

## Renseignements de base sur l'entreprise

Veillez inscrire les renseignements suivants concernant l'ensemble de l'entreprise ou du groupe (y compris toutes les filiales) qui présente une demande de police d'assurance. Tous les termes définis seront en gras et surlignés en **bleu** et peuvent être trouvés dans le glossaire à la fin de ce formulaire de demande :

Nom constitutif :	Principal secteur industriel :
Adresse principale (adresse, province, code postal, pays) :	
Description des activités commerciales :	
Adresse du site web :	
Date de création (JJ/MM/AAAA):	Nombre d'employés :
Revenu brut pour les 12 derniers mois : \$	Revenus provenant des ventes aux États-Unis (%) :
Bénéfice brut pour les 12 derniers mois : \$	
Veillez préciser la ou les institution(s) financière(s) que vous utilisez pour vos opérations bancaires commerciales :	

## Coordonnées du contact principal

Veillez fournir les coordonnées de la personne la plus compétente au sein de votre organisation en ce qui concerne la sécurité informatique. Ces coordonnées seront utilisées pour fournir des informations sur le téléchargement de notre application de réponse aux incidents et pour recevoir des alertes et des mises à jour sur la gestion des risques :

Nom de la personne de contact :	Fonction:
Adresse de courriel :	Numéro de téléphone:

## Cyber incidents précédents

Veillez cocher toutes les cases ci-dessous concernant tout incident cybernétique dont vous avez été victime au cours des trois dernières années (il n'est pas nécessaire de mentionner les événements qui ont été bloqués avec succès par des mesures de sécurité) :

Extorsion cybernétique	Perte de données	Attaque par déni de service	Violation de la propriété intellectuelle
Infection par maliciel	Atteinte à la vie privée	Rançongiciel	Vol de fonds
Autre (veuillez préciser)			

Si vous avez coché l'une des cases ci-dessus, le ou les incidents ont-ils eu une conséquence financière directe de plus de 10 k \$ sur votre entreprise ?    Oui    Non

Si oui, veuillez fournir des renseignements supplémentaires ci-dessous, incluant des détails sur l'impact financier et les mesures prises pour éviter que l'incident ne se reproduise :

## Analyse des revenus

Veillez fournir les renseignements suivants pour vos 5 clients principaux :

Nom du client :	Principaux services :	Revenus annuels provenant de ce client:
.....		
.....		
.....		
.....		
.....		

## Ressources et infrastructure informatiques

Veillez confirmer le nom de votre **fournisseur de services gérés** (le cas échéant) :

.....

Quel est le nombre approximatif de serveurs sur votre réseau ?

.....

Quel est le nombre approximatif d'ordinateurs de bureau et d'ordinateurs portables sur votre réseau ?

.....

Quel est votre budget informatique annuel ?

.....

Quel pourcentage approximatif de votre budget informatique est consacré à la sécurité informatique ?

.....

Une partie de votre infrastructure informatique est-elle sous-traitée à des fournisseurs de technologie tiers, y compris des fournisseurs de services d'application ? *Oui Non*

*Si vous avez répondu « oui » à la question ci-dessus, veuillez énumérer, ci-dessous, vos fournisseurs de technologies tiers principaux (maximum de 10), y compris un bref résumé des services technologiques qu'ils vous fournissent :*

---

## Stockage et gestion des données

Veillez indiquer le nombre approximatif d'individus uniques auprès desquels vous recueillez, stockez et/ou traitez les informations personnelles identifiables, que ce soit sur vos propres systèmes ou avec des tierces parties :

Type de données

Nombre d'individus uniques

Données sensibles (par exemple, dossiers médicaux, détails du passeport, numéros de sécurité sociale, etc) :

.....

Données non sensibles (par exemple, les noms complets, les adresses, les adresses électroniques, etc) :

.....

Veillez décrire votre approche de la protection des informations sensibles et confidentielles (par exemple, contrôles d'accès, cryptage, segmentation du réseau, etc) :

---

Veillez fournir des détails sur la fréquence à laquelle vous éliminer les enregistrements qui ne sont plus nécessaires :

---

Veillez fournir des détails sur la manière dont vous stockez vos sauvegardes de données critiques (par exemple, des sauvegardes en ligne stockées sur l'environnement réel de votre organisation, des sauvegardes hors ligne stockées sur un dispositif de stockage amovible entièrement déconnecté et inaccessible depuis l'environnement réel, des sauvegardes stockées chez un fournisseur de stockage en nuage en ligne, etc.) :

---

Veillez décrire des détails sur la fréquence des sauvegardes, y compris la fréquence des sauvegardes complètes du système et la fréquence des sauvegardes incrémentielles/différentielles des données critiques :

---

Veillez fournir des détails sur la manière dont vous sécurisez vos sauvegardes (par exemple, les sauvegardes sont déconnectées et inaccessibles depuis l'environnement réel, une authentification multifactorielle est requise pour l'accès aux sauvegardes dans le nuage, etc) :

---

Veillez fournir des détails sur la façon dont vous testez vos sauvegardes, y compris des détails sur la fréquence à laquelle vous testez la restauration complète et la récupération des configurations de serveurs clés et des données à partir des sauvegardes :

---

Veillez fournir des détails sur le nombre de copies de sauvegarde que vous faites, y compris des détails sur la façon dont vous empêchez que des copies de sauvegarde distinctes soient affectées par le même événement (le cas échéant) :

## Sécurité des points d'extrémité

Quel outil de **protection des points d'extrémité** utilisez-vous sur votre réseau ?

Veillez indiquer le nom du vendeur et l'outil utilisé :

Utilisez-vous un outil de **détection et réponse aux points d'extrémité (EDR)** sur votre réseau ? *Oui* *Non*

Si « oui » :

Quel outil utilisez-vous :

Veillez donner un aperçu de la manière dont votre outil EDR est surveillé et géré (par exemple, par une équipe informatique interne ou par une tierce partie) :

L'outil EDR est-il déployé sur tous les points d'extrémité de votre réseau ? *Oui* *Non*

Si « non » :

Quel est le pourcentage des points d'extrémité pour lesquels le système EDR n'est pas déployé et pourquoi n'est-il pas déployé sur ces points d'extrémité ?

## Sécurité du périmètre

Avez-vous déployé **des pare-feu de nouvelle génération** à tous les points d'entrée et de sortie du réseau ? *Oui* *Non*

Selon quelle fréquence procédez-vous à **le bayalage de vulnérabilité** de votre périmètre réseau ?

Selon quelle fréquence procédez-vous à des **tests d'intrusion** de votre architecture réseau ?

Veillez fournir des informations concernant les fournisseurs tiers que vous utilisez pour effectuer des tests de pénétration (le cas échéant) :

Veillez confirmer si l'authentification multifactorielle est requise pour tous les accès à distance à votre réseau : *Oui* *Non*

*Si vous utilisez une autre méthode pour sécuriser l'accès à distance à votre réseau, comme l'authentification par certificat pour les appareils, veuillez fournir des détails ici :*

Veillez confirmer si l'**authentification multifactorielle** est requise pour accéder à toutes les ressources en nuage contenant des informations sensibles ou confidentielles : *Oui* *Non*

## Sécurité du périmètre

Veillez confirmer que l'**authentification multifactorielle** est activée pour l'accès à distance à tous les comptes de messagerie de l'entreprise : *Oui* *Non*

Simulez-vous des attaques d'hameçonnage pour tester les employés au moins une fois par an ? *Oui* *Non*

Utilisez-vous un logiciel de filtrage des courriels pour analyser tous les courriels entrants et sortants afin de filtrer les pourriels et les contenus malveillants ? *Oui* *Non*

Si vous avez répondu « oui » à la question précédente, veuillez indiquer le nom du fournisseur et le produit utilisé pour le filtrage des courriels :

Si vous êtes un utilisateur d'Office 365, veuillez fournir votre Microsoft Secure Score  
(Les administrateurs peuvent trouver le score en utilisant le lien suivant <https://security.microsoft.com/securescore>):

### Sécurité du réseau

Veuillez fournir des détails sur la manière dont vous protégez les comptes d'utilisateurs privilégiés (par exemple, en utilisant des solutions de gestion des accès privilégiés, en limitant les comptes d'utilisateurs privilégiés à des appareils spécifiques, en surveillant de manière accrue les comptes pour détecter toute utilisation anormale, en activant l'authentification multifactorielle pour l'accès à distance, etc) :

Les utilisateurs non informatiques ont-ils des droits d'administrateur local sur leurs ordinateurs portables/de bureau ?    Oui    Non

Utilisez-vous une solution de [surveillance du réseau](#) pour alerter votre organisation en cas d'activité suspecte ou de comportement malveillant sur votre réseau ?

Si vous avez répondu « oui » à la question précédente, veuillez indiquer le nom du fournisseur et le produit utilisé pour la surveillance du réseau :

Veuillez indiquer si vous disposez d'un [centre des opérations de sécurité \(SOC\)](#) chargé de la surveillance et de la détection des événements, de la gestion des vulnérabilités et de la réponse aux incidents. Veuillez inclure des détails sur les heures de fonctionnement et préciser s'il s'agit d'une fonction interne ou externalisée à une tierce partie :

Utilisez-vous un logiciel en fin de vie (EOL/EOS) ?    Oui    Non

Si « oui », veuillez fournir des détails sur la nature du logiciel en fin de vie (EOL/EOS), la manière dont il est utilisé, s'il est séparé du reste du réseau et si oui, comment il est séparé :

Veuillez décrire votre processus de gestion des correctifs et la manière dont vous vous assurez que tous les correctifs critiques sont appliqués en temps opportun, y compris un calendrier de mise en œuvre des correctifs pour les vulnérabilités zero-day après leur publication par le fournisseur:

Veuillez fournir des détails sur les changements majeurs que vous avez prévus pour votre infrastructure informatique au cours des 12 prochains mois (le cas échéant) :

### Contrôles supplémentaires

Veillez confirmer qu'**avant** toute modification des détails du compte d'une tierce partie, vous obtenez l'autorisation de ce dernier par une méthode d'authentification différente de la méthode initiale utilisée pour demander la modification ? Oui Non

Veillez confirmer qu'**avant** de transférer des fonds vers un compte sur lequel vous n'avez jamais versé d'argent, vous obtenez l'autorisation du destinataire des fonds par une méthode d'authentification différente de la méthode initiale utilisée pour demander le transfert ? Oui Non

Fournissez-vous une formation sur les escroqueries par hameçonnage/ingénierie sociale à tous les employés impliqués dans le transfert de fonds au nom de votre organisation, au moins une fois par an ? Oui Non

Veillez cocher toutes les cases ci-dessous concernant les contrôles actuellement mis en place dans votre infrastructure informatique (y compris ceux qui sont fournis par un tiers). Si vous n'êtes pas sûr de ce que sont ces outils, veuillez consulter les explications à la dernière page du présent formulaire.

Utilisation d'une liste blanche des applications	Inventaire des actifs informatiques	Renseignements personnalisés de menaces	Cryptage des bases de données
Prévention des pertes de données	Atténuation des attaques de déni de service distribué	DMARC	Filtrage de noms de domaine
Formation de sensibilisation des employés	Plan d'intervention en cas d'incident	Tests d'intrusion	Pare-feu de périmètre
Gestion des informations et des événements liés à la sécurité	Réseau privé virtuel (VPN)	Pare-feu applicatif Web (WAF)	Filtrage des contenus d'Internet

Veillez fournir le nom du fournisseur de logiciels ou de services que vous utilisez pour chacun des contrôles sélectionnés ci-dessus :

### Avis important

En signant ce formulaire, vous confirmez que les renseignements fournis sont exacts et complets et que vous avez pris toutes les mesures raisonnables pour vous en assurer en vous adressant aux personnes concernées au sein de votre entreprise. CFC Underwriting utilisera ces renseignements uniquement pour fournir des services d'assurance et pour ce faire, elle pourrait partager vos données avec des tiers. Nous pourrions également utiliser des éléments dépersonnalisés de vos données pour l'analyse des tendances de l'industrie et pour fournir des données d'étalonnage. Pour des informations complémentaires concernant notre politique de confidentialité, visitez le site [www.cfcunderwriting.com/privacy](http://www.cfcunderwriting.com/privacy)

Nom de la personne de contact :

Fonction :

Signature :

Date (JJ/MM/AAAA) :

Veillez énumérer ci-dessous vos fournisseurs de technologies tiers principaux (maximum de 10).

---

### Avis important

*En signant ce formulaire, vous confirmez que les renseignements fournis sont exacts et complets et que vous avez pris toutes les mesures raisonnables pour vous en assurer en vous adressant aux personnes concernées au sein de votre entreprise. CFC Underwriting utilisera ces renseignements uniquement pour fournir des services d'assurance et pour ce faire, elle pourrait partager vos données avec des tiers. Nous pourrions également utiliser des éléments dépersonnalisés de vos données pour l'analyse des tendances de l'industrie et pour fournir des données d'étalonnage. Pour des informations complémentaires concernant notre politique de confidentialité, visitez le site [www.cfcunderwriting.com/privacy](http://www.cfcunderwriting.com/privacy)*

Nom de la personne de contact:

Fonction:

.....

Signature:

Date (JJ/MM/AAAA):

.....

## Utilisation d'une liste blanche des applications

Une solution de sécurité qui permet aux organisations de préciser quels logiciels peuvent être utilisés dans leurs systèmes afin de prévenir le fonctionnement de tout processus ou de toute application non-listé sur la liste blanche.

## Inventaire des actifs informatiques

Une liste de tout le matériel et des appareils informatiques détenus, exploités ou gérés par une entité. De telles listes sont typiquement utilisées pour évaluer les données détenues et les mesures de sécurité mises en place dans tous les dispositifs.

## Renseignements personnalisés de menaces

La collecte et l'analyse de données provenant de renseignement de sources ouvertes (OSINT) et de sources du Dark Web pour fournir aux organisations des renseignements relatifs aux menaces cybernétiques et aux auteurs de cybermenaces pertinents.

## Cryptage des bases de données

Quand les données sensibles sont cryptées pendant qu'elles sont détenues dans les bases de données. Si cette mesure est mise en place correctement, elle peut empêcher des auteurs de cybermenaces de lire les données sensibles s'ils réussissent à accéder à la base de données.

## Prévention des pertes de données

Logiciel qui peut déterminer si les données sensibles sont extraites d'un réseau ou d'un système informatique.

## Atténuation des attaques de déni de service distribué

Matériel informatique ou solutions axées sur l'informatique en nuage utilisés pour filtrer et bloquer le trafic malveillant associé à une attaque par déni de service distribué tout en permettant aux utilisateurs légitimes de continuer à accéder au site Web de l'entité ou à ses services en ligne.

## DMARC

Un protocole Internet utilisé pour lutter contre l'usurpation d'adresse électronique, une technique utilisée par les pirates informatiques dans des campagnes d'hameçonnage.

## Filtrage de noms de domaine (DNS)

Une technique précise pour bloquer l'accès à des adresses IP malveillantes reconnues aux utilisateurs de votre réseau.

## Filtrage des courriels

Logiciel utilisé pour balayer et catégoriser les courriels entrants et sortants afin de filtrer les pourriels et autre contenu malveillant.

## Sensibilisation des employés

Des programmes de formation conçus pour accroître la sensibilisation des employés en matière de sécurité. Par exemple, les programmes peuvent être axés sur le moyen d'identifier des courriels d'hameçonnage potentiel.

## Détection et réponse aux points d'extrémité (EDR)

Un outil logiciel qui fonctionne en surveillant et en collectant des données à partir de points finaux et en enregistrant les informations dans une base de données centrale où se déroulent des analyses, des détections, des enquêtes, des rapports et des alertes supplémentaires.

## Protection des points d'extrémité

Logiciel installé sur des ordinateurs individuels (points d'extrémité) qui utilise l'analyse du comportement et des signatures pour identifier et arrêter les infections par des logiciels malveillants.

## Plan d'intervention en cas d'incident

Des plans d'action pour faire face aux incidents cybernétiques afin d'aider à guider le processus décisionnel de l'organisation et revenir au fonctionnement normal le plus rapidement possible.

## Système de détection d'intrusion

Une solution en matière de sécurité qui surveille l'activité sur vos systèmes ou réseaux informatiques et génère des alertes quand elle détecte des signes d'un danger émanant d'auteurs de cybermenaces.

## Fournisseurs de services gérés

Une organisation tierce qui fournit des services informatiques, y compris des services au niveau des réseaux, de l'infrastructure, de la sécurité informatique, du soutien technique et de l'administration informatique.

## Chiffrement d'appareils mobiles

Le chiffrement implique de brouiller les données à l'aide de techniques cryptographiques afin qu'elles puissent être lues uniquement par une personne possédant une clé spécifique. Quand le chiffrement est activé le disque dur d'un appareil est crypté lorsque l'appareil est verrouillé. Le code ou le mot de passe de l'utilisateur agit comme clé spécifique.

## Authentification multifactorielle

Quand un utilisateur s'authentifie par deux moyens lorsqu'il ouvre une session à distance dans un système informatique ou un service en ligne. Ces deux moyens sont typiquement un mot de passe et un code généré par un dispositif de jeton physique ou un logiciel.

## Surveillance de réseau

Un système qui utilise le logiciel, le matériel informatique ou une combinaison des deux et qui surveille constamment les problèmes de performance et sécurité du réseau d'une organisation.

## Pare-feu de nouvelle génération

Solutions logicielles ou matérielles qui combinent la technologie traditionnelle des pare-feu avec des fonctionnalités supplémentaires, telles que l'inspection du trafic crypté, les systèmes de prévention des intrusions et les antivirus.

## Tests d'intrusion

La simulation autorisée d'attaques contre une organisation pour mettre à l'épreuve ses défenses en matière de cybersécurité. Cette technique s'appelle aussi piratage contrôlé ou méthode de l'équipe rouge.

## Pare-feu de périmètre

Des solutions de matériel informatique utilisées pour contrôler et surveiller le trafic réseau entre deux points selon des paramètres prédéfinis.

## Gestion d'information et d'événements de sécurité

Système utilisé pour cumuler, corréliser et analyser la sécurité des réseaux et de l'information, y compris les messages, les journaux et les alertes générés par différentes solutions en matière de sécurité dans l'ensemble du réseau.

## Centre des opérations de sécurité (SOC)

Une installation qui abrite une équipe de sécurité de l'information chargée de surveiller et d'analyser en permanence la posture de sécurité d'une organisation. L'objectif de l'équipe SOC est de détecter, d'analyser et de répondre aux incidents de cybersécurité en utilisant une combinaison de solutions technologiques et un ensemble de processus solides. Les SOC peuvent être internes et gérés par l'organisation elle-même ou externalisés à une tierce partie.

## Réseau privé virtuel (VPN)

Un VPN est une connexion cryptée sur l'internet entre un appareil et un réseau. La connexion cryptée permet de garantir que les données sensibles sont transmises en toute sécurité. Il est le plus souvent utilisé pour fournir une connexion à distance sécurisée au réseau d'une organisation.

## Balayage de vulnérabilité

Tests automatisés conçus pour sonder les systèmes ou les réseaux informatiques et déceler la présence de vulnérabilités connues qui permettraient à des auteurs de cybermenaces d'obtenir un accès à un système.

## Pare-feu pour applicatif Web (WAF)

Protège les serveurs Web et leurs applications d'une intrusion ou d'une utilisation malveillante en inspectant et en bloquant les demandes nuisibles et le trafic Internet malveillant.

## Filtrage de contenu d'Internet

Le filtrage de certaines pages ou de certains services Web jugés comme potentiellement menaçant à la sécurité d'une organisation. Par exemple, des sites d'Internet reconnus comme malveillants sont typiquement bloqués à l'aide d'une forme de filtrage de contenu d'Internet.