Zero trust : la nouvelle norme du paysage de la cybersécurité

inetum realdolmen
Positive digital flow

Le monde change. Votre sécurité aussi ?

Il n'y a pas encore si longtemps, un mot de passe fort, un logiciel antivirus et un pare-feu avec un VPN suffisaient pour protéger son organisation contre les cyberattaques. Malheureusement, ce temps est révolu.

Nous ne sommes plus limités à un seul poste de travail et encore moins à un seul appareil fixe. Nous travaillons en déplacement, sur différents appareils, voire sur nos appareils personnels, et de plus en plus souvent dans le cloud.

Plus notre **environnement de travail se complexifie**, plus les cyberrisques augmentent. Car s'il était facile de sécuriser un seul point sensible, il est beaucoup plus difficile de protéger plusieurs cibles mouvantes en même temps.

La cybersécurité doit impérativement s'adapter aux nouvelles réalités du monde du travail. Et il ne suffit pas d'étendre notre arsenal d'outils existants : une vision radicalement différente est nécessaire pour parvenir à une nouvelle approche. Ce **changement de paradigme sécuritaire** implique aussi un changement dans la culture des organisations et l'état d'esprit des employés.

« En 2022, les cyberattaques ont à nouveau augmenté de 32%. L'année dernière, près d'une entreprise flamande sur huit a été victime d'une cyberattaque. »

Zero trust security : de nouveaux principes de sécurité pour une nouvelle réalité

Vous avez peut-être déjà entendu parler du concept zero trust security, ou zero trust pour faire court. Cette nouvelle **approche proactive** de la sécurité vous permet de réagir plus rapidement et plus efficacement aux menaces et de combattre efficacement les attaques, voire de les prévenir.

Le modèle zero trust repose sur un large éventail d'**outils de contrôle et de mécanismes adaptatifs**. Il s'articule en outre autour d'un processus de **vérification continue**. Autrement dit, il ne suffit pas d'acquérir un produit, un service ou une technologie et de mettre en œuvre cette solution une fois pour toutes. Au contraire, le modèle zero trust exige une gestion constante, des efforts sur le long terme et une vigilance permanente face à l'émergence de nouveaux risques.

LE CONCEPT ZERO TRUST REPOSE SUR TROIS PRINCIPES FONDAMENTAUX :

1. **Vérification en profondeur :**
   Le premier principe et le plus important qui sous-tend ce modèle peut se traduire par « ne jamais faire confiance, toujours vérifier ! ». Par exemple, chaque appareil est considéré comme suspect par défaut, même s'il se connecte via un réseau autorisé et même si vous l'avez déjà vérifié par le passé.

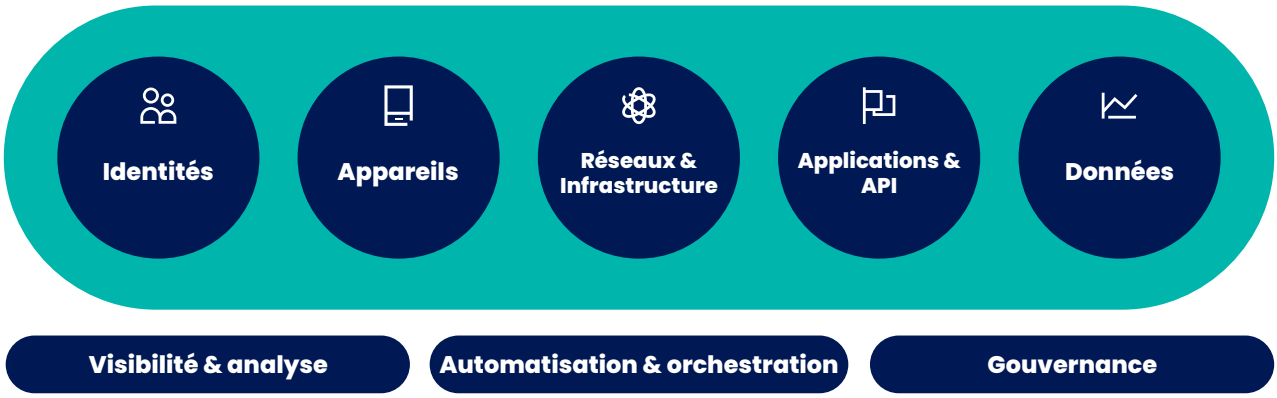
2. **Accès à moindre privilège :**
   Le principe de l'accès à moindre privilège (LPA ou Least Privileged Access) implique de limiter l'accès à votre environnement de travail au strict minimum (JEA ou Just Enough Access) et de ne l'accorder qu'au moment où il est requis, uniquement pour le temps nécessaire (JIT ou Just In Time).

3. **Présomption de violation :**
   Par mesure de précaution, vous créez une infrastructure conçue pour minimiser autant que possible l'impact d'une violation.

L’architecture zero trust security repose sur cinq piliers essentiels

EN VOICI UN BREF APERÇU :

Principes de base du modèle zero trust



Pilier 1 : sécurisez vos IDENTITÉS

Tout commence par l'utilisateur. Celui-ci peut disposer d'une seule identité ou de plusieurs identités, chacune étant liée à un certain nombre de droits d'utilisateur et parfois aussi à des droits d'administrateur. C'est pourquoi il est primordial de vérifier cette identité à chaque fois et d'authentifier chaque utilisateur avant de lui donner accès à votre environnement de travail, via la gestion des identités et des accès (IAM ou Identity & Access Management).

Un mot de passe seul, aussi fort soit-il, ne suffit plus. Aujourd'hui, l'**authentification forte** passe par l'**authentification multifactorielle ou MFA (Multi-Factor Authentication)**. Vous ajoutez ainsi une couche de sécurité supplémentaire à votre contrôle des accès.

L'important n'est pas seulement que le mode d'accès soit conforme à vos règles en matière de contrôle des accès, mais aussi que le comportement soit **typique** pour l'identité en question.
Par exemple, si un utilisateur tente de se connecter depuis l'Inde alors qu'il se trouve physiquement en Belgique, cela doit vous alerter. L'authentification doit être fondée sur une **analyse de risque** qui tient compte à la fois de l'utilisateur, de son appareil, de sa localisation et de son comportement.

Tandis que l'**authentification unique (single sign-on, SSO)** permet à un utilisateur de se connecter une seule fois pour accéder à votre environnement de travail, le principe de l'**accès à moindre privilège (LPA)** restreint les éléments auxquels il aura accès dans cet environnement.

ACCENT SUR L'AUTHENTIFICATION MULTIFACTORIELLE, L'AUTHENTIFICATION UNIQUE, LA GESTION DES IDENTITÉS ET DES ACCÈS, LA GESTION DES ACCÈS À PRIVILÈGES ET L'AUTHENTIFICATION BASÉE SUR LES RISQUES

Pilier 2 : sécurisez vos APPAREILS

Une fois que l'utilisateur est authentifié et que son identité a été vérifiée, il a accès aux ressources de votre environnement de travail, y compris vos données. Pour les récupérer, il passe généralement par un terminal, c'est-à-dire un appareil utilisateur comme un ordinateur ou un smartphone. Ce terminal constitue une **autre surface d'attaque** qu'il faut également surveiller et protéger.

Commencez par imposer des règles pour éviter qu'un appareil non sécurisé puisse accéder à votre environnement de travail (**conformité des terminaux**). Vous pouvez par exemple en limiter l'accès aux appareils achetés et/ou gérés par votre organisation. Vous pouvez aussi prescrire que chaque appareil soit équipé d'un antivirus qui surveillera en permanence son comportement et son état et qui mettra automatiquement à jour la protection (**protection des terminaux**).

En somme, ce pilier implique une gestion active des appareils de vos utilisateurs, y compris sur le plan de leur sécurisation (**gestion des appareils mobiles ou MDM**). C'est d'autant plus nécessaire que les utilisateurs apportent régulièrement leurs propres appareils au travail (**système BYOD ou Bring Your Own Device**). En outre, ils installeront souvent des applications propres à l'entreprise sur leur appareil personnel, comme des clients de messagerie. Pour limiter les risques, un système de gestion des appareils utilisateurs est donc indispensable. Un tel système peut inclure la possibilité d'effacer des données à distance en cas de perte ou de vol (**DLP ou Data Loss Prevention**).

« Outre les réseaux d'entreprise, les réseaux domestiques des utilisateurs sont de plus en plus souvent pris pour cible. Le smartphone est un point d'accès facile pour atteindre de nombreuses personnes en même temps. »

ACCENT SUR LA GESTION DES APPAREILS MOBILES, LA CONFORMITÉ DES APPAREILS ET LA PROTECTION DES TERMINAUX

Pilier 3 : sécurisez vos RÉSEAUX et votre INFRASTRUCTURE

Passé le contrôle d'accès, l'utilisateur pénètre dans votre réseau. Cette infrastructure lui permet d'accéder aux données hébergées sur les serveurs, dans les bases de données et dans les systèmes de stockage de votre centre de données.

Pour réduire cette immense surface d'attaque potentielle, il est important de **segmenter** votre réseau en unités plus petites. Vous l'avez peut-être déjà fait, par exemple en introduisant une séparation virtuelle entre les clients et les serveurs sur votre réseau avec la technologie VLAN. Cependant, cela ne suffit plus.

La **micro-segmentation** est désormais recommandée, au niveau des équipements individuels comme de leurs composants, comme les ports réseaux. En divisant votre infrastructure en zones encore plus petites et mieux protégées, vous éviterez qu'un virus puisse l'infecter en profondeur et la paralyser.

En outre, il est important d'investir dans la surveillance et la protection de votre infrastructure contre les menaces en temps réel (**real-time threat protection**). Un pare-feu vous permettra par exemple de détecter le trafic réseau suspect. Vous pouvez faire en sorte que les comportements anormaux et à risque soient automatiquement marqués et signalés, pour que vous puissiez les bloquer ou prendre d'autres mesures de protection.

Enfin, vous pouvez chiffrer votre trafic réseau (**chiffrement de bout en bout**) pour qu'il ne puisse pas être capté ou compromis.

ACCENT SUR LA SEGMENTATION, LA PROTECTION CONTRE LES MENACES ET LE CHIFFREMENT

Pilier 4 : sécurisez vos APPLICATIONS et vos API

Les applications et les API sont les interfaces qui permettent aux utilisateurs de lire et d'employer vos données. C'est pourquoi il est important de les sécuriser autant que possible.

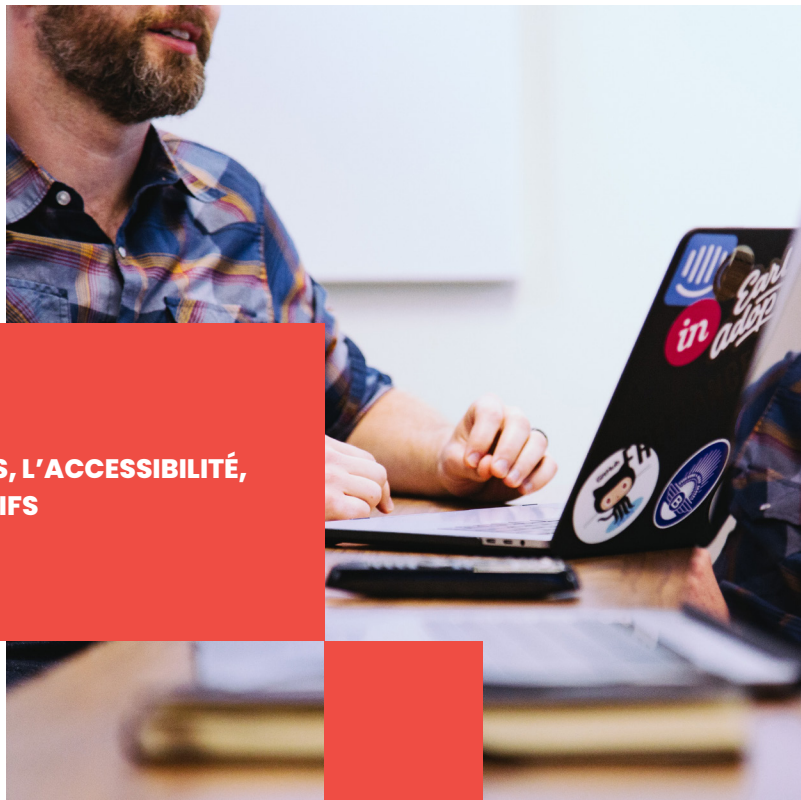
Au niveau des applications, un premier problème de sécurité majeur qui se pose aux administrateurs est le phénomène dit « **shadow IT** », à savoir, l'acquisition et l'utilisation de solutions logicielles par vos employés sans l'approbation de votre service informatique. L'absence de visibilité sur ce type de solutions utilisées « en parallèle » à votre environnement informatique régulier constitue un risque important. Pour y remédier, investissez dans des moyens d'identifier les **applications non autorisées** qui circulent au sein de votre organisation.

Toutefois, même les **applications autorisées** peuvent présenter un risque pour la sécurité. Ce n'est pas parce qu'une application est autorisée au sein de votre organisation que les employés peuvent l'utiliser n'importe comment. Par exemple, seuls les employés qui disposent des autorisations nécessaires doivent pouvoir consulter des données financières ou d'autres informations sensibles dans une application (**gestion des autorisations des applications**). Il existe des solutions pour l'octroi et la gestion de ce type d'autorisations.

Vous devez aussi pouvoir analyser vos applications pour **détecter tout comportement anormal**. Grâce à l'utilisation croissante des API, les applications peuvent désormais communiquer et extraire des données à partir de n'importe quelle source. C'est très pratique, mais le revers de la médaille est que ces applications sont plus que jamais exposées aux risques de sécurité. Il est donc recommandé de paramétrer et de maintenir des **contrôles d'accès** stricts, surtout pour vos applications critiques.

Enfin, il est impératif de **télécharger tous les correctifs** en temps voulu. Plus vous attendez, plus le risque de cyberincident augmente, car actuellement, les vulnérabilités et les erreurs internes aux programmes sont l'une des causes principales des violations de la sécurité. D'où l'importance de vous assurer que vos logiciels sont à jour à tout moment.

ACCENT SUR LES AUTORISATIONS D'ACCÈS, L'ACCESSIBILITÉ, LE CONTRÔLE ET LA GESTION DES CORRECTIFS



Pilier 5 : sécurisez vos DONNÉES

En fin de compte, tout tourne autour d'un seul objectif : la protection de vos données. Les quatre piliers précédents sont conçus à cette fin. Sans ces mesures de prévention, vos données seraient déjà vulnérables ! Mais cela n'empêche que vous ayez tout intérêt à protéger le mieux possible vos données en soi, au cas où elles quitteraient l'environnement géré de vos applications, de vos appareils, de votre infrastructure et de vos réseaux, par exemple par e-mail ou lors d'un partage de fichiers.

La première étape consiste à **classer et étiqueter** vos données. Séparez vos données publiques de vos données privées ou confidentielles, qui ne doivent en aucun cas être partagées avec des tiers, voire avec vos collaborateurs internes en dessous d'un certain niveau d'accès.

« Parmi les entreprises touchées par une cyberattaque, **23,5 %** ont été victimes de la destruction de données d'entreprise et **13,3 %** d'un vol de données. »

Sur la base de cette classification, vous pouvez configurer des mesures de **contrôle d'accès** à vos données. En appliquant à nouveau le principe de l'**accès à moindre privilège (LPA)**, vous vous assurerez que chaque utilisateur peut uniquement accéder aux données strictement nécessaires à l'exercice de sa fonction.
Vous traitez des données sensibles, comme des données médicales ? Dans l'UE, le RGPD vous impose de les traiter avec des précautions particulières. Si vous souhaitez les utiliser malgré tout, par exemple pour développer des applications, vous devrez les **anonymiser ou les pseudonymiser**.

Enfin, nous avons déjà évoqué l'importance du **chiffrement**. En chiffrant vos données critiques, vous empêcherez tout tiers de les lire en cas de perte ou de vol. Les solutions de **prévention des pertes de données (DLP ou Data Loss Prevention**) vous permettent en outre d'intervenir sur vos données après la perte ou le vol d'un appareil, par exemple en les effaçant. En dernier recours, en cas de catastrophe, il est bon de disposer d'une **sauvegarde** ou d'une copie de vos données.

ACCENT SUR LA CLASSIFICATION, L'ÉTIQUETAGE, LE CHIFFREMENT, L'ACCÈS ET LA PRÉVENTION DES PERTES DE DONNÉES, LA SAUVEGARDE ET LA RÉCUPÉRATION

Une base solide : trois fondements supplémentaires

Les cinq piliers susmentionnés sont à la base du modèle zero trust security. Ils reposent à leur tour sur trois fondements conçus pour garantir la solidité de l'architecture dans son ensemble. Il vaut la peine d'y investir également pour vous assurer une base solide.

VISIBILITÉ ET ANALYSE
Sans une bonne visibilité sur votre environnement de travail, votre environnement informatique et les dangers qui peuvent les menacer, vous ne pourrez pas mettre en place l'architecture de sécurité complexe requise pour le modèle zero trust security.

Heureusement, en investissant dans les cinq piliers de cette architecture, vous améliorerez déjà votre visibilité, notamment sur les applications shadow IT ou votre parc d'appareils utilisateurs (gestion des terminaux).

Vous obtiendrez en même temps une grande quantité de données, que vous pourrez analyser pour affiner encore votre approche de la sécurité.

AUTOMATISATION ET ORCHESTRATION
Bien entendu, il n'est pas possible d'effectuer chaque contrôle d'accès manuellement. Il en va de même pour la plupart des autres éléments d'une approche zero trust security : la micro-segmentation, le chiffrement, les sauvegardes… Une approche de sécurité vraiment efficace exige donc d'automatiser autant de processus que possible et d'orchestrer l'ensemble de ces tâches.

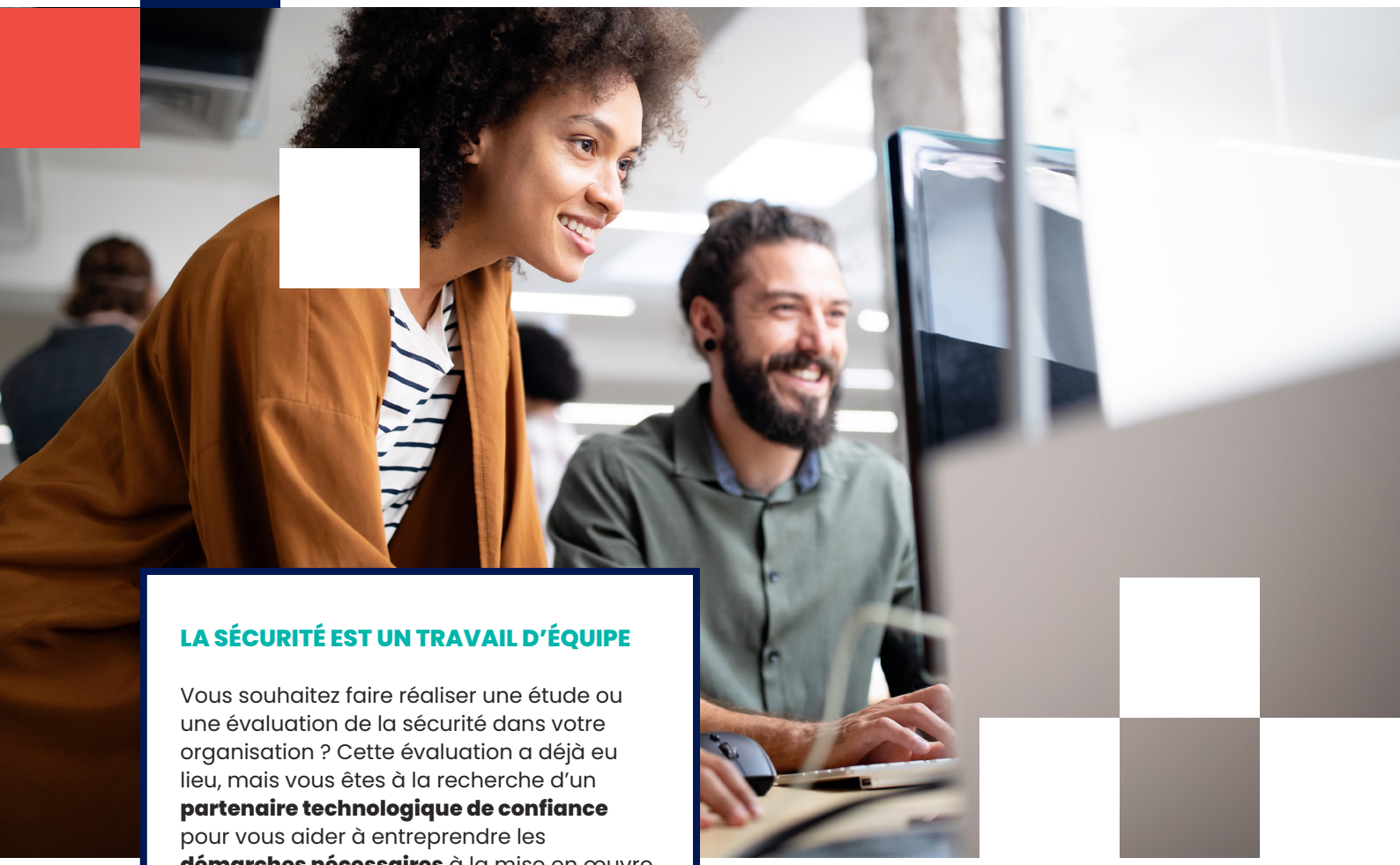
GOUVERNANCE
La mise en œuvre d'un concept zero trust security ne se résume pas à un projet délimité dans le temps, avec une date de début et une date de fin. Il s'agit d'un parcours complexe de changement stratégique à long terme, que vous devrez suivre en permanence et corriger régulièrement. Une bonne gouvernance est essentielle pour garantir l'appropriation du parcours par les bonnes parties prenantes et pour pouvoir maintenir une vue d'ensemble à tout moment.

Zero trust security : votre organisation est-elle prête ?

Le concept de zero trust security vous a convaincu, mais vous ne savez pas par où commencer ? Vous avez commencé à mettre en place une architecture zero trust, mais vous hésitez quant aux prochaines étapes ?

Dans les deux cas, une brève étude ou une **évaluation de la sécurité de votre environnement** pourra vous aider à avancer. Nous pouvons dresser un état des lieux et évaluer votre **niveau de maturité** ou de **préparation à l'application du modèle zero trust**. Ainsi, vous saurez exactement où vous en êtes.

Vous pouvez combiner cette évaluation de base avec une **feuille de route de sécurité**, pour recevoir un plan par étapes, une **classification des priorités** et des **conseils technologiques sur mesure** pour votre organisation. Cela vous donnera non seulement un aperçu clair de la suite de votre parcours, mais vous saurez aussi comment parvenir au mieux à votre destination.



LA SÉCURITÉ EST UN TRAVAIL D'ÉQUIPE

Vous souhaitez faire réaliser une étude ou une évaluation de la sécurité dans votre organisation ? Cette évaluation a déjà eu lieu, mais vous êtes à la recherche d'un **partenaire technologique de confiance** pour vous aider à entreprendre les **démarches nécessaires** à la mise en œuvre d'une architecture zero trust ?

Dans les deux cas, vous pouvez vous adresser à nous. Nous disposons de l'expertise nécessaire pour tous les piliers et tous les fondements technologiques abordés dans ce document.

La sécurité de votre environnement est un travail d'équipe !

CONTACTEZ-NOUS

Inetum-Realdolmen
A. Vaucampslaan 42
1654 Huizingen, Belgium
+32 2 801 55 55
www.inetum-realdolmen.world
info@inetum-realdolmen.world

inetum realdolmen
Positive digital flow