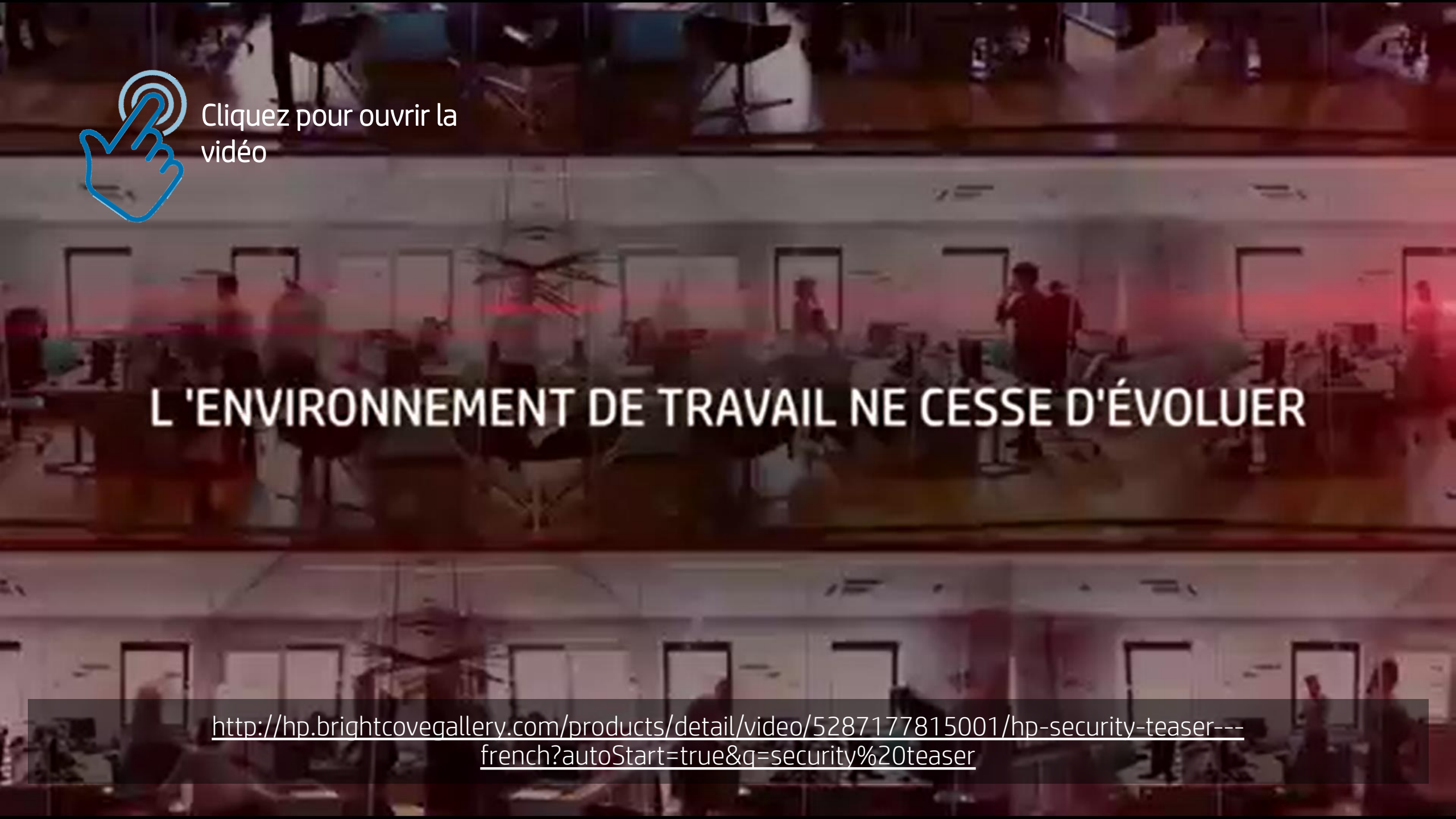
HP

SECURITÉ

Rouslan Parov
Business Developer Premium & Security



http://hp.brightcovegallery.com/products/detail/video/5287177815001/hp-security-teaser---french?autoStart=true&q=security%20teaser

MODELISATION DU FUTUR: MEGA-TENDANCES

Urbanisation rapide

8.6 milliards Population mondiale en 2030

70% de la population mondiale vivra en ville en 2050

41 megapoles d'ici 2030

Les villes génératrices de croissance: Le PIB de Tianjin sera égal à celui de la Suède en 2025

Changements démographiques

1.4 milliards de personnes auront plus de 60 ans en 2030

15 milliards $: le pouvoir d'achat des seniors en 2020

2.6 milliards de generation Z

50% de la force de travail sera composée de millennials en 2020

Hyper globalisation

143,000 entreprises Internet lancées dans les pays émergents chaque année

46% des Fortune 500 auront leur siège social dans les pays émergents en 2025

6.4 milliards d'utilisateurs de téléphone en 2030 (75% de la population mondiale)

75% des entreprises S&P 500 seront ôtés de l'index en 2027

Innovation accélérée

Des téléphones portables **1 milliard de fois** plus puissants dans 30 ans

25 milliards d'objets connectés en 2020

50x plus d'information Générée dans le monde en 2020

Connexion wifi **66x** plus rapide en 2020

https://hpmegatrends.com/

News…

IT WORLD

Cisco warns customers about attacks installing rogue firmware on networking gear

MORE

KIM ZETTER SECURITY 03.03.16 7:00 AM

INSIDE THE CUNNING, UNPRECEDENTED HACK OF UKRAINE'S POWER GRID

PCWorld FROM IDG

SUBSCRIBE

NEWS REVIEWS HOW-TO VIDEO BUSINESS LAPTOPS TABLETS PHONES HARDWARE SECURITY SOFTWARE GADGETS

Privacy Encryption Antivirus

Home / Security

NEWS

UEFI BIOS flaws can be exploited to install highly persistent ransomware

A team of researchers exploited two vulnerabilities in the firmware of Gigabyte BRIX mini PCs to demonstrate low-level ransomware

By Lucian Constantin

Romania Correspondent, IDG News Service | APR 3, 2017 12:16 PM PT

Security Response

Symantec.

Symantec Security Response

View Profile

Symantec Official Blog

Shamoon: Back from the dead and destructive as ever

+5 5 Votes

Malware hit targets in Saudi Arabia and was configured to wipe disks on November 17.

By: Symantec Security Response SYMANTEC EMPLOYEE

Created 30 Nov 2016 | 0 Comments | : 简体中文, 日本語

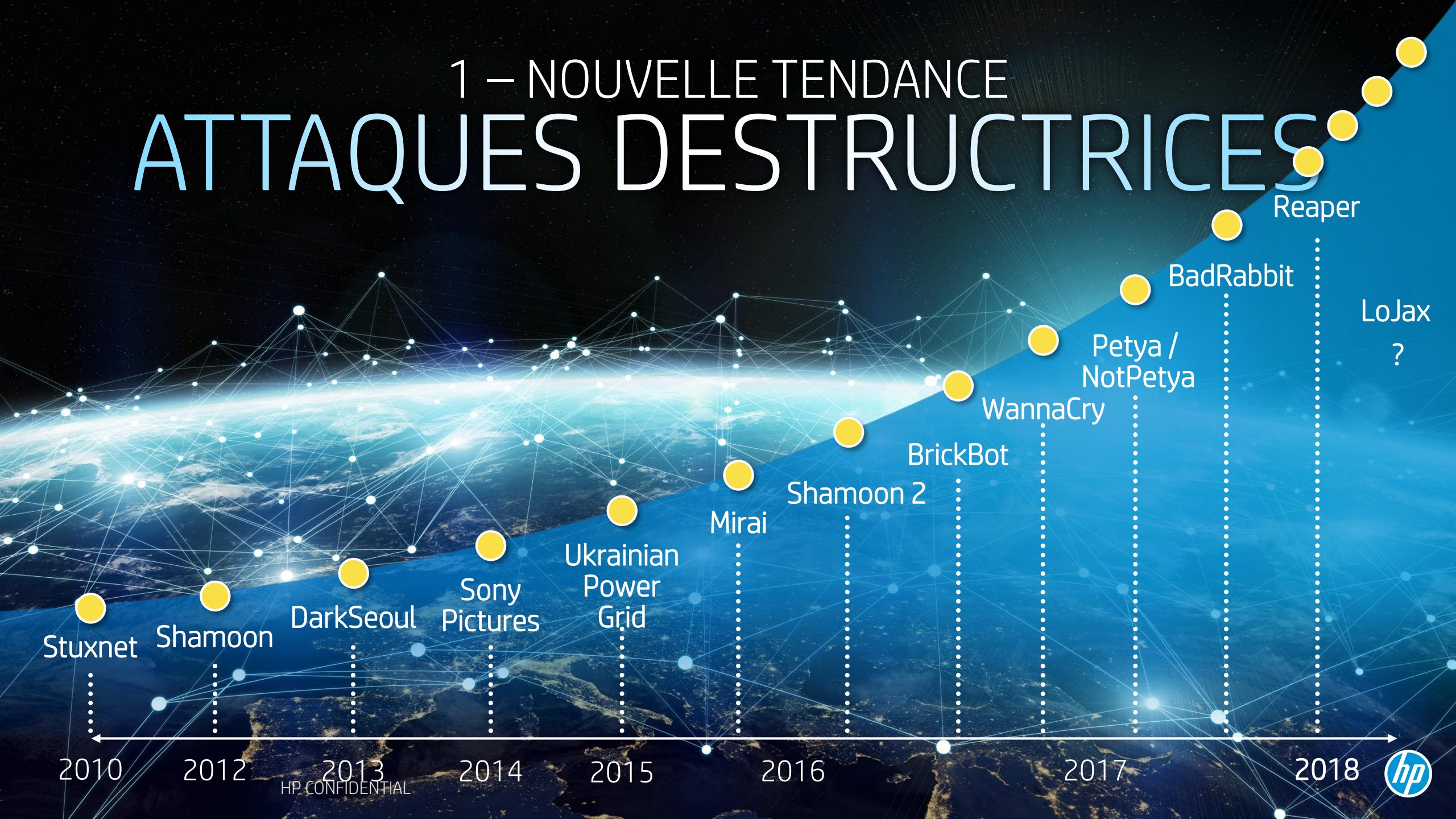
4 117 Like 4

Shamoon (W32.Disttrack), the aggressive disk-wiping malware which was used in attacks against the Saudi energy sector in 2012, has made a surprise comeback and was used in a fresh wave of attacks against targets in Saudi Arabia.

The malware used in the recent attacks (W32.Disttrack.B) is largely unchanged from the variant used four years ago. In the 2012 attacks, infected computers had their master boot records wiped and replaced with an image of a burning US flag. The latest attacks instead used a photo of the body of Alan Kurdi, the three year-old Syrian refugee who drowned in the Mediterranean last year.

1 – NOUVELLE TENDANCE

ATTAQUES DESTRUCTRICES



1 – LA CYBER SECURITE
UNE TENDANCE DE RUPTURE

En 2018, au niveau mondial, le côut de la cybercriminalité est de **$600 Milliards.**

Au premier trimestre 2017, de **nouveaux malwares** étaient créés toutes les **4.2 secondes**

GData, Malware Trends 2017, 2017

[1] https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics-for-2017.html

Le hacking est devenu un business

Annual license: $ 1500
Half-year license: $ 1000
3-month license: $ 700

Update cryptor $ 50
Changing domain $
During the term of th

Rent on our server:

1 week (7 full days):
2 weeks (14 full day
3 weeks (21 full day
4 weeks (31 full day): $ 500
24-hour test: $ 50

- There is restriction on the volume of incoming traffic to a leasehold system, depending on the time of the contract.

Providing our proper domain included. The subsequent change of the domain: $ 35
No longer any hidden fees, rental includes full support for the duration of the contract.

Blackhole Exploit Service T&C

$1500 Milliards de revenus en 2018.

Plateforme d'achat et vente du kit "crimevertising"

Le Blackhole Exploit Kit est l'une des plus grandes menaces web, qui compte pour 29% des menaces web détectées par Sophos et 91% par AVG.

2 – LES ATTAQUES VISENT DIFFERENTS DOMAINES

WannaCry
Ransomware Attack

Coût total : $100 Millions

Exemple: en UK, 80 hôpitaux, 20 000 RDV annulés, 600 opérations sans données patient.

3 – LA CYBER SÉCURITÉ

DU MATÉRIEL OBSOLÈTE

400 Millions de PC dans le monde ont 4 ans et plus, et manquent de mises à jour.

Moins de 2% des imprimantes dans le monde sont sécurisées.

3 – LES TERMINAUX
PREMIERE LIGNE DE DEFENSE

Faille humaine

Faille d'accès physique

Faille de réseau

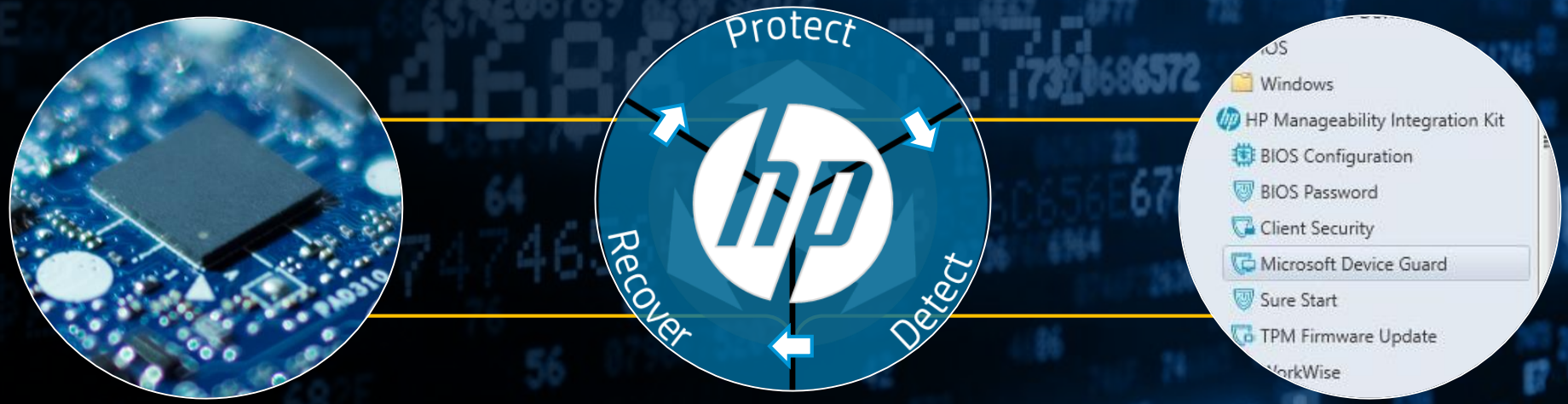
Data centers et services du cloud

DESIGN POUR LA CYBER-RESILIENCE

SECURITE INTEGREE DANS LE HARDWARE

La sécurité logicielle **ne suffit plus**

Au niveau matériel Auto-réparatrice Gérable en flotte



Elle doit commencer et reposer sur le **matériel**

CHOISIR UNE IMPRIMANTE OU UN PC EST UNE DÉCISION DE SÉCURITÉ

LES MENACES VISENT LE SYSTÈME SUR 3 NIVEAUX

AU-DESSUS DE L'OS
Gestion d'infrastructure, hacking visuel

CIBLE FACILE
Les outils de sécurité sont inutiles à moins que les règles soient appliquées. Une gestion en flotte est nécessaire afin d'avoir une sécurité efficace.

DANS L'OS
Logiciels, téléchargements

CIBLE CLASSIQUE
Les vulnérabilités de logiciels non-patchées sont faciles à exploiter.
Sites web malveillants, fichiers téléchargés infectés.

SOUS L'OS
Firmware (BIOS, etc.)

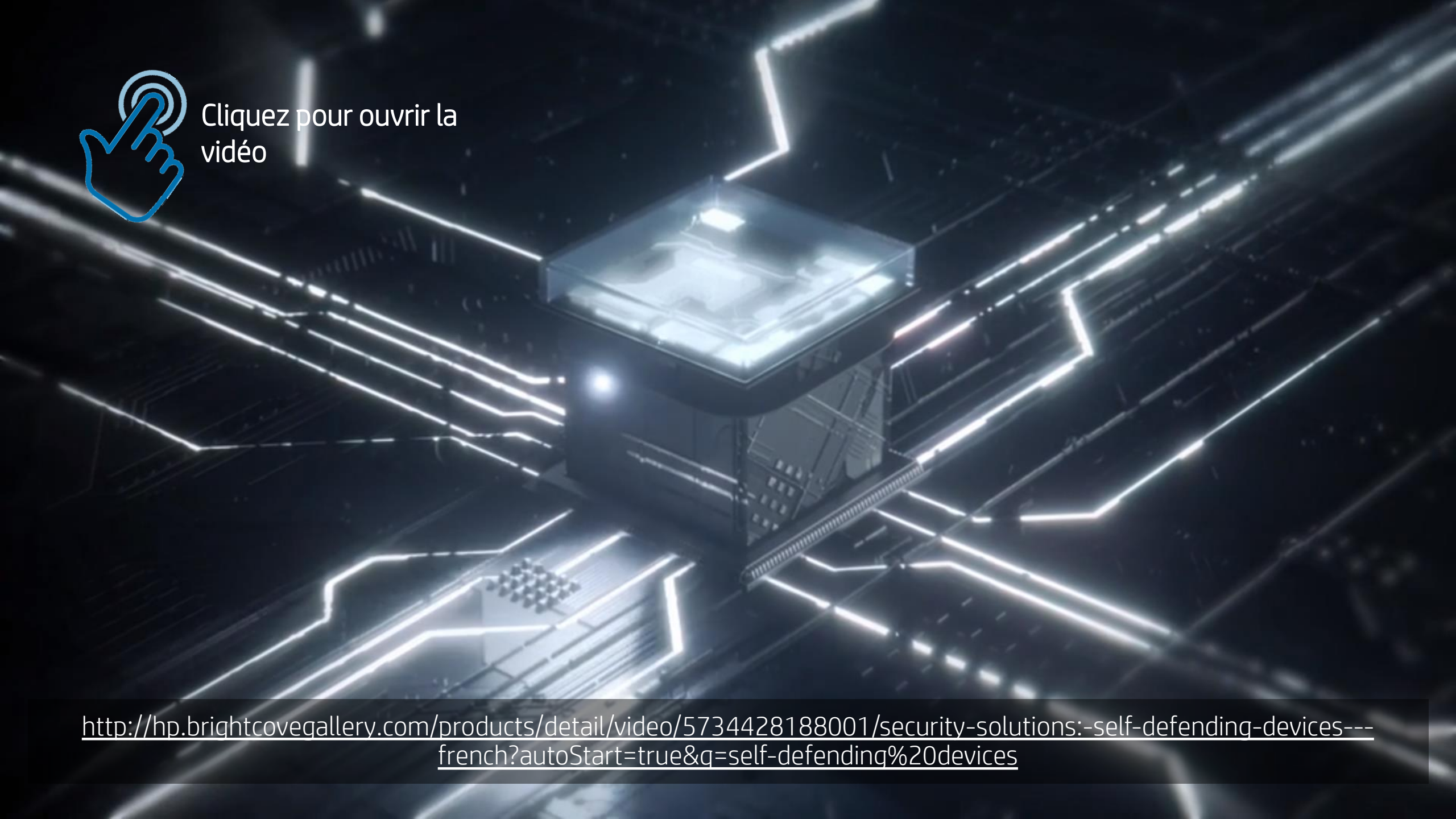
CIBLE IDÉALE
Cible complexe, mais les attaques réussies donnent un accès persistant et indétectable au malfaiteur.

MATÉRIEL

Le plus sécurisé. Très difficilement pénétrable par les hackers et les malwares.

DE NOS JOURS, LA SÉCURITÉ EST UN POINT CLÉ

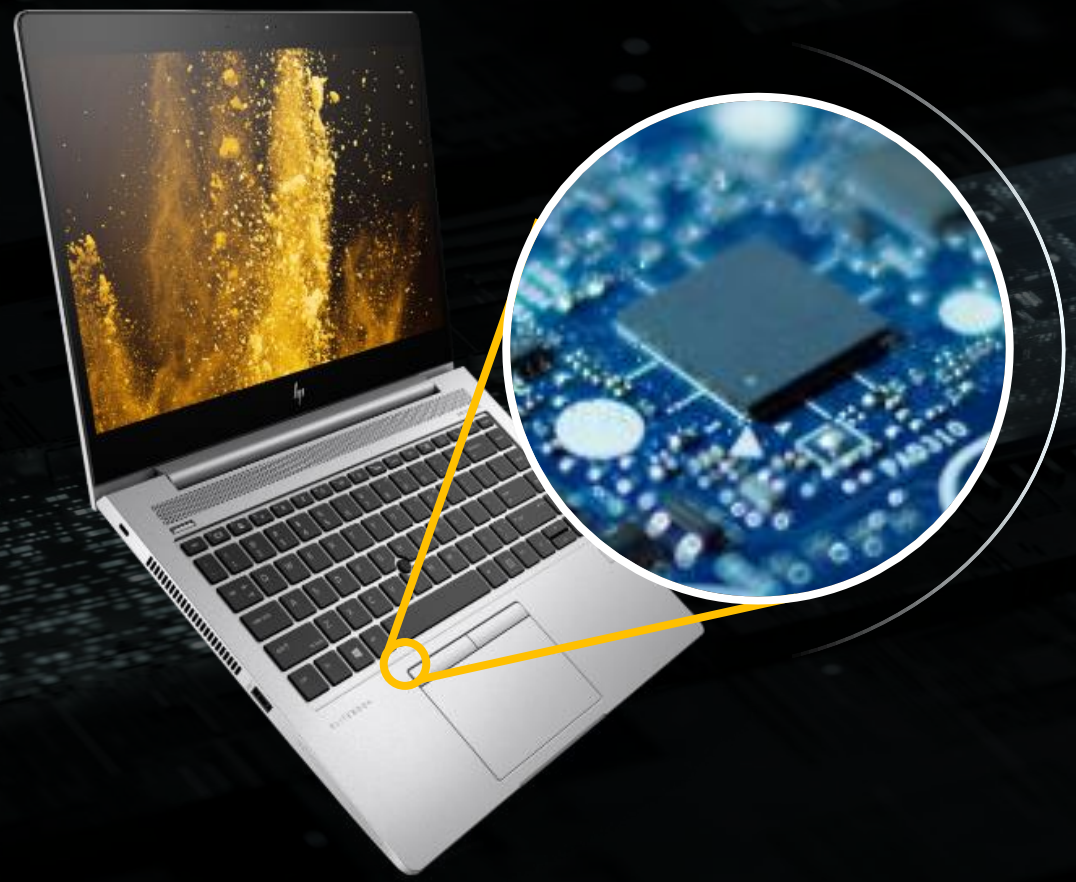
	PÉRIPHÉRIQUE	IDENTITÉ	DONNÉS
		HP Image Assistant Gen3	Nouveautés et Nouvelles versions
	HP MIK Gen2[6] Gestion centralisée de la sécurité sur le parc de PC HP		
AU DESSUS DE L'OS	Cadenas de sécurité		Cache webcam HP Sure View Gen2 Ecran de confidentialité intégré
DANS L'OS	HP Sure Recover Récupération automatique de l'image sur le ne 	HP Client Security Manager Gen4	HP Sure Click Gen2 
	HP Sure Run Protection des applications clefs 	HP Multi-Factor Authenticate Authentification à plusieurs facteurs Renforcé par Intel® Authenticate	
SOUS L'OS	HP Sure Start Gen4 Détection d'intrusion du BIOS et auto-regénération 	HP SpareKey Récupération de mot de passe via 3 questions	HP Secure Erase Suppression permanente des données sur SSD
	HP BIOSphere Gen4[10] Gestion totale du BIOS		Certified Self-Encrypting Drives Encryptage des données au niveau matériel
	 HP Endpoint Security Controller		



http://hp.brightcovegallery.com/products/detail/video/5734428188001/security-solutions:-self-defending-devices---french?autoStart=true&q=self-defending%20devices

HP Endpoint Security Controller

LA BASE DE LA SECURITE MATERIELLE ET CYBER RESILIENTE DE HP

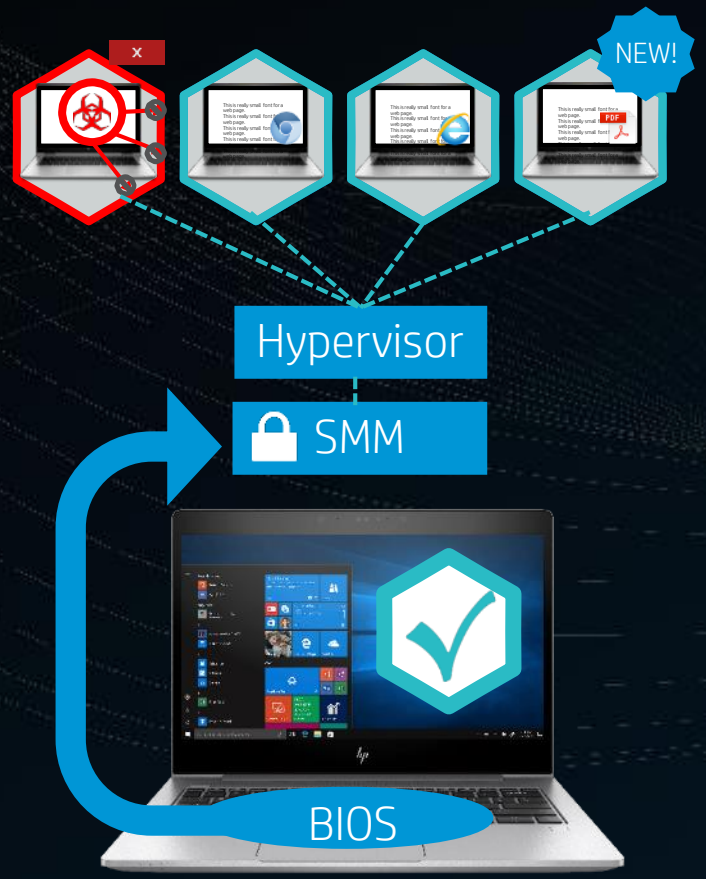


HP Endpoint Security Controller est un véritable hardware intégré dans votre ordinateur qui est à la base de la sécurité PC HP, depuis 2014.

Sécurité matérielle et cyber résiliente :

- *ECS est **isolé physiquement**,*
- ***Cryptographiquement** sécurisé (clé 2048 bits),*
- ***Impossible d'accès** pour les attaques de malwares (lecture seule).*

Chaîne de Confiance au niveau matériel



HP Sure Click
isole des attaques par malwares

HP Sure Run
S'assure que HP Sure Click n'est pas désactivé

HP Sure Start
Protège le SMM, et renforce HP Sure Run[3]

HP Sure Recover
Restaure l'image du PC automatiquement via une connexion réseau

Les PC HP Elite avec HP Sure Click offrent

une protection sécurisée renforcée au niveau matériel

pour la navigation internet.

Exemple 1 : LoJax (2018)

BIOS/UEFI ROOTKIT

Lo/Jack®

LoJack : logiciel anti-vol

- Installé dans le BIOS, pour être résistant même après un reset.
- Envoi la localisation du PC volé sur un serveur LoJack.

LoJax : malware

- Usurpe l'identité de LoJack pour rentrer dans le BIOS.
- Impossible à supprimer, à moins de changer les composants.

HP Sure Start

PROTECTION DU BIOS AVEC AUTO-RÉPARATION

HP Sure Start est le premier BIOS a reparation automatique de first.

Le BIOS est le premier million de lignes de codes qui se lance. C'est la clé de base de votre PC.

Pourquoi est-ce important?
Une fois le BIOS attaqué, les hackers ont un accès total à votre PC : toute autre protection est futile.

Les Antivirus ne sont pas capables de détecter un BIOS infecté !

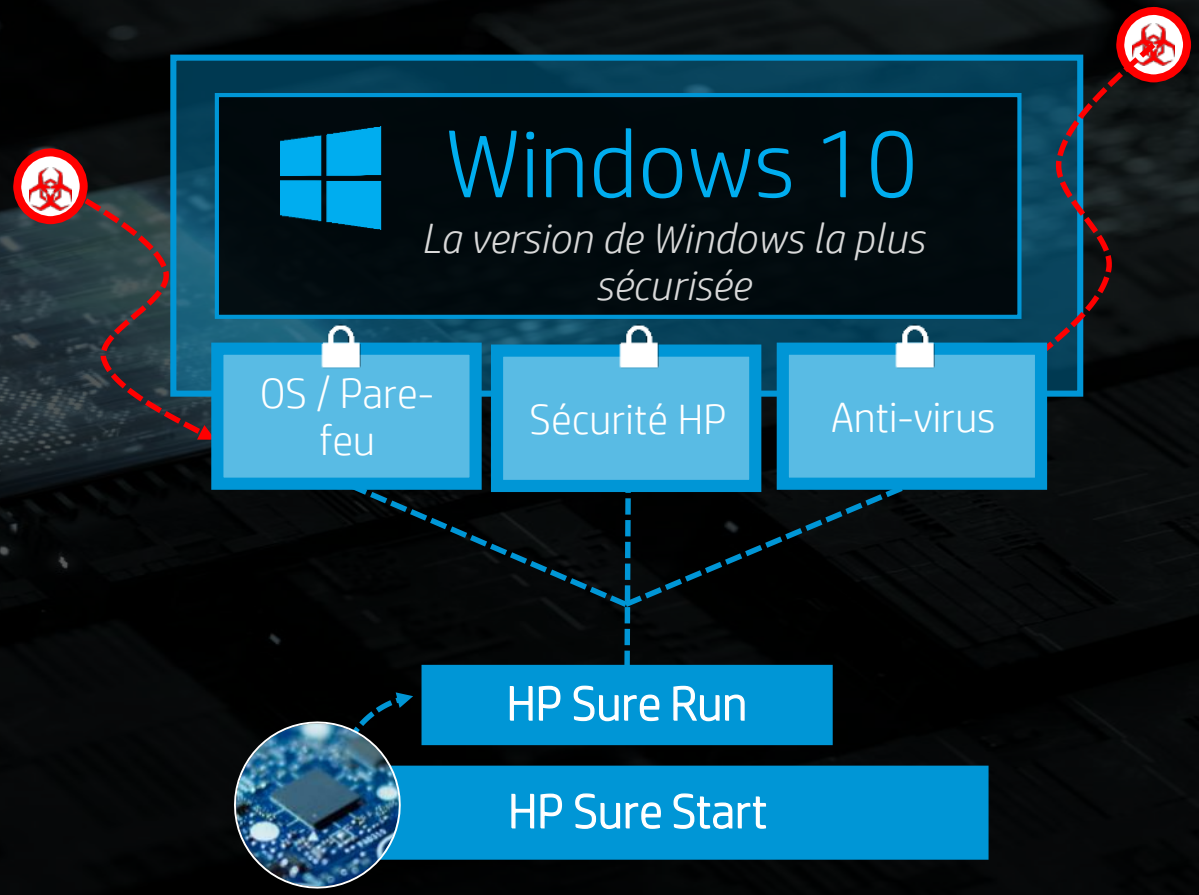
HP Sure Run

UNE PROTECTION DES PROCESSUS CRITIQUES DE SÉCURITÉ DE L'OS

L'une des **attaques** les plus courantes est la désactivation des processus de sécurité tels que l'anti-virus ou le pare-feu.

HP Sure Run est contrôlé par le HP Endpoint Security Controller afin d'assurer une protection avec auto-reparation des processus de sécurité de l'OS.

Il surveille les processus clé, alerte l'utilisateur et l'IT de leur changement ou dysfonctionnement, et les redémarre en cas d'arrêt.



HP Endpoint Security Controller permet la persistence des applications au niveau matériel

Exemple 2 : WannaCry (2017)

Ransomware

- Cryptovers
- 2017 : 250 000 PC, 150 pays
- Crypte les fichiers contre une rançon de $300 en bitcoin

- EternalBlue : faille Windows
- Installe des backdoors sur les systèmes infectés
- Gain: $108 000
- Coût total : $100 Millions

HP Sure Click

NAVIGATION WEB SECURISEE GRACE A L'ISOLATION DE CONTENU

12% des collaborateurs cliquent sur un lien infecté une fois avoir ouvert un email de phishing.

81% des professionnels de l'IT affirment qu'un explorateur insécurisé est la source principale d'attaques.

hp × Br Bromium®

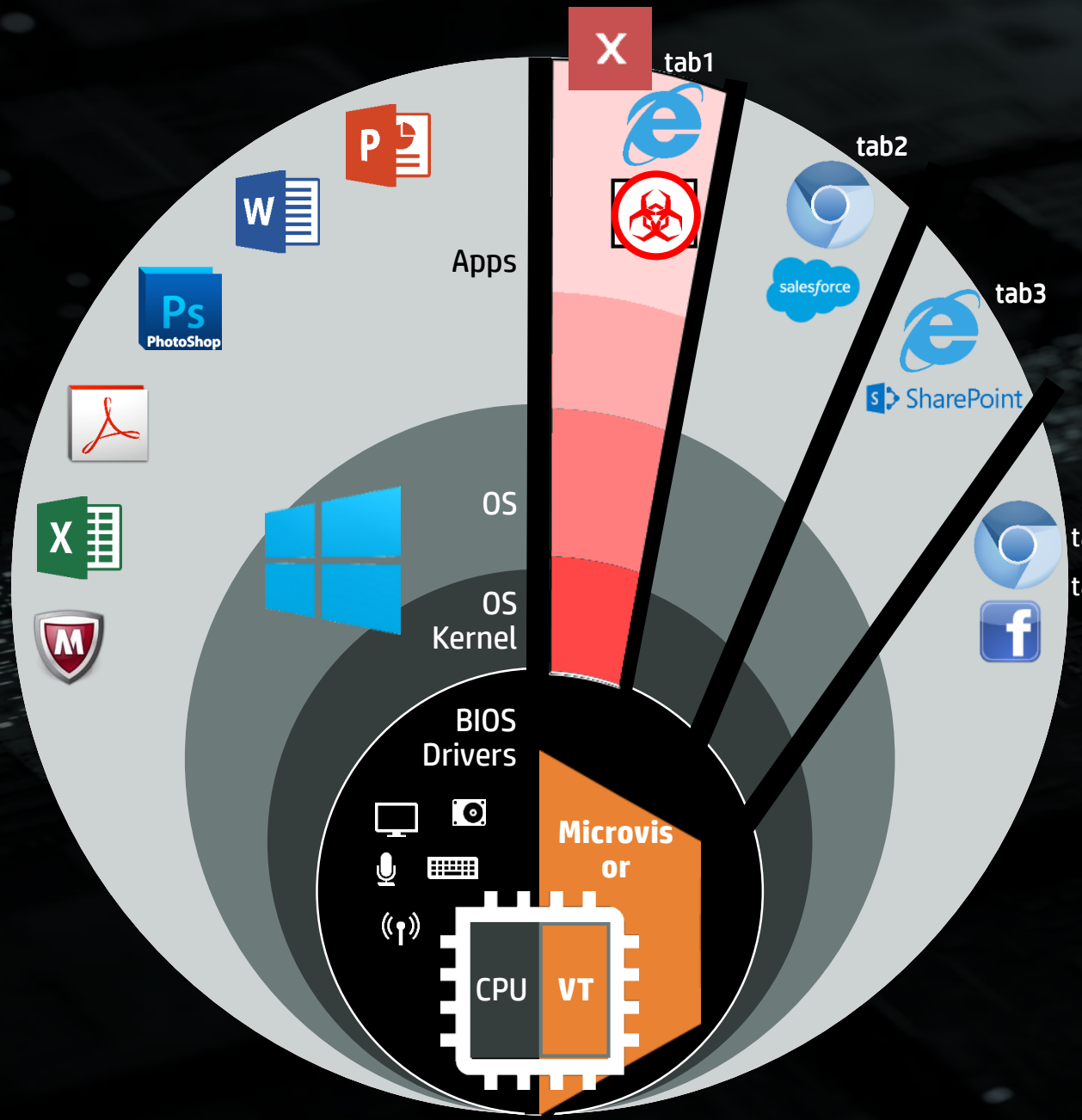
HP Sure Click

SCHÉMA D'ACTION

Protection traditionnelle par détection

Bloque seulement les attaques connues

Des fausses alertes requièrent une analyse profonde et une grande base de données



HP Sure Click

Chaque **onglet** est ouvert dans une micro-machine virtuelle séparée par le CPU

Un malware ouvert dans un onglet n'impacte pas les autres onglets ou l'OS

Fermez l'onglet et le malware disparaît

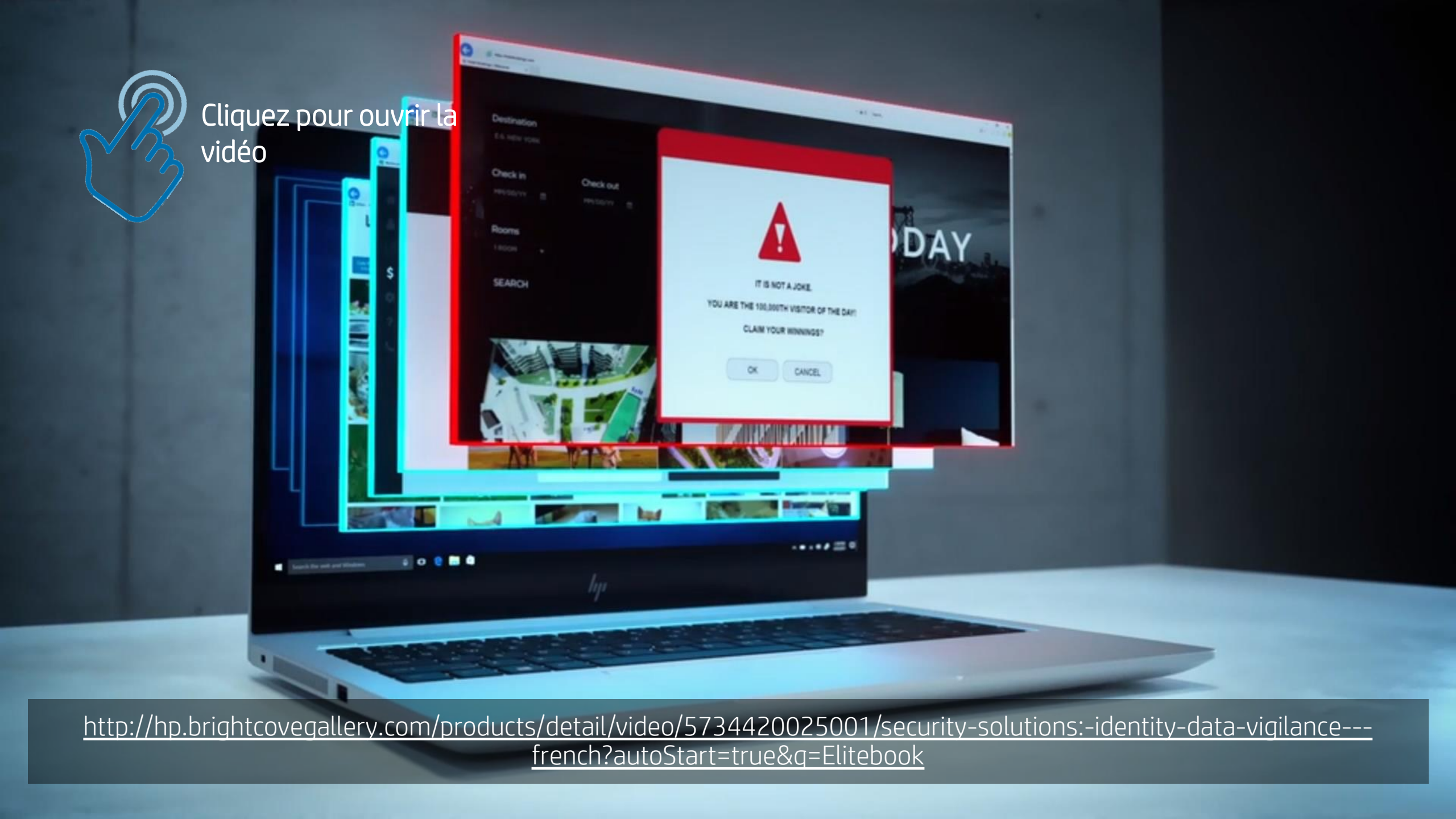
HP Sure Recover

RESTAUREZ FACILEMENT L'IMAGE DE VOTRE OS

HP Sure Recover vous permet de restaurer automatiquement votre image en toute sécurité avec une simple connexion réseau.

Coût total de l'impact de l'attaque Petya/NotPetya sur 4 grosses entreprises : $800M.

Grâce à sa presence au niveau matériel, vous pouvez réimagez votre PC même avec un disque dur efface.

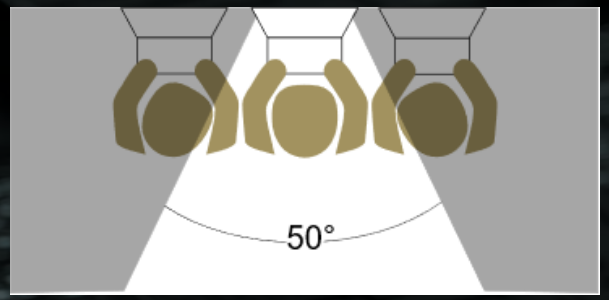


http://hp.brightcovegallery.com/products/detail/video/5734420025001/security-solutions:-identity-data-vigilance---french?autoStart=true&q=Elitebook

HP Sure View Gen2

LES DONNÉES SENSIBLES PROTÉGÉES DES REGARDS INDISCRETS EN UN BOUTON

9/10 des tentatives de hacking visuel sont réussies.



Protection visuelle à partir d'un **angle de 25°**
Réduction visuelle jusqu'à 95%

Average based on global trials conducted by Ponemon Institute during the "Visual Hacking Experiment," 2015, and the "Global Visual Hacking Experiment," 2016, both sponsored by 3M

Authentification à multifacteurs

RENDEZ L'ACCÈS À VOTRE ORDINATEUR UN MILLION DE FOIS PLUS SÉCURISÉ

63% des intrusions sont dues à un mot de passe trop faible.

La plupart des mots de passes (80-90%) peuvent être hackés en moins de 24 heures.

Commercialisation de cracking : les malfaiteurs peuvent utiliser des outils qui facilitent l'obtention de mots de passe.

HP Manageability Integration Kit

SIMPLIFIEZ LA GESTION DE VOTRE PARC DE PC

Microsoft® SCCM + HP MIK

HP MIK est

Un plugin certifié par Microsoft pour SCCM

dans sa 2ème génération

VOUS POUVEZ GÉRER VOS SOLUTIONS DE SECURITÉ EN FLOTTE

Gérer et appliques des règles pour les fonctionnalités de sécurité HP.

- HP Sure Run[3] et HP Sure Recover[4]
- Accès aux ports et TMP

Règles d'authentification : jusqu'à 3 facteurs avec HP Multi-Factor Authenticate[5]

Activez HP Sure View[7] ainsi que d'autres logiciels HP.

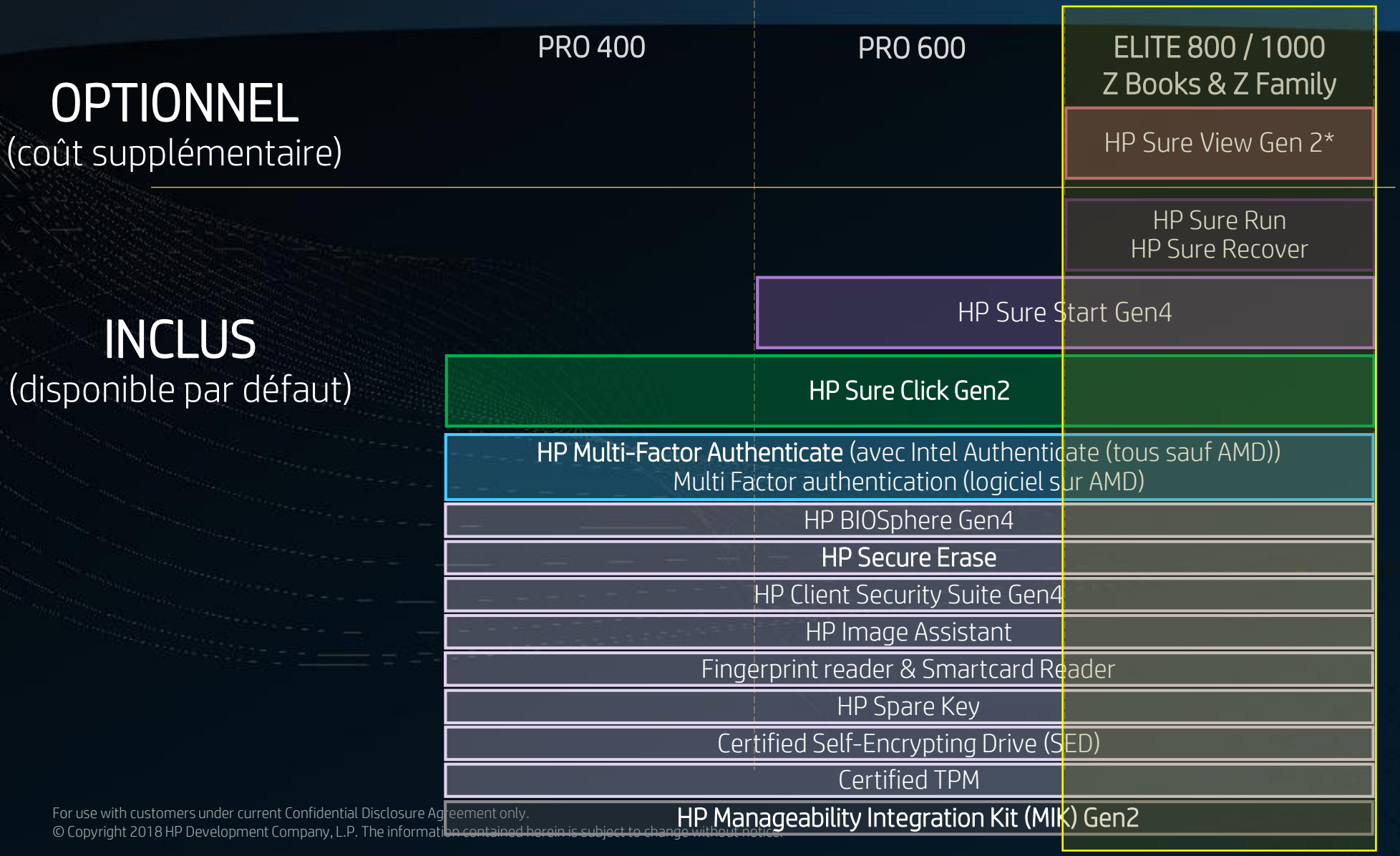
Création d'image facile avec la nouvelle interface.

DE NOS JOURS, LA SÉCURITÉ EST UN POINT CLÉ

	PÉRIPHÉRIQUE	IDENTITÉ	DONNÉS
		HP Image Assistant Gen3	Nouveautés et Nouvelles versions
		HP MIK Gen2[6]	
AU DESSUS DE L'OS	Cadenas de sécurité		Cache webcam
			HP Sure View Gen2
DANS L'OS	HP Sure Recover 	HP Client Security Manager Gen4	HP Sure Click Gen2 
	HP Sure Run 	HP Multi-Factor Authenticate	
SOUS L'OS	HP Sure Start Gen4 	HP SpareKey	HP Secure Erase
	HP BIOSphere Gen4[10]		Certified Self-Encrypting Drives
		 HP Endpoint Security Controller	

MATRICE DES SOLUTIONS DE SÉCURITÉ HP

Sur les plateformes disponibles depuis Février 2018



* disponible sur certains modèles la série 600

La gamme Elite de HP :

LES PCs LES PLUS SÉCURÉS & FACILES À GÉRER AU MONDE.[1]

LA SECURITE DES TERMINAUX
LE LEADERSHIP DE HP

Chair **Trusted Computing Group (TCG)** Technical Committee

Designed and established TPM device security standards (**International Standards Organization - ISO** 11889)

National Institute of Standards in Technology (NIST): MFD and Network Printer Checklists

Leadership with BIOS security standard since 2011 (**NIST** 800-147, **ISO** 19678)

Norme Design & mise en place des standards de sécurité TPM (ISO 11889)

Norme Directoire du Comité Technique du TCG

2002 2003 **2004** **2005** 2006 2007 2008 2009 2010 **2011** 2012 **2013** 2014 **2015** **2016** **2017** **2018**

Premier à expédier un TPM Certifié — **Leader**

Mise à jour sécurisée des BIOS — **Leader**

Leader Leadership dans les normes de sécurité BIOS depuis 2011 (NIST 800-147, ISO 19678)

Leader HP Sure Start BIOS Résilient (PC & Imprimantes)

Leader Détection d'intrusion firmware (PC & Imprimantes)

Leader Services de sécurité imprimantes

Leader Résilience OS & Software (PC)

Leader Détection comportementale de malwares imprimantes

SÉCURITÉ CONCURRENCE EN BREF

HP	DELL	LENOVO
INTÉGRÉE	OPTIONNEL (Extra $)	OPTIONNEL (Extra $)
AU NIVEAU MATÉRIEL	AU NIVEAU LOGICIEL	AU NIVEAU LOGICIEL
LEADER : INNOVATION	POSITION INTERMÉDIAIRE	PROBLÈMES DE SÉCURITÉ

	HP	Dell	Lenovo
Hardware based security	✓	✗	✓
HP Sure Start Gen 4	✓	✗	?
HP Sure Run	✓	$	✗
HP Sure Recover	✓	✗	✗
HP Sure View Gen 2	✓	✗	✓
HP Sure Click	✓	✗	✗
HP MIK Gen 2	✓	$	✗


keep reinventing