FICHE PRODUIT

LE SUMMUM DE LA PROTECTION DES DONNÉES

- Protection des données élargie, quel que soit le canal de communication : cloud, messagerie électronique, Web, terminaux, stockage.
- Diminution des faux positifs grâce à des technologies de détection globales.

INTERFACE CENTRALISÉE

- Console unique pour la gestion des politiques, l'intervention en cas d'incident, le reporting et l'administration.
- Politiques et workflow identiques pour tous les canaux de communication : cloud, messagerie électronique, Web, terminaux et stockage.

DIVERSITÉ DES INTÉGRATIONS

- Intégré à Symantec Enterprise Cloud qui prend en charge une vision SASE hybride axée données.
- Entièrement intégré à Microsoft Information Protection pour la classification des données, le chiffrement et la gestion des droits.

Symantec® Data Loss Prevention

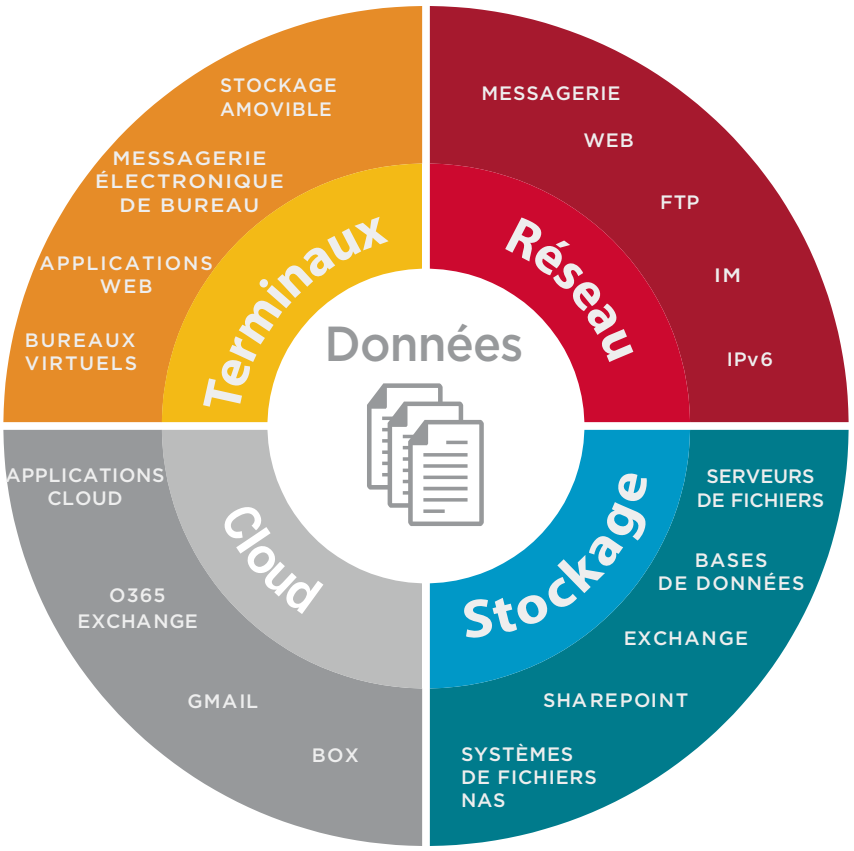
Assure la protection intégrale de vos données sensibles

Un niveau de protection extrême contre la perte de données

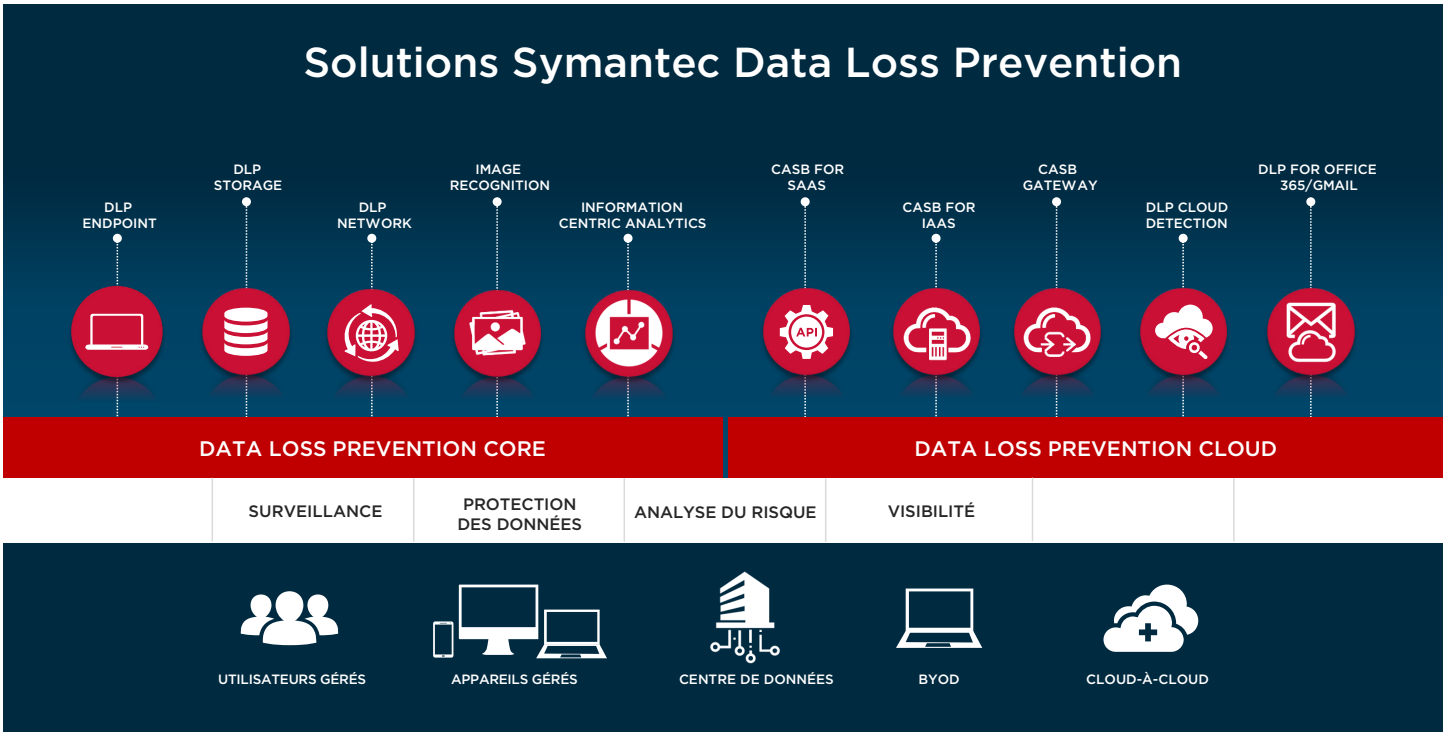
Il n'a jamais été aussi facile de protéger les informations et d'assurer leur conformité. Pourtant, les entreprises ne sont pas préparées à affronter les nouveaux problèmes de sécurité. Erreurs de configuration, exposition accidentelle des données… le grand remplacement des systèmes locaux par des services cloud fragilise les données, essentiellement par inexpérience du cloud. La sécurité dans le cloud n'est pas le seul sujet d'inquiétude des entreprises. Armés de nouveaux modes opératoires, les cybercriminels multiplient les attaques ciblées ; ils contournent les dispositifs de sécurité classiques et exploitent les utilisateurs pour s'emparer des données les plus précieuses de l'entreprise.

La solution de protection Symantec® Data Loss Prevention (DLP) assure un niveau de protection extrême qui empêche les violations de données et protège la réputation de votre entreprise. Découverte, surveillance et protection intégrales sont les atouts de notre technologie de pointe qui assure une visibilité et un contrôle absolus de vos données confidentielles.

- Détection de l'emplacement des données sur tous les canaux : cloud, messagerie électronique, Web, terminaux et stockage.
- Surveillance de l'utilisation des données, que les utilisateurs soient connectés ou non au réseau de l'entreprise.
- Protection des données en temps réel contre l'exposition ou le vol.



Symantec Data Loss Prevention



La protection adéquate, en toute simplicité

Symantec DLP embarque DLP Core et DLP Cloud pour une sécurité des informations leader sur les terminaux, le réseau, le cloud et le stockage. DLP Core assure la protection complète de l'information et intègre la reconnaissance d'image sensible et l'analytique centrée sur les données (l'analyse du comportement des utilisateurs et des entités, ou UEBA – User Entity Behavior Analytics). DLP Cloud étend les politiques DLP aux environnements cloud avec des contrôles CASB complets et des connecteurs cloud DLP pour les passerelles e-mail et web.

Sécurité des données actives sur les terminaux

Corollaire de l'usage des ordinateurs portables, la mobilité favorise les fuites et vols de données d'entreprise, que les utilisateurs soient connectés ou non au réseau de l'entreprise. DLP for Endpoint de Symantec (intégré à DLP Core) protège les données sensibles sur les terminaux. Messagerie électronique, applications cloud, protocoles réseau, stockage externe, bureaux virtuels, serveurs… tous les canaux bénéficient des fonctionnalités complètes de découverte, de surveillance et de protection des données. Avec Symantec DLP, un unique agent léger pour les terminaux active deux modules : DLP Endpoint Discover et DLP Endpoint Prevent.

- **Symantec DLP Endpoint Discover** analyse les disques durs locaux et fournit une visibilité totale sur les fichiers sensibles stockés sur les ordinateurs portables et fixes. Son vaste arsenal de ripostes inclut la mise en quarantaine de fichiers locaux et distants, le chiffrement basé sur les politiques et la gestion des droits numériques via l'API DLP Endpoint FlexResponse.
- **Symantec DLP Endpoint Prevent** surveille l'activité des utilisateurs et permet de contrôler finement un grand nombre d'applications, de terminaux et de plate-formes. Son vaste arsenal de ripostes inclut le chiffrement basé sur l'identité et la gestion des droits numériques pour les fichiers transférés sur USB. En cas d'incident, Endpoint Prevent vous permet également d'alerter les utilisateurs par le biais de fenêtres contextuelles et de notifications par courrier électronique. Le cas échéant, les utilisateurs peuvent ignorer les politiques sur présentation d'un justificatif ou en annulant l'action (en cas de faux positif).

Terminal	Disponibilité
Navigateurs	*Chrome	Safari	Firefox	IE et Edge*
Apps cloud	*Box	Dropbox	Google Drive	Microsoft OneDrive*
Apps de messagerie électronique	Outlook	Lotus Notes
Protocoles réseau	*HTTP	HTTPS	FTP*
Stockage amovible	*Appareils MSC	Appareils MTP*
Bureaux virtuels	*Citrix	Microsoft Hyper-V	VMware*
Autres	*Imprimante	Fax	Partage réseau	Presse-papiers*

Protection des données en transit sur le réseau

La généralisation des outils de collaboration et des applications cloud, couplée à des comportements à risque auxquels les entreprises ne sont pas toujours sensibilisées, augmente le risque d'exposition des données de communication. Symantec DLP for Network (intégré à DLP Core) assure la surveillance et empêche les fuites de données sensibles sur un grand nombre de protocoles de communication dans votre réseau.

DLP Network Monitor capte et analyse le trafic sortant de votre réseau d'entreprise et détecte le contenu sensible et les métadonnées sur les protocoles standard, non standard et exclusifs. Il est déployé aux points de sortie vers le réseau et s'intègre à votre TAP réseau ou à votre analyseur SPAN (Switched Port Analyzer). À l'inverse de solutions qui procèdent par échantillonnage en pic de charge et augmentent le risque de faux négatifs, Network Monitor effectue une inspection approfondie du contenu de l'ensemble des communications réseau sans aucune perte de paquet.

DLP Network Prevent for Email empêche les fuites ou les vols de messages sensibles imputables aux collaborateurs, aux sous-traitants et aux partenaires. Il surveille et analyse l'ensemble du trafic de messagerie de l'entreprise et, le cas échéant, modifie, redirige ou bloque les messages en se basant sur leurs attributs, contenu sensible ou autre. Network Prevent for Email est déployé aux points de sortie vers le réseau et s'intègre aux agents de transfert de message (mail Transfer Agents, MTA) et aux systèmes de messagerie dans le cloud, dont Microsoft Office 365 Exchange. Network Prevent for Email est déployé sous forme d'appliance logicielle ou virtuelle.

DLP Network Prevent for Web empêche les fuites de données sensibles sur le Web. Il surveille et analyse l'ensemble du trafic web et, le cas échéant, supprime le contenu HTML sensible ou bloque les requêtes. Network Prevent for Web est déployé aux points de sortie vers le réseau et s'intègre à votre serveur proxy HTTP, HTTPS ou FTP via ICAP. Network Prevent for Web est déployé sous forme d'appliance logicielle, matérielle ou virtuelle.

Protection des données au repos sur les référentiels de stockage

Les données numériques prolifèrent, essentiellement en raison de la production de documents en interne, mais peu d'entreprises se soucient de leur gouvernance et de leur protection. Symantec DLP for Storage (intégré à DLP Core) vous permet de découvrir et de sécuriser les données sensibles au repos, c'est-à-dire les données stockées sur les serveurs de fichiers, les terminaux, le stockage en cloud, les partages de fichiers réseau, les bases de données, SharePoint et autres référentiels de données.

Référentiel	Disponibilité
Serveurs de fichiers	*Windows via CIFS et DFS | Unix via NFS | Local Windows | Local Unix (Linux, AIX et Solaris) | Serveurs NAS*
Machines distribuées	*Ordinateurs portables | Ordinateurs fixes*
Référentiels de documents et de messagerie	SharePoint | LiveLink | Documentum | Lotus Notes | Microsoft Exchange | PST
Applications et contenu web	*Sites web d'entreprises | Intranet | Extranet | Applications personnalisées*
Bases de données	*Oracle | Microsoft | IBM DB2*

Symantec DLP Network Discover recherche les données confidentielles en analysant les partages de fichiers réseau, les bases de données et autres référentiels de données d'entreprise. Il s'agit, par exemple, de systèmes de fichiers locaux sur serveurs Windows, Linux, AIX et Solaris ; de bases de données Lotus Notes et SQL ; et de serveurs Microsoft Exchange et SharePoint. DLP Network Discover sait identifier plus de 330 types de fichiers, y compris personnalisés, à partir de leur signature binaire. La solution permet également l'analyse ultrarapide des grands environnements distribués et optimise les performances en analysant seulement les fichiers nouveaux ou modifiés.

Symantec DLP Network Protect enrichit Network Discover avec de solides capacités de protection des fichiers. Network Protect nettoie et sécurise automatiquement tous les fichiers exposés détectés par Network Discover, et propose un arsenal d'options de remédiation : mise en quarantaine ou déplacement des fichiers, copie des fichiers vers une zone de quarantaine ou application d'une politique de chiffrement basée sur l'identité et de droits numériques à certains fichiers. En outre, Network Protect sensibilise les utilisateurs sur les violations de politiques en ajoutant un fichier texte à l'emplacement d'origine du fichier pour expliquer le motif de la mise en quarantaine.

Symantec DLP inclut également une plate-forme API FlexResponse pour vous permettre de créer des mesures personnalisées de remédiation de fichier. FlexResponse fournit l'intégration clé en main avec d'autres solutions de protection Symantec et tierces, y compris Symantec File Share Encryption et Adobe LiveCycle.

Protection des données dans le cloud

La migration des applications héritées vers le cloud se poursuit et les questions de sécurité persistent : dans cet environnement, la visibilité et le contrôle des données sensibles ne sont pas aussi bien assurés que sur les serveurs privés. Mais Symantec DLP Cloud étend au cloud de solides contrôles de protection des données, avec tous les avantages d'une DLP cloud. Ses fonctionnalités de découverte, de surveillance et de protection s'appliquent à une large gamme d'applications cloud et locales.

Protection des données dans le cloud (suite)

Symantec DLP Cloud Detection Service inspecte le contenu d'applications cloud et du trafic web, et applique automatiquement les politiques liées aux données sensibles. Il s'intègre en cloud-à-cloud avec Symantec CloudSOC, notre solution CASB (Cloud Access Security Brokers) de pointe, pour protéger les données en transit et au repos sur plus de 100 applications cloud autorisées et non autorisées (Office 365, G-Suite, Box, Dropbox, Salesforce…). Il est ainsi possible d'étendre les politiques existantes et une solide détection aux applications cloud et de gérer tous les incidents depuis la console DLP. Parmi les contrôles, citons l'interdiction de partager les fichiers sensibles, la quarantaine, le blocage interdisant de quitter l'application, et l'application automatique du chiffrement et de droits numériques d'après l'identité à des fichiers spécifiques partagés avec des tiers. Symantec DLP Cloud Detection s'intègre également avec Symantec Web Security Service pour surveiller le trafic web, même chiffré, et protéger les utilisateurs mobiles et en déplacement.

Symantec DLP Cloud assure la surveillance précise et en temps réel du trafic de messagerie en s'appuyant sur une CTI intégrée et sur des fonctions de détection évoluées qui minimisent les faux positifs. Il assure également la protection en temps réel contre les fuites de données avec le blocage automatique de la messagerie ou la modification de message pour appliquer la mise en quarantaine ou le chiffrement en aval. Lorsque les données sont partagées avec des tiers, il peut activer automatiquement le chiffrement et les droits numériques d'après l'identité pour le corps des courriers électroniques et les pièces jointes. DLP Cloud Service for Email prend en charge Gmail for Work, Microsoft Office 365 Exchange Online et Microsoft Exchange Server. Disponible en version autonome, il est également proposé avec Symantec Email Security.cloud, un service avancé de protection contre les menaces de messagerie électronique.

Interface de gestion centralisée

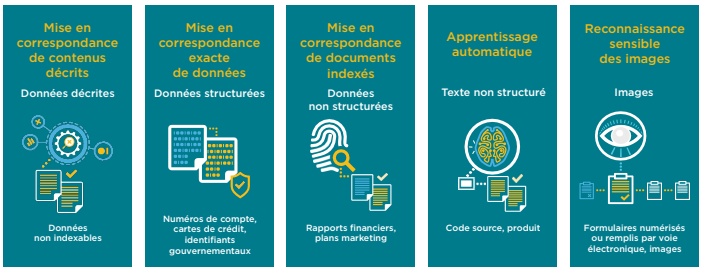
Plus votre écosystème de terminaux et de stockage est vaste, plus il est délicat de définir et d'appliquer des politiques de façon homogène. DLP Enforce Platform, la console de gestion unifiée de Symantec DLP, vous permet de définir des politiques une fois pour l'ensemble des canaux à risque de perte de données.

Avec DLP Enforce Platform :

- Utilisez une console web unique pour créer des politiques de prévention contre la perte de données, résoudre les incidents et administrer les systèmes sur l'ensemble des terminaux, des appareils mobiles, des services cloud, du réseau sur site et des systèmes de stockage.
- Profitez de plus de 70 modèles de politique prédéfinie et d'un générateur de politiques pratique pour que votre solution soit opérationnelle rapidement.
- Utilisez les fonctions efficaces de workflow et de remédiation pour rationaliser et automatiser les processus d'intervention en cas d'incident dans les environnements à fort trafic.
- Appliquez les renseignements métier à vos efforts de réduction des risques grâce à Symantec IT Analytics for DLP, un outil d'analyse perfectionné qui offre des capacités avancées de génération de rapports et d'analyse ad hoc.

Une visibilité inégalée sur les données confidentielles

Toutes les solutions DLP tiennent compte du contenu. En théorie, ces techniques de détection permettent de trouver des données sensibles où qu'elles soient stockées et quel que soit leur format. Symantec DLP se distingue par une offre complète qui combine un large éventail de technologies évoluées : Machine learning, reconnaissance d'image, identification des empreintes digitales et description permettent de classer les données avec précision sans faux positifs et sans incidence sur les utilisateurs.



- La correspondance de contenu décrit ou DCM, **Described Content Matching**, détecte le contenu en cherchant des correspondances sur des mots-clés, des expressions régulières, des modèles et des propriétés de fichier. Symantec DLP dispose de plus de 130 algorithmes prédéfinis d'identification de données qui combinent correspondance de modèles et CTI intégrée pour éviter les faux positifs.
- La mise en correspondance exacte de données ou EDM, **Exact Data Matching**, détecte les données par identification des empreintes digitales ou indexation de sources de données structurées, par exemple des bases de données, des serveurs d'annuaires et autres fichiers de données structurés.
- La mise en correspondance de documents indexés ou IDM, **Indexed Document Matching**, procède par identification des empreintes digitales pour détecter les données stockées dans des documents non structurés (documents Microsoft Office, fichiers PDF, fichiers binaires tels que les JPEG, conceptions CAD, fichiers multimédias…). IDM détecte également le contenu dit dérivé, par exemple du texte copié dans un fichier à partir d'un document source.

- La **reconnaissance sensible des images** (fournie par DLP Core) détecte le texte contenu dans des images (numérisation de formulaires, documents, captures d'écran, photos, PDF…) grâce à notre technologie exclusive de reconnaissance de formulaire (Form Recognition) et à notre moteur OCR intégré.
- **Vector Machine Learning** (VML) protège les données de propriété intellectuelle ayant des caractéristiques subtiles, rares ou difficiles à décrire, par exemple les rapports financiers et le code source. Avec VML, vous n'avez pas à localiser, décrire ou identifier par signature les données que vous voulez protéger.

Symantec DLP intègre la détection par correspondance de données structurées (Structured Data Matching) qui permet de détecter des données sensibles au format tabulaire. Ses API additionnelles, enrichies et prêtes à l'emploi, s'intègrent à de nombreux produits de sécurité tiers et d'applications cloud et exclusives que vous pouvez personnaliser : API DLP REST, API DLP FlexResponse, API DLP d'extraction de contenu, API DLP de reporting d'incident et de mise à jour, et API DLP d'appliance virtuelle de détection.

Protection des données, dépassez la simple DLP

Les données sensibles sont partagées hors site ou sur le cloud. Sorties de votre environnement géré, elles sont vulnérables à une exposition involontaire aux risques. Politique de sécurité d'accès au cloud, de classification, de chiffrement, d'analytique utilisateur, de passerelles web… notre solution assure la protection intégrale de vos données tout au long de leur cycle de vie, même en dehors de votre environnement géré.

- **Extension des politiques DLP aux applications cloud :** détection DLP, politiques et workflows peuvent être étendus aux applications cloud via l'intégration avec Symantec CloudSOC (CASB). Les incidents sont gérés depuis une console unique.
- **Simplification du tri des incidents et de la gestion des politiques :** Symantec Information Centric Analytics (ICA), outil d'analytique du comportement des utilisateurs et des entités, ou UEBA (User Entity Behavior Analytics), intégré à DLP Core, vous permet de consacrer moins de temps et d'énergie à la remédiation des incidents et à la gestion des politiques, et d'atténuer les risques d'exposition des données.
- **Sécurité renforcée du partage des données :** grâce à l'authentification renforcée, Symantec VIP Identity and Access Management empêche les accès non autorisés aux données sensibles en cas de partage de données avec des partenaires commerciaux.
- **Circulation des données interdite sur les sites non approuvés :** empêchez la circulation des données sensibles, même chiffrées, sur des sites non approuvés avec l'intégration de la DLP aux passerelles web sécurisées (SWG) Symantec : Symantec ProxySG et Web Security Service.
- **Intégration avec Microsoft Information Protection (MIP) :** Symantec DLP s'intègre aux puissantes fonctionnalités de classification et de chiffrement fournies par MIP. Cette solution permet de détecter et de lire les documents et les courriers électroniques protégés via MIP.

Configuration requise

La solution Symantec DLP intègre une plate-forme de gestion unique, un agent léger pour terminaux et de puissantes fonctionnalités de détection tenant compte du contenu. Au déploiement ultraflexible s'ajoute un grand nombre d'options multienvironnements : licences locales ; appliances virtuelles et physiques ; services de cloud public, privé et hybride ; services gérés délivrés par les Partenaires Symantec. Contrairement aux autres solutions de prévention des pertes de données, elle est reconnue pour son efficacité dans des environnements hautement distribués, couvrant des centaines voire des milliers d'employés.

Pour connaître la configuration système requise pour Symantec Data Loss Prevention, rendez-vous sur notre page de support.

Protégez vos informations dès maintenant

Symantec est la solution prête à l'emploi pour étendre votre sécurité et vos politiques de conformité au-delà de votre pare-feu. Efficace, elle vous permet de découvrir, surveiller et protéger l'intégralité de vos informations. Elle offre un coût total de possession très réduit, grâce à des méthodologies de déploiement reconnues, des outils intuitifs de gestion des politiques et des incidents, ainsi qu'une couverture complète de tous vos canaux de communication à haut risque.

Découvrez tous les avantages d'une protection complète des informations parfaitement adaptée à l'environnement actuel, mobile et relié au cloud : en savoir plus sur Symantec Data Loss Prevention.

BROADCOM®
connecting everything®

Pour plus d'informations, visitez notre site web à l'adresse suivante : www.broadcom.com

NIS-DLP-PB101_FR 30 novembre 2023