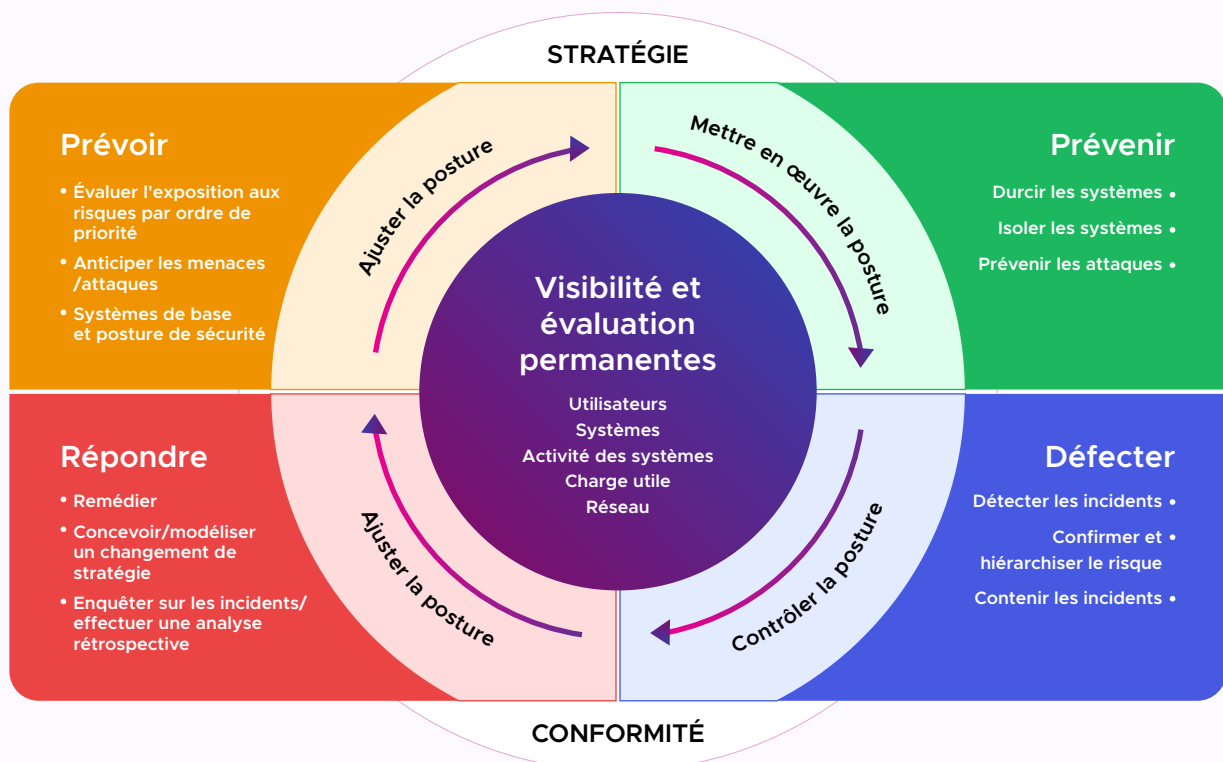
Gartner recommande une approche en quatre phases:

1. Détecter: Les équipes de sécurité doivent avoir une visibilité sur tous les aspects de l'environnement informatique afin d'identifier les menaces potentielles.

2. Réagir: Une fois qu'une menace a été identifiée, les équipes de sécurité doivent être en mesure d'évaluer rapidement l'impact et de prendre les mesures appropriées pour atténuer le risque.

3. Prévoir: Les équipes de sécurité doivent anticiper les menaces futures de manière proactive et prendre des mesures pour les empêcher de se produire en premier lieu.

4. Prévenir: En cas d'attaque réussie, les équipes de sécurité doivent être en mesure de durcir et d'isoler les systèmes afin de prévenir les failles de sécurité, de rétablir rapidement les opérations et de minimiser l'impact sur l'entreprise.



OBJECTIFS D'UNE ASA



1. Renforcer la sécurité:

Fournir un niveau élevé de sécurité pour les informations et les systèmes qui sont critiques pour l'organisation.



2. Adaptabilité:

Être capable de s'adapter rapidement à l'évolution des menaces et des vulnérabilités en matière de sécurité.



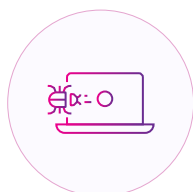
3. Réduire la propagation des menaces:

Limiter la propagation potentielle ou les mouvements latéraux d'une menace au sein d'un réseau.



4. Diminuer la vitesse de l'attaque:

Réduire la vitesse de l'attaque lorsque plusieurs assauts sont en cours.



5. Réduire la surface d'attaque:

Pour rendre la cible d'une attaque plus petite.



6. Réponse en temps réel:

Pouvoir réagir rapidement et facilement aux nouvelles menaces et vulnérabilités en matière de sécurité.

LES CHALLENGES RENCONTRÉS PAR LES ORGANISATIONS ET COMMENT LES SURMONTER AVEC UNE ASA

Les organisations doivent relever le défi de découvrir les menaces dès qu'elles se présentent, de remédier rapidement aux vulnérabilités et d'améliorer en permanence leur dispositif de sécurité, tout en protégeant les données critiques et leurs activités.

Les organisations ont besoin d'un accès sécurisé aux données sensibles et confidentielles, tout en améliorant leur capacité à analyser les données de sécurité et à identifier les attaques au moment où elles se produisent. Avec l'adoption rapide de l'IoT, du big data et de l'analytique, les risques de sécurité augmentent, ce qui entraîne le besoin de nouvelles stratégies au-delà de l'approche traditionnelle de la sécurité.

En adoptant la stratégie consistant à prévoir une menace avant qu'elle ne se produise, les équipes de sécurité informatique peuvent protéger les données de leur organisation, bien avant que les dommages ne soient causés. L'intention derrière l'utilisation d'une approche de conception de sécurité réactive est d'anticiper les menaces avant qu'elles ne se produisent. Contrairement aux approches classiques, le modèle de réponse adaptative intègre les alertes et les informations sur les menaces provenant de plusieurs domaines et technologies de sécurité.

Une ASA intègre les données de votre entreprise dans diverses mesures de sécurité, comme l'anticipation des menaces et la protection complète du réseau et des terminaux. Il permet de suivre les cybercriminels, de construire et d'améliorer un cadre de sécurité en fonction de l'état actuel du paysage des menaces, et d'éviter des pertes massives aux entreprises.

Une ASA est un ensemble de tactiques intégrées qui aide les organisations à garder une longueur d'avance sur les cybercriminels, en déclenchant des mesures de sécurité agiles qui sécurisent les données et les systèmes aussi rapidement que possible, au lieu de s'appuyer sur des stratégies de sécurité périmétrique héritées. Idéalement, l'architecture de sécurité la plus réalisable aide à construire un système de cybersécurité qui s'adapte en permanence aux défis changeants du monde numérique. Votre ASA apprend de manière autonome des succès et des échecs précédents afin d'atteindre des taux de réussite plus élevés en termes de protection et de détection des données.

Si les systèmes SIEM traditionnels seront toujours nécessaires pour gérer la détection des menaces en temps réel, les entreprises doivent commencer à inclure des systèmes axés sur l'intelligence spécifique au domaine produite par une ASA. Les innovations, telles que les algorithmes d'intelligence artificielle, peuvent aider les produits de cybersécurité à être plus adaptatifs et à apprendre lorsque des données et des modèles de comportement des systèmes sont identifiés. La sécurité axée sur l'analyse peut aider les organisations à s'adapter aux menaces plus rapidement et à y réagir.

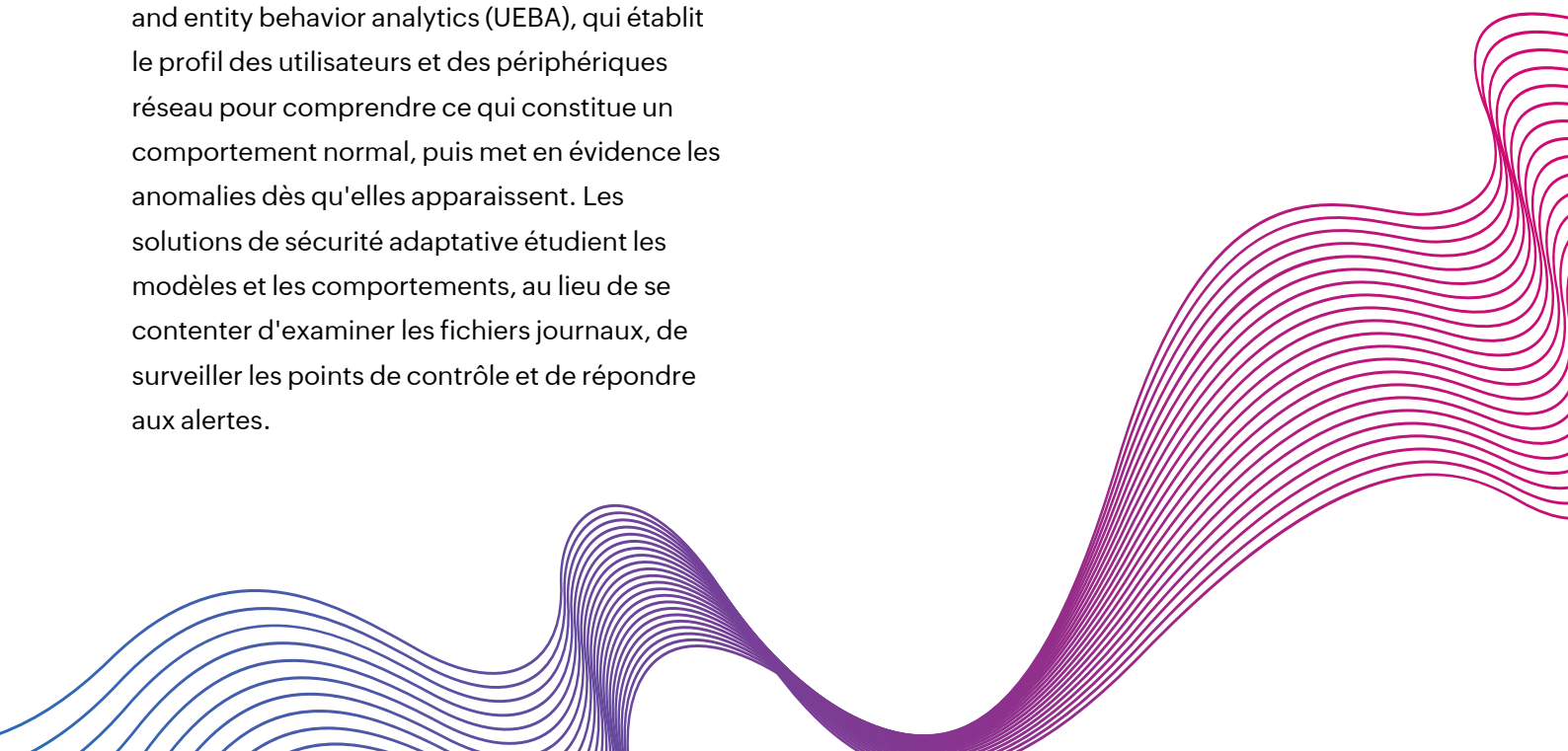
Les ASA identifient les méthodes et techniques utilisées par les cybercriminels et, à leur tour, exploitent ces informations pour prévenir les attaques.

L'analyse avancée permet d'identifier les failles de sécurité qui ne sont pas apparentes lors de la surveillance d'un système par vos propres moyens. Elle permet de découvrir des schémas permanents dans le comportement des utilisateurs, des anomalies dans le réseau et les applications, des transactions frauduleuses et d'autres changements, ce qui permet d'obtenir des informations en temps réel et de contrer les futures menaces de sécurité. Pour améliorer nos technologies, nous devons exploiter les données recueillies lors des pen tests et de l'analyse de notre infrastructure de sécurité informatique actuelle.

Les résultats des évaluations peuvent être utilisés pour affiner les mécanismes de sécurité, notamment les ajustements des processus d'apprentissage automatique. L'apprentissage automatique peut aider une équipe de sécurité en automatisant de nombreux processus, comme la reconnaissance des formes utilisée dans les analyses. Une ASA est illustré de manière efficace par un système appelé user and entity behavior analytics (UEBA), qui établit le profil des utilisateurs et des périphériques réseau pour comprendre ce qui constitue un comportement normal, puis met en évidence les anomalies dès qu'elles apparaissent. Les solutions de sécurité adaptative étudient les modèles et les comportements, au lieu de se contenter d'examiner les fichiers journaux, de surveiller les points de contrôle et de répondre aux alertes.

Une ASA doit être capable de protéger les actifs critiques de l'organisation contre une variété de menaces. Il doit être capable de détecter et de répondre aux nouvelles menaces dès leur apparition. Enfin, elle doit être capable d'améliorer en permanence la posture de sécurité de l'organisation. Pour atteindre ces objectifs, il faut une approche globale comprenant des personnes, des processus et des technologies.

Les personnes sont l'élément le plus important d'une ASA. Ils sont chargés d'identifier et de protéger les actifs critiques de l'organisation. Ils sont également responsables de la détection et de la réponse aux menaces de sécurité. Les processus sont nécessaires pour s'assurer que les personnes suivent les procédures appropriées pour l'identification, la protection, la détection et la réponse. La technologie est nécessaire pour automatiser et améliorer l'efficacité de ces processus.

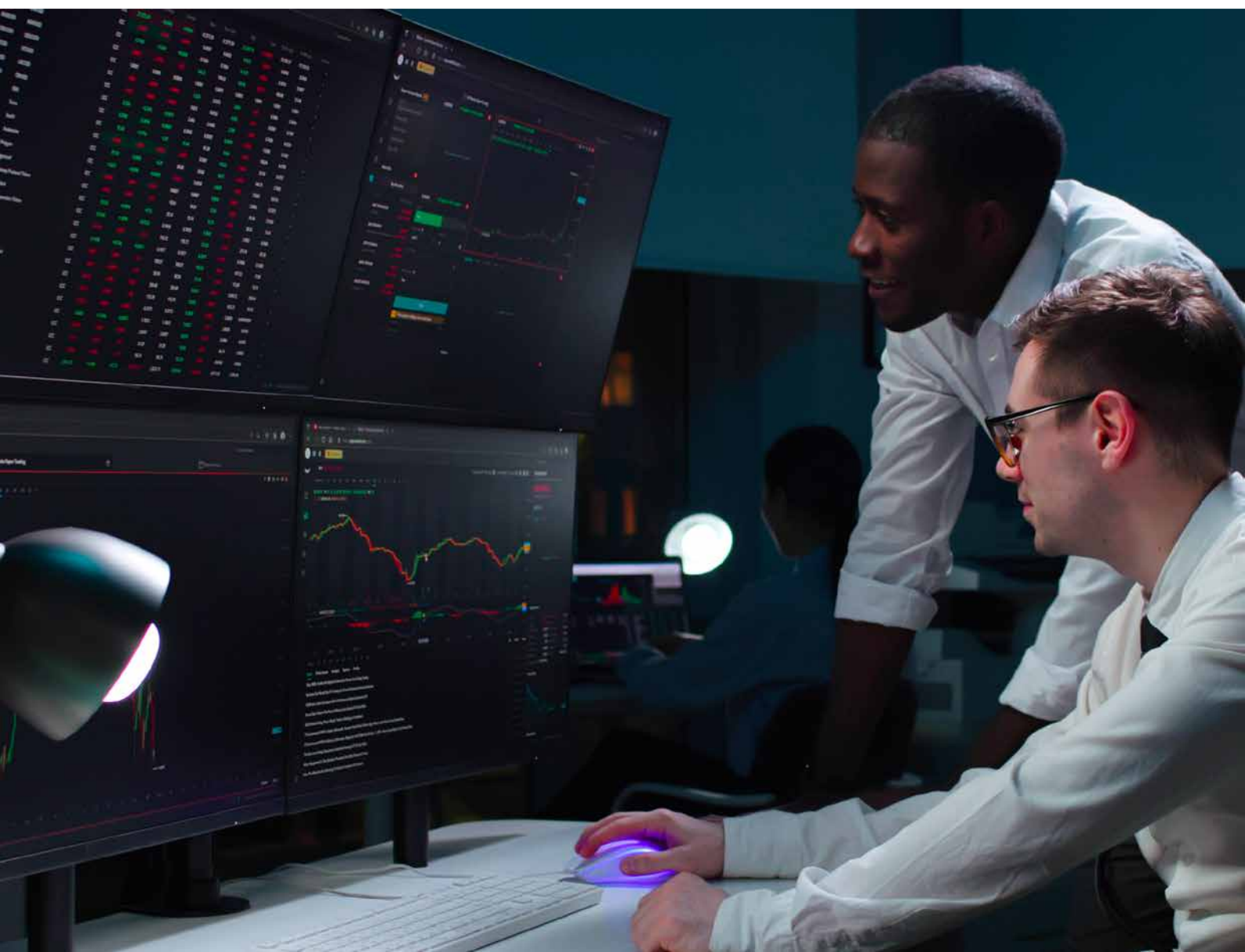


DÉTERMINER CE QUI DOIT ÊTRE PROTÉGÉ

La première étape du développement d'une architecture de sécurité solide pour une organisation consiste à comprendre ce qui doit être protégé et le risque associé. La question la plus fondamentale que vous devez vous poser est la suivante : quels sont les actifs à protéger et où sont-ils situés ? Cette question définit ce qui est inclus dans le champ d'application de l'architecture de sécurité et permet d'identifier les acteurs clés chargés d'assurer la protection.

Les actifs peuvent être à la fois tangibles et intangibles ; il peut également s'agir de données, de personnes ou d'organisations.

Selon l'entreprise, certains actifs sont susceptibles d'être plus importants que d'autres. Outre le type d'actifs, vous devez également tenir compte du risque associé à chaque actif et de l'impact que la perte de l'actif aurait sur l'entreprise.



5 ÉLÉMENTS CLÉS À PRENDRE EN COMPTE LORS DE LA MISE EN ŒUVRE D'UNE ASA



1. Adaptabilité

L'un des principaux défis de la sécurité est la menace constante d'une attaque. Une solution de sécurité étroitement intégrée et hautement personnalisée peut ne pas être en mesure de répondre aussi rapidement aux menaces en constante évolution. C'est là que le concept d'adaptabilité est important. Il est essentiel de pouvoir identifier et intégrer des composants qui peuvent être facilement modifiés ou déplacés pour répondre aux nouvelles menaces. L'architecture de sécurité doit être capable de répondre aux menaces en ajoutant de nouvelles fonctionnalités, en supprimant les composants inutiles et en modifiant les relations entre les composants. Pour ce faire, l'architecture de sécurité doit utiliser des composants ouverts, modulaires et standardisés. Les composants ouverts sont des composants qui peuvent prendre en charge un large éventail de fonctionnalités. Les composants modulaires sont des unités autonomes qui remplissent une fonction spécifique et peuvent être utilisés dans une variété de contextes différents. Les composants normalisés sont des composants construits selon une spécification standard.



2. Résilience

La continuité des activités et la reprise après incident sont des aspects importants de l'architecture de sécurité. En cas de catastrophe, les systèmes doivent avoir la capacité de se remettre de l'incident. Cela nécessite une compréhension détaillée de l'impact d'un incident, tel qu'une panne de courant ou une violation de données, et de la manière dont une organisation s'en remettra. L'impact d'un incident peut être l'arrêt d'un système spécifique, l'indisponibilité de données ou la perte de ressources critiques. Les exigences en matière de continuité des activités et de reprise après incident déterminent la sélection et la mise en œuvre des fonctions de sécurité. L'architecture de sécurité doit comporter une stratégie de protection contre les événements susceptibles de perturber la continuité des activités. L'architecture doit également disposer d'une stratégie de reprise après des incidents qui perturbent la continuité des activités .



3. Gouvernance

Une architecture de sécurité bien conçue repose sur des bases solides. Elle possède les bons composants, est bien intégrée et peut protéger contre les attaques. Cependant, si la gouvernance de l'architecture n'est pas bien mise en œuvre, l'architecture ne sera pas aussi efficace. La gouvernance de l'architecture de sécurité comprend les processus, les normes et les contrôles qui sont utilisés pour gérer l'architecture. Il est important de disposer d'un modèle de gouvernance qui identifie clairement qui est responsable de quelle partie de l'architecture de sécurité. Il est également important de garantir une approche cohérente de la gestion de l'architecture dans l'ensemble de l'organisation grâce à un ensemble commun de normes. Une approche cohérente permet de gérer l'architecture de manière plus efficace, en réduisant le risque de mauvaise configuration ou d'erreurs.



4. Visibilité

L'architecture de sécurité doit être construite en comprenant comment tout cela fonctionne ensemble, ainsi que la manière dont cela s'articule. Il est important de comprendre quels composants sont utilisés, comment ils sont configurés, quelles données circulent entre eux et comment les données sont transformées lorsqu'elles passent entre les composants. La visibilité de l'architecture de sécurité donne une indication de l'efficacité de l'architecture. Une représentation visuelle de l'architecture peut être utile pour comprendre quels composants sont utilisés, comment ils sont configurés et les flux de données entre eux. La visibilité doit être surveillée en permanence afin d'identifier les problèmes ou les risques qui peuvent survenir et de comprendre toute modification du système.

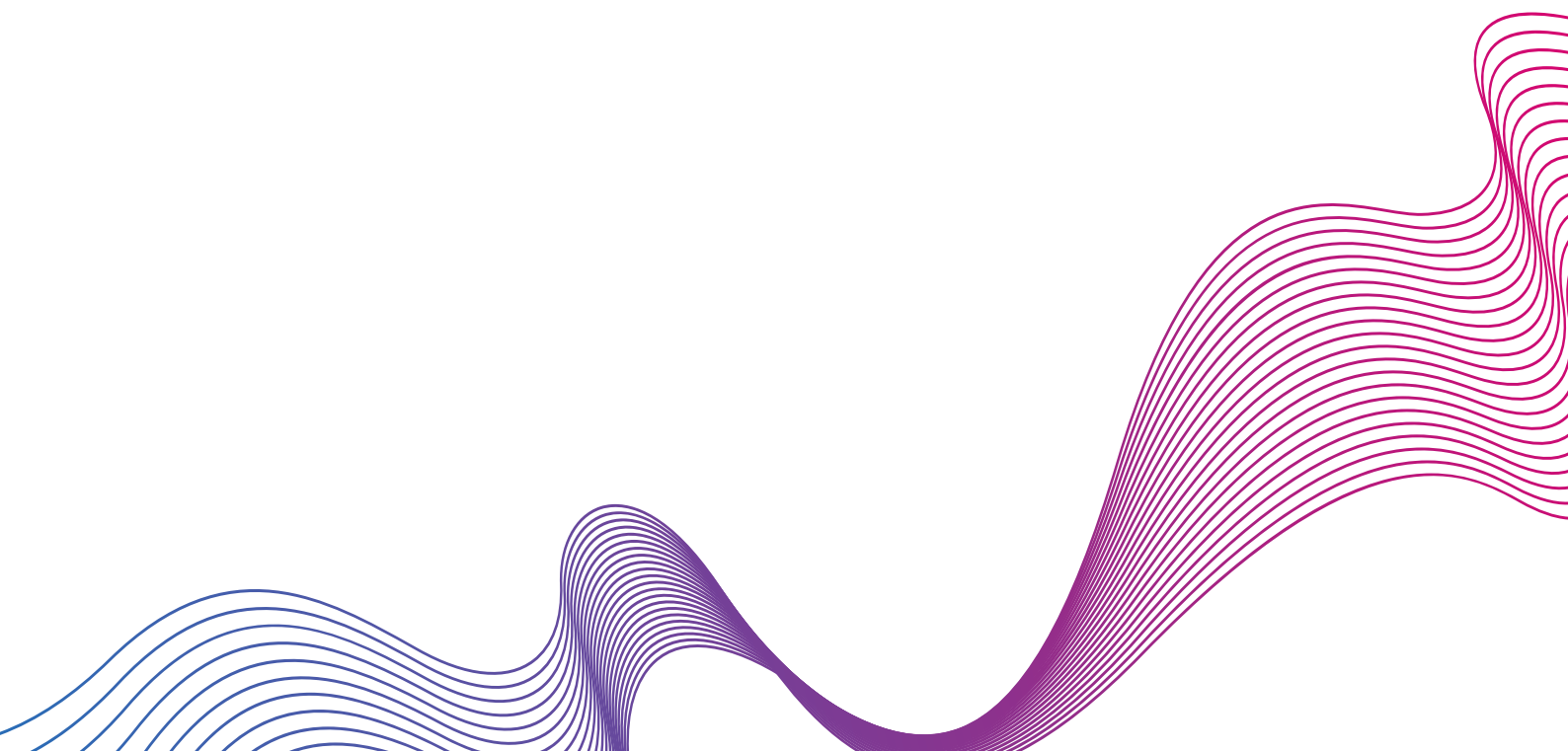


5. Vue unifiée de l'environnement

Une vue unifiée de l'environnement informatique est essentielle pour comprendre comment tout cela fonctionne ensemble. Il s'agit notamment de comprendre la relation entre les actifs, les contrôles de sécurité et les risques auxquels ils sont confrontés. Une vue unifiée de l'environnement fournit une vue d'ensemble de haut niveau des actifs et des risques de l'environnement, ainsi que des relations clés entre eux. Elle vous permet également d'identifier les domaines qui pourraient être améliorés ou modifiés.

La modélisation est le moyen le plus efficace d'obtenir une vue unifiée de l'environnement. La modélisation est le processus qui consiste à utiliser une représentation visuelle 12 de votre environnement pour identifier les actifs, les dépendances, les risques et les interconnexions entre les composants matériels et logiciels. Elle fournit une vue de l'ensemble de l'environnement, y compris les personnes, les processus et la technologie. Il existe plusieurs types de modélisation qui peuvent être utilisés à cette fin, tels que le diagramme et la modélisation de l'environnement. Le diagramme est le processus de création d'une représentation visuelle d'un environnement qui aide à comprendre les relations clés entre les différents composants.

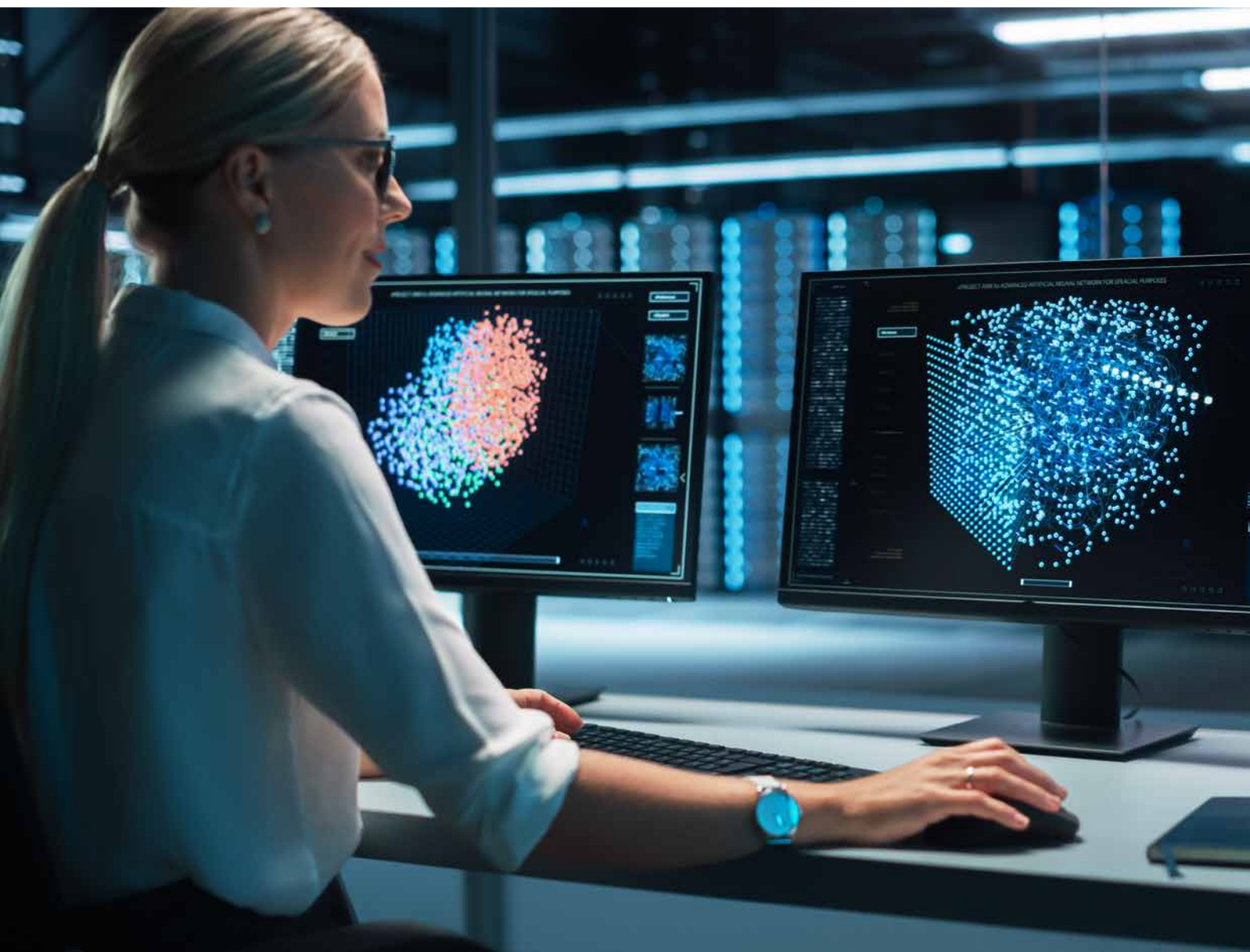
Comme nous l'avons vu, une ASA ne se limite pas à la mise en œuvre de fonctions de sécurité spécifiques dans un système. L'objectif principal de la sécurité adaptative est d'établir une boucle de rétroaction entre la connaissance des menaces, leur détection et leur prévention, un processus qui devient continuellement plus efficace. Elle implique l'élaboration d'un plan détaillé sur la manière dont les fonctions de sécurité du système doivent être mises en œuvre et configurées pour fournir des services de sécurité spécifiques. Si de nombreuses organisations reconnaissent l'importance d'une bonne architecture de sécurité, toutes ne sont pas pleinement conscientes de ce qui est nécessaire pour construire un système véritablement sécurisé. En comprenant les cinq éléments des ASA mentionnés ci-dessus, vous pouvez créer un plan pour un système sécurisé capable de faire face à l'évolution des menaces et des défis



MISE EN ŒUVRE D'UNE ASA AVEC L'AIDE D'AD360

AD360 est une solution holistique de gouvernance des identités, de sécurité et de gestion des accès. Qu'il s'agisse de la gestion des identités de vos utilisateurs, de la gouvernance de l'accès aux ressources, du provisionnement des utilisateurs, de la gestion des mots de passe en libre-service, de l'UEBA, de l'authentification adaptative et du SSO, la solution aide les organisations à construire une architecture de sécurité adaptative qui peut être gérée par une interface web simple et facile à utiliser.

Divers systèmes, tels que Windows Active Directory, les serveurs Exchange, Office 365 et plus encore, peuvent être gouvernés, surveillés, audités et sécurisés avec AD360.



15 CAPACITÉS ESSENTIELLES IAM RECOMMANDÉES PAR GARTNER DANS AD360

1



Gestion du cycle de vie des identités et exécution

Les actifs peuvent être à la fois tangibles et intangibles ; il peut s'agir de données, de personnes ou d'organisations. Selon l'entreprise, certains actifs sont susceptibles d'être plus importants que d'autres. Outre le type d'actifs, vous devez également tenir compte du risque associé à chaque actif et de l'impact que la perte de cet actif aurait sur l'entreprise.

2



Gestion des droits et privilèges

Éliminez les redondances et les erreurs humaines, et améliorez les processus métier en automatisant la gestion des droits avec délégation de privilèges en fonction du contexte.

3



Flux de travail basés sur l'approbation

Capacité de créer des flux de travail professionnels orientés vers un but précis. Créez les niveaux d'approbation requis - demandeur, réviseur, approbateur et exécuter - pour les bonnes parties prenantes. Définissez les flux d'approbation pour les processus d'entreprise tels que la création et la modification de comptes d'utilisateur, la gestion des autorisations, etc.

4



Audit des changements en temps réel

Obtenez des rapports d'audit sur l'activité des utilisateurs privilégiés, la détection des menaces internes et l'analyse des causes primaires. Surveillez et recevez des notifications sur les activités de connexion, les changements d'ACL et de mot de passe. Auditez également Azure AD, le stockage amovible, les postes de travail, les serveurs, les fichiers et les dossiers. Générez des rapports prêts à l'emploi pour GDPR, SOX, PCI, HIPAA, FISMA,

5



Gestion des politiques et des rôles

Prend en charge le contrôle d'accès basé sur les rôles, ce qui permet aux administrateurs de définir et d'attribuer des rôles granulaires aux parties prenantes, d'appliquer la politique du moindre privilège et de séparer les tâches sur les comptes privilégiés pour empêcher l'escalade des privilèges.

6



Certification des accès

Examinez les droits d'accès des utilisateurs à l'aide de rapports détaillés et assurez-vous que l'accès est conforme à la politique de sécurité interne.

7



Méthodes d'authentification des utilisateurs

Évitez les attaques par usurpation d'identité en utilisant la biométrie et d'autres méthodes d'authentification avancées. Renforcez votre sécurité en mettant en œuvre l'authentification multifonctionnelle pour les terminaux et les applications.

8



Authentification adaptative

Authentification adaptative basée sur le risque, utilisant des facteurs tels que la localisation de l'utilisateur, l'adresse IP, l'heure de la dernière connexion, l'empreinte du dispositif, etc.

9



Mise en œuvre des applications SaaS

Prend en charge le SSO basé sur SAML 2.0 pour des centaines d'applications SaaS d'entreprise telles que Salesforce, ServiceNow, Slack, etc.

10



Activation des applications non standard

Prend en charge les scripts personnalisés qui facilitent le provisionnement des identités pour les applications internes. Allez au-delà des systèmes cibles classiques comme Active Directory, Azure AD, Office 365 et étendez les capacités IAM d'AD360 à ServiceNow, Salesforce et d'autres applications tierces.

11



Demandes d'accès

La gestion des groupes en libre-service permet aux utilisateurs de demander l'adhésion à des groupes AD afin d'accéder à un ensemble de ressources informatiques spécifiques. En activant les règles de gestion des flux d'approbation pour la gestion des groupes en libre-service, les propriétaires d'applications et de ressources peuvent contrôler qui peut devenir membre d'un groupe particulier.

12



Rapports et analyses du comportement de l'utilisateur fondés sur le modèle ML

Examinez les droits d'accès des utilisateurs à l'aide de rapports détaillés et assurez-vous que l'accès est conforme à la politique de sécurité interne.

13



Facilité de déploiement

Pas de prérequis ni de déploiement compliqué. Commencez à gérer les identités dans votre environnement informatique sur site, dans le cloud ou hybride en quelques minutes.

14



Activation de la cible API

Les API REST d'AD360 facilitent le partage de données entre AD360 et toute application ou service Web tiers.

15



Haute disponibilité

Il prend en charge la haute disponibilité en cas de défaillance du système et des applications. La haute disponibilité est obtenue grâce au basculement automatique ; lorsque le service AD360 fonctionnant sur une machine tombe en panne, une autre instance du service AD360 fonctionnant sur une machine différente prend automatiquement le relais.

ManageEngine

AD360

AD360 est une solution intégrée de gestion des identités et des accès (IAM) permettant de gérer les identités des utilisateurs, de régir l'accès aux ressources, de renforcer la sécurité et de garantir la conformité. Du provisionnement des utilisateurs, de la gestion des mots de passe en libre-service et de la surveillance des modifications d'Active Directory à l'authentification unique (SSO) pour les applications d'entreprise, AD360 vous aide à effectuer toutes vos tâches IAM avec une interface simple et conviviale. Avec AD360, il vous suffit de choisir les composants dont vous avez besoin et de commencer à relever les défis de l'IAM dans les environnements sur site, dans le cloud et hybrides à partir d'une seule console. Pour plus d'informations sur AD360, veuillez consulter le site www.pgsoftware.fr/iam/ad360.

👉 Obtenir un devis

📄 Télécharger