

forum21
EUROPE

Intervenants, sessions et thématiques

okta



Sommaire

La confiance est notre super-pouvoir	3
Philipp Kristian, Pionnier de la confiance et de l'innovation	

L'avenir de la confiance numérique	4
Derek Gordon, Director, Cyber Security, PwC	

Focus sur la multiplication des cybermenaces	5
Ben King, Chief Security Officer, Okta	

Perspective d'un client	6
Markus Hilmes, CISO, AutoScout24	

L'IT hybride, évolution et avenir	7
Joshua Kroeze, Senior Director, Solutions Engineers, Okta	

Perspective d'un client	8
Liz Cocker, Identity Service Manager, ITV	

Satisfaire les nouvelles exigences des collaborateurs	9
Angela Salmeron, Associate Research Director, IDC	

Comment instaurer un climat de confiance au travail ?	10
Ian Lowe, Director of Solutions Marketing, Okta	

Perspective d'un client	11
Reem Zahran, Chief Information Officer, Vistra	

L'avenir du CIO	12
Duncan Brown, VP of Enterprise Research Europe, IDC	

Une expérience numérique optimale pour fidéliser vos clients	13
Jiong Liu, Director, Product Marketing – Customer Identity, Okta	

Perspective d'un client	14
Erwan Conq, CIO, BU France B2C & Direction Grand Public (DGP), Engie	

Établir la confiance grâce à la technologie	15
Yves Couturier, Director of Information Systems, Croix-Rouge française	

Oui à la sécurité Zero Trust, non à une société de méfiance	16
Todd McKinnon, CEO et cofondateur, Okta	

KEYNOTE

Philipp Kristian
Pionnier de la confiance
et de l'innovation



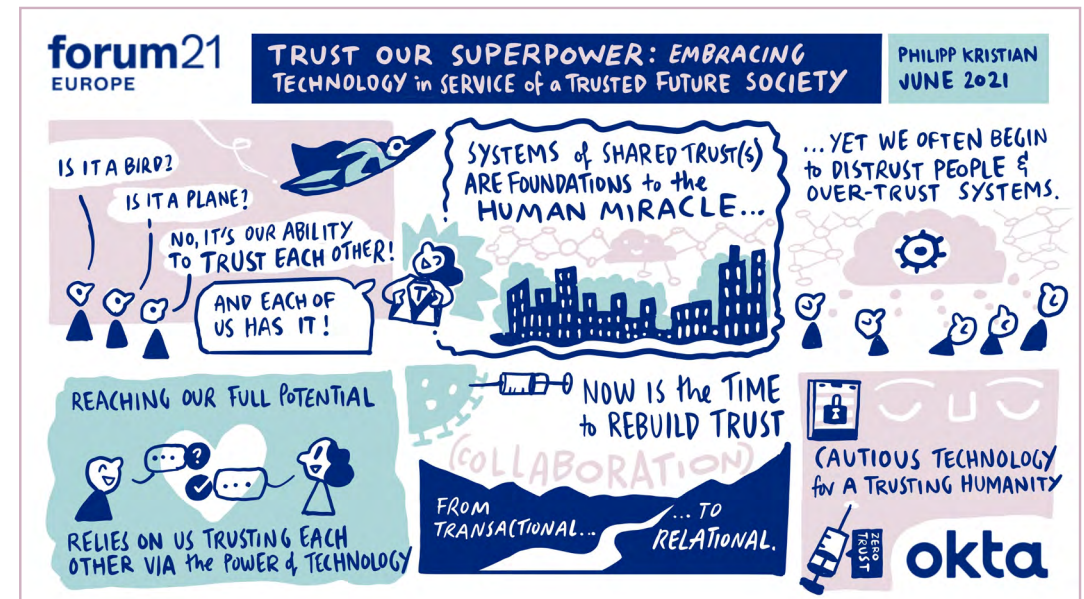
La confiance est notre super-pouvoir

Nous possédons tous ce super-pouvoir qu'est la confiance. Il nous permet de collaborer, de trouver un terrain d'entente et d'accomplir des choses extraordinaires. Si le monde tourne rond, c'est grâce à la confiance. À l'heure où nous réinventons les systèmes de collaboration, la technologie joue un rôle stratégique dans l'établissement de passerelles de confiance qui nous permettront de gagner en productivité et de mieux gérer notre temps.

Au cours des dix dernières années, des bouleversements majeurs tels que la crise financière de 2008-2009 et la pandémie de Covid-19 ont instauré un climat de méfiance. Nous avons aujourd'hui l'opportunité d'y remédier et d'abandonner le modèle de prise de décisions basé sur les règles, qui prend trop de temps et qui complique l'identification des personnes de confiance. Pour tenter de restaurer la confiance à l'échelle mondiale, nous devons créer un nouveau mode de fonctionnement pour construire une société fondée sur la confiance.

Il est d'autant plus urgent que la technologie nous aide à mieux collaborer et à parvenir à un consensus universel. Nous avons l'occasion de procéder à une remise à zéro et de rebâtir ensemble notre monde en adoptant une approche humaine, transparente et collaborative. Revenons aux racines de notre super-pouvoir.

Pour tenter de restaurer la confiance à l'échelle mondiale post-Covid, nous devons créer un nouveau mode de fonctionnement pour construire une société fondée sur la confiance.



SESSION 1 : La nouvelle culture de la sécurité

Derek Gordon
Director, Cyber
Security, PwC



L'avenir de la confiance numérique

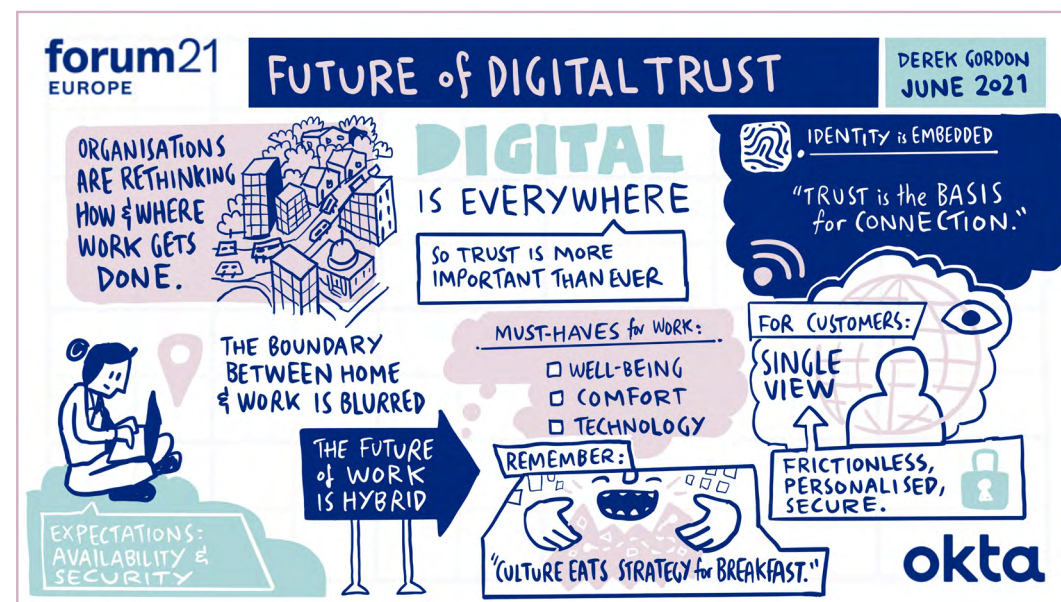
À l'ère du tout-numérique, la confiance numérique est une notion plus essentielle que jamais. Cette évolution transforme la culture et les opérations des entreprises, qui réévaluent des concepts tels que le lieu et les modalités de travail tout en s'efforçant d'optimiser l'expérience client.

Trois aspects sont importants à cet égard :

1. **Cybermenaces** – Défense contre les cybercriminels qui tentent de dérober ou compromettre vos informations et ressources numériques
2. **Données** – Protection de la valeur des données en votre possession
3. **Technologie** – Mise en place d'un environnement technologique résistant, conforme à vos objectifs métier

Lorsque les entreprises maîtrisent les principaux éléments stratégiques et opérationnels de la confiance numérique, elles bénéficient d'une valeur énorme et mesurable, et toutes les parties prenantes en tirent des avantages — clients, partenaires, investisseurs et collaborateurs.

Comment les entreprises approchent-elles la confiance numérique ? Une étude de PwC révèle que 96 % des entreprises ont l'intention de revoir leur stratégie de cybersécurité suite à la pandémie de Covid-19. 40 % d'entre elles se concentrent sur l'accélération de leur transformation digitale, tandis que la moitié prévoit d'intégrer la cybersécurité et la confidentialité à toutes ses décisions. Nous avons également observé l'émergence de la fonction de Digital Trust Officer, dont le rôle essentiel est de comprendre les aspects métier et juridiques de la confiance, tout en promouvant l'importance de l'identité, de la sécurité et de la confidentialité à l'échelle de toute l'entreprise.



50 %

des entreprises
prévoient d'intégrer
la sécurité et la
confidentialité
à toutes
leurs décisions

SESSION 1 : La nouvelle culture de la sécurité

Ben King
Chief Security
Officer, Okta



Focus sur la multiplication des cybermenaces

Les bouleversements survenus en 2020 furent une aubaine pour les cybercriminels : un nombre record de vulnérabilités ont été signalées. Même les multinationales et les administrations publiques ont été prises pour cible à de multiples reprises. D'ici 2025, la cybercriminalité devrait coûter 10,5 mille milliards de dollars à l'économie mondiale. Comment les équipes de sécurité peuvent-elles réduire les risques de manière durable ?

On distingue quatre domaines d'action :

- **Comprendre les risques** – Pour que vous puissiez concentrer vos efforts et vos ressources de manière à obtenir les meilleurs résultats, vous devez identifier les risques pour les collaborateurs, les partenaires et les fournisseurs, ainsi que pour l'infrastructure et les données.
- **Apprendre du passé** – Un grand nombre d'anciennes vulnérabilités sont exploitées pour compromettre les systèmes et accéder aux données des entreprises. Une fois les enseignements tirés, des solutions doivent être mises en place.
- **Planifier l'avenir** – Une approche Zero Trust s'impose à une époque où la mobilité est reine. Face à l'essor du travail hybride qui fait disparaître le périmètre de sécurité traditionnel, l'identité devient le point de contrôle logique.
- **Protéger les utilisateurs** – Les collaborateurs peuvent constituer des piliers de défense de l'entreprise si elle a mis en place des programmes de sensibilisation, des mesures de protection des terminaux et des processus de réponse aux incidents adéquats.



D'ici 2025, la cybercriminalité devrait coûter 10,5 mille milliards de dollars à l'économie mondiale.



SESSION 1 : La nouvelle culture de la sécurité

Perspective d'un client

AutoScout24 est le plus grand marché automobile européen en ligne. L'entreprise a pour objectif de simplifier les procédures d'achat et de vente d'une voiture, tout en protégeant les utilisateurs lors de leur parcours d'achat.

La confiance est au cœur des valeurs de l'entreprise. Celle-ci se définit comme un marché automobile en ligne de confiance, actif à l'échelle européenne, et cherche à proposer des produits et processus utiles qui répondent aux besoins de ses clients. La stratégie adoptée par AutoScout24 pour ses collaborateurs est axée sur la simplification des tâches quotidiennes, en réduisant autant que possible les points de friction. Les équipes produits peuvent s'appuyer sur une infrastructure de base sécurisée où les tâches récurrentes sont uniformisées, ce qui leur permet de se concentrer sur l'application en elle-même.

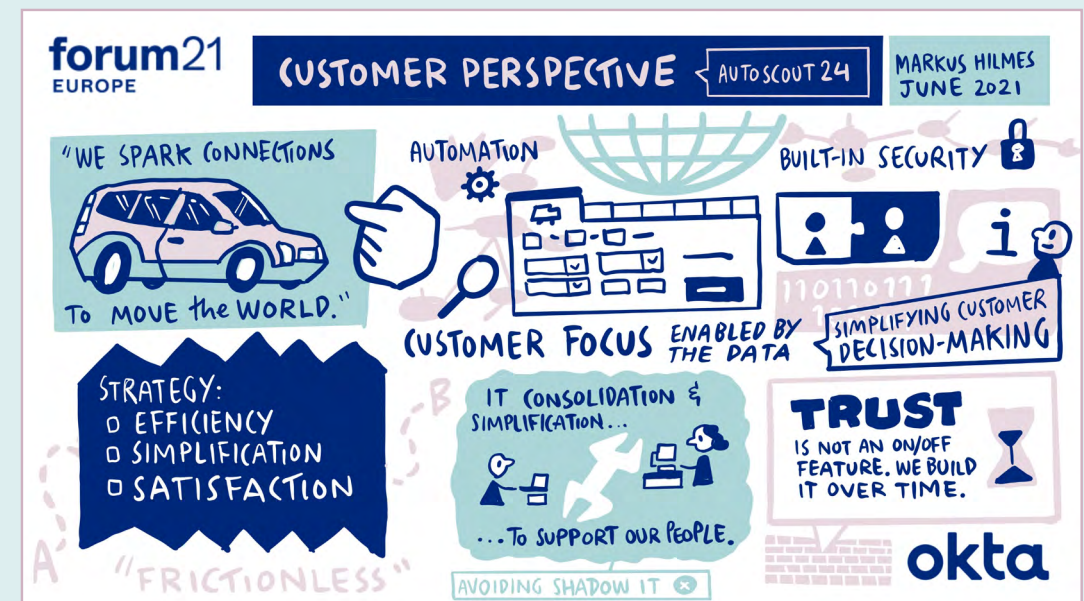
AutoScout24 fait appel à Okta pour la gestion des identités de ses clients et de ses collaborateurs. En ce qui concerne le CIAM, l'ajout de fonctionnalités de sécurité ou d'ergonomie était plus rapide avec une solution prête à l'emploi. Pour les collaborateurs (IAM), l'entreprise disposait déjà d'une solution de gestion des identités, mais souhaitait moins de friction. Grâce à Okta, elle peut désormais procéder facilement à l'onboarding des utilisateurs externes, p. ex. en cas de fusion et acquisition, mais aussi se préparer à un avenir sans mot de passe.

“

Nous sommes des experts en produits numériques, pas des spécialistes de l'identité. Nous voulions pouvoir ajouter des fonctionnalités plus rapidement.

**Auto
Scout24**

Markus Hilmes
CISO, AutoScout24



SESSION 2 : L'IT hybride, évolution et avenir

Joshua Kroeze

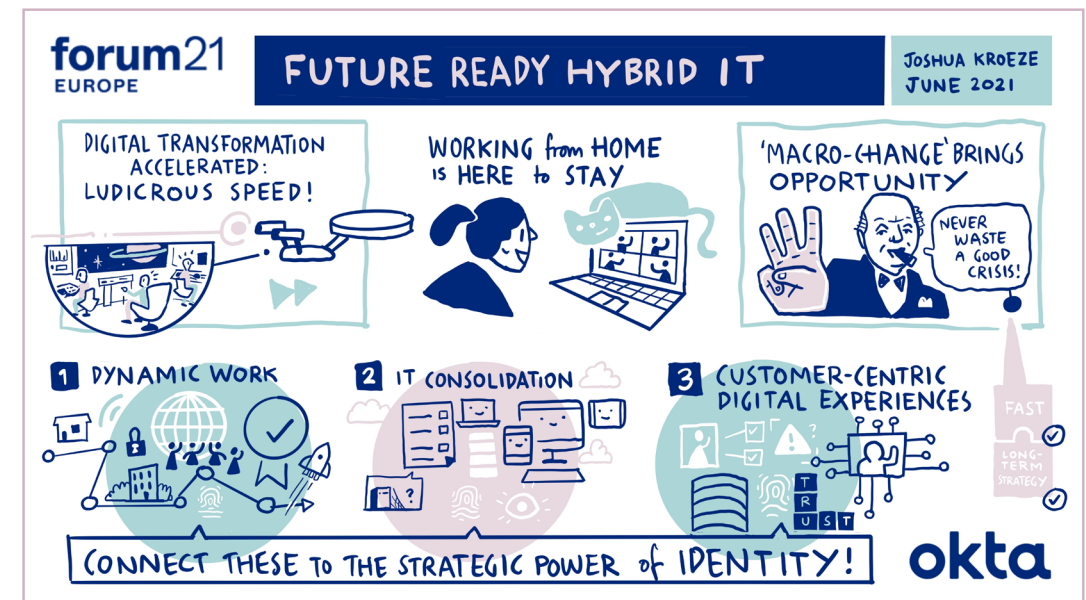
Senior Director Solutions
Engineers, Okta

IT hybride pour un monde hybride

En 2020, la pandémie de Covid-19 a donné un coup d'accélérateur brutal à la transformation IT. Le délai d'implémentation a été divisé par 20 et les entreprises se sont empressées de proposer de nouveaux services numériques plusieurs années avant la date prévue. Ce fut une période à la fois difficile et palpitante pour les responsables IT. En effet, la plupart des entreprises disposent encore d'un environnement IT hybride, alliant des systèmes on-premise et dans le cloud.

Chez Okta, nous identifions trois opportunités qui préparent votre entreprise à affronter l'avenir :

- 1. Prise en charge du travail dynamique** – Les entreprises peuvent renforcer la productivité et la sécurité des effectifs hybrides de demain en optimisant leurs outils en libre-service, en simplifiant la gestion du cycle de vie des utilisateurs et en adoptant une approche Zero Trust.
- 2. Consolidation de l'IT** – Après avoir pris une série de décisions d'achat à court terme, les responsables IT doivent faire l'inventaire des pratiques existantes : sécuriser celles qui resteront, abandonner celles qui ont perdu de la valeur et planifier à long terme l'unification de l'identité dans l'environnement cloud, on-premise et hybride.
- 3. Création d'expériences axées sur le client** – L'intégration de l'identité aux systèmes marketing offre une vue unifiée du client et des opportunités de marketing personnalisé (qui ont le potentiel d'augmenter les ventes de 15 à 20 %).



En 2020, la pandémie de Covid-19 a donné un coup d'accélérateur brutal à la transformation IT.



SESSION 2 : L'ITV hybride, évolution et avenir

Liz Cocker
Identity Service
Manager, ITV



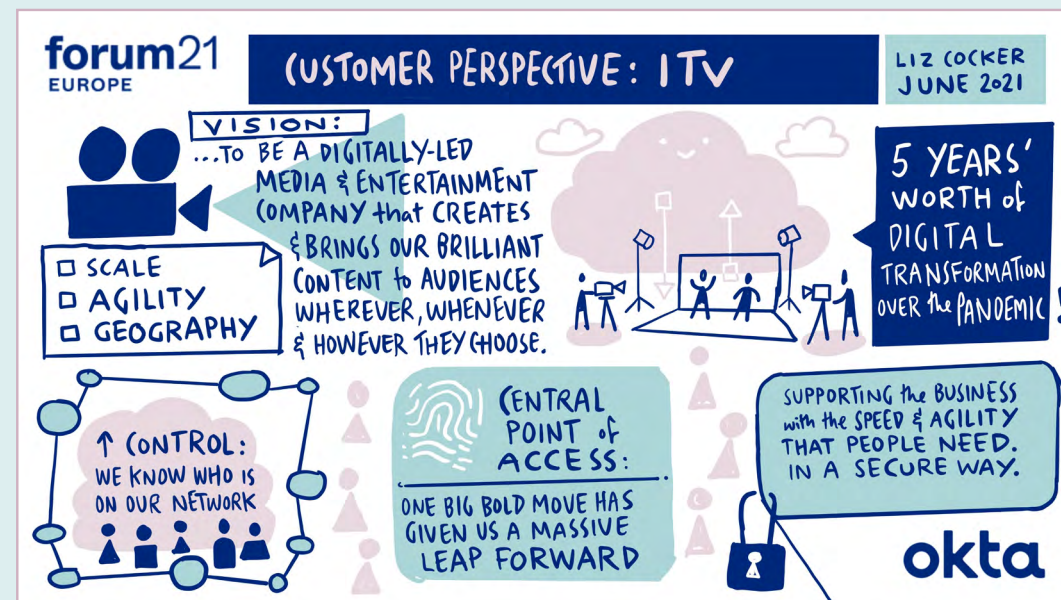
Perspective d'un client

ITV s'est donné pour mission de devenir une entreprise numérique de médias et de divertissement, créant et distribuant du contenu aux audiences où, quand et comme elles le veulent.

L'entreprise a adopté une approche radicale en implémentant Okta et en migrant ses ressources Google Workspace vers la plateforme dès le premier jour. Ce virage audacieux a obtenu l'adhésion de toute l'entreprise : séduites par la simplicité de sécurisation des applications, les équipes de développement se bousculent pour que leurs applications soient intégrées à Okta. Les responsables d'applications tirent parti des avantages d'Okta Workflows, qui leur permet de contrôler eux-mêmes les autorisations des applications grâce à des contrôles intégrés.

Pendant longtemps, ITV a disposé de plusieurs référentiels d'identités cloisonnés, notamment un Active Directory on-premise, un Active Directory de services fédérés et un annuaire Google. Les nouveaux comptes devaient être configurés à plusieurs endroits, au risque d'accorder un accès insuffisant ou excessif. Avec Okta, le nombre d'erreurs s'est effondré et les retards d'octroi des accès appartiennent désormais au passé.

La migration d'ITV vers le cloud a déjà porté ses fruits. Lorsque la pandémie de Covid-19 a contraint l'émission phare « I'm a Celebrity Get Me Out of Here » à déplacer son lieu de tournage de l'Australie au Pays de Galles, éliminant par la même occasion l'avantage du décalage horaire, les équipes de production ont dû redoubler d'inventivité pour accélérer l'étape du montage. Pour y parvenir, elles ont tiré parti de la puissance du cloud et ont réussi à abattre le travail technique normalement réalisé en cinq ans en seulement 14 mois.



“

Depuis qu'ITV a confié la gestion de ses identités à Okta, le nombre d'erreurs et les retards d'octroi des accès ont considérablement diminué.

itv

SESSION 3 : Satisfaire les nouvelles exigences des collaborateurs

Angela Salmeron
Associate Research
Director, IDC

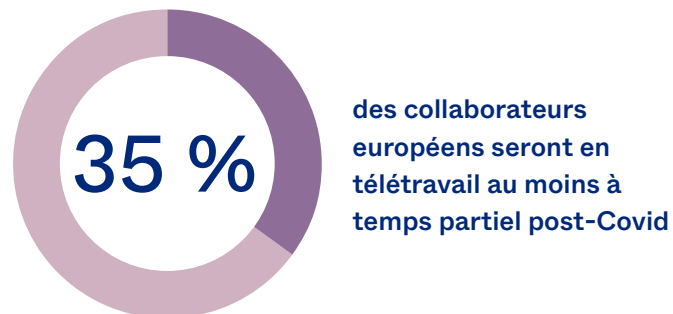
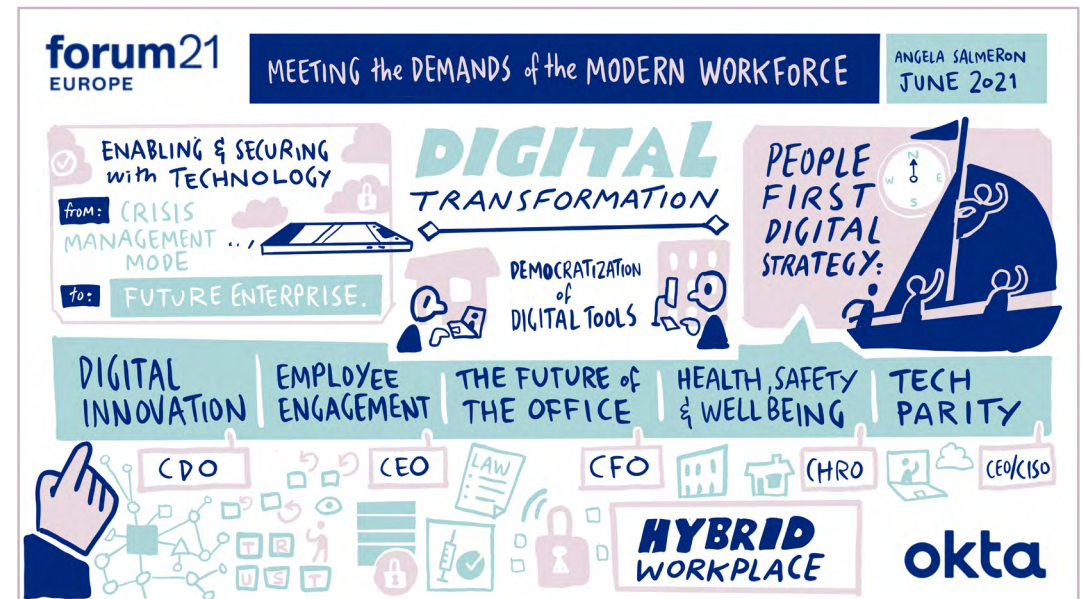


Satisfaire les nouvelles exigences des collaborateurs

La transformation digitale des entreprises est essentielle pour qu'elles puissent prospérer dans le contexte actuel. La prise en charge et la protection des équipes hybrides font partie des principaux défis technologiques : IDC prévoit que 35 % des collaborateurs européens seront en télétravail au moins à temps partiel post-Covid.

Mais les entreprises ne tireront leur épingle du jeu que si elles accordent la priorité à leurs collaborateurs. La parité des expériences de travail est primordiale. L'expérience numérique proposée par les entreprises sera décisive pour la rétention des collaborateurs. Cette tendance encourage l'adoption de suites de productivité cloud, l'implémentation de solutions de collaboration en équipe et la mise en place d'un accès distant sécurisé.

L'avenir des effectifs modernes requiert simplement que les bonnes personnes fassent partie des bonnes équipes au bon moment. De telles entreprises permettent une approche agile du travail, une collaboration interfonctionnelle et une prise de responsabilités de bout en bout. On observe ainsi l'émergence d'un nouveau paradigme organisationnel, caractérisé par la démocratisation des outils, un apprentissage continu et l'instauration d'une culture de la confiance. Celui-ci s'accompagne d'un nouveau modèle de leadership basé sur la passion, la vision, la transparence et la confiance.



SESSION 3 : Satisfaire les nouvelles exigences des collaborateurs

Ian Lowe
Director of Solutions
Marketing, Okta



Comment instaurer un climat de confiance au travail ?

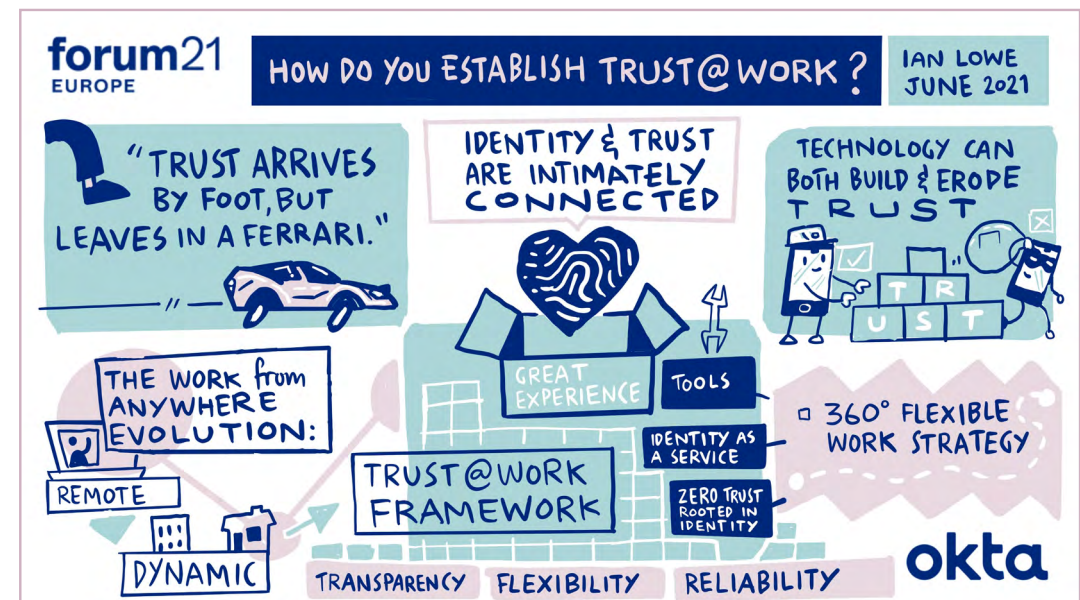
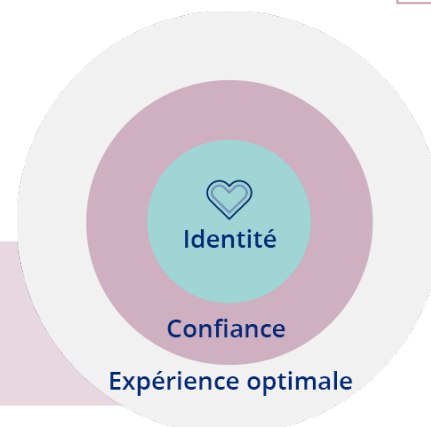
Le télétravail, en plein essor pendant la pandémie, a aujourd'hui laissé place au travail dynamique, permettant aux collaborateurs de travailler où, quand et comme ils le veulent. L'instauration d'un climat de confiance au travail offre une flexibilité inégalée. Les entreprises sont technologiquement équipées et optimisées pour prendre en charge leurs opérations quotidiennes et une confiance mutuelle est établie entre les entreprises et leurs collaborateurs.

Le modèle de confiance au travail repose sur trois grands principes :

1. **Optimiser l'outillage du télétravail.** Aujourd'hui plus que jamais, le travail repose sur vos collaborateurs. Vous devez donc mettre en place des structures de soutien numérique pour renforcer la flexibilité et le bien-être.
2. **Traiter l'identité comme un contrôle** plutôt que comme un service IT. Il s'agit de déterminer qui est l'utilisateur et pourquoi il a besoin d'un accès.
3. **Adopter une sécurité Zero Trust** pour octroyer aux bonnes personnes un accès adéquat, évalué en continu, aux ressources pertinentes.

Pour instaurer un climat de confiance au travail, l'identité doit être placée au cœur de votre architecture IT, afin de permettre à vos collaborateurs de travailler à l'endroit qui leur (et vous) convient.

La confiance et l'identité sont essentielles pour proposer des expériences optimales.



SESSION 3 : Satisfaire les nouvelles exigences des collaborateurs

Reem Zahran
Chief Information
Officer, Vistra



Perspective d'un client

Vistra est une entreprise de services professionnels évoluant dans le secteur financier, du patrimoine privé et des marchés de capitaux. Ces dernières années, des acquisitions lui ont permis de se développer considérablement. Ses priorités sont désormais tournées vers la consolidation et l'harmonisation des stratégies et systèmes technologiques disparates.

Au moment où la pandémie de Covid-19 a frappé, l'entreprise s'est retrouvée confrontée à des défis de taille : en effet, plus de 80 % de ses collaborateurs utilisaient encore des ordinateurs de bureau. Les utilisateurs avaient l'habitude de se tourner vers l'équipe IT lorsqu'ils avaient besoin d'aide. Le déploiement d'Okta a changé la donne, car il permet une connexion simple en libre-service grâce à la technologie d'authentification unique (SSO), ainsi que l'octroi plus rapide d'accès aux applications via Okta Integration Network.

Depuis le déploiement d'Okta et l'apport de modifications clés à son infrastructure, l'entreprise a complètement revu le concept de back-office. La technologie occupe désormais une place centrale et le service commercial, les opérations et l'IT travaillent ensemble vers un objectif commun.

L'entreprise est également déterminée à renforcer son niveau de sécurité en adoptant un modèle Zero Trust. Grâce à une formation continue et à l'aide du conseil d'administration, elle cherche à optimiser sa stratégie de sécurité et sa perception par les collaborateurs, avec comme objectif ultime un véritable modèle de « vérification systématique ».

“

L'entreprise a complètement revu le concept de back-office et la technologie occupe désormais une place centrale.

VISTRA 



SESSION 4 : Une expérience numérique optimale pour fidéliser vos clients

Duncan Brown
VP of Enterprise
Research Europe, IDC



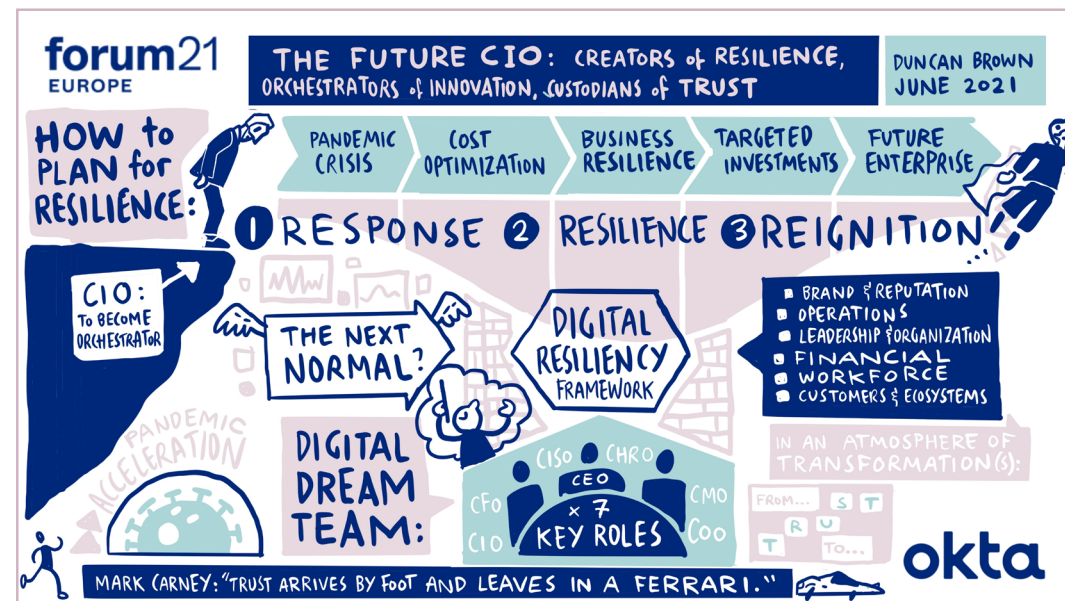
L'avenir du CIO : de la gestion de crise à l'entreprise du futur

Après 12 mois éprouvants, le premier défi que doivent aujourd'hui relever les CIO consiste à planifier la résilience. Et en particulier la résilience numérique, c'est-à-dire la capacité de l'entreprise à tirer parti de ses ressources numériques non seulement pour rétablir les opérations métier en cas de perturbation, mais aussi pour s'adapter aux nouvelles conditions.

La clé ? Une équipe numérique de choc composée d'experts de l'expérience client, des opérations, des ressources humaines, de la technologie, de la finance et de la sécurité. Si les budgets IT sont de moins en moins sous le contrôle direct du CIO, c'est tout de même à ce dernier que revient la responsabilité d'intégrer de nouvelles technologies à un plan cohérent.

De nombreuses expériences clients et collaborateurs ont besoin d'être repensées en mettant la confiance au premier plan. Dans le commerce de détail, l'essor du retrait des commandes en click & collect, sans aucun contact, exige des clients qu'ils accordent leur confiance à des personnes qu'ils ne rencontreront peut-être jamais, comme des chauffeurs-livreurs et des préparateurs de commandes. Une entreprise résiliente suscite la confiance en se concentrant sur ses principales valeurs : la responsabilité sociale et l'éthique, la sécurité, la conformité et la confidentialité. Il est crucial de trouver le juste équilibre, car si l'établissement d'une relation de confiance prend du temps, il suffit d'un instant pour la briser.

En 2021, le budget IT sera déterminé par les départements, et non par le CIO.



SESSION 4 : Une expérience numérique optimale pour fidéliser vos clients

Jiong Liu

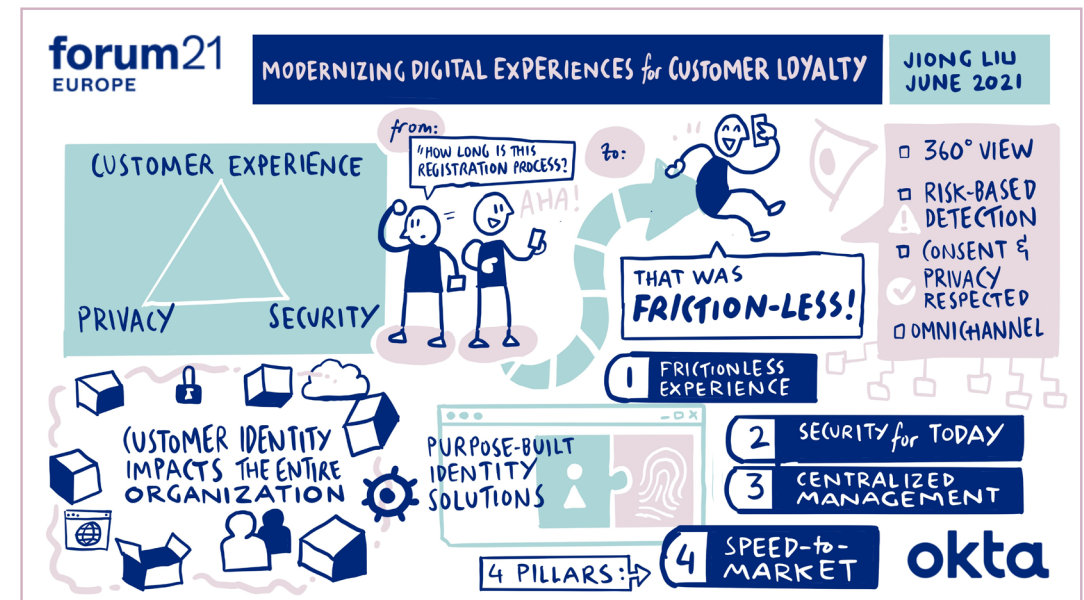
Director, Product Marketing
– Customer Identity, Okta

Une expérience numérique optimale pour fidéliser vos clients

Un juste équilibre entre facilité d'utilisation, confidentialité et sécurité est essentiel pour proposer des expériences numériques fluides aux clients. Il ne peut être atteint sans une gestion adéquate des identités. Les entreprises doivent viser quatre objectifs :

- 1. Expériences fluides** – Vous devez proposer une expérience cohérente dans toutes les applications et sur tous les terminaux que les clients sont susceptibles d'utiliser, en particulier en ce qui concerne les processus d'inscription et de connexion.
- 2. Sécurité en temps réel** – Le service d'identité doit être rigoureusement sécurisé afin de prévenir les brèches de sécurité, d'empêcher la fraude et de respecter les exigences de conformité et de confidentialité.
- 3. Gestion centralisée** – Vous devez gérer efficacement les décisions d'accès dans les diverses applications et sur les différents terminaux que les clients sont susceptibles d'utiliser, en particulier en automatisant les workflows centrés sur l'identité.
- 4. Mise sur le marché accélérée** – Les expériences clients évoluent sans cesse. Les équipes de développement doivent donc s'adapter et les optimiser en permanence. Grâce à des toolkits complets conçus à leur intention, les développeurs peuvent confier la gestion des identités à Okta et se concentrer sur leurs objectifs stratégiques.

En intégrant l'identité à leur écosystème technologique, les entreprises peuvent assurer la synchronisation des environnements et offrir les meilleures expériences possible à leurs clients.





SESSION 4 : Une expérience numérique optimale pour fidéliser vos clients

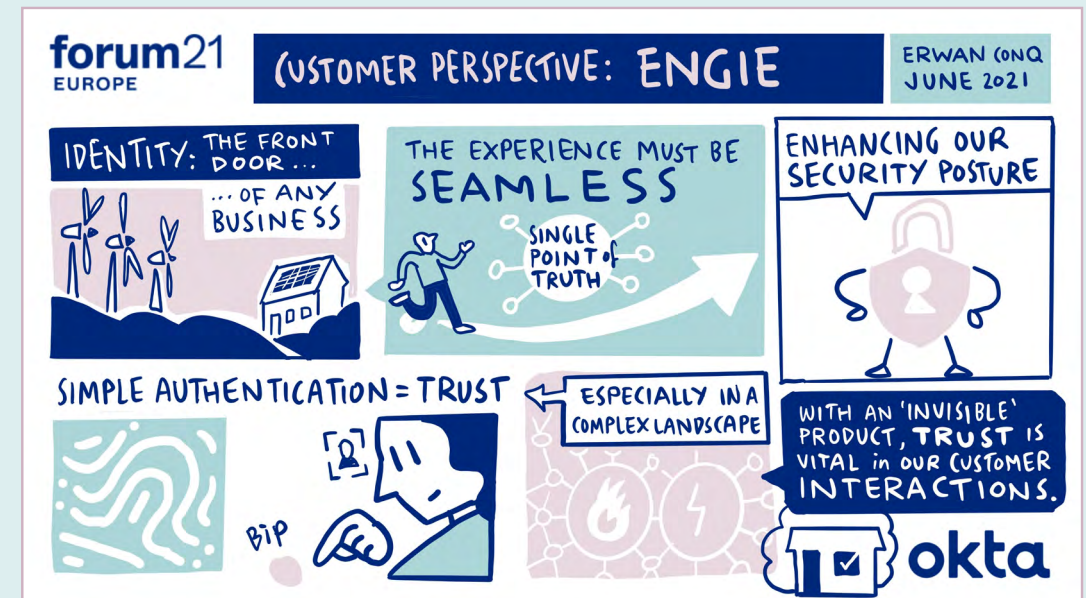
Perspective d'un client

Comme d'autres entreprises du secteur de l'énergie, le fournisseur français Engie a diversifié son offre en proposant des services d'équipement, comme des pompes à chaleur, des panneaux solaires et des bornes de recharge. Cette décision a entraîné l'augmentation du nombre de points de contact pour ses 10 millions de clients. Il est dès lors devenu indispensable de proposer une expérience utilisateur cohérente et sécurisée sur tous ces canaux.

La relation de confiance avec le client est cruciale. En tant que clients, nous utilisons de l'énergie, mais nous ne la voyons pas. Nous ne voyons que la relation que nous avons avec notre fournisseur d'énergie, p. ex. lorsque nous appelons le support client, que nous lisons notre facture ou que nous interagissons avec une application. La confiance joue un rôle déterminant dans la décision d'achat.

À mesure que l'énergie gagne en complexité, Engie estime qu'il devient de plus en plus important d'acquérir une connaissance approfondie du client. Pour préserver la confiance des clients et les fidéliser, l'entreprise s'est donnée pour mission de simplifier l'énergie pour ses clients, en leur offrant la bonne interaction, le bon produit ou le bon service au moment opportun.

Le déploiement d'Okta a permis à Engie de définir une source fiable unique pour les identités de ses clients, de mieux cerner ces derniers, de suivre leurs interactions avec la marque et de créer une expérience utilisateur fluide pour tous ses services.



“

Le monde est déjà assez complexe :
nous devons simplifier l'expérience de
tous nos clients qui utilisent de l'énergie.

ENGIE

SESSION DE CLÔTURE

Yves Couturier

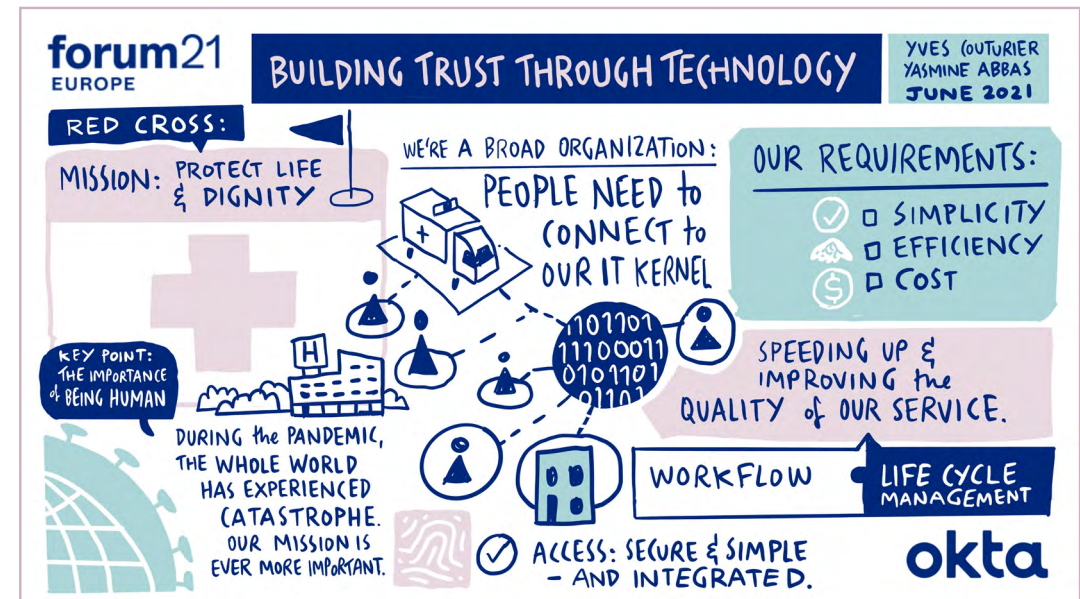
Director of Information Systems,
Croix-Rouge française

Établir la confiance grâce à la technologie

Créée il y a plus de 150 ans, la Croix-Rouge française compte aujourd'hui 60 000 volontaires du monde entier qui participent à des actions humanitaires. Il est difficile de connecter ces utilisateurs dispersés aux différents systèmes et applications dont ils ont besoin, mais c'est pourtant indispensable.

Auparavant, l'octroi d'accès était un processus chronophage (jusqu'à deux semaines pour un seul utilisateur). La Croix-Rouge nourrissait également des inquiétudes concernant la sécurité des autorisations et éprouvait des difficultés à déterminer si certains utilisateurs appartenaient toujours à l'association. Elle souhaitait une solution globale de gestion des identités et des accès permettant d'augmenter l'efficacité et de simplifier l'expérience pour ses membres.

Avec Okta, la validation d'un nouveau compte ne prend désormais pas plus de 10 minutes. Grâce à Okta Workflows, l'association a réussi à automatiser certains processus et à accélérer la gestion du cycle de vie des utilisateurs. Les utilisateurs apprécient la simplicité et la rapidité de l'accès aux applications fédérées via l'authentification unique (SSO). Dans les régions où la connectivité ne peut être garantie, les utilisateurs peuvent continuer à accéder à leurs applications et à leur boîte de réception grâce à l'authentification multifacteur hors ligne via Google Authenticator.



“

La plupart de nos activités ont lieu sur mobile. Nous disposons d'un grand nombre de terminaux, mais le déploiement d'Okta Verify s'est avéré d'une simplicité déconcertante.

croix-rouge française



SESSION DE CLÔTURE

Todd McKinnon
CEO et cofondateur,
Okta



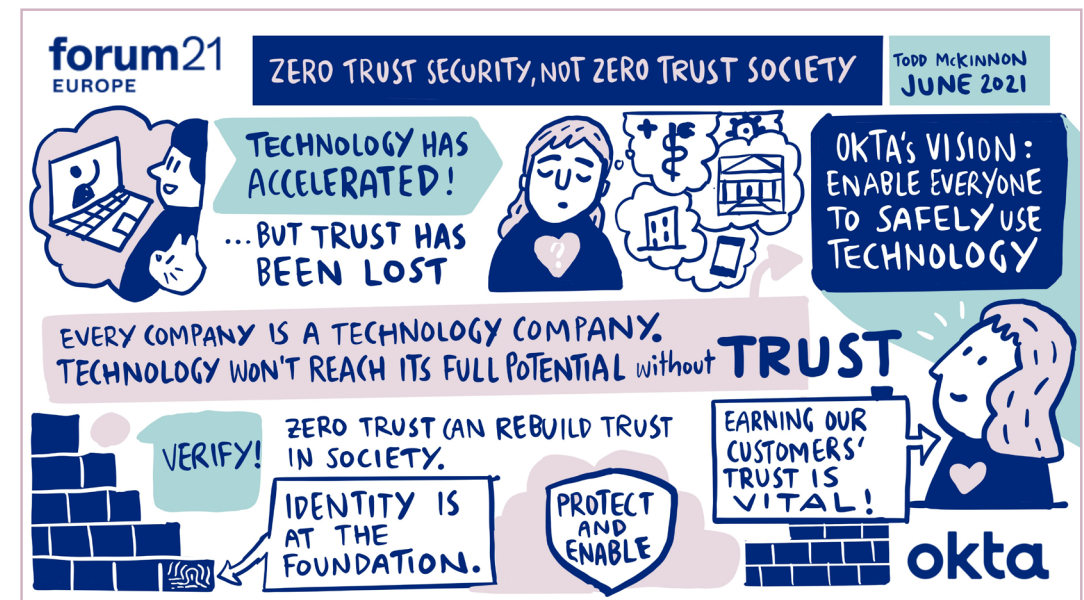
Oui à la sécurité Zero Trust, non à une société de méfiance

Ces douze derniers mois, la technologie est devenue partie intégrante de nos vies. Non seulement elle nous a permis de prendre en charge le télétravail, mais elle nous a aidés à répondre aux besoins humains fondamentaux : interagir avec ses amis et sa famille, se faire livrer de la nourriture ou consulter un médecin.

Mais elle a également apporté son lot de difficultés. Nous avons été exposés à des risques et nous nous sommes demandé comment et où nos informations étaient suivies. La confiance a été brisée, pas seulement dans la technologie, mais aussi dans les autorités, les dirigeants d'entreprise et la santé publique.

Cette question nous concerne tout particulièrement en tant que leaders technologiques, car la technologie ne pourra jamais atteindre son plein potentiel sans confiance. Au cours des dix prochaines années, notre mission sera de sécuriser ce que nous créons, de tenir compte des différentes utilisations (bonnes comme mauvaises) qui peuvent être faites de nos produits et de restaurer la confiance dans les technologies essentielles aux fondements de nos sociétés.

Chez Okta, nous pensons que la sécurité Zero Trust peut nous aider à ne pas devenir une société de méfiance. En créant des technologies qui offrent systématiquement aux utilisateurs le bon accès aux ressources pertinentes dans le contexte adéquat, nous prenons la responsabilité de la sécurité des utilisateurs plutôt que de leur faire endosser. Les leaders technologiques doivent faire de la confiance la pierre angulaire des technologies de demain. Chez Okta, nous continuerons à en faire notre priorité.



“

Les leaders technologiques doivent
faire de la confiance la pierre angulaire
des technologies de demain.

okta

forum21

EUROPE

okta

© Tous droits réservés. Okta 2021

