



Joël Mauroux, Responsable du groupe systèmes et réseau, Retraites Populaires

Visibilité et contrôle en temps réel de tous les éléments du réseau

Comment savoir en tout temps quels postes de travail sont connectés au réseau ? Sont-ils conformes aux règles de sécurité de l'entreprise ? Peut-on bloquer si nécessaire les postes illégitimes ? Si la structure du réseau est étendue ou si les visiteurs sont fréquents, ces questions peuvent présenter un défi majeur au département informatique. La société Retraites Populaires a trouvé une solution à ce problème.

Spécialiste de l'assurance vie, de la prévoyance et de la gestion d'importantes caisses de pension, Retraites Populaires est aussi active dans le domaine de l'immobilier, des prêts hypothécaires et de la gestion de fonds. La société, qui est profondément implantée dans le tissu économique vaudois, compte 350 utilisateurs répartis sur 2 sites et 16 étages. Il s'agit donc d'une structure IT importante, éparpillée, qui doit de plus compter avec la présence de nombreux visiteurs externes.

Joël Mauroux, Responsable du groupe systèmes et réseau explique : « Comme toutes les entreprises, nous avons commencé par nous protéger contre les menaces extérieures. Ensuite, nous avons étendu notre réflexion à la protection interne et nous avons remarqué par hasard qu'un consultant en visite se connectait depuis un certain temps à notre réseau avec sa machine personnelle sans que nous le sachions. »

« Nous souhaitons savoir qui est connecté à quoi, quand et de quelle façon.

En particulier, nous voulions contrôler les accès des consultants et des visiteurs à notre réseau limiter le niveau d'accès des machines professionnelles externes ou privées »

Cette constatation amène Retraites Populaires à vouloir instaurer une visibilité et un contrôle précis de tous les éléments du réseau. « Nous souhaitons savoir qui est connecté à quoi, quand et de quelle façon. En particulier, nous voulions contrôler les accès des consultants et des visiteurs à notre réseau depuis les salles de conférence et limiter le niveau d'accès des machines professionnelles externes ou privées. Et nous voulions pouvoir agir : mettre en quarantaine ou même bloquer un poste de travail en cas de menace perçue. »

CounterACT offre une visibilité complète des équipements, des applications, des utilisateurs actifs et notifie l'administrateur de tout phénomène anormal.



« CounterACT permet aussi de localiser l'emplacement physique des machines, ce qui est très utile sur un site étendu. »

CounterACT : contrôle d'accès complet au réseau

Pour répondre à ces spécifications, Navixia recommande à Retraites Populaires la solution CounterACT développée par la société américaine ForeScout. Il s'agit d'une plate-forme automatisée qui permet de voir et de contrôler l'intégralité du réseau en temps réel ou de manière ponctuelle. En pratique, CounterACT offre une visibilité complète des équipements, des applications et des utilisateurs actifs et notifie l'administrateur de tout phénomène anormal. Le traitement de ces notifications et la suite à leur donner peut être manuel ou automatique, au choix de l'administrateur. L'entreprise concède ainsi à ses visiteurs un accès contrôlé au réseau sans mettre en péril ses ressources critiques et ses données sensibles.

Retraites Populaires fait confiance à Navixia et procède au déploiement de la solution recommandée. Joël Mauroux décrit l'implantation: « *La phase préalable est assez simple, elle consiste à déterminer ce que l'on veut analyser et dans quelle partie du réseau. Ensuite, le boîtier CounterACT est mis en mode écoute pendant trois à quatre semaines et fait un inventaire de tout ce qu'il détecte. Au terme de cette période, les résultats sont analysés avec l'équipe technique et c'est à ce stade que l'on définit comment traiter les exceptions ou les cas particuliers.* »

Catégorisation et traitement des événements

Il s'agit ensuite de décider si une notification entraîne une action et laquelle. Retraites Populaires a déterminé deux manières de traiter les périphériques inconnus : leur mise en quarantaine, qui leur donne accès à internet exclusivement, et leur blocage pur et simple en cas de menace perçue.

Actuellement, Joël Mauroux et son équipe traitent encore les notifications manuellement car le réseau de Retraites Populaires est en transition : son parc de 350 ordinateurs va être intégralement renouvelé. Joël Mauroux : « *Il vaut mieux prendre son temps avant d'automatiser des actions qui bloquent l'utilisateur. Chez nous, le parc informatique actuel est assez hétéroclite. A cause de leur configuration, certains postes de travail sont détectés sur le réseau plus lentement que les autres. Ils pourraient donc potentiellement être pris pour des machines inconnues et mis en quarantaine. Cette situation bloquerait passablement d'utilisateurs légitimes. Pour contrer ce problème, il est possible d'installer un agent optionnel CounterACT sur chaque ordinateur ce qui les rend identifiables plus rapidement.* » Retraites Populaires profitera d'ailleurs du renouvellement de son parc informatique pour installer cet agent sur chaque poste de travail.

Dès cette migration achevée, Retraites Populaires automatisera le traitement des notifications. En effet, pour une entreprise qui accueille, comme elle, beaucoup d'intervenants externes, le traitement manuel des notifications nécessite une disponibilité de l'équipe IT. Mais celle-ci a trouvé une parade : « *Nous fournissons dans*

« Le produit est intéressant car il nous en apprend beaucoup sur notre réseau. Il nous a ainsi permis de détecter des pannes ou des machines au comportement bizarre qui auraient été difficilement repérables humainement. »



Autre utilité pratique : le suivi des mises à jour logicielles ou du statut de renouvellement d'un parc informatique.

certains départements une machine destinée aux invités et offrant des fonctionnalités limitées. Nous avons aussi introduit le wifi dans certaines zones où les visiteurs peuvent se connecter à internet. » Même ainsi, la visibilité globale des accès reste assurée, puisque CounterACT assure également le contrôle du réseau wireless.

Détection des pannes et suivi des mises à jour

En dehors du contrôle d'accès proprement dit, CounterACT offre d'autres fonctionnalités utiles au quotidien. *« Le produit est intéressant car il nous en apprend beaucoup sur notre réseau. Il nous a ainsi permis de détecter des pannes ou des machines au comportement bizarre qui auraient été difficilement repérables humainement. Nous avons même eu la surprise de découvrir quelques ordinateurs privés... »* Avantage supplémentaire : *« CounterACT permet aussi de localiser l'emplacement physique des machines, ce qui est très utile sur un site étendu. »*

Autre utilité pratique : le suivi des mises à jour logicielles. Joël Mauroux et son équipe ont détecté une faille dans la procédure de mise à jour de leur antivirus. CounterACT a pu y remédier : *« Lors des mises à jour, le serveur antivirus considère comme acquis que la procédure s'est bien déroulée sur tous les postes. CounterACT nous a permis de découvrir que ce n'était pas le cas: certaines machines n'avaient jamais été actualisées. Désormais, nous procédons une fois par mois à un contrôle manuel en comparant le rapport de l'antivirus avec celui de CounterACT. Le cas échéant, nous réinstallons l'antivirus manuellement là où il le faut. »*

Connaître en tout temps le statut des éléments du réseau a encore une autre utilité. Retraites Populaires pourra s'en servir pour contrôler le statut du renouvellement de son parc informatique : *« Lorsque nous aurons finalisé notre migration, CounterACT nous permettra de savoir combien il reste de postes tournant sous Windows XP, combien de versions de MS Office antérieures à 2010 sont encore en circulation et à quel emplacement physique. Il suffit pour cela de lancer un inventaire du réseau, qui ne dure que quelques minutes. »*

Recommandations et bilan

Quelles recommandations Joël Mauroux peut-il faire aux futurs acquéreurs du système ? *« Je leur conseille de procéder à une pré-analyse précise des besoins internes avant de se lancer. CounterACT a beaucoup de souplesse et répond à toutes les demandes. Mais il est important de gérer l'implémentation du produit comme un projet d'entreprise prioritaire, de manière structurée, avec une date de début et de fin - et surtout en prévoyant assez de temps. CounterACT est super, mais on se fait vite prendre de vitesse si beaucoup de projets sont en cours en parallèle. »*

Retraites Populaires a désormais un contrôle efficace de son réseau et le bilan de Joël Mauroux est positif : *« Nous sommes très satisfaits du produit, qui nous rend beaucoup de services dans notre travail de tous les jours. Dans le futur, je me*

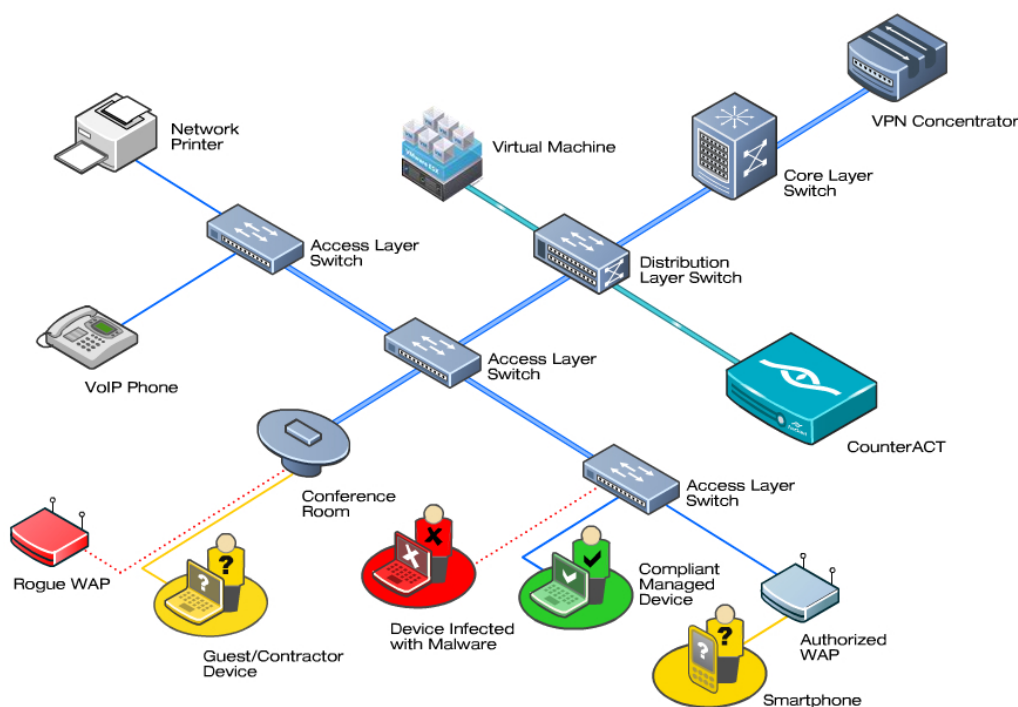
« Nous sommes très satisfaits du produit, qui nous rend beaucoup de services dans notre travail de tous les jours. »

réjouis de pouvoir automatiser au maximum la procédure de traitement des notifications. CounterACT est un produit très puissant qui a de grandes possibilités. Il convient autant à une petite société qu'à un large déploiement sur plusieurs sites. Et il a très bien évolué pendant l'année écoulée : ForeScout a corrigé certaines lenteurs et le moteur est extrêmement fluide. On peut l'utiliser de manière simple pour notifier, détecter ou retrouver des machines. Ou d'une manière plus complexe en exploitant toutes les ressources du produit, et alors il n'y a pas de limites aux finesses d'utilisation possibles. »

La solution de gestion et contrôle d'accès au réseau CounterACT est intéressante pour toute entreprise qui souhaite détecter et contrôler en temps réel les connexions au réseau et vérifier leur conformité avec les règles en vigueur.

Exemple d'architecture

« CounterACT est un produit très puissant qui a de grandes possibilités. Il convient autant à une petite société qu'à un large déploiement sur plusieurs sites. »



Navixia SA
 Route du Bois 1
 CH - 1024 Ecublens
 Tél.:
 + 41 (0)21 324 32 00
 Fax:
 + 41 (0)21 324 32 01
 E-mail:
 info@navixia.com
 Web:
 www.navixia.com

ForeScout CounterACT est facile à installer et maintenir car il ne requiert ni software, ni agents, ni mises à jour hardware ou reconfigurations. Tout est intégré dans un seul boîtier, physique ou virtuel.

- Intégration facile à la structure existante car supporte les solutions matérielles et logicielles d'un grand nombre de fabricants.
- Supporte 802.1x, LDAP, RADIUS, Active Directory, Oracle et Sun.
- Gestion et surveillance facilitées avec les outils de reporting et d'inventaire intégrés