LIVRE BLANC

Livre Blanc IGEL sur la Sécurité

Contenu

Introduction:

À mesure que les charges de travail des entreprises s'éloignent de plus en plus du Terminal pour s'exécuter dans des environnements hébergés comme l'infrastructure de bureau virtuel (VDI), le bureau virtuel mis à disposition en tant que service (DaaS) ou des applications purement basées sur le cloud telles que les solutions de type SaaS, les organisations se voient offrir une occasion unique de repenser leur stratégie concernant les terminaux, et en particulier une meilleure approche de la sécurité du Terminal. Alors que les stratégies actuelles de sécurité des terminaux d'aujourd'hui consistent en grande partie à empiler des couches de défense pour protéger les vulnérabilités inhérentes à la machine, IGEL adopte une approche différente en utilisant un système d'exploitation Linux sécurisé qui élimine ces vulnérabilités grâce à un Modèle de Sécurité Préventive™. Dans ce document, nous discuterons des composantes du Modèle de Sécurité Préventive, des normes auxquelles IGEL peut adhérer, et des partenaires de sécurité avec lesquels IGEL collabore pour fournir une solution de sécurité complète, et qui prend en charge les meilleures pratiques de sécurité telles que le Zero Trust.

Modèle de Sécurité Préventive

IGEL OS est conçu autour du Modèle de Sécurité Préventive, qui élimine les vecteurs d'attaque exploités par des acteurs malveillants pour diffuser des attaques de ransomware et lancer d'autres types de cyberattaques. Grâce au Modèle de Sécurité Préventive, IGEL peut jouer un rôle clé dans la mise en œuvre des approches de sécurité informatique de type Zero Trust.

Principes clés du Modèle de Sécurité Préventive d'IGEL :

Système d'exploitation en lecture seule

- Les utilisateurs ne peuvent installer, ni à leur insu ni par malveillance, de malware sur le Terminal, réduisant ainsi le risque de ransomware et autres cyberattaques pour leurs organisations.

Pas de stockage de données local

- Aucune donnée client, patient ou financière n'est stockée sur le terminal, éliminant ainsi les risques de violations de données en cas de perte ou de vol du terminal.

Plateforme d'applications de confiance

- Une chaîne de confiance sécurisée dès le démarrage garantit que l'IGEL OS n'a pas été altéré.

Conception modulaire

- En ne livrant que ce qui est nécessaire au Terminal, la surface d'attaque est réduite au minimum. Le Portail d'Applications IGEL permet l'installation d'applications partenaires selon les besoins.

Chiffrement du disque

- La partition contenant les paramètres, mots de passe et profils de navigateur est chiffrée avec un cryptage AES-256 en mode XTS-plain64 avec une clé de 512 bits. La clé peut être sécurisée via TPM 2.0.

Prise en charge des principales solutions d'authentification et de single sign-on (SSO)

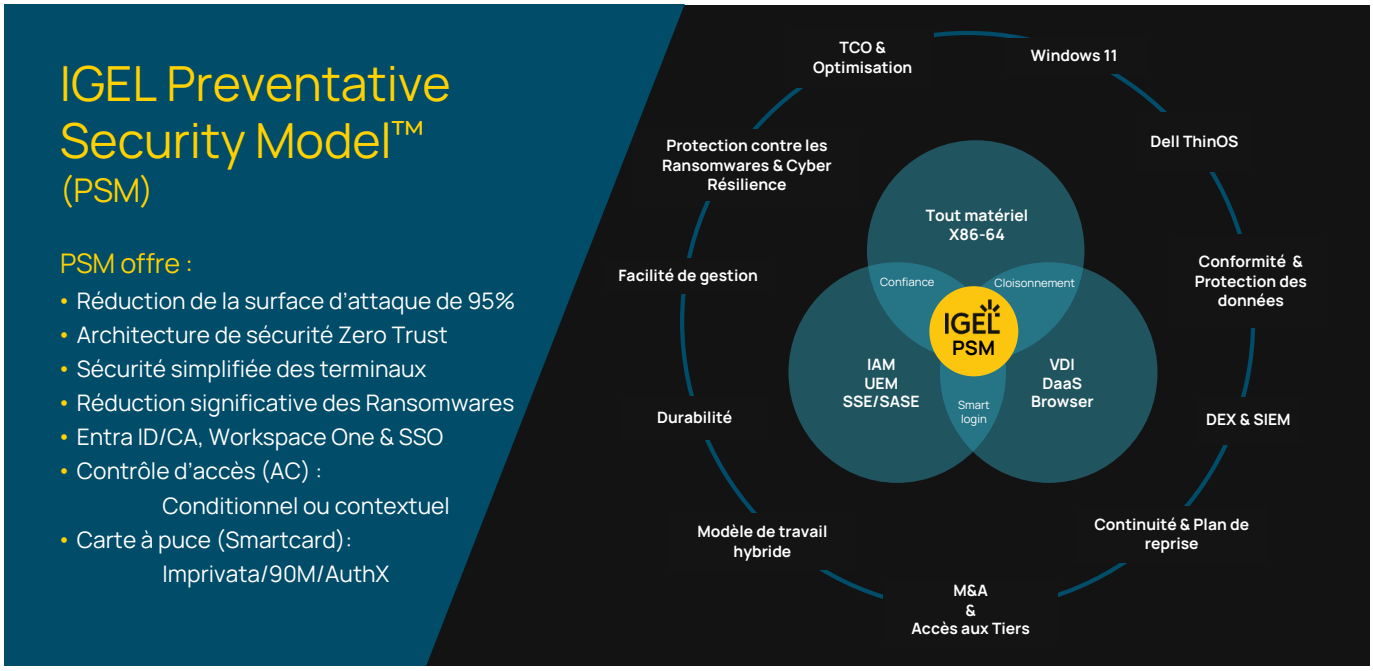
- IGEL s'intègre aux principales solutions d'authentification et de SSO pour garantir un accès rapide et sécurisé aux bureaux et applications.
    - o 90meter
    - o Imprivata
    - o Microsoft EntraID, EntraID-CA
    - o Okta
    - o OpenID Connect
    - o Ping Identity Ping One
    - o VMware Workspace One Access

Gestion centralisée

L'UMS, fournit un point de gestion unique pour des dizaines de milliers de terminaux IGEL, qu'ils soient connectés ou non au réseau de l'entreprise. L'UMS peut gérer tous les aspects de l'IGEL OS, y compris :

- **Règles** – Définir des règles prédéfinies par appareil ou par groupe.
- **Mises à jour** – Déployer les mises à jour de l'OS et des applications sur les terminaux IGEL.
- **Configuration** – Appliquer des configurations telles que la langue, le firmware, l'interface et les paramétrages USB.
- **Performance** – Collecter des données de performance des différents terminaux ainsi que les journaux. Ces logs peuvent être exportés vers des plateformes SIEM pour assurer la conformité avec les politiques en vigueur.

Grâce au Modèle de Sécurité Préventive d'IGEL, les organisations peuvent économiser des ressources significatives sur l'acquisition, les tests, la gestion et le dépannage des outils de sécurité et de gestion, tels que les antivirus, les outils assurant la détection et la réponse à des infections des terminaux (EDR), la prévention de la perte de données (DLP), la sauvegarde et la récupération, et bien plus encore.



Une stratégie de sécurité des terminaux pour aujourd'hui et demain

De nombreuses organisations bénéficient déjà des avantages en matière de sécurité liés au déplacement des workloads applicatives du Terminal vers des environnements VDI, DaaS et SaaS. Il a été prouvé que la possibilité d'utiliser un système d'exploitation sécurisé dès la conception réduisait les risques de sécurité et le temps de récupération en cas de tentative d'attaque. En supprimant le besoin d'agents de sécurité et de gestion des points finaux, y compris AV, EPP, EDR, AV, DLP, sauvegarde et récupération, etc., les organisations peuvent économiser des CAPEX et OPEX significatifs.

Alors que les organisations réfléchissent à stratégie de migration vers Windows 11, beaucoup envisagent de déplacer Windows 11 vers le cloud en utilisant Microsoft Azure Virtual Desktop, Windows 365 et Cloud PC. Avec les bureaux et les applications Windows hébergés dans le cloud, les organisations peuvent repenser leur stratégie concernant les terminaux en déployant un système d'exploitation sécurisé, conçu pour les nouvelles architectures orientées cloud.

Fonctions de sécurité d'IGEL

Plateforme applicative de confiance IGEL OS

- Une chaîne de confiance de démarrage sécurisée garantit que les composants d'IGEL OS n'ont pas été modifiés
- Une séquence de démarrage contrôlée est initiée à la mise en marche du dispositif.
- Les contrôles de signature sur les processus de mise à jour et de démarrage des partitions système et utilisateur détectent les altérations et empêchent le chargement de code modifié. Si les signatures ne sont pas validées, alors le système ne démarre pas.
- Si d'autres partitions sont affectées, le système démarrera en désactivant les modules impactés. Les supports flash ne pourront être montés sur aucun autre périphérique.
- IGEL utilise son propre système de partitionnement avec des partitions compressées qui obscurcissent les données. Les sommes de contrôle des partitions IGEL empêchent le chargement de code modifié.
- Le chargeur de démarrage de l'OS IGEL, signé par Microsoft (au nom du Forum UEFI) démarre sur les systèmes dont l'option « UEFI Secure Boot » est activée. Seuls les programmes de démarrage signés avec des clés autorisées par IGEL ou Microsoft peuvent charger le système d'exploitation. IGEL génère et gère les clés d'échange cryptographiques de la plateforme, incluses dans les versions UEFI correspondantes.
- Si une altération est détectée, le système ne démarre pas.
- Les fichiers de configuration sont écrits sur une partition dédiée et chiffrée, garantissant la sécurité des informations de configuration.
- Les mises à jour du système se terminent toujours complètement tout en maintenant la capacité de démarrage de l'appareil. Les mises à jour critiques sont toujours traitées en deux phases pour garantir leur succès.
- Avec IGEL OS 12, les applications et services sont séparés du système de base. Seules les fonctionnalités et services nécessaires sont déployés sur le terminal, en fonction des décisions de l'administrateur. Cela permet d'optimiser le système en le gardant aussi léger que possible pour réduire la surface d'attaque, minimisant ainsi les risques de malware, y compris les attaques par ransomware. Des fonctionnalités supplémentaires et des intégrations tierces de partenaires peuvent être téléchargées depuis l'App Store d'IGEL et distribuées via l'UMS, Universal Management Suite, par l'administrateur.
- La chaîne de confiance d'IGEL fonctionne sur tout dispositif x86 64 bits compatible, supportant l'UEFI et le démarrage sécurisé.
- Si les utilisateurs se connectent à un environnement VDI ou cloud, l'es logiciels d'accès tels que Citrix Workspace App ou VMware Horizon vérifieront le certificat du serveur auquel ils se connectent.

Cette chaîne garantit l'intégrité du système en s'assurant qu'aucun des composants de votre environnement n'a été altéré - une capacité clé du Modèle de Sécurité Préventive.

Authentification

IGEL OS supporte les méthodes d'authentification modernes, notamment :

- Gestion des tickets Kerberos, basée sur le nom d'utilisateur et le mot de passe, avec des solutions de carte à puce à double facteur (carte à puce et code PIN) et régit par les échanges tripartites (service fournisseur, service demandeur et serveur de contrôle de session Kerberos)
- Options de middleware pour la prise en charge la carte à puce et du code PIN.
- Authentification multi-facteurs.
- Périphériques d'extrémité alimentés par IGEL OS.
- Infrastructure Active Directory.
- Service compatible Kerberos (comme Citrix XenApp ou XenDesktop).

L'authentification peut être renforcée avec des partenaires IGEL, notamment :

- 90meter
- DeviceTRUST
- Evidian
- Imprivata
- Microsoft Entra ID
- Okta
- Ping Identity Ping One
- VMware Workspace One Access
- Yubikey

IGEL s'associe à des fournisseurs de premier plan dans le domaine des applications et de la sécurité. Le programme de partenariat IGEL Ready garantit que les solutions sont rigoureusement testées et prises en charge, même dans les environnements les plus exigeants. Les partenariats et intégrations en matière de sécurité incluent :

Navigateurs d'entreprise sécurisés	Navigateur sécurisé avec accès restreint aux données sensibles permettant un accès contrôlé par l'entreprise aux protocoles et sites web basés sur HTML.
Plusieurs solutions VPN intégrées pour accéder par tunnel aux ressources protégées et aux ressources de l'entreprise sur site.	OpenVPN Connect Client VPN NCP-e standard et gouvernemental Prise en charge de Genua GenuCard pour des connexions hautement sécurisées via le boîtier VPN HW
Chiffrement du clavier	Le chiffrement du clavier via la carte Cherry Secure Board garantit un chiffrement immédiat des frappes afin d'empêcher l'enregistrement et la falsification des frappes. Support des stations de travail Secunet SINA IGEL OS supporte les stations de travail SINA de Secunet qui sont approuvées pour le traitement d'informations classifiées jusqu'à et y compris SECRET, SECRET OTAN et SECRET UE/EU.
Une large gamme de solutions de cartes à puce répondant aux besoins de différents secteurs verticaux tels que les soins de santé et les services financiers.	• IGEL Smartcard SafeNet Aladdin eToken • Thales SafeNet middleware pour Gemalto/SafeNet eToken, IDPrime cartes à puce et token • Cryptovision sc/interface middleware pour les cartes à puce Cryptovision • NXP Cryptas IDProtect middleware pour les cartes à puce IDProtect • A.E.T. SafeSign middleware pour les cartes à puce SafeSign Pointsharp Net iD middleware pour les cartes à puce Net iD Coolkey middleware Coolkey • Logiciel intermédiaire OpenSC OpenSC • Logiciel intermédiaire 90meter

Large gamme de lecteurs de cartes à puce pour répondre aux besoins verticaux spécifiques et aux critères de conformité.	Elatec TWN4 CCID PC/SC Lite M.U.S.C.L.E. HID OMNIKEY REINER SCT cyberjack
Soutien aux fournisseurs d'identité	Imprivata OneSign ProveID Agent IGEL embarqué pour Imprivata Evidian AuthMgr contextualisant l'accès à VMware Workspace One Service basé sur OpenID Connect, y compris Microsoft EntraID, Okta, Ping Identity
Accès contextuel aux services et aux applications. Le contexte d'un appareil est essentiel dans un monde mobile pour fournir un accès à l'infrastructure de l'entreprise en temps réel et en toute sécurité.	DeviceTRUST prend en compte diverses informations contextuelles (IP, géolocalisation, réseau, etc.) lors du contrôle de l'accès aux données et aux applications, ce qui permet un contrôle d'accès conditionnel granulaire et conforme.
Intégration des solutions biométriques	Lecteurs d'empreintes digitales HID Global. Scanner de veines de la paume de la main Fujitsu.

IGEL permet également la prise de contrôle sécurisée à distance des appareils pour fournir un accès sécurisé instantané aux agents du helpdesk. L'accès basé sur les rôles et les journaux de transactions garantissent un haut niveau de sécurité et de conformité.

Gestion IGEL

L'UMS (Universal Management Suite) garantit que les terminaux IGEL sont à jour et configurés avec les bonnes applications et services, pour assurer la meilleure expérience utilisateur possible et les plus hauts niveaux de sécurité.

Les fonctions de sécurité de l'UMS d'IGEL incluent :

- **Tunnels TLS (Transport Layer Security) chiffrés**
  Les tunnels TLS garantissent que les connexions et les transferts de fichiers entre la console de gestion UMS et le terminal sont sécurisés.
- **Mises à jour centralisées et cryptographiques**
  Les mises à jour envoyées depuis l'UMS sont validées par IGEL OS avant leur installation sur les terminaux cibles. Les administrateurs informatiques peuvent facilement et rapidement déployer les mises à jour de sécurité depuis une seule console vers des dizaines de milliers de terminaux, d'une manière adaptée au réseau.
- **Prise en main sécurisée**
  La supervision permet au personnel informatique de prendre en charge de manière sécurisée un terminal distant à des fins de dépannage. Par exemple, un ingénieur du service d'assistance peut prendre le contrôle du clavier et de la souris de l'appareil. La console UMS, ou un visualiseur VNC externe, établit une connexion sécurisée avec le serveur UMS, qui crée ensuite un tunnel TLS vers le terminal. La vérification est effectuée via un mot de passe à usage unique émis par l'UMS et envoyé à IGEL OS sur l'appareil cible pour accorder l'accès. Chaque session de prise de contrôle à distance sécurisée est enregistrée par l'UMS.
- **Rationalisation des correctifs de sécurité**
  Grace à la conception modulaire d'IGEL OS, les mises à jour et correctifs sont moins nombreux et moins volumineux par rapport aux mises à jour traditionnelles des terminaux. Une extension à haute disponibilité assure la mise à jour simultanée des terminaux dans les grands environnements à partir de la console UMS.
- Gestion des accès aux périphériques connectés aux terminaux IGEL OS
- Un administrateur informatique peut gérer les ports USB et les types de périphériques, comme les périphériques USB HID ou les périphériques de stockage USB, sur un terminal IGEL OS via la console de gestion.
- Extension Haute Disponibilité

- L'extension Haute Disponibilité améliore le déploiement des nouveaux paramètres sur des dizaines de milliers de dispositifs simultanément. Cela est rendu possible grâce à une architecture distribuée de l'Universal Management Suite (UMS), qui optimise le processus de distribution pour garantir que chaque appareil peut mettre à jour ses paramètres à tout moment, tout en maintenant l'efficacité du réseau. Des informations supplémentaires sont disponibles dans la base de connaissances.
- Déconnexion automatique
- En associant un type de session à une commande de déconnexion automatique, l'appareil peut déconnecter l'utilisateur de la dernière session. Un nom d'utilisateur et un mot de passe sont nécessaires pour se reconnecter.

Comment IGEL participe au Zero Trust

IGEL aide les organisations à réduire considérablement le risque de ransomware ou de malware sur les terminaux, s'inscrivant ainsi dans une approche Zero Trust pour les organisations qui la mettent en œuvre. Grâce aux intégrations avec les partenaires de sécurité de premier plan, le support d'IGEL pour le Zero Trust va au-delà du simple appareil et peut inclure :

Utilisateur/Identité

- IGEL s'associe avec les principaux fournisseurs d'authentification pour offrir la gestion des identités et des accès, l'authentification multi-facteurs ainsi que l'accès conditionnel et contextuel.
- Aucune information d'identification de l'utilisateur n'est stockée sur le terminal, ceci garantissant qu'aucune information de session ne peut être récupérée.
- IGEL s'intègre avec les principaux fournisseurs de Secure Access Service Edge (SASE) et de Secure Service Edge (SSE) pour renforcer les initiatives de sécurité et de Zero Trust.

Terminal

- Le Modèle de Sécurité Préventive d'IGEL élimine les vulnérabilités courantes des terminaux qui sont ciblées lors des cyberattaques. En s'assurant que le terminal ne puisse pas être compromis grâce à une série de mesures de conception sécurisée, comprenant un système d'exploitation en lecture seule, l'absence de stockage de données en local et une conception modulaire, IGEL est alors en mesure de répondre directement à de nombreuses fonctionnalités de protection des terminaux, notamment :
    - o Inventaire des appareils
    - o Détection et conformité des appareils
    - o Autorisation des appareils
    - o Accès à distance
    - o Gestion des correctifs

  Gestion des terminaux
- De plus, la nécessité d'une couche complexe d'outils de sécurité et de gestion est supprimée, permettant ainsi des économies significatives des budgets CAPEX et OPEX tout en améliorant considérablement la sécurité de ces équipements.

Applications et charges de travail

- Avec IGEL OS, les utilisateurs n'ont pas la possibilité d'installer des applications sur le terminal, garantissant que des applications malveillantes, corrompues ou non autorisées ne puissent pas être introduites sur le terminal. Cela réduit la charge opérationnelle liée à la détection et à l'audit des instances d'applications et des licences sur le terminal, permettant aux organisations de se concentrer sur les instances d'applications virtualisées ou SaaS.
- Le déploiement des logiciels ne peut être initié que par l'administrateur IGEL. Cela s'applique aux mises à jour autorisées et aux correctifs disponibles auprès d'IGEL ou aux applications certifiées IGEL Ready disponibles via l'IGEL Application Store.

Données

- Aucune donnée n'est stockée sur un terminal IGEL OS. En cas de perte ou de vol d'un appareil, les organisations peuvent être certaines qu'aucune information client, patient ou toute autre information confidentielle n'aura été compromise et/ou dérobée.

Automatisation et Orchestration

- L'IGEL Universal Management Suite (UMS) est utilisée pour configurer et déployer des politiques sur les périphériques IGEL OS. Les administrateurs disposent d'une vue unique pour la création et le déploiement des politiques. Des politiques détaillées peuvent être créées, avec plus de neuf mille options disponibles.
- Les logs IGEL peuvent être consommés par les principales plateformes SIEM pour s'intégrer dans les programmes de sécurité existants.

Visibilité et Analyse

- Les événements liés aux utilisateurs, aux connexions, aux comptes et à la configuration sont enregistrés et peuvent être consommés par des plateformes SIEM via l'interface Rsyslog ou Filebeats pour une analyse et une corrélation d'événements approfondies. Des systèmes comme Splunk ou Graylog en sont des exemples.

Soutien d'IGEL à la sécurité et à la conformité des métiers

Le Modèle de Sécurité Préventive d'IGEL apporte un changement fondamental dans l'approche de la sécurité des terminaux, bénéfique pour toutes les industries, en éliminant de nombreux vecteurs d'attaque présents dans les solutions traditionnelles de terminaux. Cela réduit immédiatement les risques de ransomware et de malware, simplifie l'opérationnalisation de la sécurité des terminaux et diminue les coûts associés. Voici quelques exemples de la manière dont IGEL peut soutenir les initiatives de sécurité et de conformité dans cinq industries spécifiques :

Santé

L'une des principales préoccupations informatiques des organismes de santé est le ransomware, qui peut perturber les soins aux patients en :

- Rendant indisponibles les dossiers médicaux critiques et autres systèmes informatiques.
- Entraînant la divulgation publique des informations des patients.

Grâce au Modèle de Sécurité Préventive d'IGEL, les organisations de santé dans le monde entier peuvent réduire considérablement le risque d'une cyberattaque basée sur les terminaux, tout en réduisant les coûts logiciels et matériels, ainsi que les heures opérationnelles consacrées à la planification, la mise en œuvre, la fourniture et la gestion des terminaux dans les environnements de soins hospitaliers, ambulatoires et primaires.

Le Modèle de Sécurité Préventive peut améliorer la sécurité des données de santé protégées (DSP) et des informations personnelles identifiables (PII), et simplifier directement les exigences de sécurité des terminaux imposées par :

- HIPAA
- GDPR Santé
- Data Security Protection Toolkit (DSPT – NHS)
- Cadre de cybersécurité de la CISA

L'intégration avec les principales solutions d'authentification et d'authentification unique, telles qu'Imprivata, Okta et Microsoft Entra ID, associée à un support étendu des périphériques critiques tels que les imprimantes, scanners, tablettes de signature, lecteurs de badge et microphones de dictée, garantissent qu'IGEL peut être intégré dans un large éventail de cas d'utilisation et de flux de travail.

Services financiers

Les organisations de services financiers sont à la pointe de la transformation numérique, exploitant la technologie pour offrir des services innovants et améliorer l'expérience client tout en réduisant les coûts. Cependant, comme dans d'autres secteurs, elles sont des cibles majeures pour les cyberattaques. Cette innovation, associée à des réglementations strictes en matière de conformité, pousse les organisations de services financiers à repenser le modèle informatique des terminaux, en centralisant les données et les ressources via les services cloud.

Le Modèle de Sécurité Préventive d'IGEL joue un rôle crucial en comblant les lacunes de sécurité qui justifient le passage à une infrastructure cloud. En simplifiant et en sécurisant les terminaux avec IGEL, les organisations de services financiers peuvent répondre aux exigences de sécurité des terminaux nécessaires pour protéger les informations de l'industrie des cartes de paiement (PCI) et les informations personnelles identifiables (PII), tout en respectant les réglementations en matière de conformité.

Manufacture

La convergence des systèmes informatiques (IT) et des technologies opérationnelles (OT) crée d'importants défis de sécurité pour les organisations manufacturières. Cette convergence a exposé des réseaux autrefois isolés aux risques d'attaques provenant des réseaux IT.

IGEL aide les organisations manufacturières à réduire considérablement le risque de ransomware et de malware en minimisant le potentiel d'une cyberattaque sur les terminaux. Associé à la virtualisation des terminaux et aux solutions d'espaces de travail dans le cloud, IGEL permet à des équipes décentralisées de collaborer sur des tâches complexes de conception, logistique et administratives, tout en protégeant la propriété intellectuelle et les informations financières de l'organisation. De plus, en tant que système d'exploitation basé sur Linux sécurisé, IGEL peut être déployé dans les réseaux OT pour réduire davantage la surface d'attaque de ces dispositifs vulnérables.

Commerce de détail

Les grands détaillants sont régulièrement pris pour cible en raison des grandes quantités d'informations sur les clients et les paiements financiers qu'ils détiennent. L'interruption de service provoquée par une attaque de ransomware peut coûter aux détaillants des centaines de millions en termes de perte d'activité, d'atteinte à la réputation et d'impact sur le cours de l'action de l'entreprise.

Le commerce de détail a un large éventail de cas d'utilisation qui exigent que les terminaux soient positionnés dans des endroits relativement peu sécurisés, y compris les points de vente (PDV), la salle des stocks, les entrepôts et d'autres environnements logistiques en plus du back-office, du centre d'appels et d'autres rôles centrés sur l'administratif.

Le Modèle de Sécurité Préventive IGEL, en conjonction avec les applications VDI, DaaS et SaaS, joue un rôle essentiel dans la stratégie de sécurité informatique du commerce de détail, en sécurisant les informations PCI, PII, logistiques et financières nécessaires au fonctionnement des détaillants.

Gouvernement

Face à la montée des attaques d'États-nations et de la cyberguerre, les gouvernements du monde entier sont incités à renforcer leur cybersécurité. Ces menaces vont des attaques coordonnées contre les infrastructures critiques au vol ciblé des ordinateurs portables de dirigeants politiques. Aux États-Unis, le décret exécutif de la Maison-Blanche (EO14028) sur l'amélioration de la cybersécurité nationale accélère l'adoption des services cloud et d'une architecture Zero Trust. Le Bureau de la gestion et du budget de la Maison-Blanche a fixé au 30 septembre 2024 la date limite pour que les agences fédérales et civiles adoptent un certain niveau d'architecture Zero Trust, avec l'objectif d'atteindre une implémentation complète d'ici 2027.

En France, promulguée pour la première fois en 2013 pour une période de six ans (2014-2019), la Loi de programmation Militaire (LPM) a été renouvelée pour 2019-2025, puis pour 2024-2030. Avec un accent de plus en plus fort sur la cybersécurité au fur et à mesure des années, la loi inclut des dispositions spécifiques visant à renforcer la sécurité des

IGEL OS - Le système d'exploitation sécurisé pour aujourd'hui et demain

Le Modèle de Sécurité Préventive d'IGEL OS adopte une approche sécurisée par conception, en remplaçant le modèle dépassé de surveillance, détection et remédiation par un modèle simplifié de prévention. Le Modèle de Sécurité Préventive élimine les vulnérabilités ciblées par les acteurs malveillants, réduisant ainsi de manière significative les risques de ransomware et de malware.

En sécurisant les terminaux de l'entreprise, en réduisant le coût total de possession (TCO), en permettant la réutilisation rapide des appareils existants et en offrant une expérience utilisateur de première classe, IGEL apporte de la valeur à un large éventail d'initiatives à l'échelle de l'entreprise, notamment :

- Protection des données et conformité
- Expérience numérique des employés (DEX)
- Travail hybride
- Fusions et acquisitions (M&A)
- Initiatives de développement durable

L'objectif d'IGEL est de fournir le meilleur système système d'exploitation pour les espaces de travail numériques et cloud. La sécurité et la protection des données sont au cœur de la conception et du développement de l'OS d'IGEL. Les informations ci-dessus représentent un ensemble de capacités intégrées, en constante expansion, conçues pour réduire la surface d'attaque des terminaux et offrir la meilleure protection possible.

Restez connecté avec IGEL pour vous tenir informé des dernières nouveautés et fonctionnalités qui peuvent aider à durcir vos terminaux et à assurer une transition vers le cloud aussi fluide et sécurisée que possible.

Démonstration d'IGEL sur vos propres appareils

Téléchargez des licences gratuites sur **IGEL.com/form-download**

Plus d'informations sur **IGEL.com**

Suivez-nous sur

@IGEL_Technology I igel.technology I IgelTechnologyTV I igel-technology I IGEL.com