STORMSHIELD

PROTECTION DES SERVEURS, POSTES ET TERMINAUX

# SÉCURITÉ ENDPOINT

NETWORK SECURITY | ENDPOINT SECURITY | DATA SECURITY

# UN CONSTAT : LES POSTES DE TRAVAIL ET SERVEURS SONT ENCORE À RISQUE

## DES OUTILS TRADITIONNELS INSUFFISANTS

Malgré les millions d'investissements réalisés, les entreprises font face à **l'échec des outils de défense traditionnels** dans la lutte contre les attaques ciblées ou sophistiquées.

Les outils de type antivirus ou HIPS proposent, en effet, une approche réactive et non proactive pour détecter les programmes et comportements malveillants. Ils utilisent une base de signatures limitée aux menaces connues et se retrouvent souvent impuissants face aux toutes nouvelles attaques.

De plus, les hackers mettent en place des mécanismes de camouflage évolués pour dissimuler leurs agissements et ainsi passer au travers de ces protections par signatures.

## DES ATTAQUES DE PLUS EN PLUS AVANCÉES ET CIBLÉES

Une attaque est considérée comme sophistiquée quand elle peut contourner les mécanismes de sécurité traditionnels.

Cette sophistication est obtenue grâce à la combinaison de multiples méthodes d'attaques évoluées comme, par exemple, l'exploitation d'une vulnérabilité applicative (serveur web, lecteur de fichier pdf) ensuite la propagation d'un malware au travers du réseau de l'entreprise ou la récupération d'accès à des actifs sensibles via l'élévation de privilèges.

## L'IMPACT DES MENACES EN CHIFFRES

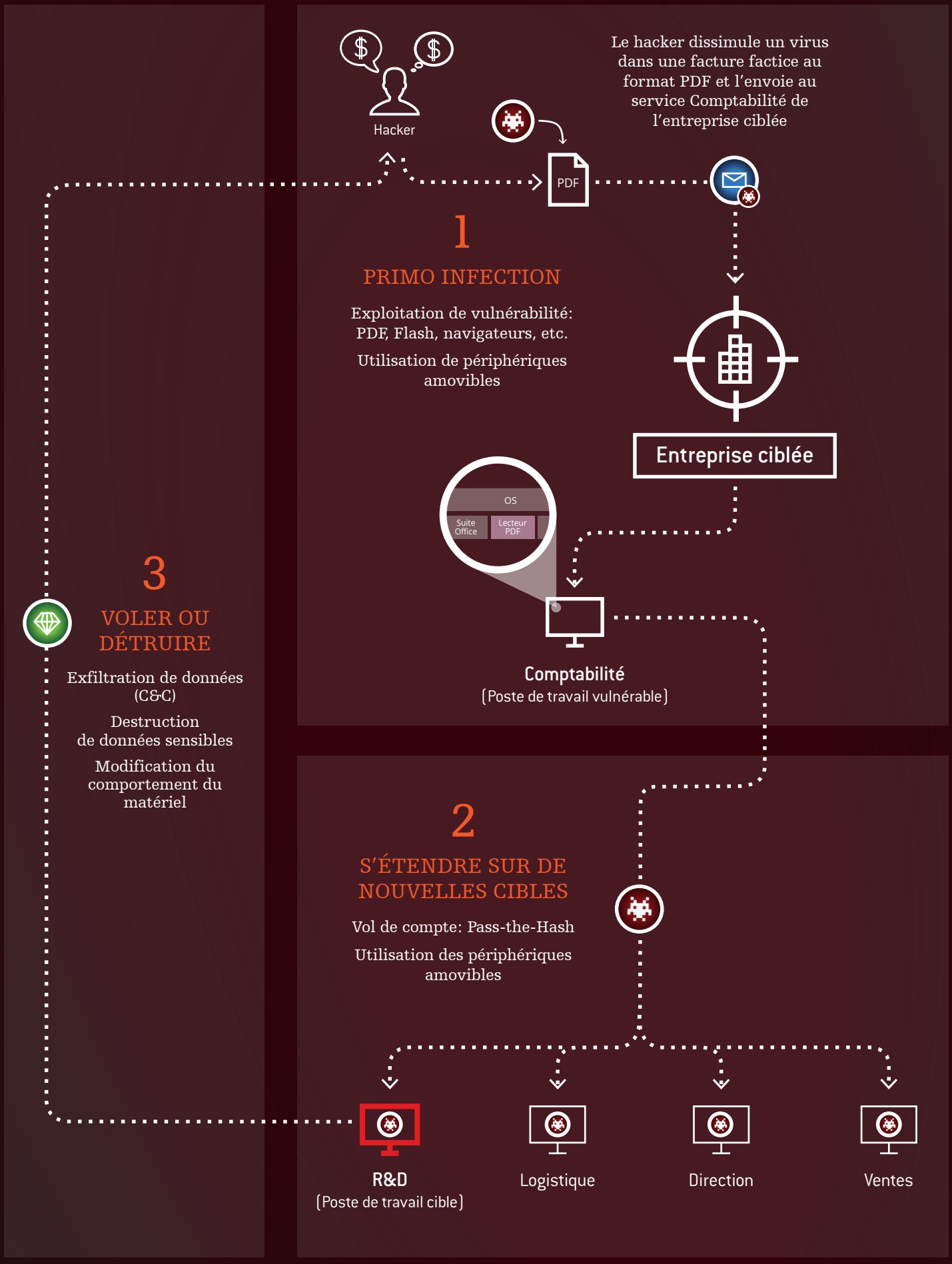
**14 Md €**
Coût des investissements en outils traditionnels de sécurité en 2014

**53%**
Augmentation du coût financier de l'intrusion en 1 an

(Source : Global State of Information Security Survey)

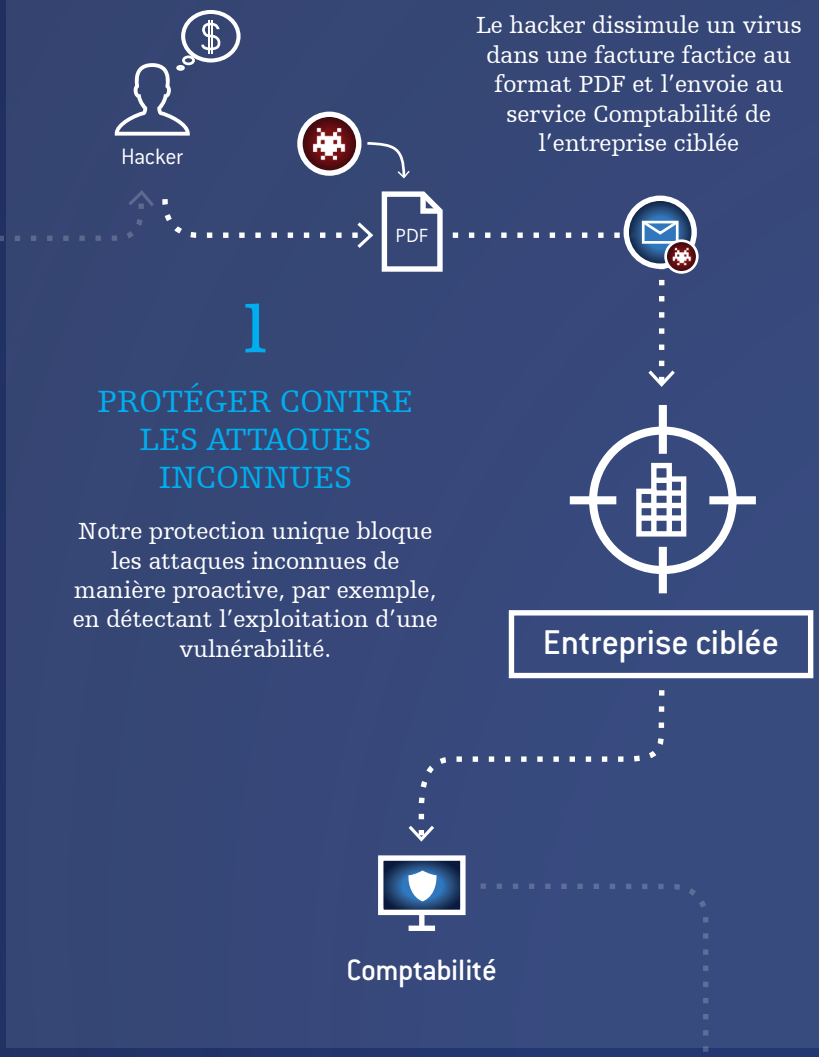
Explication d'une attaque sophistiquée

# Fonctionnement des Advanced Targeted Attacks (ATA)



Une solution existe

# Stormshield Endpoint Security vous protège des Advanced Targeted Attacks (ATA)




## 1

### PROTÉGER CONTRE LES ATTAQUES INCONNUES

Notre protection unique bloque les attaques inconnues de manière proactive, par exemple, en détectant l'exploitation d'une vulnérabilité.

## 2

### BLOQUER LA PROPAGATION DE LA MENACE

Stormshield Endpoint Security permet d'empêcher le vol de données de compte par un contrôle granulaire des opérations réalisées sur le disque dur, sur les clés USB, sur la base de registre ou encore sur les processus du système d'exploitation.

R&D | Logistique | Direction | Ventes

## 3

### PROTÉGER ET CONSERVER LES DONNÉES

Stormshield Endpoint Security intègre un large éventail de protections, à la fois à base de signatures et d'analyses comportementales, qui visent à détecter les transferts de données ou les manipulations indésirables.

La protection complète et éprouvée des serveurs et des terminaux

# Stormshield Endpoint Security
# 2 produits

## FULL PROTECT

Le produit Full Protect
une technologie proactive unique, sans signatures,
qui protège efficacement
des attaques inconnues et sophistiquées.

### PROTECTION CONTRE LES MENACES INCONNUES

Protection contre l'exploitation de vulnérabilité sur le système d'exploitation

Protection contre l'exploitation de vulnérabilité des applications tierces

Contrôle de l'intégrité de la mémoire du système

### PROTECTION DU POSTE DE TRAVAIL

Détection des logiciels malveillants par analyse comportementale

Durcissement du système d'exploitation

Contrôle applicatif (par liste blanche et liste noire)

Contrôle granulaire des droits utilisateurs

Contrôle granulaire de l'exfiltration de données sensibles

### PRÉVENTION D'INTRUSION

Pare-feu

Détection d'intrusion réseau

## FULL CONTROL

Le produit Full Control permet de définir,
de manière granulaire, la protection des postes de travail dans un cadre d'utilisation
conforme à la politique de sécurité de l'entreprise.

### CONTRÔLE ET AUDIT DES PÉRIPHÉRIQUES

Autorisation ou blocage d'un périphérique par son type ou son numéro de série

Blocage ou restriction de différentes opérations d'utilisation du périphérique

Protection contre l'infection par un périphérique externe (par exemple, une clé USB infectée)

Suivi des fichiers chargés sur un périphérique particulier et/ou par un utilisateur particulier

Evaluation des transferts de fichiers (appropriés ou non)

### CONTRÔLE DES COMMUNICATIONS

Pare-feu

Mise en quarantaine des ordinateurs infectés

Autorisation des hotspots Wifi publics uniquement si le VPN de l'entreprise est utilisé

Liste blanche des points d'accès Wifi de l'entreprise

Imposition des normes de sécurité WPA/WPA2

Interdiction du Wifi en mode ad-hoc

Les deux produits peuvent être activés dans la même console de management et sur le même agent.

## DIFFÉRENTES OPTIONS SONT DISPONIBLES

### ENCRYPTION

#### CHIFFREMENT DE SURFACE

Chiffrement du disque avec authentification pre-boot

Authentification unique (SSO) avec la session Windows

Administration centralisée, ségrégation des rôles

Effacement sécurisé des fichiers

### SECURITY MONITORING

#### OFFRE DE SERVICE DE VEILLE AVANCÉE

Analyse des vulnérabilités qui touchent les systèmes d'exploitation ou les applications

Envoi périodique d'un rapport d'analyse attestant du niveau de protection effectif

Fourniture de recommandations pour traiter les éventuels risques résiduels

Réponse efficace pour les systèmes d'exploitation qui ne sont plus supportés

# STORMSHIELD ENDPOINT SECURITY EN QUELQUES POINTS-CLÉS

## UNE RÉPONSE À CHAQUE MENACE

Vous êtes protégé contre l'exploitation de vulnérabilité à distance, contre la menace d'un utilisateur interne malveillant, contre la fuite de données, contre les attaques spécifiques à certains environnements sensibles (SCADA, point of Sale, etc.).

## UNE INTÉGRATION FACILE

Compatibilité avec les autres solutions de protection antivirale, Stormshield Endpoint Security vous offre un niveau de sécurité supplémentaire.

## UNE ADMINISTRATION CENTRALISÉE

Les produits et options de Stormshield Endpoint Security sont facilement managés dans une console unique.

## UNE SOLUTION ADAPTÉE AUX ENVIRONNEMENTS NON CONNECTÉS

Pour les environnements les plus contraints comme les systèmes industriels, l'approche proactive de la solution maintient en condition de sécurité optimale sans mise à jour de bases de signatures.

## UNE SOLUTION CLOUD-READY

Le serveur de management de Stormshield Endpoint Security peut s'installer dans une infrastructure Cloud publique ou privée, ce qui vous permet d'intégrer notre solution de sécurité sans contrainte matérielle.

STORMSHIELD

Stormshield, filiale à 100% d'Airbus Defence and Space, propose des solutions de sécurité de bout-en-bout innovantes pour protéger les réseaux (Stormshield Network Security), les postes de travail (Stormshield Endpoint Security) et les données (Stormshield Data Security).

WWW.STORMSHIELD.EU