sonio.

Votre environnement de travail numérique est en feu.

Et votre service informatique s‘occupe d‘éteindre les incendies au lieu de poser les fondations.

Environnement de travail numérique : pilotage à l'aveugle.

Pourquoi les choix d'outils précipités hérités de la pandémie paralysent aujourd'hui les équipes IT.

Dans les services informatiques de nombreuses entreprises, un schéma s'est installé sans que personne ne l'ait sciemment souhaité : un compte ne fonctionne pas, un appareil tombe en panne, un accès fait défaut. On supprime, on rafistole, on improvise. Jour après jour, les tickets s'accumulent, et il ne reste tout simplement plus de temps pour le travail stratégique. Ce n'est pas un échec des équipes informatiques prises individuellement. C'est la conséquence logique d'une évolution qui a débuté il y a quelques années avec une crise mondiale.

La COVID-19 n'a pas accéléré la numérisation, elle l'a imposée. En l'espace de quelques semaines, les entreprises ont dû se doter des moyens nécessaires au télétravail. Vidéoconférences, stockage dans le cloud, plateformes de chat, accès VPN : chaque outil répondait à un problème urgent, et les décisions

RÉSUMÉ

Vous connaissez cette situation ? Les tickets s'accumulent, l'équipe informatique est en état de stress permanent et les collaborateurs perdent des heures à attendre l'assistance. La frustration l'emporte sur la motivation. Et tandis que votre service informatique éteint les incendies les uns après les autres, il ne reste plus de temps pour s'attaquer à la cause réelle du problème.

Ce qui a commencé en 2020 comme une solution d'urgence est aujourd'hui un problème structurel : sous la pression énorme de la pandémie de COVID-19, les entreprises ont dû se mettre au télétravail en l'espace de quelques semaines. Les outils se sont succédé, les décisions ont dû être prises à la hâte pour maintenir l'activité. Aujourd'hui, plusieurs années plus tard, il est nécessaire de remettre de l'ordre dans ces fondations. Le résultat de ces mesures d'urgence : des identités fragmentées, un « shadow IT », un périmètre de sécurité qui s'effrite et des coûts de licence dont près de la moitié part en fumée.
Ce livre blanc montre ce que cela coûte concrètement, pourquoi multiplier les logiciels ne résout pas le problème et comment mettre en place une infrastructure solide. Il aborde le contexte réglementaire suisse, présente des indicateurs concrets et formule des recommandations d'action pour trois horizons temporels.

devaient être prises à la hâte. Ce qui relevait alors du pragmatisme est aujourd'hui un patchwork. Et ce patchwork génère précisément les incendies que votre service informatique doit éteindre quotidiennement.

Dans la pratique, nous le constatons régulièrement : cinq à dix solutions qui se chevauchent constituent la norme, et non l'exception. Et ceux qui pensent que c'est exagéré devraient observer une journée de travail type.

> L'équipe informatique est en état de stress permanent, les tickets s'accumulent, les collaborateurs perdent du temps à attendre indéfiniment l'assistance ou à contacter le service d'aide. La frustration l'emporte sur la motivation.
>
> Sonio AG, Digital Workplace en pratique

L'offre se trouve sur OneDrive. Le dossier du projet est chez le partenaire externe, sur Dropbox. Les plans de construction sont sur le NAS local. Trois emplacements de stockage, un document que personne ne trouve du premier coup. Le partage s'effectue en parallèle via Teams, le canal Slack non officiel du service spécialisé – et quand il faut vraiment faire vite, le message atterrit dans un groupe WhatsApp. Chaque service gère ses tâches de son côté : les cadres dans Planner, la gestion de projet dans Asana, l'informatique dans Jira, les ventes dans Salesforce. Quatre systèmes, aucune vue d'ensemble.

Ce n'est pas un exemple extrême. C'est un lundi typique.

Une part considérable de ces applications n'a jamais été validée par le service informatique, mais payée par carte bancaire au sein du service métier. Si l'on demande qui a une vue d'ensemble, on n'obtient aucune réponse.

Ce que coûte réellement la prolifération anarchique

Ces chiffres ne sont pas un simple accroc, mais un signal d'alarme. Une entreprise de taille moyenne exploite aujourd'hui en moyenne environ 275 applications SaaS. Le service informatique en ignore environ un tiers : elles relèvent du « shadow IT », totalement hors de son champ de vision. Environ 70 % des dépenses logicielles sont désormais contrôlées par les services métier, et non par le service informatique (Zylo SaaS Management Index 2025).
Mais les logiciels ne constituent qu'un aspect du problème. De l'autre côté, il y a le matériel : les pénuries d'approvisionnement, la hausse des prix des composants et le raccourcissement des cycles de vie font grimper les coûts d'acquisition. Parallèlement,

EXEMPLE DE CALCUL : ce que coûte ce patchwork à une PME

Situation de départ : entreprise comptant 150 collaborateurs

Tickets d'assistance :	Ø 60/mois × 45 min. × 120 CHF de coût horaire = 54'000 CHF/an
Licences inutilisées :	150 utilisateurs × 80 CHF/mois × 50 % de non-utilisation = 72'000 CHF/an
Retard d'intégration :	15 collaborateurs/an × 3 jours × 600 CHF/jour = 27'000 CHF/an

Total des coûts évitables : ≈ 153'000 CHF/an

Ces chiffres sont calculés de manière prudente et ne tiennent compte ni des incidents de sécurité ni des atteintes à la réputation.

la charge administrative liée à un parc d'appareils de plus en plus hétérogène ne cesse d'augmenter : plus de modèles, plus de plateformes, plus de configurations manuelles. En Suisse, le SWICO ICT Index montre que, malgré la pression sur les coûts, les dépenses informatiques continuent d'augmenter – sans que l'efficacité progresse proportionnellement. La prolifération incontrôlée des logiciels et la pression sur le matériel s'additionnent pour former une spirale des coûts qui ne se résoudra pas d'elle-même sans intervention structurelle.

Pire encore : près de la moitié de toutes les licences logicielles achetées restent inutilisées. Selon Flexera, en moyenne 27 % des dépenses liées au cloud sont absorbées par des licences inutilisées et des outils redondants. Pour un budget SaaS d'un million de francs, cela représente plus de 250'000 francs par an qui ne profitent à personne.

Quatre points chauds dans votre environnement de travail numérique

IDENTITÉS FRAGMENTÉES :
Les collaborateurs disposent de comptes dans des dizaines de systèmes. Personne ne sait avec certitude qui a accès à quoi. Lorsqu'un collaborateur quitte l'entreprise, ses accès restent souvent actifs pendant des mois. Une porte ouverte aux attaques.

SHADOW IT :
Les services métier acquièrent des outils sans passer par le service informatique. Les données de l'entreprise se retrouvent dans des systèmes que personne n'a jamais vérifiés. Cela représente à la fois un risque de sécurité et un risque de non-conformité.

PÉRIMÈTRE FLOU :
Le travail s'effectue au bureau, en télétravail et en déplacement. Les concepts conçus pour le réseau d'entreprise ne sont tout simplement plus adaptés.

SHADOW AI :
Les collaborateurs transfèrent des données d'entreprise vers des comptes ChatGPT privés ou d'autres comptes d'IA, sans que personne ne contrôle cela. Il s'agit de la nouvelle forme la plus dangereuse de « shadow IT » et, actuellement, l'un des points sensibles les plus souvent cités par les CISO suisses.

Source : Zylo SaaS Management Index 2025. Pour la Suisse, le SWICO ICT Index révèle que, malgré la pression sur les coûts, les dépenses informatiques continuent d'augmenter – sans pour autant s'accompagner d'une hausse proportionnelle de l'efficacité. HR Today / Kienbaum Vergütungsreport Schweiz 2025 : hrtoday.ch

Le pare-feu ne suffit plus.

Le pare-feu protège le périmètre. Mais ce périmètre n‘existe plus tel quel. Aujourd‘hui, la sécurité doit agir là où l‘on accède aux données.

Autrefois, c’était simple : à l’intérieur du réseau d’entreprise, c’était la confiance ; à l’extérieur, la méfiance. Le pare-feu faisait office de rempart. Ce modèle est révolu – non pas parce qu’il était mal conçu, mais parce que le monde du travail a fondamentalement changé. Le problème, c’est que de nombreuses entreprises continuent de sécuriser un monde qui n’existe plus.

Le travail hybride est la norme, et non un scénario exceptionnel

Aujourd‘hui, les collaborateurs travaillent depuis le bureau, en télétravail, dans le train ou au café. Ils utilisent aussi bien des appareils professionnels que personnels. Les données sont stockées dans le cloud, sur des serveurs locaux et dans des applications SaaS, souvent tout à la fois. Il n‘y a plus de distinction entre « intérieur » et « extérieur ». Il n‘y a plus que des accès – et chacun d‘entre eux relève d‘un choix de confiance. Celui qui laisse ce choix au hasard a déjà perdu.

Le pirate ne « pirate » plus. Il se connecte.

Les attaquants ont compris cette évolution depuis longtemps. Selon le rapport Verizon Data Breach Investigations Report 2025, 80 % des fuites de données sont dues à des identifiants compromis ou volés. Microsoft bloque désormais plus de 7‘000 attaques basées sur des mots de passe par seconde – soit une augmentation de 75 % par rapport à l’année précédente. Les attaques visant les comptes de messagerie professionnels (BEC) ont augmenté de 34 % en 2025. Les e-mails de phishing générés par l’IA sont désormais pratiquement impossibles à distinguer des vrais. Le rapport « ENISA Threat Landscape 2025 » le confirme : les identités constituent la principale porte d’entrée des attaquants dans les entreprises européennes.

> Le travail hybride sans architecture « zero trust » est une promesse de sécurité sans fondement.
>
> Sonio AG, Digital Workplace en pratique

Conséquence : lorsqu’un compte est compromis, l’attaquant est, dans la plupart des cas, considéré par le système comme un collaborateur légitime – et bénéficie ainsi de tous les droits d’accès associés à ce compte. Dans un environnement hétéroclite où les identités sont fragmentées, cela peut se traduire par un accès complet, inaperçu, pendant des semaines. L’authentification multifactorielle a constitué la première étape importante vers la protection des identités. La prochaine étape consiste à adopter les clés d’accès et les architectures sans mot de passe : elles éliminent complètement le mot de passe en tant que point de vulnérabilité, résistent au phishing

et garantissent la sécurité des identités même lorsque les identifiants de connexion provenant d'autres sources sont divulgués.

Contexte réglementaire suisse : ce qui s'applique actuellement

Pour les entreprises suisses, la pression réglementaire s'intensifie simultanément à plusieurs niveaux :

- **nLPD (nouvelle loi sur la protection des données) :** En vigueur depuis septembre 2023. Les entreprises doivent être en mesure de prouver quelles données elles traitent, à quelles fins et qui y a eu accès. En cas de violation de la sécurité des données, il existe une obligation de déclaration auprès du PFPDT. Conséquences en cas d'infraction : amendes pouvant aller jusqu'à 250'000 CHF pour les personnes responsables, atteinte à la réputation et responsabilité civile envers les per sonnes concernées. PwC Suisse estime qu'une grande partie des PME suisses ne satisfait pas encore pleinement à ces exigences.

- **Loi sur la sécurité de l'information (LSI) :** À partir de 2025, les exploitants d'infrastructures critiques seront tenus de signaler les cyberattaques graves à l'OFCS (ex-NCSC) dans un délai de 24 heures. En cas de non-respect, des amendes pouvant aller jusqu'à 100'000 CHF sont encourues. Le rapport semestriel 2025/2 de l'OFCS montre que le phishing et les ransomwares restent les vecteurs d'attaque dominants en Suisse.

- **Exigences de la FINMA :** Les établissements financiers sont soumis à des prescriptions strictes en matière de contrôles d'accès, de pistes d'audit et de souveraineté des données. Les infractions peuvent entraîner le retrait de la licence, des amendes et la responsabilité personnelle de la direction. Un environnement de travail numérique sans traçabilité complète ne constitue pas un modèle opérationnel pour les entreprises réglementées, mais un risque direct en matière de responsabilité.

- **Cloud Act américain et souveraineté des données :** Toute entreprise utilisant les services de cloud public de fournisseurs américains doit savoir que les autorités américaines peuvent accéder à ces données en vertu du Cloud Act, quel que soit l'emplacement physique des serveurs. Pour les entreprises suisses détenant des données clients sensibles, un modèle de déploiement en Suisse n'est pas une option, mais une obligation.

Tout se joue dans les fondations.

Une architecture Workplace intégrée réduit la complexité et renforce la sécurité.

Lorsque quelque chose ne fonctionne pas dans l'environnement de travail numérique, le réflexe est presque toujours le même : un nouvel outil. La collaboration pose problème ? Un outil de collaboration. Les fichiers sont éparpillés ? Une nouvelle solution de stockage. Le service d'assistance croule sous les demandes ? Un système de tickets. Chacune de ces décisions était compréhensible – et a aggravé le problème sur le plan structurel.

> Celui qui commence par les outils, en haut de la pyramide, plutôt que par l'identité, en bas, construit sur du sable. Cela peut bien se passer pendant des années. Jusqu'au premier incident de sécurité.
>
> Sonio AG, Digital Workplace en pratique

Car ce réflexe traite les symptômes, pas les causes. Chaque outil supplémentaire dépourvu de fondement architectural accroît la complexité qu'il était censé réduire. Résultat : plus de tickets, plus de « shadow IT », plus de failles de sécurité – et des coûts plus élevés. Vous n'achetez donc pas la solution, mais le prochain problème.

Ce que nous avons retenu de dizaines de projets « Digital Workplace » : le Digital Workplace ne fonctionne pas comme un ensemble d'outils, mais comme une architecture. La productivité, la sécurité et la satisfaction découlent d'une base bien pensée et intégrée, reposant sur l'identité, la gestion des terminaux et le contrôle d'accès. C'est la structure qui fait la différence. Pas les outils.

C'est ce qui détermine si un nouvel outil est opérationnel en quelques jours ou en plusieurs mois. Si le départ d'un collaborateur est géré sans heurts en quelques minutes ou en plusieurs semaines. Et si un mot de passe compromis reste un simple désagrément ou s'il permet d'accéder à l'ensemble des données de l'entreprise.

Commencer par l‘outil, c‘est construire à l‘envers.

Identité, sécurité, terminaux et intégration forment la base d‘un Digital Workplace sûr, évolutif et prêt pour l‘IA.

Un Digital Workplace solide se construit comme un bâtiment : de bas en haut. Les outils visibles, avec lesquels les collaborateurs travaillent au quotidien, constituent le dernier étage. En dessous se trouvent quatre couches porteuses. Le tout est encadré par la gouvernance et la conformité.
Celui qui ignore ces fondations et commence directement par les outils construit sur du sable. Tôt ou

COUCHE	CE QU’ELLE APPORTE
Gouvernance et conformité	Le cadre qui régit tout : traçabilité, souveraineté des données (nLPD, Cloud Act), règles claires sur qui a le droit de faire quoi et où se trouvent les données.
Outils visibles + IA	Collaboration, communication, applications métier, assistants IA. Ce que voient les collaborateurs. C’est important, mais cela n’est sécurisé que si les fondations sont solides.
4. Intégration	Relier le cloud et les infrastructures sur site, contrôler les flux de données, éviter les solutions en silos. Un seul environnement de travail, pas dix.
3. Terminaux gérés	Gestion unifiée des terminaux pour Windows, macOS, iOS et Android. Chaque appareil est identifié, conforme et peut être verrouillé à distance en cas d'urgence.
2. Sécurité / Zero Trust	Pas de confiance implicite. Chaque accès est vérifié : qui, d'où, avec quel appareil. Les clés d'accès (Passkeys) et l'authentification sans mot de passe constituent la prochaine étape.
1. Identité	Le fondement. Une identité centrale et unique par personne. Une entrée, une sortie, un modèle d’autorisation. C’est là que commence la sécurité.

Le modèle fondamental : à lire de bas en haut. Les outils se trouvent tout en haut, car ils constituent la base de tout le reste.

tard, il glissera – lors du premier incident de sécurité, du prochain départ d'un collaborateur ou, au plus tard, lorsque le prochain audit révélera que plus personne ne sait qui a accès à quoi.

> La préparation à l'IA ne commence pas par l'outil d'IA. Elle commence par la question de savoir qui a accès à quoi aujourd'hui.
>
> Sonio AG, Digital Workplace en pratique

L'ordre est déterminant. Celui qui met d'abord de l'ordre dans la couche d'identité peut ensuite remplacer les outils presque à sa guise. Celui qui achète d'abord les outils consolide le chaos – et en paie le prix double : une fois à l'achat, une fois lors de la gestion quotidienne des urgences. Et encore une réflexion d' , qui prend aujourd'hui de plus en plus d'importance : la préparation à l'IA ne commence pas par l'outil d'IA. Elle commence précisément ici – par une structure d'identité claire, des modèles d'autorisation précis et une base qui contrôle qui a le droit d'accéder à quoi. Celui qui dispose de cette base peut utiliser les systèmes d'IA de manière sûre et pertinente. Celui qui ne l'a pas rend son entreprise plus vulnérable aux attaques via l'IA.

Moins d‘efforts. Plus d‘impact.

Un Digital Workplace bien pensé réduit les coûts et les risques, allège la charge des équipes IT et rend les collaborateurs plus productifs dès le premier jour.

Un environnement de travail numérique bien conçu transforme le quotidien de manière mesurable, selon cinq dimensions :

- **Sécurité :** Identité et « Zero Trust » plutôt qu’un périmètre ouvert. Étant donné que 80 % des fuites de données trouvent leur origine dans des identifiants compromis, une gestion centralisée des identités associée à une authentification multifactorielle (MFA) résistante au phishing (clés d’accès) constitue le levier de sécurité le plus efficace. Aucun autre investissement n’offre une meilleure protection par franc.

- **Coûts :** Consolidation des licences qui se chevauchent. Si environ la moitié des licences reste inutilisée et qu’un bon quart des dépenses cloud est gaspillé, une entreprise de 150 personnes dispose d’un potentiel d’économies annuel de 70‘000 à 150‘000 CHF rien qu’en rationalisant ses licences.

- **Rapidité :** Dès leur premier jour, les nouveaux collaborateurs reçoivent un appareil entièrement configuré avec tous les droits d’accès, au lieu d’attendre plusieurs jours pour que leurs comptes soient activés. Lorsqu’ils quittent l’entreprise, tous leurs accès sont révoqués de manière centralisée et immédiate. En quelques minutes, pas en plusieurs semaines.

- **Contrôle et conformité :** Qui a accédé à quoi et quand ? Où se trouvent quelles données ? Grâce à une architecture épurée, ces rapports sont disponibles en un clic – et ne posent plus aucun problème lors des audits nLPD ou des contrôles de la FINMA.

- **Allègement de la charge de travail du service informatique :** Les appareils standardisés et gérés génèrent nettement moins de tickets d’assistance. Dans le cadre de projets accompagnés, le nombre de tickets d’assistance a pu être réduit de 35 à 50 % une fois la mise en place complète de l’infrastructure de base. Votre service informatique gagne ainsi du temps pour se consacrer à la stratégie plutôt qu’à la gestion des urgences.

Un autre avantage rarement quantifié : Les collaborateurs dont les outils fonctionnent simplement préfèrent travailler – et restent plus longtemps. En Suisse, le recrutement d’un spécialiste coûte entre 15‘000 et 40‘000 CHF selon le poste (annonce d’emploi, recrutement, intégration). Un environnement de travail numérique fluide, en tant qu’argument de marque employeur, n’est donc pas un indicateur subjectif, mais bien un indicateur concret.

Au plus tard en cas d‘incident, c‘est l‘architecture qui compte.

Appareils perdus, accès mal maîtrisés et tickets de support inutiles montrent ce que coûte réellement l‘absence de fondations.

Deux scénarios tirés de la pratique illustrent ce que signifie au quotidien la différence entre une approche axée sur les outils et une approche axée sur l’architecture.

L’appareil perdu – et aucune réponse à la question « Qu’y avait-il dessus ? »

Une entreprise comptant environ 200 collaborateurs équipe ses équipes de nouveaux ordinateurs portables pour le travail hybride. Les appareils sont modernes, les collaborateurs satisfaits – le projet est considéré en interne comme un succès. Mais ce que personne n’a mis en place, c’est l’architecture sous-jacente : pas de gestion centralisée des terminaux, pas de contrôle d’accès, pas de chiffrement des appareils avec gestion centralisée des clés. Lorsqu’un ordinateur portable est perdu dans le train, personne ne peut dire quelles données s’y trouvaient, et personne ne peut le verrouiller ou l’effacer à distance. L’appareil atterrit quelque part – avec un accès potentiel aux e-mails de l’entreprise, à SharePoint et aux outils internes. Résultat : urgence informatique, enquête juridique, obligation de déclaration selon la nLPD. Acheter de nouveaux appareils, c’est facile. Mettre en place une architecture qui les rende sécurisés, voilà la véritable tâche.

> Les problèmes informatiques les plus coûteux ne sont pas dus à de mauvais outils. Ils résultent d’une architecture défaillante – et n’apparaissent que lorsqu’il est trop tard.
>
> Sonio AG, Digital Workplace en pratique

40 % de tickets en moins après la mise en place de Fundament

Une entreprise du secteur des services (environ 120 collaborateurs) a constaté que son équipe informatique traitait plus de 80 tickets par mois, dont plus de la moitié étaient dus à des problèmes d’accès, à des configurations manquantes et à des statuts d’appareils flous. Après la mise en place structurée d’une gestion centralisée des identités, d’une gestion des terminaux et d’un processus d’intégration rigoureux : baisse du nombre de tickets mensuels à moins de 50 en l’espace de trois mois – soit une réduction d’environ 40 %. Pendant cette période, le service informatique a pu, pour la première fois, travailler sur une feuille de route en matière de sécurité, au lieu de passer ses journées à éteindre des incendies.

C'est l'ordre qui fait la différence.

D'abord comprendre, puis structurer, intégrer et consolider : c'est ainsi que naît un Digital Workplace qui fonctionne sur la durée.

Comment passer de la gestion des urgences à la construction ? D'après notre expérience en matière de projets, une approche en cinq étapes a fait ses preuves. L'ordre des étapes n'est pas une simple suggestion, mais le cœur même de la méthode. Il ne s'agit pas d'un projet « Big Bang », mais d'un parcours ponctué de succès intermédiaires.

Le simple état des lieux permet déjà de mettre au jour des licences inutilisées et des accès à risque, qui peuvent être immédiatement corrigés. En adoptant une approche structurée, le travail d'architecture est souvent financé par les économies réalisées dès les premiers mois.

La démarche en 5 étapes vers un Digital Workplace pérenne

ÉTAPE 1
État des lieux : Quels outils, identités, appareils et accès existent réellement ? Y compris le « shadow IT » et le « shadow AI ». Cet inventaire est décevant, mais indispensable.

ÉTAPE 2
Définir les fondements : Définir le modèle d'identité et d'accès, ancrer les principes du « zero trust », planifier la feuille de route vers les clés d'accès (passkeys) et l'authentification sans mot de passe. Une identité par personne, un accès avec des droits minimaux.

ÉTAPE 3
Mettre en place la couche « appareils et intégration » : Déployer une gestion unifiée des terminaux (Unified Endpoint Management), connecter de manière transparente les systèmes cloud et sur site, garantir la souveraineté des données.

ÉTAPE 4
Ancrer la gouvernance : Établir des règles claires concernant les nouveaux outils, le stockage des données, l'utilisation de l'IA et les accès. Suffisamment souples pour être respectées au quotidien. Suffisamment contraignantes pour empêcher le retour d'une gestion anarchique.

ÉTAPE 5
Consolider et optimiser les outils : Remplacer les solutions redondantes, intégrer correctement les outils restants, former et accompagner les collaborateurs.

Pas un fournisseur d'outils de plus. Un partenaire pour l'ensemble.

Sonio accompagne le Digital Workplace de manière globale : de l'identité et la sécurité à l'exploitation courante, en passant par l'intégration et la gouvernance.

La plupart des entreprises ne disposent ni des connaissances spécialisées ni des capacités disponibles pour mettre en place une architecture de l'environnement de travail en parallèle de leurs activités quotidiennes. Ce dont elles ont besoin, ce n'est pas d'un simple vendeur de logiciels, mais d'un partenaire qui prenne le temps de comprendre leur situation – puis qui mette en œuvre l'architecture et en assume la responsabilité lors de l'exploitation.

C'est précisément le rôle de Sonio. Nous nous concentrons sur la stratégie, les fondements techniques et l'accompagnement de l'environnement de travail numérique :

- **Gestion des identités et des accès :** Une couche d'identité centralisée et structurée, fondement de la sécurité, de la conformité et de la préparation à l'IA.
- **Gestion moderne des terminaux :** Gestion unifiée des terminaux sur toutes les plateformes, y compris les services de déploiement, de la phase de préparation à l'accompagnement sur site et à la formation des collaborateurs.
- **Sécurité « zero trust » et authentification sans mot de passe :** Sécurité des terminaux, contrôle d'accès, clés d'accès et, sur demande, connexion à un centre d'opérations de sécurité. Une approche proactive plutôt que réactive.
- **Intégration du cloud et des environnements sur site :** Une connectivité sécurisée plutôt que des solutions en silos, adaptée à l'infrastructure existante et aux exigences en matière de souveraineté des données.
- **Gouvernance, conformité et souveraineté des données :** Structures traçables, exploitation en Suisse, conformité à la nLPD et à la LSI.
- **Gestion du changement et autonomisation :** Les collaborateurs doivent devenir productifs avec les nouveaux outils. Nous accompagnons ce processus : de la formation dès le premier jour au développement continu des compétences numériques.

Structurer, plutôt qu‘éteindre des incendies.

Identité, sécurité et gouvernance posent les fondations d‘un Digital Workplace.

Votre environnement de travail numérique est en feu, et votre service informatique s’occupe de l’éteindre. La vérité, c’est que tant que personne ne posera les fondations, le feu continuera de brûler. Multiplier les outils ne résout pas un problème structurel – cela ne fait que l’aggraver.

Les enseignements clés :

- **La gestion des urgences est un symptôme, pas une stratégie.** Si votre service informatique ne fait plus que lutter contre les incendies, ce n’est pas de sa faute, mais celle d’un environnement de travail dépourvu de fondations.

- **L’identité est le nouveau périmètre.** 80 % des fuites de données trouvent leur origine dans des identifiants compromis. Celui qui ne maîtrise pas la couche d’identité perd le contrôle.

- **La prolifération anarchique a un coût.** Près de la moitié des licences ne sont pas utilisées, un quart des dépenses liées au cloud part en fumée sans apporter de valeur ajoutée. Remédier à cela n’est pas un programme d’économies – c’est la fin d’un désordre coûteux.

- **La préparation à l’IA commence par les fondations.** Pour utiliser l’IA de manière judicieuse et sécurisée, il faut d’abord disposer d’identités fiables, de modèles d’autorisation clairs et de la souveraineté des données. Sans ces fondations, l’IA rend une entreprise plus vulnérable, et non plus productive.

- **La réglementation n’attend pas.** nLPD, LSI, FINMA : le cadre réglementaire suisse est en vigueur. Des amendes pouvant atteindre 250‘000 CHF, des obligations de déclaration et une responsabilité personnelle sont les conséquences pour les entreprises ne disposant pas d’une architecture rigoureuse.

Pas demain.Maintenant.

Avec les bonnes mesures immédiates, un plan à 90 jours clair et une feuille de route à long terme, la lutte permanente contre les incendies laisse peu à peu place à un Digital Workplace maîtrisable.

Réparties selon trois horizons temporels – pour les responsables informatiques, les CIO et les directeurs financiers.

Mesures immédiates : cette semaine

1. Faites le point sur la réalité des tickets : demandez à consulter les tickets d'assistance des trois derniers mois. Quelle part correspond à des interventions récurrentes de « pompier » ? Ce chiffre constitue votre argumentaire auprès de la direction.
2. Effectuez un bilan de l'IA : quels outils d'IA vos collaborateurs utilisent-ils déjà – officiellement et officieusement ? Quelles données de l'entreprise y sont stockées ? C'est votre risque de « shadow IT » le plus urgent aujourd'hui.
3. Lancez un inventaire des outils : quelles applications sont utilisées ? Qui les paie, qui les utilise réellement ? Attendez-vous à des surprises.
4. Effectuez un test de départ : imaginez le départ fictif d'un collaborateur ; combien de temps faut-il pour que tous ses accès soient révoqués ? Si la réponse se mesure en jours, vous connaissez votre plus grande lacune en matière de conformité.

À moyen terme : au cours des 90 prochains jours

1. Inventaire complet : Trecensez systématiquement les outils, les identités, les appareils et les accès, y compris le « shadow IT » et le « shadow AI ». Résiliez immédiatement les licences inutilisées.
2. Définir un modèle d'identité et d'accès : une identité par personne, l'authentification multifactorielle (MFA) généralisée, une feuille de route vers les clés d'accès (passkeys) et l'authentification sans mot de passe, un accès fondé sur le principe du moindre privilège.
3. Mettre en place la gestion des terminaux : Jchaque appareil doit être identifié, conforme et gérable à distance. Les appareils professionnels ainsi que les appareils privés ayant accès au réseau de l'entreprise doivent être intégrés dans ce système de gestion.
4. Organiser un entretien-conseil : discutez avec un partenaire qui prend le temps de comprendre votre situation et qui analyse honnêtement votre architecture avant de formuler des recommandations.

Stratégie : votre feuille de route pour l'environnement de travail

1. Ancrer la gouvernance : des règles claires pour les nouveaux outils, l'utilisation de l'IA, le stockage des données et les accès. Simples, contraignantes, conformes à la nLPD.
2. Consolider les outils : remplacer les solutions redondantes, intégrer proprement celles qui restent. L'objectif est d'avoir un seul environnement de travail, pas dix.
3. Passer du réactif au proactif : mettre en place une surveillance et une automatisation permettant de résoudre les problèmes avant même que les collaborateurs ne s'en aperçoivent.
4. Garantir la préparation à l'IA : mettre en place les fondements qui rendent l'utilisation de l'IA sûre : identités claires, modèles d'autorisation, souveraineté des données.

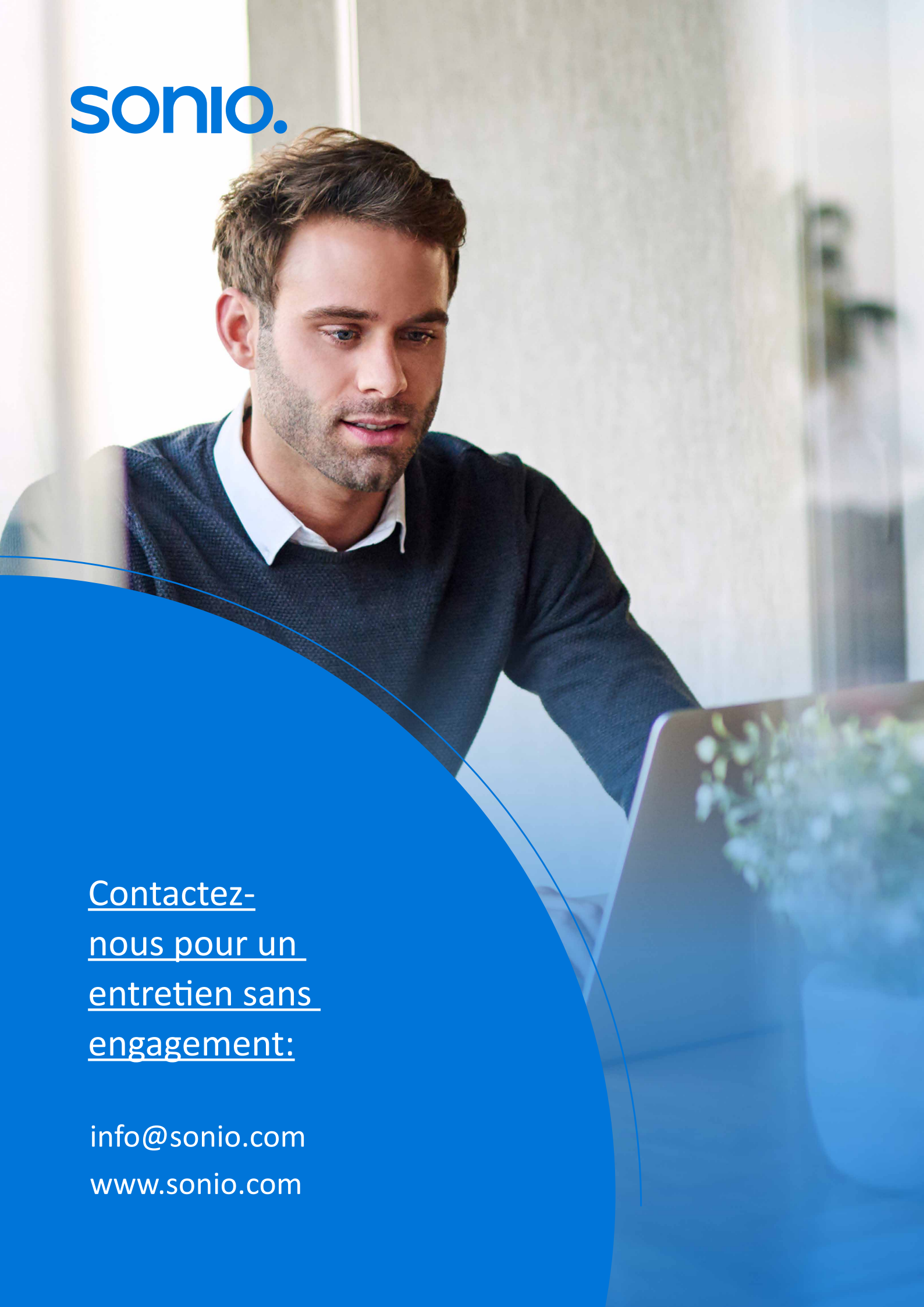
FAIRE LE PREMIER PAS DÈS MAINTENANT.

Analysons ensemble l'architecture actuelle de votre environnement de travail : où en sont vos fondations, où se trouvent les principaux points sensibles et quelles mesures ont un effet immédiat.
Nous prenons le temps de comprendre votre situation avant de vous faire des recommandations.

Prenez rendez-vous dès maintenant pour un premier entretien sans engagement :

info@sonio.com
www.sonio.com/fr-ch/digital-workplace

Sources : Source primaire : entretien avec Michael Wilkens (responsable de l'environnement de travail numérique, Sonio AG) et Jonny Neumann-Nitsche (expert en sécurité et travail moderne, Sonio AG), juillet 2026. Cet entretien a constitué la base thématique du livre blanc : les observations pratiques, le modèle fondamental, la métaphore de la lutte contre les incendies, l'approche de la « préparation à l'IA » ainsi que le positionnement de Sonio dans le domaine de l'environnement de travail numérique proviennent directement de cet entretien. Sources suisses et européennes : rapport semestriel 2025/2 de l'OFCS (phishing et ransomwares comme principales menaces en Suisse). SWICO ICT INDEX T3 2026 (pression sur les coûts et efficacité sur le marché suisse). ENISA Threat Landscape 2025 v1.2 (les identités comme porte d'entrée, UE). PwC Suisse : « Quels changements importants la révision de la LPD entraîne-t-elle ? » (Conséquences financières de la nLPD en Suisse). nLPD (loi fédérale sur la protection des données, en vigueur depuis septembre 2023). LSI (loi sur la sécurité de l'information, RS 128). Sources internationales : Zylo SaaS Management Index 2025 (275 applications SaaS en moyenne, un tiers de « shadow IT », environ 50 % de licences inutilisées). Flexera State of the Cloud 2025 (27 % des dépenses cloud gaspillées). Verizon Data Breach Investigations Report 2025 (80 % des fuites de données dues à des identifiants compromis). Rapports de sécurité Microsoft 2025 (plus de 7'000 tentatives de piratage de mot de passe bloquées par seconde, +75 % en glissement annuel ; BEC +34 %). Sonio AG : article de blog « Workplace Rollout Services : votre avantage concurrentiel dans la transformation numérique », juillet 2025 ; « La réussite de l'environnement de travail numérique passe par des services professionnels de préparation et de déploiement » ; pages d'accueil sonio.com/digital-workplace, sonio.com/digital-workplace-firefighting.



Contactez-
nous pour un
entretien sans
engagement:

info@sonio.com
www.sonio.com