LIVRE BLANC

# LES CINQ PRINCIPAUX DEFIS DE SECURITE DES PETITES ET MOYENNES ENTREPRISES

**Cisco fournit des réseaux capables de se défendre tout seuls spécifiquement adaptés aux besoins des petites et moyennes entreprises.**


## RESUME

Les petites et moyennes entreprises utilisent Internet et les applications en réseau pour répondre plus efficacement aux besoins de leur clients et en conquérir de nouveaux. Dans le même temps, les nouvelles menaces de sécurité et les impératifs de la législation imposent une pression croissante sur la fiabilité et la sécurité des réseaux d'entreprise. Cisco fournit aux petites et moyennes entreprises des solutions de sécurité intégrée complètes, économiques et taillées sur mesure qui les aident à garantir leur continuité métier, à maintenir la confidentialité de leurs informations clients et à réduire leurs frais d'exploitation. L'entreprise peut ainsi, en toute confiance, consacrer moins de temps à ses soucis de sécurité et davantage à son développement.


## LES DEFIS POSES AUX ENTREPRISES

Les PME/PMI doivent aujourd'hui évoluer dans un environnement concurrentiel mondialisé qui les amène à développer leurs activités et à améliorer la satisfaction de leurs clients tout en gardant un contrôle strict sur les coûts. Heureusement, Internet et les applications en réseau ont uniformisé les règles du jeu. Les PME peuvent utiliser leurs réseaux pour toucher des marchés plus lointains et communiquer plus vite et plus économiquement avec leurs clients et leurs partenaires. Toutefois, cette réactivité et cette agilité sont à double tranchant : Internet n'est pas uniquement utilisé par des gens de bonnes intentions et les failles de sécurité peuvent devenir extrêmement coûteuses. Plus que jamais, il est essentiel de disposer d'un réseau fiable, sécurisé et disponible.

## LES DEFIS DE SECURITE

De récentes études ont montré que la sécurité est le principal défi qui se pose aux PME/PMI. Les menaces de sécurité sont en constante évolution : provenant de l'extérieur comme de l'intérieur du réseau de l'entreprise, elles peuvent faire des ravages sur ses activités, réduire sa rentabilité et mécontenter sa clientèle. Les petites et moyennes entreprises doivent également se conformer aux nouvelles réglementations et lois destinées à protéger la vie privée des consommateurs et à maintenir la confidentialité des informations électroniques.

### Défi de sécurité n° 1 – les vers et les virus

Les vers et les virus demeurent la menace de sécurité la plus courante : au cours de l'année dernière, 75 % des petites et moyennes entreprises ont été touchées par au moins un virus*. Les vers et les virus peuvent avoir des conséquences dévastatrices sur la continuité des activités et sur les résultats financiers. Les souches virales sont chaque jour plus malignes et plus destructrices, elles se propagent toujours plus vite et peuvent infecter l'intégralité d'une entreprise en quelques secondes. Il faut beaucoup plus de temps pour nettoyer les ordinateurs infectés. Ces attaques ont des conséquences parfois catastrophiques : pertes de commandes, bases de données corrompues ou clients furieux. Alors que l'entreprise se débat pour installer les derniers correctifs de systèmes d'exploitation et les logiciels antivirus les plus récents sur ses ordinateurs, de nouveaux virus sont capables de pénétrer ses défenses à n'importe quel moment. Dans le même temps, les employés diffusent, parfois à leur insu, les virus et les logiciels espions en accédant à des sites Web malveillants, en téléchargeant des fichiers dangereux ou, sur leur messagerie électronique, en ouvrant des pièces jointes contaminées. Bien que ces attaques ne soient pas intentionnellement amenées dans l'organisation, elles peuvent être à l'origine de pertes financières importantes. Les systèmes de sécurité doivent détecter et repousser les vers, les virus et les logiciels espions en tous points du réseau.

### Défi de sécurité n° 2 – le vol d'informations

Le vol d'informations est une activité florissante. Les pirates malveillants pénètrent dans les réseaux d'entreprise pour y dérober des numéros de cartes de crédit ou de sécurité sociale dont ils pourront tirer profit. Les petites et moyennes entreprises sont en danger car elles représentent une proie apparemment plus facile que les grandes sociétés. Si la protection du périmètre du réseau est un bon point de départ, elle n'est pas suffisante : en effet, à l'intérieur de l'entreprise, de nombreux voleurs d'informations bénéficient de l'aide d'une personne de confiance, comme un employé ou un sous-traitant.

Le vol d'informations peut coûter cher aux PME/PMI car la satisfaction de leur clientèle et leur bonne réputation sont les bases de leur développement. L'entreprise qui ne protègerait pas correctement les informations qui lui sont confiées risque une mauvaise publicité, encoure des amendes et peut même être poursuivie en justice. Une stratégie de sécurité bien conçue doit empêcher le vol des informations électroniques confidentielles qu'elle détient, de l'intérieur comme de l'extérieur.

### Défi de sécurité n° 3 – la disponibilité métier

Les vers et les virus informatiques peuvent affecter de manière considérable la fiabilité des ressources réseaux qui, à leur tour, conditionnent la capacité de l'entreprise à réagir rapidement aux demandes de ses clients ; toutefois, les vers et les virus ne sont pas les seules menaces qui pèsent sur la disponibilité de l'entreprise. Les réseaux sont devenus tellement essentiels aux transactions commerciales quotidiennes que les cyber-terroristes se lancent dans le racket informatique, menaçant les entreprises de paralyser leurs sites Web et leurs opérations de commerce électronique si leurs exigences ne sont pas satisfaites. Leur arme : l'attaque par saturation qui envoie de lourds volumes de trafic en direction d'un élément critique du réseau, entraînant sa mise hors service ou l'impossibilité de traiter le trafic légitime. Une fois encore, les résultats peuvent être désastreux : pertes de données ou de commandes, demandes clients non satisfaites, etc. Si ces attaques sont rendues publiques, c'est la crédibilité de l'entreprise qui en souffre. Bien que les médias ne parlent essentiellement que des attaques par saturation qui frappent les grandes banques et les multinationales les plus importantes, les petites et moyennes entreprises ne sont pas à l'abri. Les pirates les considèrent en effet comme des victimes moins bien défendues que les grandes sociétés.

Il existe bien d'autres attaques, moins spectaculaires mais tout aussi réelles qui menacent la disponibilité des PME/PMI, et par conséquent leur rentabilité et la satisfaction de leurs clients. Le vol de ressources, par exemple, qui consiste à pénétrer les ordinateurs et des réseaux de l'entreprise pour en faire une base de partage illégal de fichiers audio, vidéos ou logiciels. Le plus souvent, l'entreprise ignore totalement que ses défenses ont été contournées, mais, dans le même temps, ses ordinateurs et ses réseaux sont lents à répondre à sa clientèle tandis que sa participation, même involontaire, au partage illégal de fichiers, la rend passible de poursuites judiciaires.

### Défi de sécurité n° 4 – l'inconnu

Pour un pirate, chaque avancée technologique en informatique et en communication peut être exploitée pour gagner de l'argent ou faire de nouveaux ravages. Les nouvelles versions matérielles et logicielles sont autant d'occasions de nuire. Les réseaux « peer-to-peer » et la messagerie Internet venaient à peine de voir le jour que leurs utilisateurs étaient attaqués par du code malveillant spécifiquement écrit pour ces nouvelles applications. Les téléphones mobiles font désormais partie des cibles des virus. Personne ne sait ce que l'avenir lui réserve, mais la meilleure défense est celle qui saura s'adapter facilement aux futures menaces sans qu'il soit nécessaire de casser sa tirelire.

* Maritz Research, 2005

### Défi de sécurité n° 5 – les réglementations de sécurité

Parallèlement aux menaces de sécurité liées à la malveillance, de nouvelles lois et réglementations exigent que les entreprises protègent la confidentialité et l'intégrité des informations qui leur sont confiées. L'Union européenne et, individuellement, de nombreux autres pays se sont dotés de législation pour la protection des données personnelles détenues par les organisations. Certains ont également adopté des lois complémentaires sur certains types d'informations, comme les informations de santé. Il appartient à l'entreprise de se mettre en conformité avec les lois et réglementations qui s'appliquent à ses activités sur ses marchés. Malheureusement, les ressources des structures les plus petites ne sont pas indéfiniment extensibles, tandis que leurs clients veulent l'assurance que les informations qu'ils leurs confient demeureront confidentielles.

Chaque société doit prendre les mesures nécessaires pour protéger son infrastructure métier, mais les petites et moyennes entreprises en particulier ont besoin de solutions simples, bien dimensionnées et abordables. Cisco a développé une solution de sécurité spécifiquement adaptée aux PME/PMI et qui incorpore les principes du réseau capable de se défendre tout seul de Cisco.

## LE RESEAU CAPABLE DE SE DEFENDRE TOUT SEUL

Le réseau capable de se défendre tout seul – Cisco Self-Defending Network – est la stratégie à long terme définie par Cisco pour la protection des processus métiers. Capable d'identifier, de prévenir et de s'adapter aux menaces tant internes qu'externes, il protège l'entreprise dès l'installation et évolue en fonction de ses besoins. Grâce à Cisco, l'entreprise protège non seulement son réseau mais également ses investissements informatiques : elle améliore ainsi ses processus métiers tout en réalisant de substantielles économies.

Trois caractéristiques font du réseau capable de se défendre tout seul une solution originale et performante. En premier lieu, il intègre la sécurité à tous les éléments du réseau afin que chaque point de celui-ci soit capable de se défendre lui-même contre les menaces internes et externes. Deuxièmement, ces éléments de réseau collaborent pour échanger des informations qui permettent d'assurer une protection complémentaire. Enfin, le réseau utilise la reconnaissance comportementale, une technologie innovante qui lui permet de s'adapter aux nouvelles menaces à mesure qu'elles se manifestent.

La solution de fondation réseau sécurisée Cisco constitue une offre de sécurité simplifiée mais complète et économique pour toutes les PME/PMI qui souhaitent disposer d'un réseau fiable et capable de se défendre lui-même.

## SOLUTION DE FONDATION RESEAU SECURISEE

La solution de fondation réseau sécurisée permet aux petites et moyennes entreprises de recentrer leurs ressources sur la rentabilité plutôt que sur leurs réseaux. Cette solution fournit, de manière traditionnelle ou sans fil, des services réguliers et sécurisés à tous les utilisateurs. Les services de sécurité sont intégrés sur les routeurs, les commutateurs et les serveurs de sécurité Cisco afin d'aider les PME/PMI à rationaliser leurs activités et à réduire leurs coûts.

La solution intègre la technologie de sécurité réseau qui protège les réseaux dès aujourd'hui et peut s'adapter aux besoins de sécurité de demain. L'entreprise peut continuer à fonctionner, même en cas d'attaque, et répondre aussi bien aux besoins de ses clients qu'à ceux de la réglementation en matière de sécurité et de confidentialité des données.

### Continuer à travailler, même en cas d'attaque

Alors que les attaques se multiplient, l'entreprise comme ses clients doivent pouvoir se protéger contre les interruptions de service, le coût qu'elles représentent et la corruption des données. Le réseau capable de se défendre tout seul Cisco est une démarche multifactorielle qui protège l'entreprise contre les effets désastreux des vers et des virus ou les attaques des cyber-terroristes et autres.

Les virus et les vers informatiques, de même que les logiciels espions, pénètrent le plus souvent dans l'entreprise par l'intermédiaire du courrier électronique ou des applications de messagerie Internet, des téléchargements Web ou des transferts de fichiers, bien que certaines attaques plus subtiles puissent passer par les services mobiles sans fil ou ceux des systèmes d'exploitation. Figurant parmi les meilleurs du marché, les systèmes de

prévention des intrusions (IPS) de Cisco examinent, en temps réel, l'intégralité du trafic entrant à la recherche d'irrégularités connues qui peuvent être à l'origine d'une attaque. Dès qu'une anomalie est détectée, un serveur de sécurité Cisco évalue la gravité du risque et communique avec les autres composantes du réseau sensibles à la sécurité. Ensemble, ils peuvent bloquer immédiatement la menace à la source et l'empêcher de se propager à d'autres parties du réseau.

Toutefois, les vers, les virus et les logiciels espions ne sont pas les seules attaques que peuvent subir l'entreprise. Les serveurs de sécurité Cisco exploitent les mêmes fonctionnalités d'inspection du trafic et des applications afin de détecter et de repousser les attaques par saturation ainsi que d'autres menaces si nouvelles qu'elles n'ont pas encore de nom.

La sécurité intégrée dans toute l'entreprise bloque les attaques connues et inconnues en temps réel, tandis que les communications entre les composantes du réseau permettent à celles-ci de s'adapter à l'évolution des conditions de sécurité. Ces couches successives de protection donnent aux PME les moyens de continuer à répondre à leurs clients et de poursuivre leurs activités même lorsqu'elles sont attaquées.

### Protéger la vie privée des clients

Les solutions Cisco utilisent de nombreux outils pour maintenir les informations clients hors de portée des utilisateurs non autorisés, qu'ils soient internes ou externes à l'entreprise. Les réseaux privés virtuels, ou VPN (Virtual Private Networks), permettent aux petits bureaux et aux employés en déplacement de communiquer entre eux et avec le siège social en totale confidentialité, même lorsqu'ils utilisent l'Internet public pour acheminer leurs données. Les normes les plus élevées d'authentification utilisateur garantissent que seules les personnes habilitées ont accès au réseau VPN, tandis que des technologies de cryptage robustes rendent les données inintelligibles pour tous ceux qui tenteraient d'intercepter les communications VPN sur le réseau public.

Le pare-feu et le système de prévention des intrusions sont présents sur chaque point d'entrée du réseau : ils contribuent ainsi à bloquer les vers, les logiciels espions ou les agissements des pirates qui tentent de pénétrer sur le réseau pour y voler des informations. Les pare-feux servent également à empêcher les utilisateurs internes d'accéder aux informations confidentielles. Les politiques de pare-feu interne peuvent, par exemple, empêcher les employés non autorisés d'accéder aux ordinateurs qui gèrent les finances, les ressources humaines ou la comptabilité, et même de visionner le trafic qui part de ces machines ou qui y aboutit. Les réseaux locaux virtuels, ou VLAN (Virtual LAN), permettent à l'entreprise de segmenter davantage encore les communications internes au sein de l'organisation. Les informations financières ou clients de nature confidentielle peuvent être placées sur des VLAN spécifiques et logiquement distincts des réseaux locaux des employés.

Les solutions Cisco permettent à l'entreprise de se mettre en conformité avec la réglementation sur la sécurité et la confidentialité des informations clients en protégeant le réseau des attaques et des intrus, qu'ils soient à l'intérieur ou à l'extérieur du réseau.

### Contrôle des coûts

Les solutions Cisco aident les petites et moyennes entreprises à contrôler leurs coûts de deux manières : premièrement, en évitant les frais inutiles liés aux attaques réussies, et ensuite en utilisant des composantes de sécurité multifonction, abordables et intégrées qui évoluent avec les besoins de l'entreprise. La sécurité intégrée simplifie la gestion du réseau, réduit les frais de maintenance et limite ainsi le coût total d'acquisition du réseau.

Les attaques réussies sur la sécurité du réseau ont un prix, et celui-ci peut être à la fois direct et caché. Dans de nombreux cas, par exemple l'attaque d'un virus relativement bénin, les dégâts sont limités et leur coût direct est lié au temps et aux ressources consacrés au nettoyage des systèmes infectés. Sachant que ce coût augmente avec le nombre de systèmes atteints, les capacités de protection et de détection sont d'autant plus économiques qu'elles sont rapides. Le temps de travail perdu par les employés pendant les opérations de nettoyage génère des coûts moins visibles. Parmi ces coûts cachés figurent les opportunités commerciales manquées, les clients perdus, l'atteinte à la réputation de l'entreprise ou les frais juridiques associés à ces attaques réussies. Même si c'est moins fréquent, les sommes en jeu peuvent atteindre des sommets. L'an passé, la criminalité en ligne a coûté aux entreprises britanniques près de 2,4 milliards de livres**, soit plus de 3,5 milliards d'euros. Les solutions Cisco permettent à l'entreprise d'éviter aussi bien les coûts directs que les coûts cachés des attaques réussies, de réduire le risque pour son activité et d'améliorer sa crédibilité et la confiance de ses clients.

Les PME/PMI ne disposent généralement pas des ressources humaines ou financières suffisantes pour déployer et gérer des solutions de sécurité complexes. Cisco propose une solution sûre, fiable et simple qui réduit le coût d'acquisition du réseau pour permettre à l'entreprise de se concentrer sur ses activités et non sur sa sécurité. Elle s'adapte aisément à l'évolution des besoins de l'entreprise et de ses conditions de sécurité, garantissant ainsi le maintien des coûts dans les limites imposées par sa croissance.

### Construire une fondation de réseau sécurisée

La solution Cisco s'appuie sur deux grandes familles de produits – la famille des routeurs à services intégrés Cisco ISR et la gamme des serveurs de sécurité adaptatifs Cisco ASA 5500 – qui sont les pierres angulaires du réseau capable de se défendre tout seul pour les petites et moyennes entreprises.

Comme leur nom l'indique, les routeurs à services intégrés réunissent de nombreuses fonctions dans une même plate-forme de routage fiable et économique pour un télétravailleur ou un bureau de petite taille ou de taille moyenne. Un routeur Cisco ISR fait, à lui seul, le travail d'un routeur d'accès DSL haut-débit avec liaison redondante intégrée, d'un commutateur de réseau LAN, d'un point d'accès sans fil et d'un commutateur de réseau WLAN. Ces fonctionnalités peuvent être ajoutées une à une, ce qui permet aux routeurs Cisco ISR de s'adapter à l'évolution des besoins des PME/PMI. Par ailleurs, les routeurs à services intégrés disposent de nombreuses fonctionnalités de sécurité de base comme le pare-feu, la détection des intrusions ou la connectivité VPN.

Les serveurs de sécurité adaptatifs de la gamme Cisco ASA 5500 constituent une famille d'unités de sécurité intégrée à hautes performances qui s'appuient sur les technologies éprouvées de Cisco en matière de sécurité. Capables de réagir et de s'adapter pour protéger le réseau contre toutes les menaces connues et inconnues, les serveurs de la gamme Cisco ASA 5500 réunissent ce qui se fait de mieux en matière de pare-feu, de prévention des intrusions, d'antivirus de réseau, d'inspection des applications et de connectivité VPN à accès distant ou de site à site. Un serveur Cisco ASA 5500 offre le meilleur niveau de protection contre les accès utilisateurs non autorisés, les vers, les virus, les logiciels espions et les applications non sécurisées ou malveillantes. Cette unité mono-poste, qui intègre des technologies de sécurité éprouvées, est conçue pour les réseaux modernes des PME/PMI. Elle est économique, facile à déployer et à gérer et est évolutive. A mesure qu'apparaissent de nouvelles menaces sur la sécurité des réseaux, des extensions de sécurité et des mises à niveau qui peuvent être installées par l'utilisateur permettront aux produits de la famille Cisco ASA de s'adapter afin de continuer à protéger l'entreprise. La gamme Cisco ASA 5500 est le choix idéal pour le déploiement d'un réseau pleinement sécurisé au siège social ou dans une agence distante.

En complément, les commutateurs de la gamme Cisco Catalyst® Express 500 sont des unités de commutation intelligentes, simples et sécurisées spécifiquement conçues pour les PME/PMI. Tous les commutateurs Cisco Catalyst disposent de fonction de sécurité qui détectent les irrégularités dans le trafic et les empêchent de saturer le commutateur ou de se répandre à d'autres points du réseau. Optimisés pour la transmission des données et de la voix et la connectivité sans fil, les équipements de la gamme Cisco Catalyst Express 500 vous apportent la fiabilité et la sécurité des commutateurs Catalyst dans une unité peu encombrante qui s'installe en quelques minutes. Chaque commutateur Cisco Catalyst Express 500 est livré pleinement fonctionnel avec Cisco Network Assistant, un outil de configuration capable de reconnaître les autres composantes du réseau.

Autres compléments, les points d'accès Cisco Aironet® ouvrent aux bureaux de petite taille et de taille moyenne un accès de réseau WLAN sécurisé. Les produits sans fil Cisco offrent le même niveau de sécurité, d'évolutivité et de simplicité de gestion que celui des réseaux LAN filaires. Les points d'accès Cisco Aironet supportent le roaming rapide et sécurisé lorsqu'ils sont utilisés avec des unités clients Cisco ou compatibles, afin de permettre aux utilisateurs authentifiés de se déplacer en toute sécurité d'une zone de couverture à une autre.

** National Hi-Tech Crime Unit

### Comment mettre en oeuvre une fondation réseau sécurisé

L'excellence et l'exhaustivité du service après vente et de l'assistance technique sont des facteurs essentiels pour la réussite à long terme d'une solution de réseau, quelle qu'elle soit. Le programme d'assistance Cisco SMB Support Assistant a été spécifiquement conçu pour répondre aux besoins des petites et moyennes entreprises. Ce programme d'assistance simple et économique permet de résoudre les problèmes les plus

couramment rencontrés par les PME et contribue à la disponibilité et à la sécurité de leurs réseaux. Il offre un diagnostic rapide, fournit des conseils précis de dépannage et permet le remplacement anticipé des pièces. L'une des composantes clés de ce programme est le portail Cisco SMB Support Assistant, ensemble sécurisé d'outils en ligne pour permettre à nos clients de récupérer leurs mots de passe, d'accéder à une documentation technique, de contrôler la santé de leur réseau, de télécharger des correctifs logiciels et d'ouvrir, si nécessaire, un dossier d'assistance technique.

## POURQUOI CISCO ?

Les solutions Cisco pour les petites et moyennes entreprises permettent d'assurer la continuité des processus métiers, la confidentialité des informations clients et le contrôle des coûts liés à l'entretien d'un réseau disponible, sécurisé et capable de se défendre lui-même. Ces qualités augmentent à leur tour la confiance de vos clients, renforcent l'efficacité de vos employés, garantissent la conformité réglementaire et réduit le coût total d'acquisition. Elles permettent également de renforcer leur productivité, de supporter des services innovants, d'améliorer la satisfaction de leurs clients et de réduire leurs frais d'exploitation. Disposant de capacité avancées en matière de voix, de sécurité, de mobilité et de protection des investissements, les solutions Cisco répondent aux besoins des PME/PMI dès maintenant et pour de nombreuses années.

Cisco et ses Partenaires s'engagent à apporter aux PME la meilleure expérience client possible. Nos options de financement, nos services et notre assistance technique maintes fois récompensés, ainsi que les formations personnalisées vous aideront à tirer tout le profit de votre solution Cisco.

Cisco est un des leaders mondiaux du routage, de la commutation et de la sécurité. Nos solutions souples répondent dès maintenant aux besoins des PME/PMI et pour de longues années en permettant à l'entreprise de croître sans perdre son agilité. La stratégie de sécurité de Cisco repose sur le réseau capable de se défendre tout seul qui intègre la sécurité à chaque point de l'infrastructure, travaille en collaboration pour renforcer la protection et s'adapte à l'évolution des conditions de travail du réseau comme aux nouvelles menaces de sécurité.

## LES PROCHAINES ETAPES

Pour toute information complémentaire sur la solution Cisco Secure Network Foundation, contactez votre représentant Cisco ou visitez la page http://www.cisco.fr/go/pme.

Pour connaître le partenaire Cisco le plus proche, visitez : http://www.cisco.com/go/partnerlocator.

Pour toute information complémentaire sur le financement de votre solution Cisco, visitez : http://www.cisco.fr/go/ciscocapital.


**Corporate Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

**European Headquarters**
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

**Asia Pacific Headquarters**
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799


Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe




205364.I_ETMG_KL_9.05

Printed in the USA