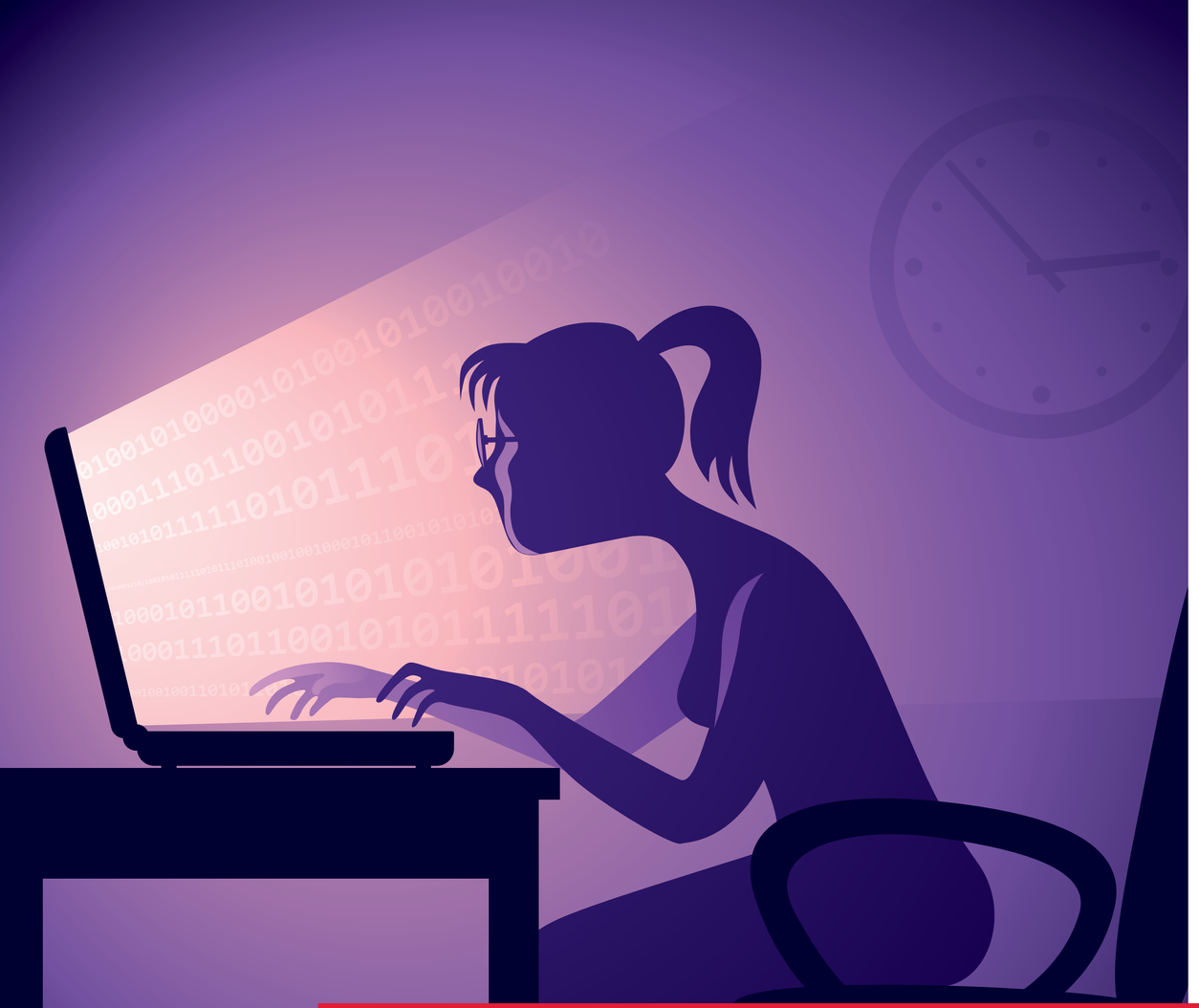
D-Zone DNS Firewall de l'ACEI dans le réseau IntraRISQ

La cybersécurité améliorée

Services de cybersécurité de l'ACEI



90 % des logiciels malveillants utilisent le DNS

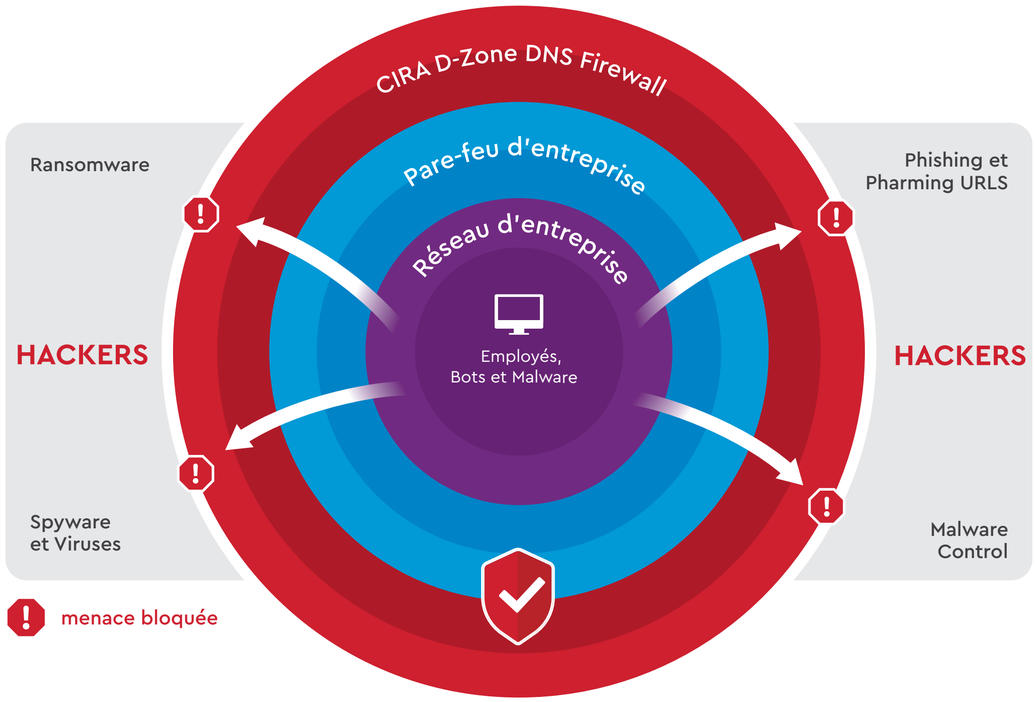
LE SPECTRE DES MENACES S'EST ÉLARGI

La protection traditionnelle des points terminaux et des pare-feu ne bloque pas tout. De plus, des couches supplémentaires rentables sont requises pour faire face à la multiplication des menaces.

La plupart des membres du RISQ exercent leurs activités dans des environnements ouverts qui présentent des profils de risque qui leur sont propres et qui en font des cibles bien en vue pour les rançongiciels et d'autres types de logiciels malveillants. De nombreux membres ont aussi besoin d'un filtrage de contenu adapté en fonction de l'âge. L'ACEI est heureuse d'offrir une solution de D-Zone DNS Firewall pensée pour les membres du RISQ.

L'ACEI OFFRE AUX MEMBRES DU RISQ LA POSSIBILITÉ D'UTILISER LA COUCHE DNS EN TANT QUE PROTECTION

Le D-Zone DNS Firewall empêche les utilisateurs et les robots de recherche de visiter des sites qui servent au hameçonnage ou qui contiennent des rançongiciels ou d'autres logiciels malveillants. Infonuagique, de grande valeur, facile à configurer, facile à gérer.



« En bloquant instantanément les nouvelles menaces ciblées, nous avons réduit de 90 % le nombre d'ordinateurs touchés. »

— *Trent University*

LA SÉCURITÉ INFONUAGIQUE DÉPLOYÉE EN QUELQUES MINUTES

Pour déployer un DNS firewall, les organisations n'ont qu'à relier leur DNS au service de l'ACEI, qui répondra ensuite aux requêtes. Les serveurs DNS de l'ACEI sont accessibles directement par le service IntraRISQ afin de permettre une optimisation de la livraison des différents contenus disponibles sur le réseau. Les services de TI ou de sécurité TI peuvent surveiller et gérer le blocage des menaces au moyen d'un tableau de bord simple à utiliser.

100 000 NOUVELLES MENACES BLOQUÉES CHAQUE JOUR GRÂCE À LA SCIENCE DES DONNÉES D'AKAMAI

Les couches fonctionnent seulement si elles offrent un moyen unique de bloquer efficacement les menaces. Le pare-feu DNS de l'ACEI est bâti avec la technologie de DNS récursif et le flux dynamique de cybermenaces à l'avant-garde d'Akamai.

Au cœur de toute solution de sécurité se trouvent les données et la science des données utilisées pour générer le flux de menaces. En combinant la science des données avancée avec la visibilité sur 3 % trafic DNS mondial et 30 % du trafic Internet mondial, le flux de menaces d'Akamai offre une couche de protection supplémentaire puissante.

Une protection sur laquelle vous pouvez compter

« La mise en œuvre de D-Zone s'est révélée très facile. En tant qu'équipe très sollicitée, il est possible de mettre en place le D-Zone DNS Firewall de l'ACEI en tant que couche de protection ne nécessitant que quelques minutes de configuration pour chaque réseau sécurisé. L'architecture facilite également la sécurisation accrue des sites distants et de tout réseau séparé, comme les réseaux WiFi publics. »

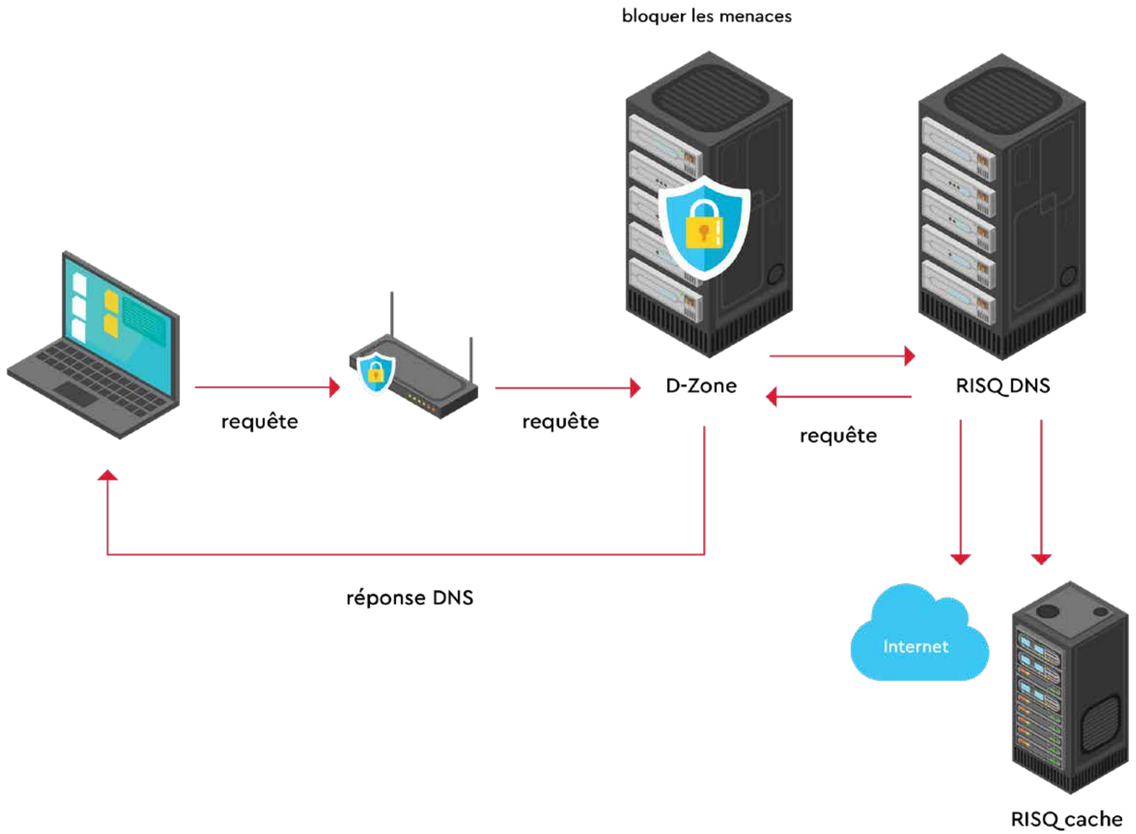
— *Commission scolaire de Rouyn-Noranda*

D-Zone DNS Firewall et IntraRISQ : une équipe gagnante!

Le service IntraRISQ offre toute la sécurité et la robustesse nécessaires pour satisfaire les besoins les plus exigeants des membres et partenaires du RISQ.

La collaboration ACEI/RISQ permet de rendre accessible le service D-Zone DNS Firewall directement via l'IntraRISQ. L'expérience client s'en trouve grandement améliorée et optimale.

. Aucune congestion pour les requêtes DNS
. Performance
. Faible latence
. Sécurité et robustesse élevées
. Solution canadienne
    . centre de données canadiens



Un Internet sécuritaire, un Internet plus rapide, un Internet plus rentable

Pour en apprendre davantage

Communiquez avec nous à **info@d-zone.ca**

Ou visitez **www.acei.ca/cybersécurité**