# G DATA WhitePaper

## La sécurité multi-couche

G DATA Software AG | Juillet 2017

# Table des matières

# Introduction

Pour lutter efficacement contre les menaces qui ciblent les processus opérationnels des entreprises, une solution de sécurité qui en englobe tous les aspects doit être mise en place. La sécurité dite « multi-couche » combine la protection antivirus traditionnelle à de nouveaux mécanismes de détection et de monitoring.  Ce document évoque différents types de risques ciblant les entreprises et présente les couches de protection pour y faire face.

# 1. Classification du risque

La mission de l'administrateur IT est de garantir la productivité à travers les outils digitaux mis à disposition des employés. Dans ce contexte, un logiciel de sécurité est un moyen, mais n'est pas une fin en soi. L'administrateur doit connaître les risques de son infrastructure et installer les solutions correspondantes pour la défendre.
Pour avoir une vue d'ensemble sur les menaces pouvant impacter les opérations digitales, il est recommandé de procéder à une classification des différents types de risque. Selon la taille de l'entreprise et de l'infrastructure, la gestion du risque doit être formalisée par un cadre standard tel qu'ISO 2700x, PCI DSS ou Common Criteria. Ces normes et directives ne doivent pas remplacer une stratégie personnalisée et exhaustive de gestion du risque : elles sont des aides non négligeables afin de définir le cadre d'un concept de sécurité adapté.

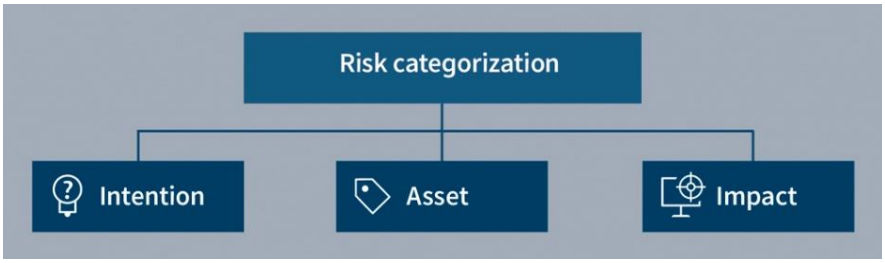


*Figure 1 : Classification du risque*

Trois catégories sont à prendre en compte dans un plan de gestion des risques : l'intention, l'actif (asset) et l'impact.
Les incidents qui affectent une entreprise ne sont pas tout le temps le résultat d'une action délibérée, planifiée par un adversaire. Classifier les risques en prenant en compte le facteur intentionnel a l'avantage de mettre l'attention sur les menaces visant l'infrastructure IT, un domaine qui est généralement sous-estimé. Les éléments climatiques sont par exemple des facteurs à prendre compte : un orage ou des pluies excessives peuvent causer des dommages immenses à une infrastructure informatique, sans raison délibérée. Il y a une pléthore d'autres risques qui peuvent – sans intention de nuire – avoir un impact important sur les procédures quotidiennes, comme des bugs dans les composants tiers, des erreurs de configurations ou la suppression accidentelle de données.

Analyser les risques en prenant en compte les actifs est une autre possibilité. Pour tout processus digital en entreprise, il y a au minimum un actif concerné parmi le matériel, le logiciel, les données

ou le personnel. Pour chaque catégorie citée, des sous-catégories peuvent être créées et chacune représente des risques. Pour le matériel, les risques sont par exemple l'accessibilité, la protection contre le mauvais usage et la performance, tandis que les risques se rapportant aux données doivent être analysés selon les critères de sauvegarde, protection et d'accès non autorisés.

Dans ce processus de catégorisation, mesurer les impacts potentiels est une démarche difficile. Cet exercice est toutefois nécessaire : le risque avec l'impact le plus important doit être traité avec la plus haute priorité. L'impact peut être exprimé en termes de temps, de coût et de perte de confiance. Des incidents qui causent une panne d'infrastructure coûtent du temps, une perte de productivité et influencent négativement les finances. Pour les entreprises tournées vers le digital comme le e-commerce, les pannes d'infrastructure ont des conséquences encore plus importantes.

# 2. Modèle de sécurité multi-couche

Face à des risques multiples, les logiciels de sécurité ont dû évoluer. Pour garantir la productivité des employés et la disponibilité de l'infrastructure, les solutions doivent contenir différents modules coopérants qui constituent une sécurité dite « multi-couche ».

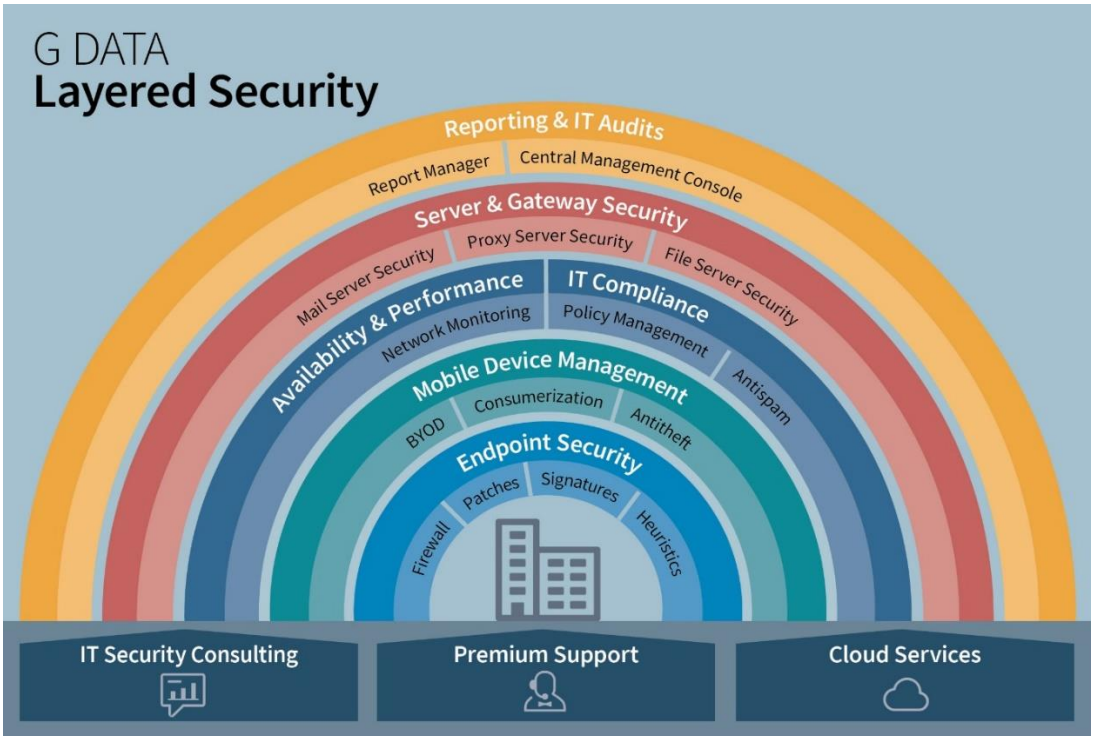


*Figure 2: Modèle de sécurité multi-couche*

## 2.1. Sécurisation des terminaux

La protection efficace d'un endpoint (terminal) repose sur plusieurs composants.

### 2.1.1. Pare-feu

Le pare-feu bloque le trafic non autorisé lors d'une phase précoce. Au niveau du réseau, les paquets de données envoyés depuis Internet vers le terminal sont autorisés ou bloqués selon des règles de sécurité définies. Le pare-feu contrôle également le trafic au niveau des applications. Cela permet un contrôle plus fin en autorisant des mesures de sécurité spécifiques même quand l'appareil est utilisé en dehors du réseau de l'entreprise. Quand un ordinateur portable est utilisé sur un réseau tiers, alors le client pare-feu garantit que le niveau de sécurité reste identique au réseau de l'entreprise.

### 2.1.2. Correctifs

Des failles de sécurité sont découvertes régulièrement dans les systèmes d'exploitation et les programmes. Leur dangerosité s'étend de la possibilité d'attaque par déni de service à l'accès à distance ou encore à l'exécution de code à distance. Les éditeurs publient des correctifs régulièrement, mais durant le laps de temps entre la découverte de la faille et le déploiement du correctif, un malware est souvent prêt à exploiter cette faille. Aussitôt que le correctif est publié, le composant affecté doit être mis à jour le plus rapidement possible. Mais dans une entreprise le nombre important de correctifs à gérer rend cette tâche complexe. C'est pourquoi l'utilisation d'une solution de gestion centralisée de correctifs est conseillée.

### 2.1.3. Signatures

La détection basée sur les signatures est une des plus anciennes méthodes pour trouver des virus. Le malware est détecté en comparant les fichiers avec des signatures de malwares connus, en utilisant une méthode statistique. Quand les informations correspondent, le fichier est considéré comme malveillant, est bloqué, nettoyé ou supprimé. La détection basée sur les signatures offre une détection très performante d'une grande quantité de malware connus et ainsi forme une partie cruciale de la conception d'une sécurité multi-couche.

### 2.1.4. Heuristique

Tandis que la détection basée sur les signatures a besoin de signatures pour créer des échantillons de malware déjà connus, les méthodes heuristiques sont basées sur les caractéristiques générales de fichiers malveillants. Par exemple, même si un virus est très récent et ne fait pas l'objet de signature à ce moment, la détection heuristique peut le détecter comme malveillant en se basant sur son en-tête de fichier ou d'autres parties de son code. La méthode heuristique garantit que les virus soient détectés avant leur exécution, même si aucune signature spécifique n'est disponible.

Comme la méthode heuristique, les technologies basées sur le comportement bloquent des malwares sans signatures prédéfinies. Mais, contrairement à l'heuristique, ils se basent sur les actions du malware et non sur son code. Les malwares agissent selon des modèles déterminés. Par exemple, pour garantir la persistance, certains ajoutent des entrées au registre ou se copient dans des locations spécifiques. D'autres téléchargent une charge malveillante depuis un serveur ou manipulent des espaces en mémoire. Les technologies basées sur le comportement identifient ces comportements et arrêtent l'attaque avant qu'elle ne s'exécute. Elles permettent ainsi de détecter des menaces encore inconnues.

## 2.2. La gestion des appareils mobiles

Depuis que les smartphones et les tablettes ont conquis les consommateurs, le paysage des technologies est devenu plus complexe. Les tendances telles que la consumérisation de l'IT et le phénomène BYOD (Bring Your Own Device) ont fait apparaître une multitude d'appareils dans les entreprises. Les administrateurs ont la tâche de fournir un accès large aux ressources tout en garantissant la sécurité. La gestion des appareils mobiles intègre cette hétérogénéité aux procédures administratives. Les composants typiques incluent une protection anti-malware, la détection antivol et les directives d'utilisation des appareils.

## 2.3. Disponibilité & performance

L'infrastructure informatique doit être sécurisée, mais ce n'est pas le seul facteur à prendre en compte. Sa disponibilité doit également être garantie. La perte de performance et les coupures influencent directement le fonctionnement de l'entreprise. En interne, les employés ont besoin d'une infrastructure disponible dès qu'ils en ont besoin pour éviter la perte de productivité. En externe, les partenaires ont besoin de systèmes de communication et de connexions inter-système fiables. Les clients doivent bénéficier de boutiques en ligne accessibles et réactives. Pour s'assurer de la disponibilité et des performances de l'infrastructure, une solution de sécurité multi-couche englobe des composants de surveillance adaptés.

## 2.4. Conformité IT

Envoyer des emails, naviguer sur Internet, utiliser des programmes, etc. sont les tâches quotidiennes d'un employé. Mais sans contrôle, un usage abusif des services informatiques peut impacter sa productivité. Réglementer l'utilisation d'Internet peut donc se révéler utile, tout comme le filtrage des spams, à des fins de productivité et de sécurité.
S'assurer de la confidentialité des informations est une autre nécessité. L'utilisation de clés USB doit être limitée à des services où aucune information confidentielle n'est traitée. De même, l'utilisation de programmes a besoin d'être régulée pour empêcher que des fichiers confidentiels ne soient distribués par email, messagerie instantanée ou autre. Les données peuvent se perdre également sans intention malveillante. Une panne de disque dur ou une suppression accidentelle de fichiers peut affecter sévèrement la continuité des affaires. Particulièrement pour les

entreprises sujettes à la législation sur la confidentialité des données comme la RGPD ou des cadres stratégiques de sécurité comme PCI DSS, un concept robuste de sécurité des données et de sauvegarde est requis, pour prévenir les problèmes, garantir des réponses rapides et des temps de récupération en cas d'urgence.

## 2.5. Sécurité des serveurs & des passerelles

Dans certaines infrastructures, un contenu transite par un serveur de messagerie ou un serveur proxy avant d'atteindre un poste client. Ces passerelles filtrent le contenu afin de délivrer un flux aussi sécurisé que possible. Par exemple, des serveurs de messagerie comme Exchange, Sendmail ou Postfix peuvent utiliser des plug-ins pour analyser les emails contre les spams et les malwares. D'une façon similaire, les serveurs de passerelle web telle que Squid peuvent sécuriser le trafic web en utilisant des technologies antivirus, antispam ou antiphishing avant de les transférer au poste concerné.
Les serveurs et les passerelles de messagerie complètent l'utilisation d'un pare-feu. Tandis que ces derniers autorisent ou empêchent le trafic en se basant sur des règles de connexions prédéfinies, les serveurs email et des passerelles analysent le contenu du trafic.
Dans le cas d'utilisation de terminaux non pris en charge, tels que les smartphones privés, le filtrage en passerelle se révèle là encore utile.

## 2.6. Compte-rendu & audits IT

La sécurité multi-couche doit intégrer des modules de compte-rendu & d'audits IT. Ils doivent fournir aux administrateurs des informations fiables sur l'état de sécurité du réseau et des endpoints. Ainsi informés, ils sont à même de prendre des mesures rapides et d'appliquer de nouvelles configurations dans leur infrastructure.

## 2.7. Services de conseil, assistance et cloud

Les couches de protection doivent être également complétées par un accompagnement technique adapté. L'éditeur de la solution multi-couche doit être à même d'accompagner l'utilisateur dans la mise en place de sa stratégie de protection. Choix des modules et configuration adéquate sont un préalable à une sécurité optimale. Une assistance réactive est un autre pilier.

# 3. Choisir une solution de sécurité multi-couche

Beaucoup de réseaux sont protégés par une succession de composants de sécurité indépendants. Même s'ils représentent toutes les couches importantes de la sécurité, ils sont rarement coopérants. Cette situation rend l'infrastructure sujette aux erreurs de configuration et augmente les temps de gestion et de maintenance. Il est donc préférable d'opter pour une solution multi-couche unifiée et pouvant être gérée à partir d'une seule interface. Autre atout non négligeable :

une solution intégrée est souvent financièrement plus avantageuse comparée à l'achat de composants individuels.

Avant d'opter pour une solution spécifique, les administrateurs doivent trouver quelle partie de l'infrastructure a besoin d'être sécurisée et quels risques s'appliquent. La solution potentielle ne doit pas seulement couvrir tous les types de risques et couches de sécurité, mais doit aussi tenir compte de la diversité des terminaux. Les couches de sécurité telles que les détections basées sur les signatures ou heuristiques doivent être disponibles pour tous les types de terminaux (clients Windows, Mac, Linux et les serveurs). La gestion d'appareils mobiles doit être implémentée pour que les terminaux Android ou iOS soient utilisés de façon sûre et en conformité avec les directives de l'entreprise. Mettre en place des couches de sécurité basées sur un ou plusieurs serveurs ou infrastructures tels que la gestion réseau aide à couvrir un nombre large de terminaux à la fois et à résoudre des problèmes de disponibilité et de performance.

G DATA offre des solutions qui couvrent un large spectre de composants de sécurité multi-couche, incluant une multitude de types de terminaux tout comme les serveurs de messagerie, proxy ou de fichiers. En combinant les solutions avec un ou plusieurs modules optionnels, elles s'adaptent à tout réseau et garantissent la sécurité, la disponibilité la performance, la productivité et la confidentialité des données. G DATA offre également de multiples services qui vont de l'assistance à la sécurité de terminaux complètement hébergée. Plus d'informations sur les solutions G DATA pour entreprises : https://www.gdata.fr/entreprises.