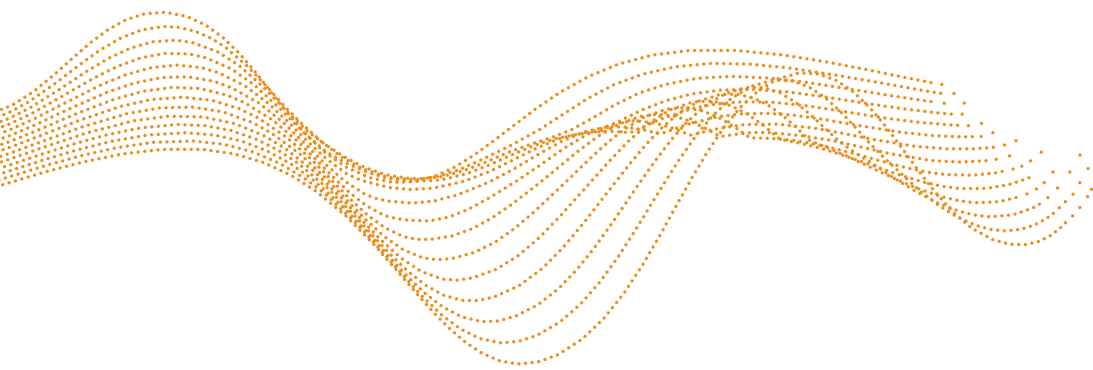




Security Guide

Sécurisez votre entreprise, protégez vos données.

SHARP



Protection immédiatement efficace.

En effet, saviez-vous que des imprimantes non protégées peuvent constituer une porte dérobée ouverte à la mise en danger ou au vol de vos précieuses données?

Les imprimantes font partie intégrante de la plupart des lieux de travail. Elles sont utilisées de manière routinière tous les jours et leur aspect extérieur n'a guère changé au cours des vingt dernières années. Cependant, comme les administrateurs informatiques le savent, les imprimantes multifonctions (MFP) et les imprimantes sont devenues des systèmes informatiques sophistiqués, connectés au réseau de votre entreprise et à Internet.

Alors que la sécurité des données est l'une des priorités de la plupart des entreprises, leurs équipements d'impression sont malheureusement souvent négligés. En effet, un tiers des petites et moyennes entreprises (PME) européennes ne disposent pas de mesures de sécurité informatique pour les imprimantes*. Cela en fait une cible pour les pirates et autres acteurs malveillants, d'autant plus que l'évolution vers des postes de travail hybrides a ouvert des brèches supplémentaires. Les imprimantes non sécurisées offrent souvent une porte d'entrée facile dans votre entreprise et permettent d'accéder aux informations sensibles contenues dans les travaux d'impression et de numérisation, et peut-être même à l'ensemble de votre réseau informatique.

La menace est très réelle – et les failles qui se présentent sont exploitées. Près d'un cinquième (19%) des PME européennes ont déjà été victimes d'une violation de la sécurité d'une imprimante*. En outre, une perte de données, surtout si elles tombent entre de mauvaises mains, peut causer un préjudice énorme et durable à l'image de l'entreprise.

Toute entreprise, quelle que soit sa taille, doit s'assurer que son environnement de production de documents est protégé par la technologie et par un comportement sécurisé des utilisateurs – tout comme n'importe quel ordinateur portable ou PC professionnel. C'est pourquoi la sécurité est au cœur de tous les développements de produits de Sharp. Nous voulons garantir que nos produits et services rendent la vie professionnelle des gens plus facile et plus productive, tout en gardant les données en sécurité.

Comprendre les risques

Les entreprises modernes traitent un grand nombre d'informations, mais n'ont souvent pas de réelle visibilité sur la manière dont elles sont créées, stockées, partagées et récupérées. Cela entraîne inévitablement des risques potentiels pour la sécurité et la conformité, qui peuvent inclure des violations de la protection des données, des fichiers non sécurisés, des erreurs humaines et un accès non autorisé aux informations.

* Source: L'étude a été menée par Censuwide entre le 1er et le 13 février 2023. Au total, 5770 décideurs informatiques et personnes responsables des achats informatiques dans les PME de 11 pays (Allemagne, Autriche, Suisse (DACH) ainsi que Belgique, France, Italie, Pays-Bas, Pologne, Espagne, Suède et Royaume-Uni) ont répondu aux questions de l'étude, dont 1543 personnes dans la région DACH.



Pour être réellement efficace, votre sécurité de l'information doit protéger vos imprimantes et les informations de votre entreprise contre toutes les formes d'accès et d'utilisation non autorisés, ainsi que contre la divulgation, la modification ou la destruction. Il s'agit des éléments suivants:

Menaces physiques

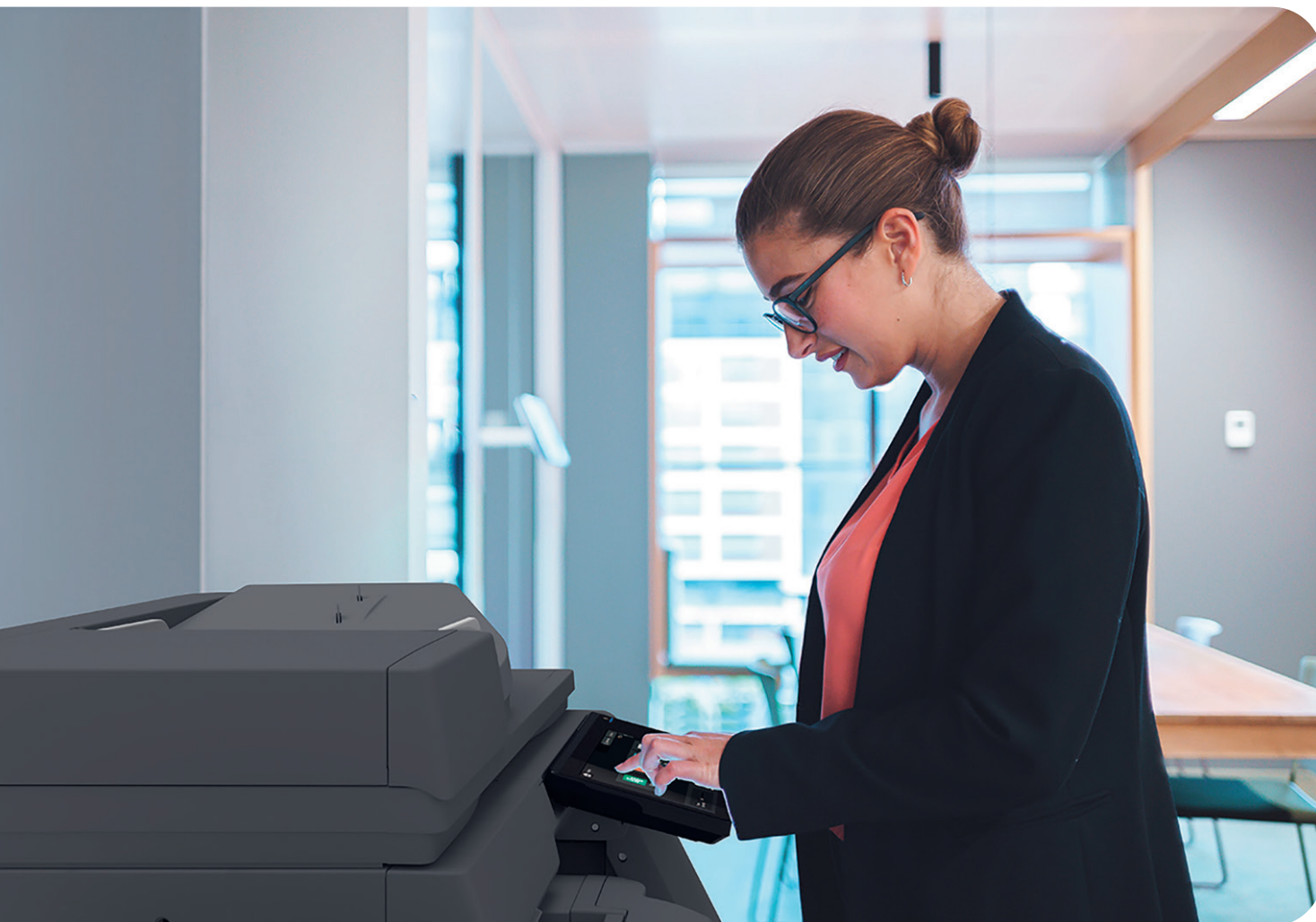
Toutes les actions et tous les événements physiques susceptibles d'entraîner une perte ou une détérioration grave des informations ou des systèmes, qu'ils soient de nature interne (p. ex. une alimentation électrique instable) ou externe (par exemple dus à la foudre) ou d'origine humaine (p. ex. par un employé mécontent ou en raison de documents sensibles laissés sans surveillance dans le bac de sortie).

Menaces sur le réseau

Toute activité permettant un accès non autorisé à votre réseau, généralement dans le but d'accéder à des données ou de les compromettre par le biais de virus et de logiciels malveillants, de voler des informations confidentielles par le biais de campagnes d'hameçonnage ou d'accéder au système à l'aide d'attaques par déni de service (Denial of Service, DoS) ou de rançongiciels.

Obligations légales

La protection de toutes les données sensibles qu'une entreprise possède (comme p. ex. données relatives aux employés, informations sur les clients et données bancaires), conformément aux réglementations nationales ou sectorielles en vigueur (comme p. ex. du RGPD) – quel que soit leur emplacement de stockage.



Être en sécurité tout en restant productif.

En effet: dans le monde d'aujourd'hui, constamment interconnecté, les menaces sont de plus en plus complexes.

Les mesures de sécurisation des imprimantes multifonctions devraient l'être également – sans compromettre la productivité. Chez Sharp, nous sommes conscients du fait que la protection des données de votre entreprise et de vos utilisateurs est décisive pour votre succès – et pour votre survie. Mais nous savons aussi que des mesures de sécurité trop strictes ou mises en œuvre de manière inefficace peuvent avoir de graves conséquences sur la productivité. Nos imprimantes et systèmes multifonctions sont dotés d'une série de fonctions avancées de gestion des informations et des événements de sécurité (Security Information and Event Management, SIEM), conçues pour protéger vos informations et documents contre un large éventail de menaces de sécurité physiques et cybernétiques, y compris les attaques les plus persistantes et les plus tenaces. Ils vous aident également à vous conformer à des exigences légales et réglementaires de plus en plus strictes, comme le règlement général sur la protection des données (RGPD) par exemple.

Nous vous donnons les outils pour contrôler et gérer vos politiques de sécurité d'impression et accéder en toute sécurité à vos informations confidentielles, quelle que soit la manière dont elles sont saisies, stockées, imprimées ou partagées sur votre réseau:

- Codage automatique de tous les documents enregistrés sur l'appareil ou qui lui sont envoyés par e-mail
- Technologie d'auto-guérison pour la récupération sécurisée d'un terminal en cas d'attaque
- Whitelisting des applications et des micrologiciels qui peuvent communiquer avec l'appareil
- Validation de certificat SSL/TLS pour vérifier la sécurité des serveurs tiers qui communiquent avec votre terminal
- Audit Trail et des fonctions de journal des tâches (job log) pour fournir un aperçu complet de toutes les activités des utilisateurs
- L'autorisation est prise en charge dans différentes procédures d'autorisation (notamment les systèmes MPS locaux et basés sur le cloud). Pour la dernière génération d'appareils, également avec MS Entra-ID
- Surveillance anti-malware Bitdefender pour assurer la sécurité de vos données, de vos terminaux et de l'ensemble du réseau (en option)
- Voyant LED clignotant pour rappeler que les documents ne doivent pas être laissés sur le plateau du chargeur de documents

Pour encore plus de sécurité

Nos imprimantes multifonctions «Future Workplace» sont dotées de fonctions de sécurité basées sur le BIOS qui empêchent immédiatement le démarrage de l'appareil si des erreurs sont détectées. En outre, les mises à jour de sécurité sont automatiquement fournies à partir du cloud, de sorte que la protection contre les cyberattaques est toujours à jour. De plus, ces MFP offrent encore plus de sécurité grâce au logiciel anti-malware avec Bitdefender*.

Afin d'empêcher toute utilisation non autorisée, nos MFP les plus récentes contiennent également des certificats racine préinstallés. En outre, elles surveillent automatiquement les tentatives d'accès et n'accordent l'accès qu'aux applications et aux systèmes d'exploitation figurant sur une liste blanche approuvée. Toutes les autres applications externes sont immédiatement bloquées, consignées et signalées. La détection d'intrusion offre un niveau de protection supérieur et protège votre MFP* contre les tentatives d'accès réseau suspectes. En effet, les informations échangées entre une MFP et une autre application ou un système de messagerie peuvent également être interceptées ou compromises.

Une gestion de la sécurité tournée vers l'avenir

Pour une infrastructure informatique sûre et stable, il est nécessaire de procéder à une maintenance régulière et d'installer des mises à jour en temps voulu pour tous les systèmes. En effet, les systèmes informatiques non corrigés ou corrigés trop tard peuvent présenter des failles de sécurité importantes dues à des logiciels et des systèmes d'exploitation obsolètes et entraîner un fonctionnement instable. Les mises à jour du micrologiciel devraient donc être distribuées le plus rapidement possible.

Nos imprimantes multifonctions sont très résistantes et à l'épreuve du temps grâce à leur fonction de mise à jour du micrologiciel. Les systèmes détectent de manière autonome la disponibilité d'une nouvelle version, la téléchargent en toute sécurité et installent le micrologiciel en flux tendus, sans intervention coûteuse d'un technicien.

Et il arrive un moment où l'imprimante multifonction est définitivement débranchée. Une dernière règle de sécurité, absolument essentielle, doit encore être respectée: la mémoire/ SSD/le disque dur, les données orientées utilisateur, les carnets d'adresses et les paramètres informatiques doivent impérativement être effacés de manière irréversible. Vous jouez ainsi la carte de la sécurité.



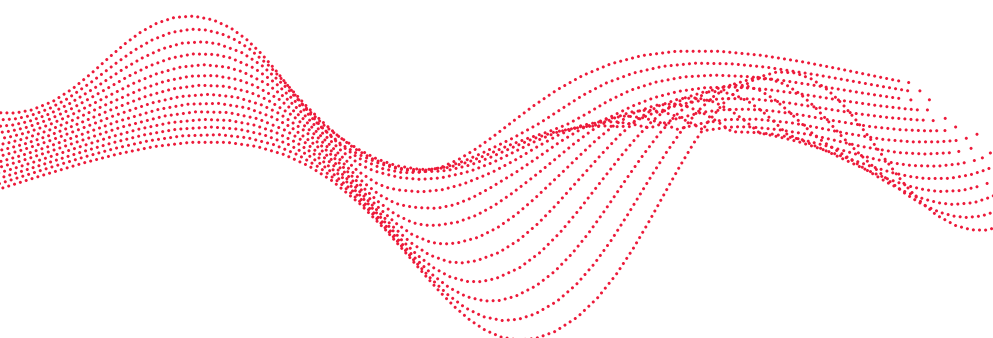
*en option; pas disponible pour tous les modèles.

Une protection complète.

Les mesures de sécurité devraient offrir une protection complète contre toutes les vulnérabilités et tous les points d'attaque importants.

Alors que les PC, les ordinateurs portables et les serveurs sont de mieux en mieux protégés contre les attaques, il est devenu indispensable de protéger également d'autres appareils en réseau, comme les imprimantes ou les systèmes multifonctions, contre les accès extérieurs. C'est pourquoi nous avons récapitulé pour vous un aperçu détaillé des fonctions de sécurité de nos **MFP et imprimantes** dans les pages suivantes.

Aperçu des modèles pour les pages suivantes				
BP-22C25 BP-C131WD BP-C131PW	MX-CxxxP/P MX-BxxxP/W/P/PW	BP-30C25	MX-M1206 MX-M1056 MX-8081 MX-7081	BP-90Cxx BP-71/61/51/56Cxx BP-70Mxx BP-71/51Mxx BP-B547WD/B537WR BP-C5xxWD/WR
Désignations des modèles				
MFP A3				
BP-22C25		BP-30C25	MX-M1206/MX-M1056 MX-8081/MX-7081	BP-90C80/BP-90C70 BP-70M90/BP-70M75 BP-71C65/BP-71C55 BP-71C45/BP-71C36/BP-71C31 BP-61C45/BP-61C36/BP-61C31 BP-51C65/BP-51C55 BP-51C45/BP-51C36/BP-51C31/BP-51C26 BP-56C26 BP-71M65/BP-71M55 BP-71M45/BP-71M36/BP-71M31 BP-51M65/BP-51M55 BP-51M45/BP-51M36/BP-51M31/BP-51M26
MFP A4				
BP-C131WD	MX-C528F/MX-C428F MX-C358F MX-B557F MX-B468F/MX-B427W			BP-B547WD/BP-B537WR BP-C542WD/BP-C533WD/BP-C533WR
Imprimantes A4				
BP-C131PW	MX-C428P MX-B557P MX-B468P/MX-B427PW			



Data Security	BP-22C25 BP-C131WD BP-C131PW		MX-CxxxP/P MX-BxxxP/ W/P/PW		BP-30C25		MX-M1206 MX-M1056 MX-8081 MX-7081		BP-90Cxx BP-71/61/51/56Cxx BP-70Mxx BP-71/51Mxx BP-B547WD/B537WR BP-C5xxWD/WR	
	Fonctions de sécurité standard	Fonctions de sécurité standard*	Fonctions de sécurité standard	avec Data Security Kit installé	Fonctions de sécurité standard	avec Data Security Kit installé	Fonctions de sécurité standard	avec Data Security Kit installé		
Trusted Platform Module (TPM)	—	✓ ^{†1} + ^{†1} — ^{†1}	—	✓	—	✓	✓	✓		
Méthode de réécriture des données (HDD)	—	✓ NIST ^{†2} DoD 5220.22-M	—	—	✓ 0-FF de nombre aléatoire DoD 5220.22-M	✓ 0-FF de nombre aléatoire DoD 5220.22-M	—	—		
Méthode de réécriture des données (Flash, SSD)	✓ AES 256bit CBC	✓ eMMC	✓	✓	—	—	✓	✓		
Réécriture des données à la fin de la tâche	✓	✓ Cycle unique ou multiple selon NIST ^{†2}	✓	✓	✓ jusqu'à 10 x	✓ jusqu'à 10 x	✓	✓		
Réécriture des données sur demande	—	✓	—	✓	—	✓	—	✓		
Effacement de toute la mémoire	—	✓	—	✓	—	✓	—	✓		
Suppression de toutes les données dans la liste d'état des tâches sous «clôturé».	—	✓	—	✓	—	✓	—	✓		
Suppression des données d'archivage des documents	—	✓	—	✓	—	✓	—	✓		
Suppression du carnet d'adresses/ des données enregistrées	—	✓	—	✓	—	✓	—	✓		
Effacement automatique des données après la tâche	—	✓	—	✓	—	✓	—	✓		
Fonction Auto-Clear à la mise en marche	—	—	—	✓	—	✓	—	✓		
Fonction End-of-Lease (Effacement de toute la mémoire et création d'une confirmation)	✓	✓	✓ Effacement de sécurité	✓ Effacement de sécurité	✓ Écrasement des valeurs par «0»	✓ Écrasement des valeurs par «0»	✓ Effacement de sécurité	✓ Effacement de sécurité		
Codage des données (AES 256 octets)	✓ AES 256bit	✓ Mode ECB ^{†3}	✓ Mode ECB ^{†3}	✓ Mode ECB ^{†4}	✓ Mode ECB ^{†3}	✓ Mode ECB ^{†4}	✓ Mode ECB ^{†4}	✓ Mode ECB ^{†4}		
PDF crypté	✓ uniquement pour l'impression par IPP (AirPrint)	✓	✓	✓	✓	✓	✓	✓		
Suppression du classement des documents (classement rapide, impression par lots, stockage/sauvegarde des données de classement des documents)	—	✓	✓	✓	✓	✓	✓	✓		
Suppression programmée des données de classement des documents	—	—	✓	✓	✓	✓	✓	✓		
Blocage du fonctionnement en cas d'erreur de saisie du mot de passe de classement	—	✓ Verrouillage de l'utilisateur	—	✓	—	✓	—	✓		
Mise sur liste blanche des applications	✓	—	✓	✓	✓	✓	✓	✓		
Protection contre les attaques de micrologiciels et auto-récupération	—	—	✓	✓	✓	✓	✓	✓		

Légende

✓ Par défaut

+ En option

— Non disponible

*Les MX-B427W et MX-B427PW ne prennent pas en charge toutes les fonctions. Les MX-C607P et MX-B557P ne prennent pas en charge les fonctions de sécurité liées aux MFP pour la numérisation et la télécopie. Veuillez vous informer dans la fiche technique correspondante ou sur le web. ^{†1} Différent selon le modèle ^{†2} National Institute of Standards and Technology ^{†3} Electronic Code Book Mode ^{†4} Cipher Block Chaining Mode

Sécurité de réseau et de communication	BP-22C25 BP-C131WD BP-C131PW	MX-CxxxF/P MX-BxxxF/ W/P/PW	BP-30C25		MX-M1206 MX-M1056 MX-8081 MX-7081	BP-90Cxx BP-71/61/51/56Cxx BP-70Mxx BP-71/51Mxx BP-B547WD/B537WR BP-C5xxWD/WR		
	Fonctions de sécurité standard	Fonctions de sécurité standard*	Fonctions de sécurité standard	avec Data Security Kit installé	Fonctions de sécurité standard	avec Data Security Kit installé	Fonctions de sécurité standard	avec Data Security Kit installé
Protection de la communication réseau: HTTPS, IPsec et TLS	✓	✓	✓	✓	✓	✓	✓	✓
Protection de la communication réseau: Wireless LAN	✓	✓	✓	✓	✓	✓	✓	✓
Kerberos	—	✓	✓	✓	✓	✓	✓	✓
Cryptage S/MIME	—	✓	✓	selon le réglage	✓	✓	✓	selon le réglage
Filtre d'adresses IP	✓	✓	✓	✓	✓	✓	✓	✓
Filtre d'adresses MAC	✓	—	✓	✓	✓	✓	✓	✓
Gestion des ports (ouverture et fermeture de ports)	✓	✓	✓	✓	✓	✓	✓	✓
Prise en charge de SNMPv3 – SHA1, AES 128 octets	✓	✓	✓	✓	✓	✓	✓	✓
Certificats de terminal préinstallés	✓	✓	✓	✓	✓	✓	✓	✓
Mesure de Cross-Site Request Forgery (CSRF)	✓	—	✓	✓	✓	✓	✓	✓
Denial of Service (DoS)	—	—	✓	✓	uniquement MX-xx81	uniquement MX-xx81	✓	✓
Authentification IEEE802.1X™	✓	✓	✓	✓	✓	✓	✓	✓
IPP over SSL	✓	✓	✓	✓	✓	✓	✓	✓
Wireless LAN	✓	✓**	✓	✓	✓	✓	✓	✓
Avertissement e-mail/état	—	✓	✓	✓	✓	✓	✓	✓
Exploitation à distance (Remote)	✓	✓	✓	✓	✓	✓	✓	✓
Classeur officiel/NAS, connexion cloud, exportation des journaux de tâches/Syslog/journaux d'audit, sauvegarde de la mémoire, clonage d'appareils	—	✓	✓	✓	✓	✓	✓	✓
Active Directory Integration	—	✓	✓	✓	✓	✓	✓	✓
Cryptage TLS	✓	✓	✓	✓	✓	✓	✓	✓
Gestion des directives de sécurité	✓	✓	✓	✓	✓	✓	✓	✓

Légende ✓ Par défaut + En option — Non disponible

* Les MX-B427W et MX-B427PW ne prennent pas en charge toutes les fonctions. Les MX-C607P et MX-B557P ne prennent pas en charge les fonctions de sécurité liées aux MFP pour la numérisation et la télécopie. Veuillez vous informer dans la fiche technique correspondante ou sur le web. ** En option pour BP-22C25

Authentification et contrôle des accès

BP-22C25
BP-C131WD
BP-C131PW

MX-CxxxP/P
MX-BxxxP/
W/P/PW

BP-30C25

MX-M1206
MX-M1056
MX-8081
MX-7081

BP-90Cxx
BP-71/61/51/56Cxx
BP-70Mxx | BP-71/51Mxx
BP-B547WD/B537WR
BP-C5xxWD/WR

	Fonctions de sécurité standard	Fonctions de sécurité standard*	Fonctions de sécurité standard	avec Data Security Kit installé	Fonctions de sécurité standard	avec Data Security Kit installé	Fonctions de sécurité standard	avec Data Security Kit installé
Authentification d'utilisateurs (Local/LDAP/Active Directory/Kerberos)	✓	✓	✓	✓	✓	✓	✓	✓
LDAP-SSL / Secure	✓	✓ sauf BP-B427W et BP-B427PW	✓	✓	✓	✓	✓	✓
Authentification des cartes d'identité	✓	✓	✓	✓	✓	✓	✓	✓
Authentification NTLMv2-pour LDAP pour SMB	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓
Authentification des directives d'impression	✓	✓	✓	✓	✓	✓	✓	✓
Active Directory Integration (la MFP est incluse dans le domaine AD)	—	✓	✓	✓	✓	✓	✓	✓
Active Directory Integration Single Sign-On ((classeurs, e-mail, registre d'accueil)	—	✓	✓	✓	✓	✓	✓	✓
Accès admin protégé par mot de passe à la page d'accueil de l'appareil	✓	✓	✓	✓	✓	✓	✓	✓
Directive de mot de passe administrateur/utilisateur	—	✓	—	—	—	—	✓	✓
Protection du mot de passe administrateur (lors de connexion par FTP)	✓	✓	✓	✓	✓	✓	✓	✓
User-Lockout	✓	✓	✓	✓	✓	✓	✓ ^{*1}	✓ ^{*1}
Authentification Entra-ID (Microsoft)	—	—	—	—	—	—	✓ —	✓ —
Longueur et exigences du mot de passe	Utilisateur 0-255/ Admin 5-255	Aucune condition spécifique, mais longueur maximale = 128. Tous les caractères spéciaux sont acceptés	Utilisateur 0-255 Admin 5-255	Utilisateur/admin N-255 (N: 5 à 32; Admin spécifiable) signes: 52 lettres, 10 chiffres, 10 symboles spécifiques	Utilisateur 0-255 Admin 5-255	Utilisateur/admin N-255 (N: 5 à 32; Admin spécifiable) signes: 52 lettres, 10 chiffres, 10 symboles spécifiques	Utilisateur 0-255 Admin 5-255	Utilisateur/admin N-255 (N: 5 à 32; Admin spécifiable) signes: 52 lettres, 10 chiffres, 10 symboles spécifiques

Sécurité d'impression

BP-22C25
BP-C131WD
BP-C131PW

MX-CxxxP/P
MX-BxxxP/
W/P/PW

BP-30C25w

MX-M1206
MX-M1056
MX-8081
MX-7081

BP-90Cxx
BP-71/61/51/56Cxx
BP-70Mxx | BP-71/51Mxx
BP-B547WD/B537WR
BP-C5xxWD/WR

	Fonctions de sécurité standard	Fonctions de sécurité standard*	Fonctions de sécurité standard	avec Data Security Kit installé	Fonctions de sécurité standard	avec Data Security Kit installé	Fonctions de sécurité standard	avec Data Security Kit installé
Authentification d'ordres d'impression	✓	✓	✓	✓	✓	✓	✓	✓
Validation de l'impression par code PIN/mot de passe	✓	✓	✓	✓	✓	✓	✓	✓
Validation de l'impression sans serveur	—	—	✓	✓	✓	✓	✓	✓
Impression par USB (si permis)	✓	✓	✓	✓	✓	✓	✓	✓
Désactivation de l'impression des listes	—	✓	—	✓	—	✓	—	✓
Désactivation du classement des documents	—	—	—	✓	—	✓	—	✓
Désactivation des ordres d'impression qui ne sont pas des tâches d'attente d'impression	✓	✓	✓	✓	✓	✓	✓	✓
Désactivation de l'affichage de la liste des travaux d'impression terminés	—	—	—	✓	—	✓	✓	✓
Impression du modèle de contrôle des documents	—	—	—	✓	—	✓	—	✓
Arrêt des travaux en cas de détection d'un motif de contrôle de document	—	—	—	✓	—	✓	—	✓
Maintien des ordres d'impression	✓	✓	✓	✓	✓	✓	✓	✓

* Les MX-B427W et MX-B427PW ne prennent pas en charge toutes les fonctions. Les MX-C607P et MX-B557P ne prennent pas en charge les fonctions de sécurité liées aux MFP pour la numérisation et la télécopie. Veuillez vous informer dans la fiche technique correspondante ou sur le web. *1 Ces appareils prennent en charge l'autorisation Entra-ID; BP-71/61/51/56Cxx, BP-71/51Mxx.

Fonctions de numérisation et applications Sharp OSA®	BP-22C25 BP-C131WD BP-C131PW	MX-CxxxF/P MX-BxxxF/ W/P/PW	BP-30C25		MX-M1206 MX-M1056 MX-8081 MX-7081	BP-90Cxx BP-71/61/51/56Cxx BP-70Mxx BP-71/51Mxx BP-B547WD/B537WR BP-C5xxWD/WR		
	Fonctions de sécurité standard	Fonctions de sécurité standard*	Fonctions de sécurité standard	avec Data Security Kit installé	Fonctions de sécurité standard	avec Data Security Kit installé	Fonctions de sécurité standard	avec Data Security Kit installé
Saisie directe du domaine	✓	✓	✓	✓	✓	✓	✓	✓
Sharp OSA: application externe ACM & EAM	—	—	✓	✓	✓	✓	✓	✓
Numérisation vers des dossiers partagés	✓	✓	✓	✓	✓	✓	✓	✓
Numérisation sur USB	✓	✓	✓	✓	✓	✓	✓	✓
Numériser vers e-mail	✓	✓	✓	✓	✓	✓	✓	✓
Numériser sur FTP	—	✓	✓	✓	✓	✓	✓	✓
Numérisation vers des e-mails pour des destinations pour lesquelles le chiffrement S/MIME n'est pas disponible	✓	✓	✓	✓	✓	✓	✓	✓
Numériser sur SMB	✓	✓	✓	✓	✓	✓	✓	✓
Numérisation vers une clé USB	✓	✓	✓	✓	✓	✓	✓	✓
Numérisation à partir d'un PC distant	✓	✓	✓	✓	✓	✓	✓	✓
Sharpdesk Mobile	✓	—	✓	✓	✓	✓	✓	✓
Classement de documents – classeur à accès rapide	—	✓	✓	✓	✓	✓	✓	✓
Classement de documents – sauvegarde/exportation de données	—	✓	✓	✓	✓	✓	✓	✓

Fonctions Mobile et Cloud	BP-22C25 BP-C131WD BP-C131PW	MX-CxxxF/P MX-BxxxF/ W/P/PW	BP-30C25		MX-M1206 MX-M1056 MX-8081 MX-7081	BP-90Cxx BP-71/61/51/56Cxx BP-70Mxx BP-71/51Mxx BP-B547WD/B537WR BP-C5xxWD/WR		
	Fonctions de sécurité standard	Fonctions de sécurité standard*	Fonctions de sécurité standard	avec Data Security Kit installé	Fonctions de sécurité standard	avec Data Security Kit installé	Fonctions de sécurité standard	avec Data Security Kit installé
Cloud Connect (OneDrive, SharePoint Online, Google Drive™, Dropbox, Box)	—	✓	✓	✓	✓	✓	✓	✓
MS Teams Connector (Microsoft Teams)	—	—	—	—	—	—	✓	✓
Email Connect (Exchange Server, Gmail™)	—	—	✓	✓	✓	✓	✓	✓
Impression mobile (AirPrint, Android™)	✓	✓	✓	✓	✓	✓	✓	✓
Impression mobile (Sharpdesk® Mobile, Sharp Print Service Plugin)	✓	—	✓	✓	✓	✓	✓	✓

Légende ✓ Par défaut + En option — Non disponible

* Les MX-B427W et MX-B427PW ne prennent pas en charge toutes les fonctions. Les MX-C607P et MX-B557P ne prennent pas en charge les fonctions de sécurité liées aux MFP pour la numérisation et la télécopie. Veuillez vous informer dans la fiche technique correspondante ou sur le web. ** Tous les connecteurs ne sont pas disponibles.

Audit Trail et autres mesures de sécurité

BP-22C25
BP-C131WD
BP-C131PW

MX-CxxxP/P
MX-BxxxP/
W/P/PW

BP-30C25

MX-M1206
MX-M1056
MX-8081
MX-7081

BP-90Cxx
BP-71/61/51/56Cxx
BP-70Mxx | BP-71/51Mxx
BP-B547WD/B537WR
BP-C5xxWD/WR

	Fonctions de sécurité standard	Fonctions de sécurité standard*	Fonctions de sécurité standard	avec Data Security Kit installé	Fonctions de sécurité standard	avec Data Security Kit installé	Fonctions de sécurité standard	avec Data Security Kit installé
Protocole de commande et preuve d'utilisation	—	—	✓	✓	✓	✓	✓	✓
Suivi des modifications par Admin (SIEM et Syslog Integration)	✓	✓	✓	✓	✓	✓	✓	✓
Micrologiciel signé numériquement	✓	✓	✓	✓	✓	✓	✓	✓

Sécurité du fax Option fax nécessaire le cas échéant

BP-22C25
BP-C131WD
BP-C131PW

MX-CxxxP/P
MX-BxxxP/
W/P/PW

BP-30C25

MX-M1206
MX-M1056
MX-8081
MX-7081

BP-90Cxx
BP-71/61/51/56Cxx
BP-70Mxx | BP-71/51Mxx
BP-B547WD/B537WR
BP-C5xxWD/WR

	Fonctions de sécurité standard	Fonctions de sécurité standard*	Fonctions de sécurité standard	avec Data Security Kit installé	Fonctions de sécurité standard	avec Data Security Kit installé	Fonctions de sécurité standard	avec Data Security Kit installé
Séparation de fax et réseau	✓	✓	✓	✓	✓	✓	✓	✓
Fax confidentiel	—	—	✓	✓	✓	✓	✓	✓
Filtre à spams	—	✓	✓	✓	✓	✓	✓	✓

Gestion de sécurité

BP-22C25
BP-C131WD
BP-C131PW

MX-CxxxP/P
MX-BxxxP/
W/P/PW

BP-30C25

MX-M1206
MX-M1056
MX-8081
MX-7081

BP-90Cxx
BP-71/61/51/56Cxx
BP-70Mxx | BP-71/51Mxx
BP-B547WD/B537WR
BP-C5xxWD/WR

Sharp Smart Security Service	✓	✓	✓	✓	✓	✓
Surveillance de la sécurité des appareils par SRDM	—	—	✓	✓	✓	✓
Reconnaissance des virus grâce à Bitdefender	—	—	—	—	—	+

Légende

✓ Par défaut

+ En option

— Non disponible

* Les MX-B427W et MX-B427PW ne prennent pas en charge toutes les fonctions. Les MX-C607P et MX-B557P ne prennent pas en charge les fonctions de sécurité liées aux MFP pour la numérisation et la télécopie. Veuillez vous informer dans la fiche technique correspondante ou sur le web.

Termes techniques | Glossaire

Active Directory (AD)

Une base de données et un ensemble de services qui connectent les utilisateurs aux ressources du réseau dont ils ont besoin pour travailler. La base de données (ou répertoire) contient des informations importantes sur l'ensemble de l'environnement. p. ex. quels sont les utilisateurs et les ordinateurs disponibles et qui est autorisé à faire quoi. En particulier, la vérification d'un ID utilisateur et d'un mot de passe saisis permet généralement de s'assurer que chaque personne est bien celle qu'elle prétend être (authentification) et qu'elle n'a accès qu'aux données qui lui sont autorisées (autorisation).

BIOS

En informatique, le BIOS est un micrologiciel qui fournit des services d'exécution pour les systèmes d'exploitation et les programmes et qui effectue l'initialisation du matériel pendant le processus de démarrage.

Antivirus Bitdefender

Bitdefender est un moteur anti-malware primé qui protège l'utilisateur contre toute une série de cybermenaces. Il complète les fonctions de sécurité natives des systèmes multifonctions et protège contre les menaces connues et inconnues de logiciels malveillants tels que les virus, les chevaux de Troie, les vers, les rançongiciels, les logiciels espions et les menaces persistantes.

Data Security Kit

Le kit de sécurité des données Sharp élève la sécurité de l'appareil à un niveau supérieur avec des fonctions telles que l'écrasement manuel des données, l'écrasement automatique des données à la mise sous tension, l'impression et la détection de motifs cachés et bien plus encore. Il est ainsi possible de répondre à des exigences réglementaires ou de désamorcer des menaces spécifiques. En outre, certains modèles de MFP sont équipés d'une puce TPM (voir aussi page 14) qui empêche l'accès indésirable aux zones de stockage des données, dont font partie le lecteur de disque dur (HDD) et le lecteur Solid-State (Solid State Drive, SSD).

Denial of Service/Distributed Denial of Service (DoS/DDoS)

Le DoS est un type d'attaque par interférence qui bloque ou perturbe le fonctionnement normal ou le service d'un réseau ou d'un appareil. DDoS désigne une attaque DoS dans laquelle plusieurs (de nombreux) systèmes attaquants sont utilisés pour amplifier le trafic réseau, ce qui inonde et éventuellement submerge les systèmes ou réseaux cibles.

Fonction End-of-Lease

Lorsqu'une imprimante multifonction est mise au rebut, il est important de supprimer les données stockées dans l'appareil ou de les mettre dans un format illisible. Les MFP Sharp sont dotées de fonctionnalités standard de fin de vie afin de garantir que toutes les données confidentielles sont écrasées avant que le modèle ne quitte l'établissement ou l'environnement du client. Une fois lancées, les données sont écrasées jusqu'à 10 fois. Si un kit de sécurité des données Sharp est installé ou si la fonction de sécurité MFP standard est activée, les données sont écrasées par des nombres aléatoires.

Authentication Entra-ID (Microsoft)

Entra ID est un service cloud destiné à la gestion des identités utilisateur, particulièrement adapté à une utilisation avec les applications Microsoft telles que Microsoft 365. Il permet notamment de créer une solution d'authentification unique à grande échelle.

IEEE802.1x

Un protocole d'authentification réseau qui ouvre des ports pour l'accès au réseau lorsqu'une organisation authentifie l'identité d'un utilisateur et lui permet d'accéder au réseau. L'identité de l'utilisateur est établie sur la base d'informations de connexion ou d'un certificat.

Internet Printing Protocol (IPP)

Un protocole d'impression en réseau qui permet l'authentification et la gestion des files d'attente de travaux d'impression. L'IPP est pris en charge par la plupart des imprimantes et systèmes multifonctions modernes et est activé par défaut.

Adresse Internet Protocol (IP)

Chaque appareil connecté à Internet doit avoir un numéro unique (adresse IP) pour pouvoir se connecter à d'autres appareils. Actuellement, il existe deux versions d'adressage IP: IPv4 et une version mise à jour ultérieure appelée IPv6.

Filtrage d'adresses IP ou MAC

Les adresses IP et MAC sont des numéros uniques utilisés pour identifier les appareils sur Internet (IP) ou dans un réseau local (MAC). Le filtrage garantit que les adresses IP et MAC sont comparées à une «liste blanche» (voir aussi page 14) avant que les appareils ne puissent se connecter à votre réseau.

Internet Protocol Security (IPSec)

Une série de protocoles pour sécuriser la communication IP au niveau du réseau. IPSec comprend également des protocoles pour la création de clés cryptographiques.

Adresse Media Access Control (MAC)

L'adresse MAC d'un appareil est un identifiant unique attribué à un contrôleur d'interface réseau (NIC). Cela signifie qu'un appareil connecté au réseau peut être identifié de manière unique grâce à son adresse MAC.

Attaque de malware

Les logiciels malveillants (malware) peuvent être considérés comme des logiciels indésirables qui s'installent sur votre système sans votre consentement. Ils peuvent s'attacher à un code légitime et se propager; ils peuvent aussi se cacher dans des applications utiles ou se répliquer sur Internet.

Attaque Man-in-the-Middle (MITM)

Dans une attaque MITM, l'attaquant s'installe secrètement entre deux parties qui pensent être directement connectées et communiquent en privé. Le pirate «écoute» et peut également modifier la communication entre les parties.

Services réseau

Les services réseau facilitent le fonctionnement d'un réseau. Ils sont généralement fournis par un serveur (sur lequel un ou plusieurs services peuvent être exécutés) sur la base de protocoles de réseau. Quelques exemples sont le Domain Name System (DNS), le Dynamic Host Configuration Protocol (DHCP) ou le Voice over Internet Protocol (VoIP).

Attaque d'hameçonnage (phishing)

L'hameçonnage est une pratique frauduleuse qui consiste à envoyer des e-mails prétendant provenir d'entreprises légitimes afin d'inciter les individus à divulguer des informations personnelles telles que des mots de passe et des numéros de carte de crédit.

Ports

Les ports sont utilisés par les appareils en réseau (PC, serveurs, imprimantes, etc.) pour communiquer entre eux (p. ex. un ordinateur de bureau connecté à une imprimante). Les ports et services ouverts non surveillés peuvent être utilisés par des pirates pour téléverser p. ex. des logiciels malveillants (malware).

Protocols (protocoles)

Un protocole est défini comme un ensemble de règles et de formats qui permettent aux systèmes d'information d'échanger des informations. Dans un contexte de réseau, il y a par exemple les protocoles IP et TLS/SSL.

Single Sign-On (SSO, connexion unique)

Certaines MFP Sharp offrent des options d'authentification unique pour simplifier l'utilisation tout en validant l'accès des utilisateurs à l'imprimante multifonctions et au réseau. Lorsqu'une MFP rejoint un domaine, elle établit des connexions de confiance avec les ressources du réseau. Les administrateurs informatiques peuvent déployer une SSO Kerberos sécurisée basée sur un jeton pour les dossiers réseau et privés ainsi que pour les serveurs Microsoft® Exchange. Pour le service de stockage en ligne Google Drive™, le service de webmail Gmail™ et certains services cloud, un jeton OAuth est utilisé pour la mise en place du SSO.

Secure/Multipurpose Internet Mail Extensions (S/MIME)

Une série de spécifications pour la sécurisation des e-mails. S/MIME est basé sur le standard MIME largement répandu et décrit un protocole visant à renforcer la sécurité grâce aux signatures numériques et au cryptage.

Attaque de spoofing (usurpation)

Dans une attaque par usurpation, une partie se fait passer pour un autre appareil ou un autre utilisateur sur un réseau afin de lancer des attaques sur les hôtes du réseau, de voler des données, de diffuser des logiciels malveillants ou de contourner les contrôles d'accès.

Transport Layer Security/Secure Sockets Layer (TLS/SSL)

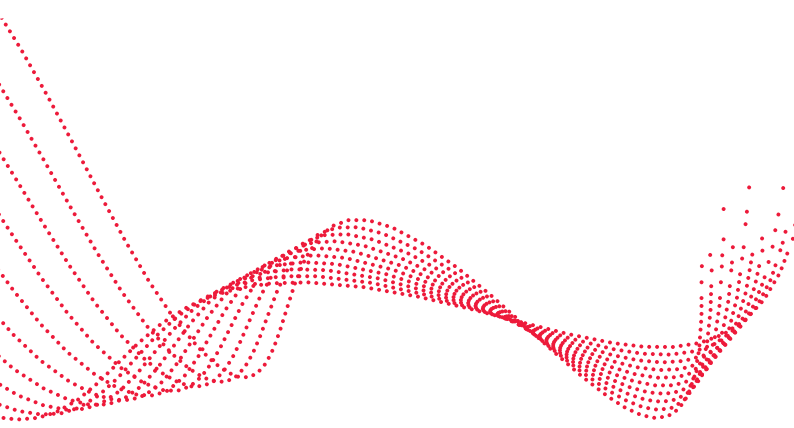
Une technologie qui crypte les données lorsqu'elles sont transportées ou transmises entre deux appareils afin d'empêcher leur interception ou leur accès par des tiers. TLS/SSL est souvent utilisé pour les sites web, mais peut également être utilisé pour protéger d'autres services.

Trusted Platform Module (TPM)

Une puce informatique aux normes industrielles qui utilise la technologie du cryptoprocèsseur pour protéger le matériel tel que les disques durs et les lecteurs solid state des MFP et des imprimantes. Lorsqu'une imprimante multifonction Sharp est installée avec un kit de sécurité des données ou TPM, la puce TPM initie une clé cryptographique à laquelle le logiciel n'a pas accès. Une clé cryptographique appropriée est encodée pendant le processus de démarrage. Si les deux clés ne correspondent pas, l'accès à l'appareil est refusé.

Whitelist (liste blanche)

Une liste blanche est une liste de personnes, d'installations, d'applications ou de processus sélectionnés auxquels des autorisations ou des droits d'accès spéciaux sont accordés. Au sens commercial, il pourrait s'agir par exemple des collaborateurs d'une organisation et de leurs droits d'accès au bâtiment, au réseau et à leurs ordinateurs. Dans un réseau ou un ordinateur, une liste blanche peut définir les applications et les processus qui ont le droit d'accéder aux magasins de données dans des zones sécurisées.





Sûr? Bien sûr. Sharp.

Chaque entreprise est unique et doit faire face à des défis particuliers. C'est pourquoi vos systèmes de sécurité devraient également être adaptés de manière optimale à vos besoins. La sécurisation de l'infrastructure d'impression revêt aujourd'hui une importance capitale, mais il convient également de garantir un accès facile à l'impression pour la productivité de l'entreprise. Pour relier au mieux ces deux pôles, nous proposons une analyse du paysage de l'impression ainsi que des formations dispensées par nos spécialistes.

C'est dans ce contexte que Sharp a également lancé le Smart Security Service, une offre de services innovante qui définit la sécurité «as a service». Il s'agit d'un service de profilage personnalisé, conçu pour garantir que vos MFP Sharp sont immédiatement sécurisées et dotées de fonctions de sécurité avancées, soigneusement adaptées à vos besoins, de sorte que votre agilité et votre productivité professionnelles ne soient pas compromises.

Nous commençons par passer en revue avec vous les menaces actuelles et potentielles pesant sur les données en ce qui concerne les MFP, afin de pouvoir définir une politique de sécurité d'impression appropriée pour vous. Nos experts de sécurité développent alors une configuration de sécurité personnalisée

pour vos MFP, qui répond exactement aux besoins de votre entreprise, en activant tous les paramètres de sécurité pertinents parmi plus de 200 pré-réglages.

Cela nous permet d'offrir le meilleur niveau de sécurité d'impression possible, sans pour autant limiter la flexibilité dont vos employés et vous avez besoin dans votre travail quotidien. Cela signifie également que nous préconfigurons, livrons, installons et intégrons vos nouvelles MFP de la manière la plus simple et la plus sûre possible. Ainsi, dès la première feuille imprimée, vous avez la certitude que vos systèmes et vos informations sont aussi sûrs que possible à l'heure actuelle.

SHARP BUSINESS SYSTEMS
DEUTSCHLAND GMBH
Industriestraße 180, D-50999 Köln
Tel.: +49 2236 323 100
www.sharp.de

Sharp Electronics Europe GmbH,
Zweigniederlassung Österreich
Handelskai 342, A-1020 Wien
Tel.: +43 1 727 19-0
www.sharp.at

SHARP ELECTRONICS (SCHWEIZ) AG
Moosstrasse 2a, CH-8803 Rüschlikon
Tel.: +41 44 846 61 11
www.sharp.ch

Bienvenue chez Sharp

Sharp Europe aide les organisations à réussir dans un monde du travail en constante évolution. En mettant en relation les personnes et la technologie, l'entreprise propose des solutions fiables et sur mesure pour les lieux de travail et les espaces publics, qui augmentent l'efficacité et améliorent les performances au sein des organisations, tout en permettant aux clients de se concentrer sur leur cœur de métier.

Basée à Londres, Sharp Europe collabore avec des clients privés aussi bien qu'avec le secteur public. Le portefeuille s'étend des imprimantes et technologies d'affichage avancées aux services informatiques, en passant par les plateformes de collaboration telles que les services Synappx. Membre du groupe Sharp Corporation, qui emploie plus de 39000 personnes dans le monde entier, Sharp Europe compte plus de 700 spécialistes informatiques, des bureaux dans 17 pays et quatre sites de production en Europe.

En tant que partie de Sharp Corporation, Sharp Europe investit dans de nouveaux domaines technologiques et joue ainsi un rôle de premier plan dans le secteur. Les besoins des organisations évoluant constamment, Sharp Europe est le partenaire idéal pour fournir les technologies qui permettent à ses clients de développer leur activité.

État: 02/26 | M30 Security-Guide-V01-26

La conception et les spécifications techniques peuvent être modifiées sans préavis. Toutes les informations étaient correctes au moment de l'impression. Sharp, Synappx et toutes les marques associées sont des marques commerciales ou des marques déposées de Sharp Corporation et/ou de ses filiales. Microsoft, Microsoft Teams, OneDrive et SharePoint sont des marques commerciales du groupe Microsoft. Android et Google sont des marques commerciales de Google LLC. AirPrint est une marque déposée d'Apple Inc. aux États-Unis et dans d'autres pays et régions. Tous les autres noms de sociétés, noms de produits et logos sont des marques commerciales ou des marques déposées appartenant à leurs propriétaires respectifs. | ©Sharp Corporation. Toutes marques reconnues. S. E. & O.

SHARP