cira | DNS Firewall

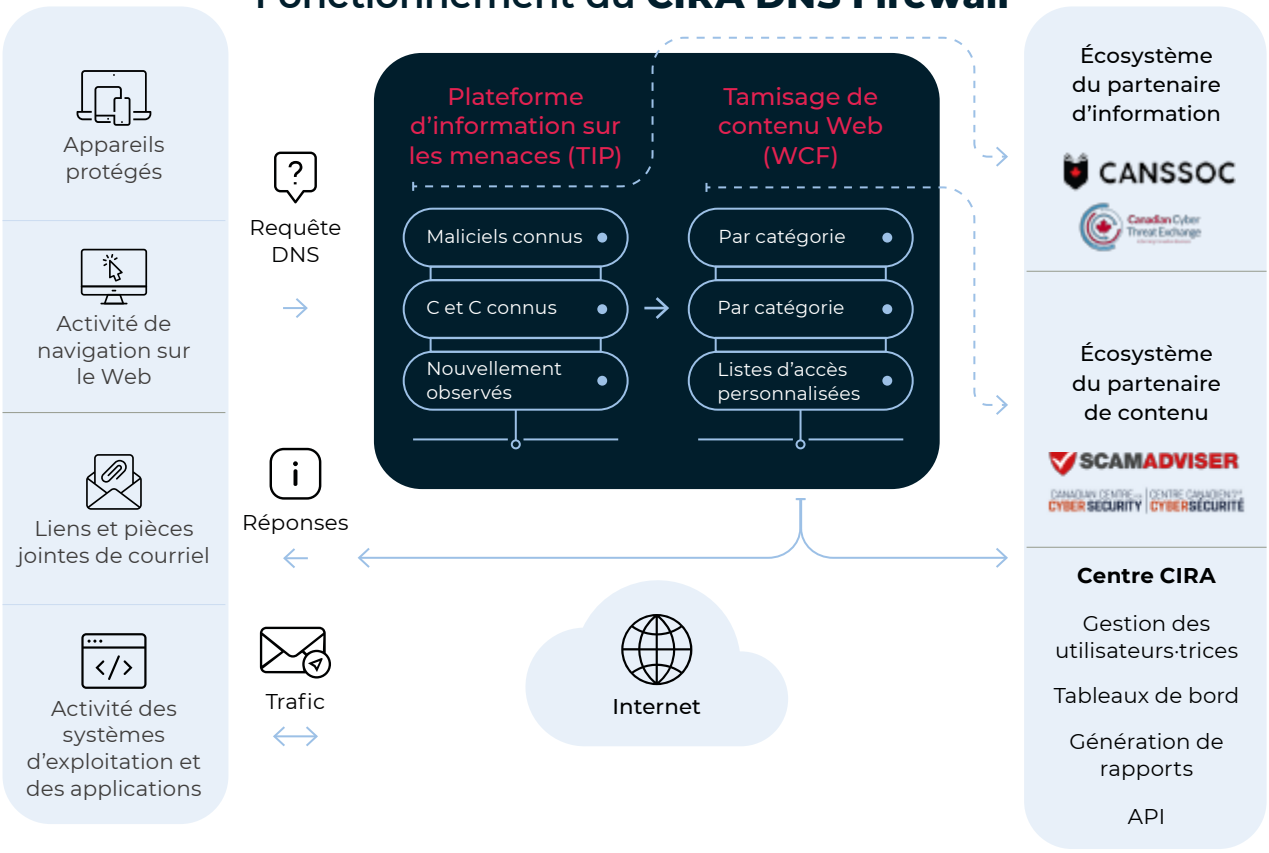
# Renforcez la sécurité de votre réseau et de vos points d'extrémité grâce à **la surveillance des menaces DNS**

Le CIRA DNS Firewall aide à protéger votre trafic réseau en bloquant les attaques d'hameçonnage émergentes et les menaces par maliciels lorsqu'elles surviennent. Les clients d'affaires peuvent également appliquer leur politique d'utilisation d'Internet de manière à s'assurer que les employés peuvent utiliser les ressources de la société en toute sécurité grâce au tamisage des contenus interdits et potentiellement malveillants.

CIRA.CA/FR/CYBERSECURITE/DNS-FIREWALL

**« Mais nous avons déjà un pare-feu. »** Les pare-feu ne se valent pas tous. Et, comme tous les Canadiens·ennes, vous comprenez sans doute l'importance de la superposition des couches de protection. S'il est vrai que les pare-feu de nouvelle génération ont recours à une technologie avancée pour améliorer la sécurité des réseaux et les capacités de prévention des menaces, certaines attaques DNS peuvent passer entre les mailles du filet et constituent alors une menace potentielle, pour les organisations, d'atteinte à la sécurité des données, d'infection par maliciel, d'attaque de réseau zombie et plus encore. En ajoutant le CIRA DNS Firewall à votre pile de sécurité, votre organisation obtient une couche de défense supplémentaire pour contrer efficacement les menaces DNS.

## Fonctionnement du **CIRA DNS Firewall**



## CIRA DNS Firewall en chiffres

**85 %**
des menaces détectées n'ont pas été découvertes par les autres solutions.

**4,1** millions
d'utilisateurs·rices canadiens·ennes protégés par le CIRA DNS Firewall.

**90 %**
de réduction des ordinateurs touchés par des attaques par hameçonnage.

**100 000**
nouveaux domaines malveillants bloqués chaque jour.

## *CE QU'EN DISENT* NOS UTILISATEURS·RICE·S

Il ajoute une couche supplémentaire de sécurité et de contrôle du contenu. La redondance à elle seule en vaut la peine, mais elle améliore aussi nos autres outils de sécurité. C'est très simple à configurer. Les politiques peuvent être larges ou granulaires, selon vos besoins. Il détecte les charges utiles des maliciels qui n'ont pas encore été détectées par d'autres fournisseurs.

J'adore les outils simples, efficaces et abordables. Le pare-feu DNS Firewall de CIRA répond à toutes ces exigences. »

**— JAYMON, DIRECTEUR DES TI**

**Pour en savoir plus, consultez la page cira.ca/fr/dns-firewall/** ou balayez le code QR pour réserver une rencontre gratuite sans obligation **avec l'un de nos experts en cybersécurité.**

## Fonctionnalités du pare-feu DNS Firewall de CIRA

**Protection contre l'hameçonnage** – de nouveaux domaines d'hameçonnage sont détectés et ajoutés à la liste des interceptions en temps réel ou presque.

**Désactivation des maliciels par la perturbation des commandes et des contrôle** – plus de 80 % des maliciels peuvent être freinés par un pare-feu DNS qui perturbe sa communication de commandes et de contrôles.

**Déploiement complet en quelques minutes seulement** – protection de tous les appareils et utilisateurs·trices sur les réseaux et prise en charge des adresses IP dynamiques.

**Sécurité automatisée** – Capacités CCS améliorées grâce à l'intégration SIEM/SOAR.

**Production d'un flux dynamique de menaces à partir des données DNS mondiales** – plus de 100 000 domaines malveillants sont ajoutés quotidiennement à la liste des menaces.

**Tamisage personnalisé des contenus Web** – application des politiques d'utilisation d'Internet grâce à des filtres de contenu Web faciles à configurer sur mesure au niveau individuel des URL.

**Intégration API** – facile à intégrer dans des tableaux de commande existants ou des solutions de gestion des informations et des événements de sécurité (SIEM) pour la gestion des politiques, des journaux, des alertes, etc.