Février 2017

# Transformer la sécurité des terminaux : Pour dépasser largement la seule détection des attaques

*Fermer la boucle de la sécurité en intégrant la prévention, la détection, l'investigation et la réponse*

IBM

## Introduction

Comme les cyber-attaques semblent réussir à chaque tentative, les terminaux restent leur vecteur le plus vulnérable et préféré, offrant aux cybercriminels le plus faible des points de résistance. La sécurisation des terminaux nécessite une approche multifacette et continue, afin de réduire proactivement leur surface exposée aux attaques, contenir et résoudre réactivement les attaques détectées.

L'industrie de la sécurité a réagi en fournissant des solutions conçues pour détecter et contrer les malware et les comportements malveillants. Cependant, indépendamment de l'efficacité de ces outils, de tels efforts présentent plusieurs faiblesses cruciales. Les approches principalement centrées sur la détection ne traitent normalement qu'une partie du vaste problème auquel toute entreprise est confrontée. Une sécurité approfondie nécessite non seulement une détection efficace des menaces, mais aussi des efforts qui vont plus loin que la seule détection pour évaluer et assimiler la situation complète de la sécurité de l'entreprise. Sur cette base, il devient possible d'agir efficacement pour éliminer les conséquences des attaques et prévenir leur retour à l'échelle de toute l'organisation.

## Le mythe zéro-jour

Alors que de nombreuses entreprises se concentrent sur la préparation d'une attaque zéro-jour, pas une seule attaque zéro-jour n'a été impliquée dans une violation de sécurité de haut niveau pendant les 24 mois antérieurs à septembre 2016, d'après un récent rapport de la National Security Administration (NSA).[1] Comme Curtis Dukes, directeur assistant national des systèmes de sécurité à la NSA, l'a expliqué : « dans chacun de ces incidents nous sommes confrontés au problème fondamental du manque de cyber-hygiène ».[1]

La plupart des incidents sont en réalité provoqués par des techniques d'attaque relativement simples, telles que le harponnage, l'attaque de point d'eau et l'attaque par clé USB. Elles exploitent des vulnérabilités connues, qui persistent souvent parce l'application des corrections n'est pas systématique, ou la gestion et le contrôle des terminaux manquent de rigueur. Pourquoi les attaques zéro-jour sont-elles aussi rarement employées ? Elles sont très difficiles à développer et par conséquent relativement coûteuses à utiliser, en particulier parce que la fenêtre d'opportunité d'un exploit zéro-jour est brève. En outre, lorsqu'elles ont été découvertes, elles ne peuvent plus être utilisées sans modification.

## Lorsque les solutions conventionnelles échouent

### Manque de visibilité

Visibilité incomplète sur le statut des terminaux générant un contexte insuffisant pour une détection efficace

### Complexité des investigations

Des compétences et des données limitées empêchent des investigations et des prises de décision précises.

### Résolution inefficace

La disparité des équipes et des outils réduit votre aptitude à protéger et à réagir avec efficacité

Lorsque des solutions échouent, les entreprises laissent la porte ouverte aux attaques, ne détectent pas les attaques dans le contexte et ne peuvent pas apporter de réponse appropriée.

En d'autres termes, si d'autres méthodes plus faciles fonctionnent, les criminels préfèreront les utiliser. Il incombe donc aux services de sécurité informatique des entreprises de bloquer ces méthodes plus faciles, forçant les criminels à utiliser des attaques zéro-jour. Cela implique évidemment que la sécurité mise en place soit prête à détecter et contrer de telles attaques.

## Les défis de la sécurité des terminaux

Peu d'entreprises ont le budget, le personnel et l'expertise nécessaires pour protéger en permanence chaque mètre carré de leur organisation, incluant chaque terminal, alors que telle est exactement la mission de leurs équipes de sécurité. Dans un processus dont l'objectif semble impossible à atteindre, de nombreuses entreprises, dont l'approche est uniquement basée sur la sécurité, sont confrontées à des challenges importants :

- **Visibilité insuffisante :** Des solutions généralement focalisées sur la détection et le confinement manquent souvent d'informations contextuelles sur l'état réel des terminaux qu'elles protègent. Elles n'ont qu'une visibilité limitée sur la configuration des terminaux, sur le logiciel installé et son utilisation. Même les entreprises ayant une bonne visibilité sur les terminaux grâce à d'autres outils peuvent être submergées par les données obtenues. Elles ne sont pas en mesure de faire les corrélations nécessaires entre leurs données et les activités suspectes pour créer une base indispensable à toute investigation, sans laquelle aucun plan de contre-mesure ne peut être développé.
- **Complexité des investigations :** Comme la détection est seulement le début du processus de résolution, il est indispensable de développer un historique aussi détaillé que possible couvrant l'environnement et les activités qui s'y déroulent. Ensuite, l'investigation doit déterminer la véracité et l'envergure de l'attaque en posant diverses questions, telles que : Cette activité est-elle une attaque réelle ? Quelle est sa cause fondamentale ? Combien de dispositifs sont concernés ? Combien de dispositifs pourraient être concernés ? En fonction des réponses apportées par l'investigation, il sera possible de déterminer les étapes requises pour contenir et résoudre le problème. Avec une équipe de sécurité souvent réduite et surchargée, une visibilité limitée sur l'environnement, et pas assez de temps pour assimiler toutes les données descriptives de la menace, les entreprises ont des difficultés considérables pour arriver à des conclusions appropriées.
- **Résolution inefficace :** Comme les équipes de sécurité et leurs outils ont progressé organiquement, leurs méthodes ne se sont pas forcément développé de manière complémentaire. À tel point que ce développement a souvent créé des silos d'équipes et d'outils. En ajoutant de nouveaux rôles et de nouveaux outils pour répondre à des besoins spécifiques émergents, les entreprises peuvent se voir obligées de payer l'installation, la configuration, la gestion, les corrections et les mises à jour de douzaines de solutions non-intégrées fournissant des vues limitées de leur environnement. Un client IBM utilisait 85 outils de sécurité différents conçus par 45 fournisseurs différents. Non seulement ces infrastructures en patchwork sont coûteuses, mais elles renforcent aussi le niveau de difficulté des investigations et des conclusions déjà complexes. Chaque outil du patchwork apporte seulement une fine vue en coupe de la situation générale.

  Comme l'a conclu la NSA, le manque de cyber-hygiène, et non pas les attaques zéro-jour si craintes, étaient la cause principale de toutes les attaques de haut niveau examinées pendant les deux années couvertes par l'étude. Dans de nombreux cas, l'entreprise avait laissé les portes et les fenêtres ouvertes, n'ayant pas appliqué des correctifs à des vulnérabilités connues, par exemple, invitant ainsi des criminels à choisir la plus simple des méthodes d'intrusion. Une fois à l'intérieur d'un réseau, les responsables de l'attaque sont libres d'y travailler pendant des mois. En fait, des attaques mal intentionnées ou criminelles sont restées indétectées pendant 229 jours.[2]

  Une récente étude sur les violations de données a révélé que plus de 99,9 % des vulnérabilités exploitées l'avaient été plus d'un an après la publication du dictionnaire des vulnérabilités de sécurité (Common Vulnerability and Exposure – CVE). [3] Avec des outils hétérogènes, il est difficile de renforcer proactivement des terminaux contre des menaces potentielles, ou d'analyser tout l'espace informatique de l'entreprise à la recherche de malware dormants. Ce travail exige une hygiène rigoureuse des terminaux, incluant une surveillance des activités, une gestion des configurations et des correctifs, une application stricte des contrôles de sécurité et une détection avancée des malware.

Tous ces challenges aboutissent à une stratégie de défense fragmentée, qui ne permet pas de bénéficier de la visibilité et de la coordination requises pour prévenir, détecter et contrer efficacement les attaques actuelles.

## Une nouvelle approche de la sécurité des terminaux

Alors que les entreprises dépendent de plus en plus des services informatiques pour générer de la valeur commerciale, les menaces sur les infrastructures informatiques continuent de se multiplier. En fait, 387 nouvelles menaces dans la catégorie des malware sont identifiées chaque minute.[4] Pour rester à la hauteur de ces attaques, une nouvelle approche de la sécurité des terminaux est nécessaire : une solution adaptative intégrée qui ferme la boucle de la sécurité des terminaux avec une combinaison de meilleures pratiques et de solutions fonctionnelles.

Une approche efficace de la sécurité des terminaux doit apporter une visibilité claire de l'infrastructure et des activités, une compréhension complète des attaques et des contre-mesures nécessaires, des actions précisément définies pour contenir et résoudre les attaques. Elle permet à l'entreprise de :

- Corriger et résoudre en continu les vulnérabilités qui peuvent être utilisées pour créer une tête de pont dans votre environnement, et réduire votre surface d'exposition aux attaques.
- Analyser et enregistrer en continu les activités sur les terminaux pour faciliter la détection des événements liés à tout type d'attaque (incluant l'exploitation de vulnérabilités connues, les attaques zéro-jour ou les intrusions non associées à un malware).
- Réduire la durée de détection d'une violation et la durée de séjour d'un processus d'attaque dans l'infrastructure après un accès réussi.
- Renforcer l'efficacité des outils de détection basés sur des définitions, en combinaison avec des systèmes d'analyse des comportements, et des méthodes heuristiques, pour établir des corrélations entre plusieurs événements révélateurs d'un comportement suspect.
- Employer un agent en mode kernel pour bénéficier d'une visibilité complète sur les activités des terminaux, au lieu d'un agent en mode utilisateur susceptible d'ignorer un malware plus sophistiqué et furtif.
- Supporter des fonctions d'investigation et de contre-mesures intelligentes, avec des outils d'évaluation de l'envergure des attaques, pour définir leur niveau de priorité, et fournir une capacité de résolution immédiate.
- Améliorer et automatiser les efforts de conformité en organisant l'application continue de politiques de sécurité sur les terminaux. Contrôler directement une gamme étendue de normes et de réglementations industrielles, pour faciliter la préparation d'audit, dans un environnement de sécurité globale.
- Fournir une visibilité complète et continue sur tous les terminaux susceptibles d'être partagés par plusieurs équipes, et faciliter la collaboration entre les opérations du service informatique et les opérations de sécurité.
- Supporter des déploiements rapides et fournir une valeur tangible après des heures ou des jours de travail, au lieu de semaines et de mois d'efforts.

## Protection intelligente des terminaux

IBM® BigFix représente une nouvelle catégorie de protection intelligente des terminaux, permettant d'appliquer une stratégie de sécurité complète, qui met en œuvre des mesures de sécurité proactives et des contre-mesures directes sur la même plateforme.

L'addition du module IBM BigFix Detect est une réponse adaptée à la réalité actuelle des menaces, où des intrus peuvent pénétrer dans n'importe quel environnement informatique, en déclenchant une attaque grâce à la participation d'une personne malintentionnée extérieure à l'entreprise ou à l'erreur innocente d'un utilisateur autorisé. Outre les capacités proactives prouvées de la plateforme BigFix, et sa visibilité sur les activités et les configurations des terminaux, qui permettent de gérer les préparations préalables à des attaques, BigFix Detect apporte des fonctions de réactivité, avec une capacité de résolution adaptée aux attaques et aux malware.

BigFix Detect apporte trois fonctions essentielles conçues pour fermer la boucle de la sécurité des terminaux : La protection continue, la détection intelligente et la réponse assistée se combinent avec une visibilité en temps réel sur les activités des terminaux et le statut de la sécurité, permettant à l'entreprise de comprendre clairement et complètement la situation, afin d'agir avec précision et contrer efficacement les menaces.

### Protection continue

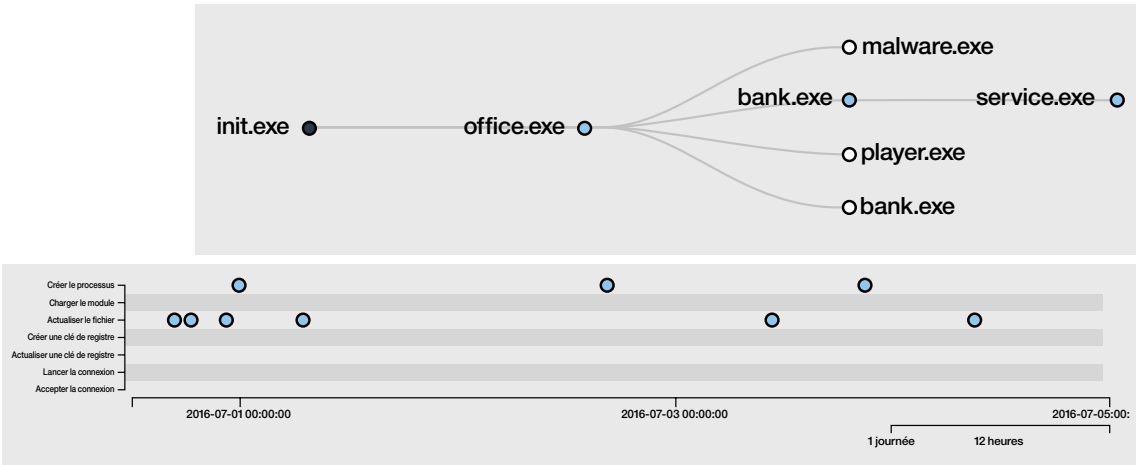
La protection continue permet aux entreprises d'esquiver les menaces connues et émergentes. La protection continue, qui commence par la détection des anomalies, est l'équivalent de la fermeture des portes et des fenêtres. Elle force les cybercriminels à travailler davantage pour pénétrer, incluant des attaques zéro-jour plus complexes et plus onéreuses. La protection continue permet aux entreprises de :

- Superviser en continu les contrôles de sécurité.
- Maintenir des lignes de base normalisées et pertinentes en termes de sécurité, de conformité, de configuration et d'application des correctifs.
- Déployer des mises à jour d'applications du système d'exploitation prévérifiées, dans des délais courts en minutes ou en heures, au lieu de jours et semaines.
- Déployer, contrôler et appliquer des agents de sécurité tiers.
- Faciliter la collaboration pour renforcer la gestion des correctifs et des configurations entre les services informatiques et les opérations de la sécurité.

### Détection intelligente

La détection intelligente emploie un agent en mode kernel qui permet de collecter les données de toutes les activités sur les terminaux critiques, contrairement aux agents en mode utilisateur moins efficaces. Elle applique ensuite des analyses de comportements et d'informations sur les menaces, à la place des méthodes de détection de malware inefficaces basées sur des définitions. La détection intelligente exploite les informations collectées sur des millions de terminaux actifs sur la plateforme BigFix afin de corréler les événements, identifier les comportements malintentionnés, analyser les causes fondamentales et accélérer la résolution.

## Détection intelligente




La détection intelligente assure la corrélation des événements, identifie les comportements malveillants, analyse les causes fondamentales, pour accélérer les résolutions.

### Réponse assistée

La réponse assistée et contextuelle d'un outil d'assistance logiciel prouvé permet de démarrer efficacement des investigations basées sur les activités détectées. Elles incluent la définition de la véracité, de l'exposition et de l'envergure de chaque incident, pour fournir des suggestions de résolution. La réponse assistée exploite une énorme bibliothèque de systèmes d'exploitation multifournisseur prévalidés et des packages d'installation de contenus applicatifs, pour générer des options de résolution pertinentes en quelques minutes, soit pour un terminal spécifique, un groupe de terminaux, ou la totalité de l'environnement.

La réponse assistée supporte des résolutions rapides en créant des messages IBM Fixlet, les messages BigFix qui donnent des instructions aux agents pour exécuter des actions spécifiques. Les messages Fixlet peuvent être déployés immédiatement dès que la contre-mesure appropriée est définie. Ces actions incluent des correctifs, des reconfigurations, des mises en quarantaine des terminaux concernés, ou même la réinitialisation à distance de leur image.

### Visibilité en temps réel

La plateforme BigFix apporte une visibilité continue en temps réel pendant tout le cycle de sécurité des terminaux. Elle supporte la découverte et l'audit de tous les terminaux, collecte un inventaire de toutes les utilisations et licences. Elle évalue en continu les configurations, la sécurité, la conformité et la situation des correctifs.

Des milliers d'attributs sont collectés en continu sur les terminaux et envoyés à un seul serveur de gestion par un seul agent polyvalent. L'agent peut être utilisé pour tous les types de terminaux, depuis les PC, les serveurs, jusqu'aux distributeurs de billets, et dispositifs de vente, incluant les unités sous Microsoft Windows, Microsoft Windows Mobile, UNIX, différentes distributions de Linux et Apple Mac OS, que ces terminaux soient physiques ou virtuels, fixes ou mobiles. L'agent utilise une quantité de mémoire minimale, calcule les ressources et la bande passante.

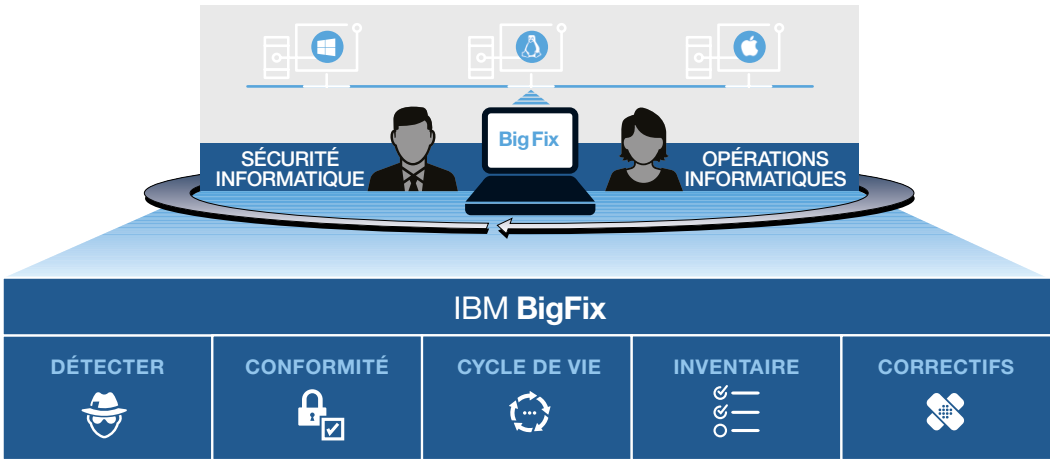
Même si la solution fournit une configuration étendue et des rapports de conformité, un outil ad-hoc permet aux administrateurs d'interroger les terminaux et d'extraire des résultats précis en quelques secondes.

## Une plateforme collaborative de gestion et de sécurité des terminaux

Dans une industrie habituée à des solutions locales trop diversifiées et à des technologies fragmentées, BigFix apporte une alternative incontournable : une plateforme basée sur une seule console et un seul agent, qui prend en charge les opérations, la sécurité et la conformité en temps réel et à une échelle globale. Un serveur BigFix peut supporter plus de 200 000 terminaux, permettant aux entreprises d'exploiter au mieux leurs investissements dans la gestion des systèmes et la sécurité.

La plateforme BigFix combine plusieurs composants intégrés :

- **IBM BigFix Detect :** Détection, investigation contextuelle et résolution focalisée avec précision sur des menaces actives grâce au plus récent module de la plateforme BigFix.
- **IBM BigFix Compliance :** Conformité continue aux politiques réglementaires, opérationnelles et de sécurité.
- **IBM BigFix Lifecycle :** Distribution, fourniture et application des correctifs logiciels, et contrôle à distance des terminaux.
- **IBM BigFix Inventory :** Visibilité sur les logiciels installés et leurs utilisations, contribuant à réduire les coûts et à améliorer la conformité.
- **IBM BigFix Patch :** Fonctions pour compresser les cycles de correction en minutes ou heures, au lieu de jours ou semaines, avec un taux de réussite à la première tentative supérieur à 98 %.




BigFix combine sur une seule plateforme des fonctions de sécurité complètes pour les terminaux.

## Pourquoi IBM ?

Dans le monde de la sécurité informatique en évolution constante , il peut être difficile d'avoir la certitude que votre entreprise applique toutes les mesures nécessaires pour prévenir, détecter et résoudre les menaces avec efficacité et rapidité. Pour aider les entreprises à atteindre un tel niveau, IBM BigFix fournit une plateforme intégrée qui combine une sécurité proactive des terminaux avec des mécanismes de détection intelligente et des réponses assistées et contextuelles.

Cette collection complète de capacités permet aux entreprises d'améliorer leur situation sécuritaire à chaque étape du cycle de protection des terminaux. Elles peuvent alors changer les résultats potentiels, pendant et après chaque attaque :

- **Préparation, au lieu d'infiltration :** Un solide programme de sécurité fondamental permet à l'entreprise de se mettre dans la meilleure position possible en cas d'attaque, et de la préserver en continu.
- **Prévention, au lieu d'exploitation :** Une gestion des terminaux en continu et prioritisée peut prévenir la majorité des attaques qui exploitent des vulnérabilités pour assurer leur pénétration.
- **Détection, au lieu d'expansion :** La collecte complète des activités sur les terminaux et leur corrélation accélèrent la détection pour empêcher les attaquants de naviguer latéralement sur le réseau et d'exploiter d'autres vulnérabilités après leur pénétration.
- **Analyse, au lieu d'exfiltration des données :** Les analyses et les réponses contextuelles peuvent servir à générer un Fixlet de résolution ou pour signaler aux administrateurs des activités malintentionnées avant l'exfiltration des données.
- **Contre-mesures, au lieu d'une attaque exécutée :** Les administrateurs peuvent évaluer et exécuter plusieurs options de résolution immédiates.

## Pour plus d'informations

Pour en savoir plus sur IBM BigFix, visitez **ibm.com**/security/bigfix pour regarder une vidéo de la démonstration du produit en action, ou contactez votre représentant IBM ou un partenaire commercial IBM pour organiser une validation de concept dans votre environnement.

[1] Chris Bing, NSA : aucune technique zéro-jour n'a été utilisée dans les violations de haut niveau au cours des 24 derniers mois, *FedScoop*, 15 septembre 2016. http://fedscoop.com/nsa-no-zero-days-were-used-in-any-high-profile-breaches-over-last-24-months

[2] Étude sur le coût des failles de sécurité 2016 : Analyse globale, *Ponemon Institute LLC*, Juin 2016. http://www-03.ibm.com/security/data-breach/

[3] 2015 Data Breach Investigations Report, *Verizon Enterprise Solutions*, 2015. http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report_2015_en_xg.pdf

[4] McAfee Labs Threat Report, *McAfee Labs*, Février 2015. http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2014.pdf

**Compagnie IBM France**
17 avenue de l'Europe
92275 Bois-Colombes Cedex
France

La page d'accueil d'IBM se trouve sur **ibm.com**/fr



WGW03269-FRFR-00