

Emotet et Matrix : Analyse, Protection Next-Gen, apports de l'IA et de l'EDR

Michel Lanaspèze
Directeur Marketing Europe de l'Ouest

Agenda

- Introduction
- Emotet
- De SamSam à Matrix: ransomwares ciblés
- Protections Next-Gen
- Mieux répondre aux attaques: démocratiser l'EDR avec l'IA

Sophos en quelques chiffres

 **1985**
FONDÉ À OXFORD
(Royaume-Uni)

 **770 M\$**
ANNÉE FISCALE 2018
(VENTES)

 **3 300+**
EMPLOYÉS
(APPX.)

 **SIÈGE**
ABINGDON, RU

300 000+
ENTREPRISES CLIENTES  **100M+**
UTILISATEURS

 **39 000+**
PARTENAIRES
CHANNEL

Premier éditeur d'origine européenne de solutions de sécurité pour les entreprises

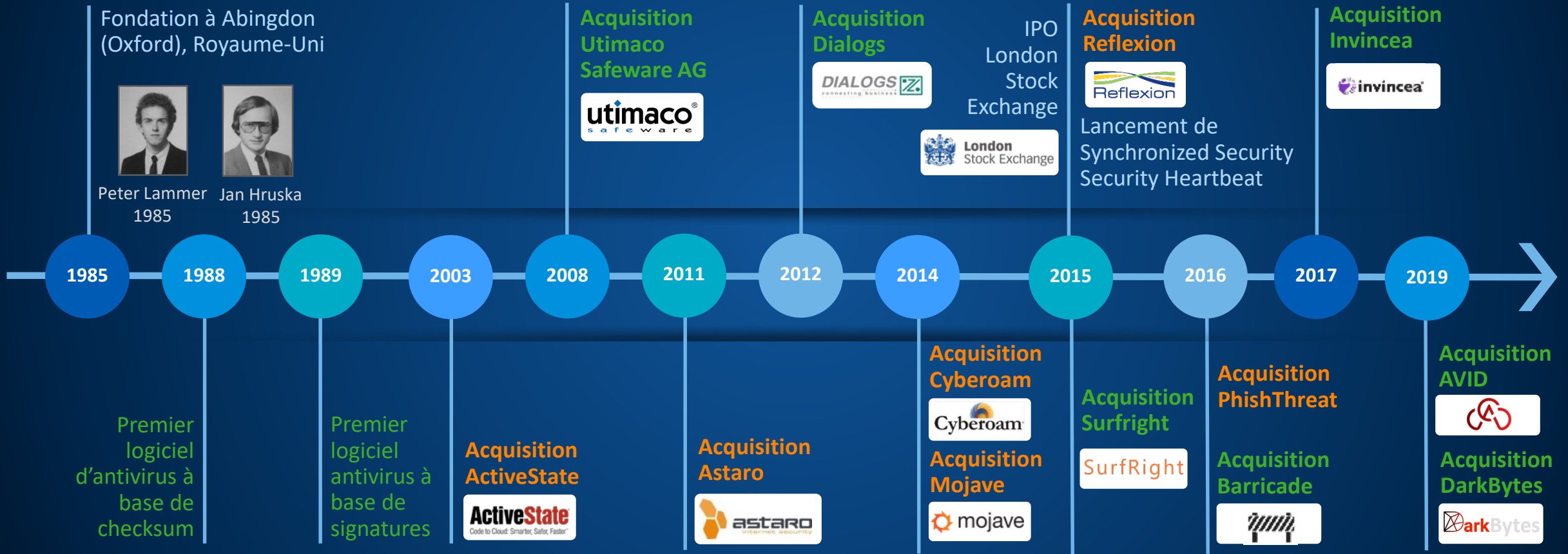
- 5 SophosLabs dont **2 en Europe**
Oxford, Budapest, Vancouver, Ahmedabad, Sydney
- 12 Centres de R&D dont **7 en Europe**
*RU: Oxford Allemagne: Dortmund, Karlsruhe Autriche: Linz
Hongrie: Budapest Irlande: Cork Pays-Bas: Hengelo
Canada: Vancouver USA: Boston, Fairfax, San Francisco
Inde: Ahmedabad*



Sophos en quelques dates

Évolution vers une sécurité complète

- Société
- Protection Utilisateurs
- Protection Réseaux



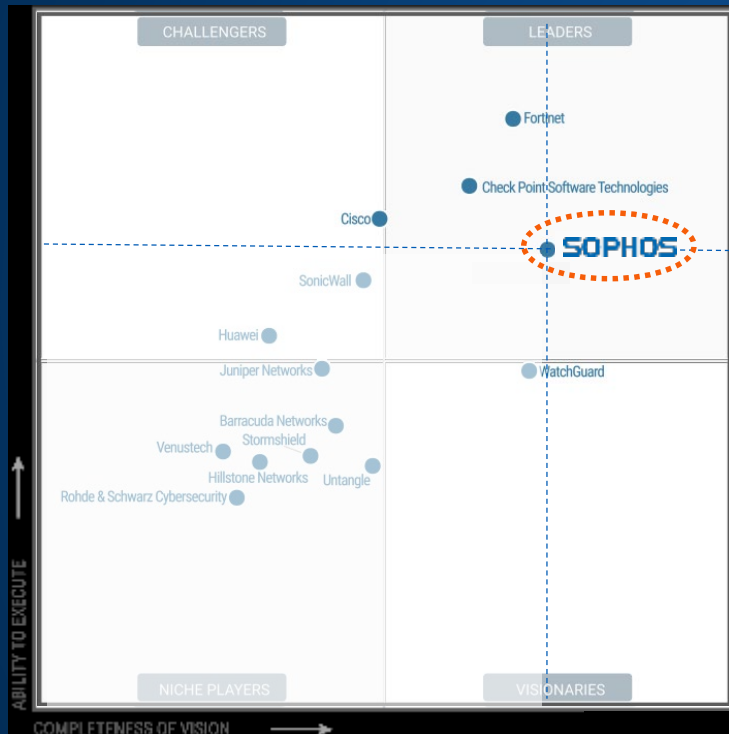
Sophos: double Leader Réseaux + Endpoint



Seul éditeur double leader des Magic Quadrants **UTM** + **Endpoint Protection**



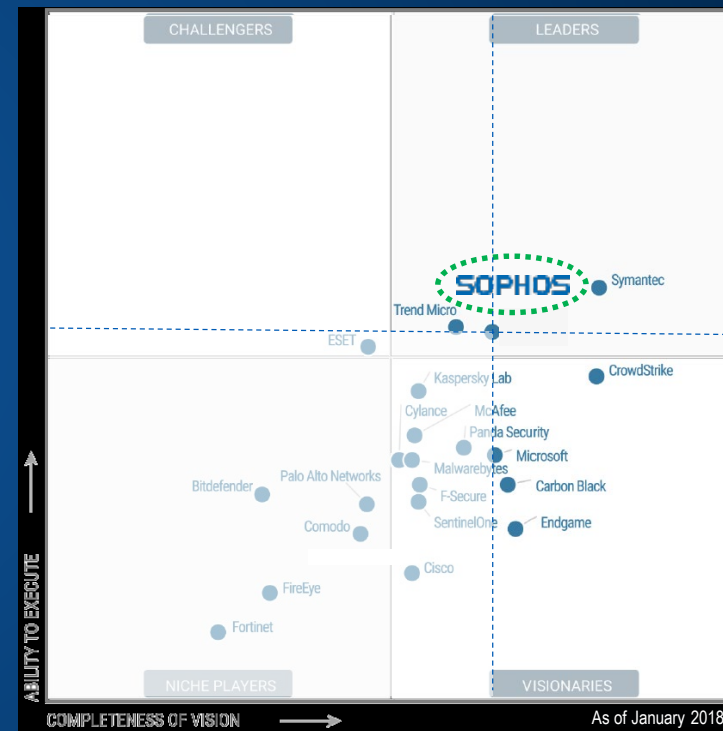
Gartner Magic Quadrant UNIFIED THREAT MANAGEMENT



Magic Quadrant for Unified Threat Management
Rajpreet Kaur, Claudio Neiva - 20 septembre 2018



Gartner Magic Quadrant ENDPOINT PROTECTION PLATFORMS



Magic Quadrant for Endpoint Protection Platforms
Ian McShane, Avivah Litan, Eric Ouellet, Prateek Bhajanka - 24 janvier 2018

These graphics are published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner documents are available upon request from Sophos.

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. All statements in this report attributable to Gartner represent Sophos' interpretation of data, research opinion or viewpoints published as part of a syndicated subscription service by Gartner, Inc., and have not been reviewed by Gartner. Each Gartner publication speaks as of its original publication date (and not as of the date of this presentation). The opinions expressed in Gartner publications are not representations of fact, and are subject to change without notice.

Sécurité Synchronisée



 **Analytics** | Analyse les données provenant de tous les produits Sophos pour une meilleure visibilité, corrélation et automatisation



 **Sophos Labs** | Réseau d'analystes mondial 24x7x365 | URL Database | Malware Identities | File Look-up | Genotypes | Reputation | Behavioural Rules | APT Rules Apps | Anti-Spam | Data Control | SophosID | Patches | Vulnerabilities | Sandboxing |

2015

- Endpoint + Firewall
- Security Heartbeat™
- Isolement Automatique

2016

- Endpoint + Chiffrement
- Heartbeat™ Destination
- Absence d'état Heartbeat™

2017

- Contrôle applicatif synchronisé
- Heartbeat™ sur Linux
- Heartbeat™ sur Mac Os

2018

- Endpoint & Mobile + WiFi
- Endpoint & Email + PhishThreat
- Blocage des attaques latérales



EMOTET

EMOTET

“Amongst the most costly and destructive threats to U.S. businesses right now”

U.S. Department for Homeland Security, 2018

Cheval de Troie dérobant silencieusement les informations de compte bancaire des victimes

Évolution continue

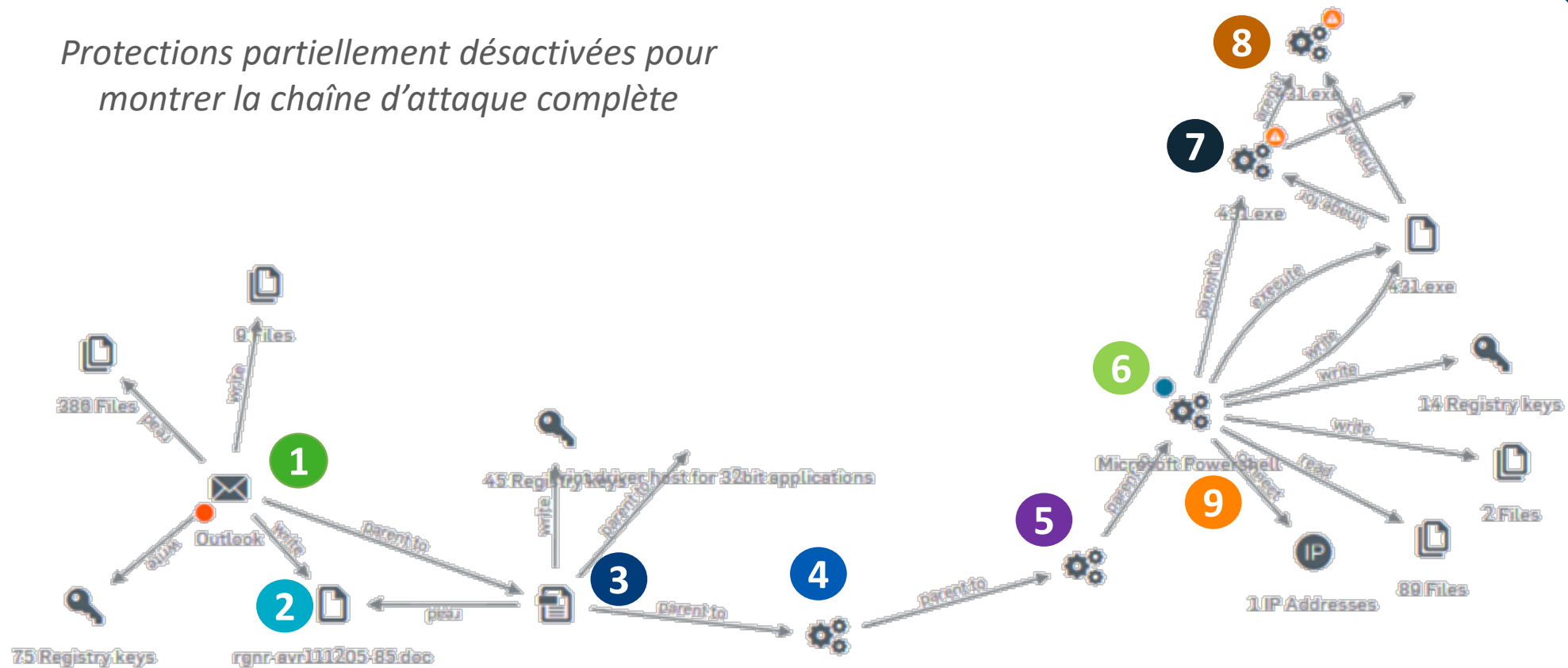
Ver réseaux hautement sophistiqué distribuant d'autres malwares, en particulier des Chevaux de Troie bancaires

2014

2019

EMOTET : Chaîne d'attaque

Protections partiellement désactivées pour montrer la chaîne d'attaque complète



1. L'utilisateur reçoit un email malveillant (malspam)

2. L'utilisateur clique sur une pièce jointe malveillante: rgrn-avr111205-85.doc

3. L'utilisateur active des macros malveillantes dans le document

4. La macro utilise CMD (Command Prompt) pour exécuter un code obfusqué

5. CMD lance une deuxième copie de CMD

6. La seconde copie lance Microsoft PowerShell.

7. Powershell se connecte à une adresse IP et télécharge un fichier appelé 431.exe

8. Powershell exécute 431.exe

9. Sophos HIPS détecte la connection Powershell vers une adresse IP suspecte avec téléchargement d'exécutable de réputation douteuse, et intervient

EMOTET : Quels sont ses buts ?

Ecran de fumée
pour des
attaques de
ransomware
ciblées

Infections secondaires

Se diffuse à
travers le
réseau

Envoie du spam
pour infecter
d'autres
organisations

Atteinte à la réputation

Vole les
historiques des
navigateurs,
noms et mots
de passe

Violations de sécurité



Recherche les
adresses
emails et les
contacts

Atteintes aux données personnelles

Télécharge
une charge
virale

Infection primaire

EMOTET : Pourquoi est-il si dangereux ?

Une machine
suffit

Evolution
continue

Réinfections
incessantes

De SamSam à Matrix: ransomware ciblé

Du ransomware de masse ... au ransomware ciblé

WannaCry, NotPetya etc...

SamSam, Matrix ...

Diffusion
explosive

Quelques
attaques par jour

Attaques
indiscriminées

vs.

Attaques
ciblées

Quelques
semaines

Perdurent
des années

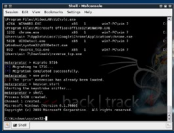
Des familles nombreuses et anciennes

	SamSam	Dharma	Matrix	BitPaymer	Ryuk	GandCrab
Active	No	Yes	Yes	Yes	Yes	Yes
First appeared	2015	2016	2016	2017	2018	2018
Type	Targeted	Targeted	Targeted	Targeted	Targeted	Targeted
Infection vector	RDP Exploit	RDP	RDP Exploit	RDP	RDP	RDP Email Exploit
Victim size	Med/large	Small/med	Med/large	Med/large	Med/large	Any
computers targeted	Servers/ endpoints	Servers	Any	Servers	Servers	Any
Attack frequency	Med	High	Low	Med	Med	High
Regions affected	All	All	All	All	All	All
Decryption available	No	No	No	No	No	Some variants
Ransom currency	Bitcoin	DASH	Bitcoin	Bitcoin	Bitcoin	Bitcoin
Avg.ransom	\$50k	\$5k	\$3.5K	\$500k	\$100k	\$800
Payment method	Dark Web	Email	Email	Email Dark Web	Email	Dark Web

Persistence

Techniques d'attaques de style APT

- Choix et étude minutieuse de la victime
- Infiltration + Expansion « *Land + Expand* »
- Persistence + Progression silencieuse et manuelle



MIGRATION
DE PROCESSUS
MALVEILLANT



ÉLÉVATION
DE PRIVILÈGES
DE PROCESSUS



VOL
D'IDENTIFIANTS



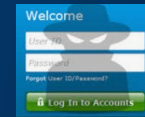
MODIFICATIONS
DE LA BASE
DE REGISTRES



CODE
CAVE



VIOLATION APC
ATOM BOMBING



MAN-IN-THE-
BROWSER

- Recherche des ressources les plus sensibles (serveurs)
- Frappe brutale et ciblée

Protection Next-Gen

Protection Next-Gen

Une nouvelle approche de la sécurité



PROTECTION NEXT-GEN



Prédictive



Sans signatures



Remédiation



Multi-vecteurs



Ensemble



Synchronisée

Protection Réseaux Next-Gen



Protection Endpoint Next-Gen

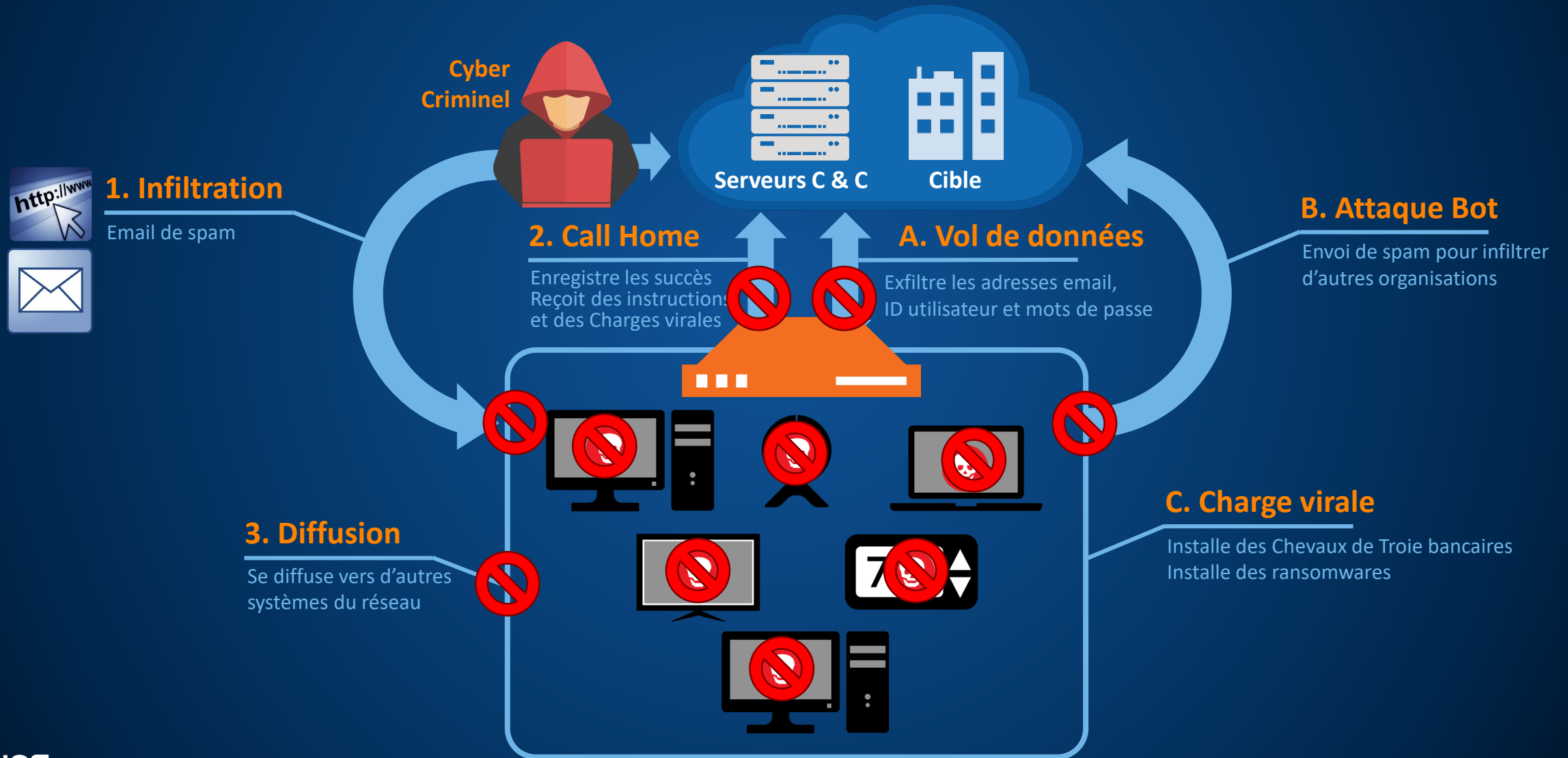


Sécurité Synchronisée



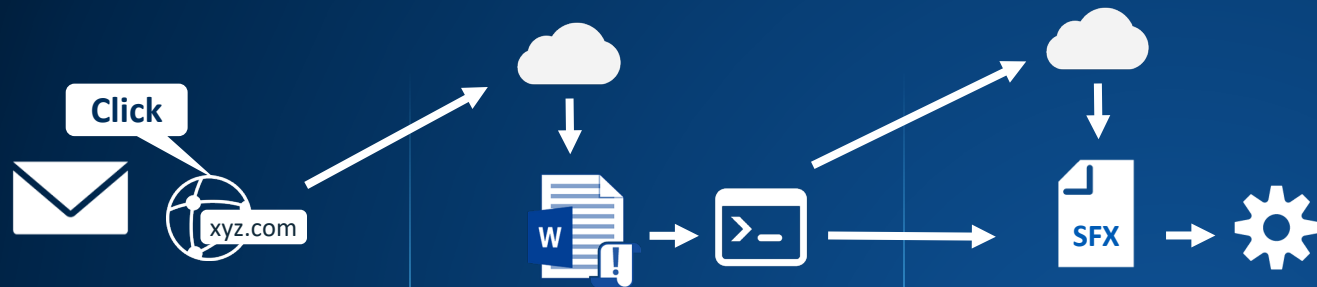
Intervenir à tous les niveaux de l'attaque

L'exemple d'EMOTET



Intervenir à tous les niveaux

L'exemple d'EMOTET



Livraison

Exploitation

Installation

Commande & Contrôle

Actions sur la cible

WEB PROTECTION

CODE/MEMORY/APC
MITIGATIONS

APPLICATION
LOCKDOWN

LOCAL PRIVILEGE
MITIGATION

APPLICATION
CONTROL

DEEP
LEARNING

HIPS

NETWORK THREAT
PROTECTION

ANTI-RANSOMWARE

CREDENTIAL THEFT
PROTECTION

RUNTIME HIPS

THREAT CASE (RCA) & EDR

Protection Endpoint Next-Gen

Protections avancées sans signatures



Anti-Exploit

Anti-piratage (APT) & Anti-ransomware

Deep Learning

EDR Endpoint Detection & Response

Blocage des techniques utilisées par les exploits

- 24+ techniques bloquées
- Protection Zero-Day
- Bloque les attaques en mémoire sans fichiers
- 10+ ans d'expertise en R&D et de technologies **SurfRight**

Enforce Data Execution Prevention (DEP)	Empêche les débordements abusifs de mémoire tampon.
Mandatory Address Space Layout Randomization (ASLR)	Traverse tous l'emplacements de code prédictibles.
Bottom-Up ASLR	Améliore les caractéristiques de l'allocation d'emplacements de code.
Null Page (Null Dereference Protection)	Bloque les exploits venant de la page Zero.
Heap Spray Allocation	Zones de mémoire réservées pré-allouées pour bloquer les attaques.
Dynamic Heap Spray	Bloque les attaques qui diffusent des séquences suspectes dans la mémoire dynamique.
Stack Pivot	Bloque les attaques contre le pointeur de retour de fonction de la pile.
Stack Exec (MemProc)	Bloque le code d'un parasite sur la pile.
Stack-based ROP Mitigations (Callix)	Bloque les attaques connues de type "Return-Oriented Programming".
Branch-based ROP Mitigations (Hardware Augmented)	Bloque les attaques ROP avancées.
Structured Exception Handler Overwrite Protection (SEHOP)	Bloque l'utilisation abusive du gestionnaire d'exceptions.
Import Address Table Filtering (IAF) (Hardware Augmented)	Bloque les pirates cherchant les adresses des API dans l'API.
Load Library	Empêche le chargement de bibliothèques à partir des chemins UNC.
Reflective DLL Injection	Empêche le chargement d'une bibliothèque depuis la mémoire sur un processus hôte.
VBScript God Mode	Empêche l'utilisation abusive de VBScript dans IE pour exécuter du code malveillant.
WoW64	Bloque les attaques visant la fonction API lors de processus WoW64.
Syscall	Bloque les pirates tentant de contourner les points de branchement (hook) de sécurité.
Hollow Process	Bloque les attaques utilisant des processus légitimes pour cacher du code malveillant.
DLL Hijacking	Donne la priorité aux bibliothèques du système pour les applications téléchargées.
Application Lockdown	Bloque les attaques logiques contournant les mitigations.
Java Lockdown	Empêche les attaques utilisant abusivement Java pour lancer des exécutables Windows.
Executable AppLocker Bypass	Empêche regsvr32 d'exécuter à distance des scripts et du code.
CVE-2013-5233 & CVE-2014-4133 via Metasploit	Charges virales en mémoire: Meterpreter & Meterpreter.

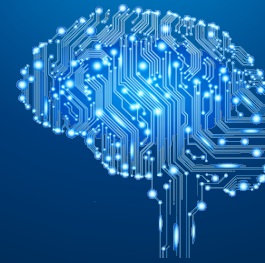
Détection des menaces avancées

- **Anti-piratage (APT)**
 - Credential Theft, Code Cave Utilization, Malicious Process Migration, Process Privilege Escalation, APC violation, Registry modification, Process Lockdown
- **Anti-Ransomware**
 - Blocage du chiffrement malveillant
 - Analyses comportementales
 - Restitution des fichiers originaux



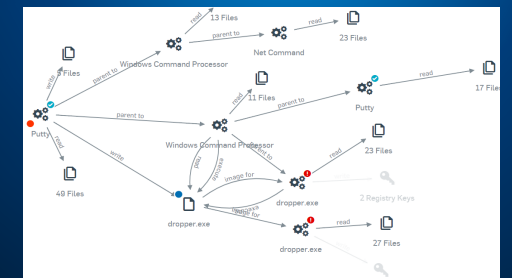
Anti-malware à base de Deep Learning

- Sans signatures
- Fiable et éprouvé
- 10+ ans d'expertise en R&D et de technologies **Invincea**
- Enrichi de l'expertise et des données des **SophosLabs**



Détection, analyse et réponses automatisées

- Détection des menaces latentes infiltrées dans la chaîne d'attaque
- Analyse détaillée assistée par Deep Learning et les **SophosLabs**
- Remédiation automatisée
- Nettoyage avancé



Anti-Exploit: des vulnérabilités toujours plus présentes

Un des principaux risques en matière de sécurité



Source: NIST National Vulnerability Database

<https://nvd.nist.gov/vuln-metrics/visualizations/cvss-severity-distribution-over-time>

Anti-Exploit: protection à large spectre

10+ années d'expertise anti-exploit | 25+ techniques d'exploit bloquées



Enforce Data Execution Prevention (DEP)	Empêche les dépassements abusifs de mémoire tampon
Mandatory Address Space Layout Randomization (ASLR)	Prévient l'abus d'emplacements de code prédictibles
Bottom Up ASLR	Améliore le caractère aléatoire de l'allocation d'emplacements de code
Null Page (Null Dereference Protection)	Bloque les exploits venant de la page Zéro
Heap Spray Allocation	Zones de mémoire courantes pré-allouées pour bloquer les attaques
Dynamic Heap Spray	Bloque les attaques qui diffusent des séquences suspectes dans la mémoire dynamique
Stack Pivot	Bloque les attaques contre le pointeur de retour de fonction de la pile
Stack Exec (MemProt)	Bloque le code d'un pirate sur la pile
Stack-based ROP Mitigations (Caller)	Bloque les attaque communes de type "Return-Oriented Programming"
Branch-based ROP Mitigations (Hardware Augmented)	Bloque les attaques ROP avancées
Structured Exception Handler Overwrite Protection (SEHOP)	Bloque l'utilisation abusive du gestionnaire d'exceptions
Import Address Table Filtering (IAF) (Hardware Augmented)	Bloque les pirates cherchant les adresses des API dans l'IAT
Load Library	Empêche le chargement de bibliothèques à partir des chemins UNC
Reflective DLL Injection	Empêche le chargement d'une bibliothèque depuis la mémoire sur un processus hôte
VBScript God Mode	Empêche l'utilisation abusive de VBScript dans IE pour exécuter du code malveillant
WoW64	Bloque les attaques visant la fonction 64 bits du processus WoW64
Syscall	Bloque les pirates tentant de contourner les points de branchement (hooks) de sécurité
Hollow Process	Bloque les attaques utilisant des processus légitimes pour cacher du code malveillant
DLL Hijacking	Donne la priorité aux bibliothèques du système pour les applications téléchargées
Application Lockdown	Bloque les attaques logiques contournant les mitigations
Java Lockdown	Empêche les attaques utilisant abusivement Java pour lancer des exécutables Windows
Squiblydoo AppLocker Bypass	Empêche regsvr32 d'exécuter à distance des scripts et du code
CVE-2013-5331 & CVE-2014-4113 via Metasploit	Charges virales en mémoire: Meterpreter & Mimikatz

Protection contre attaques avancées et APT

Protection contre les techniques d'attaques ciblées



ANTI-RANSOMWARE



Stoppe les techniques d'attaque par ransomware



VOL D'IDENTIFIANTS



Stoppe les techniques qui collectent les identifiants utilisateur



ÉLÉVATION DE PRIVILÈGES DE PROCESSUS



Détecte l'insertion d'un jeton de noyau pour élever les privilèges



MIGRATION DE PROCESSUS MALVEILLANT



Empêche le mouvement vers des processus distants pour persistance



CODE CAVE



Détecte le code caché dans des applications légitimes



VIOLATION APC et ATOM BOMBING



Détecte les violations APC et les abus sur la table ATOM



MODIFICATIONS DE LA BASE DE REGISTRES



Empêcher l'exécution de code arbitraire via la base de registres



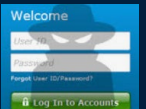
VERROUILLAGE DE PROCESSUS



Bloque le lancement de Powershell, de macros ... pour injecter du code



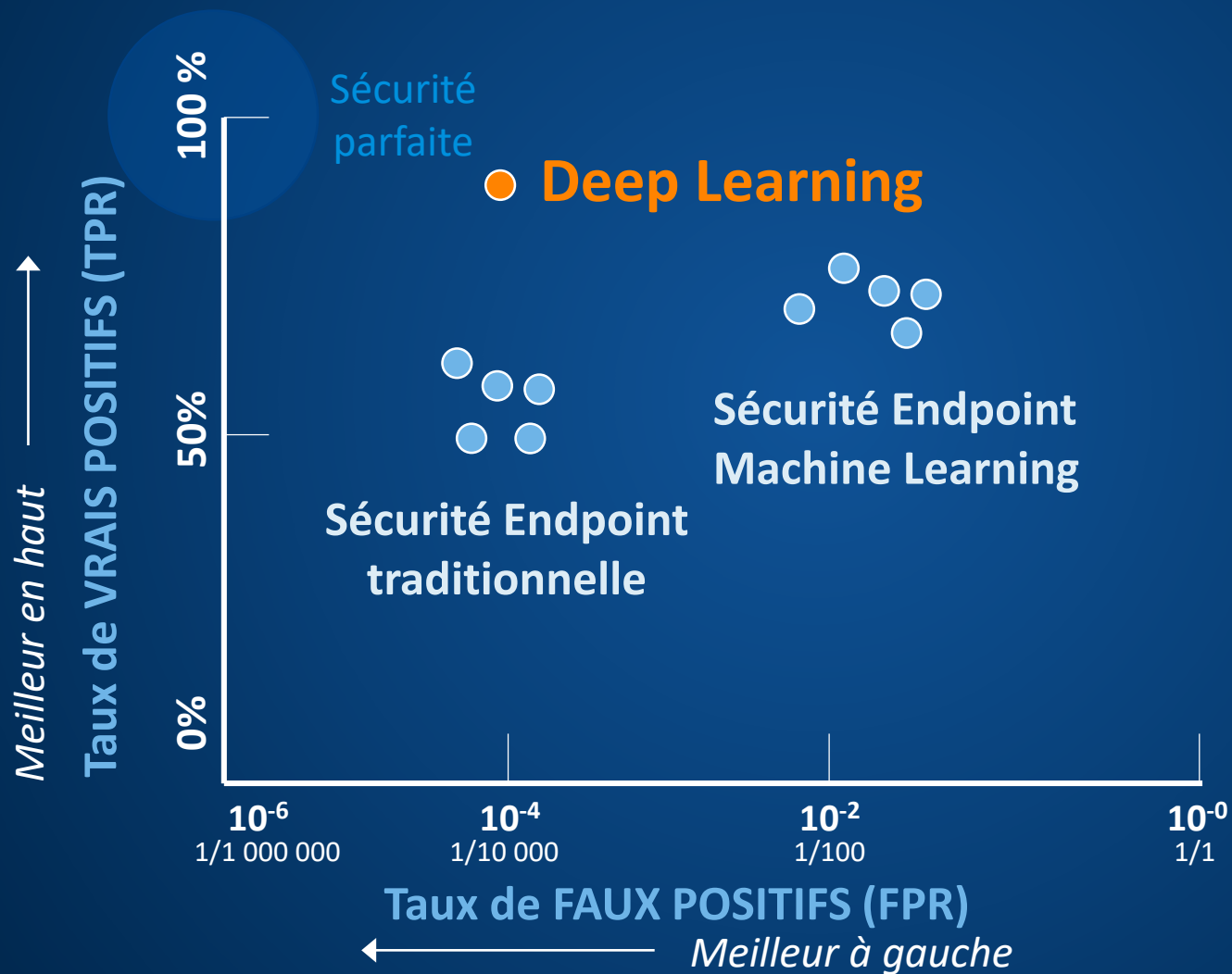
MAN-IN-THE-BROWSER



Prévient les modifications illicites du browser pouvant conduire à des attaques

Deep-Learning: bloquer les menaces inconnues

Meilleure protection, meilleure précision, meilleures performances



Meilleure protection



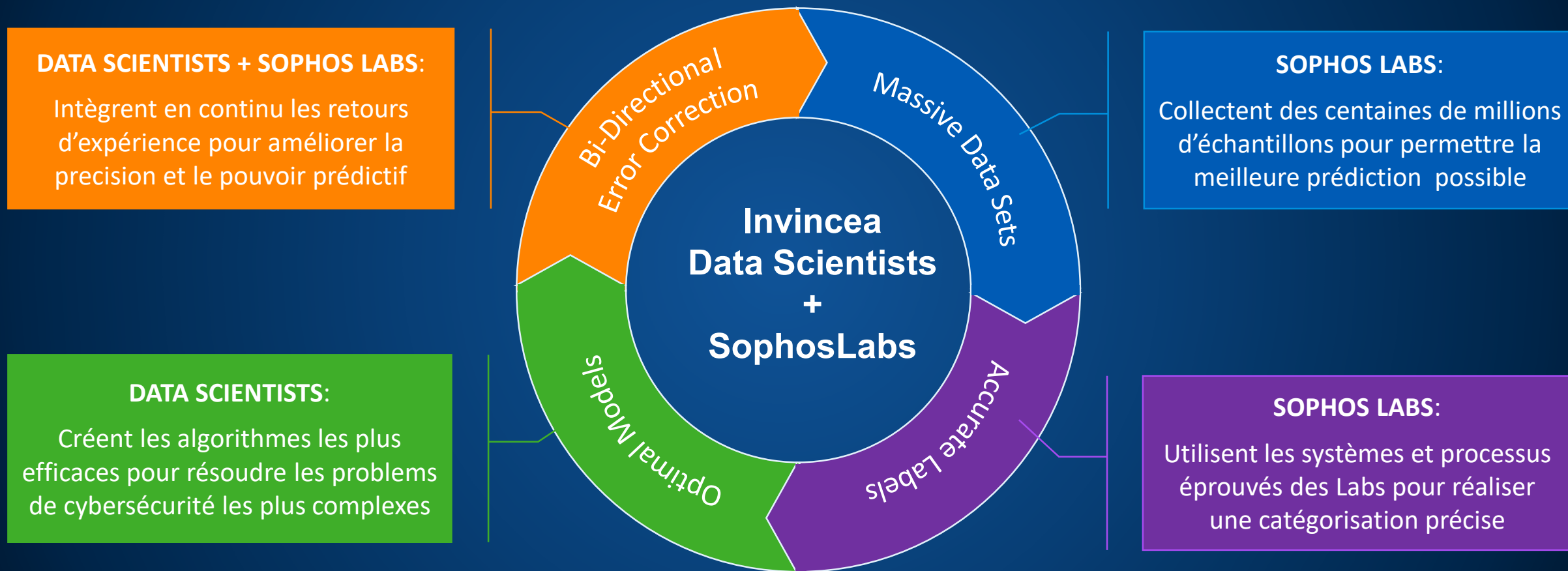
Meilleure précision



Meilleures performances

Deep-Learning: bloquer les menaces inconnues

L'union fait la force: Data Scientists Invincea + SophosLabs



“Pour la première fois, nous pouvons prendre en compte tout l'univers des données observables.”

XG Firewall – Bloquer l'infiltration

Bloque Emotet avant qu'il n'atteigne le réseau



Web and Email Protection



Sandboxing



Intrusion Prevention System



Application Control



Advanced Threat Protection



Synchronized Security

Malware Scanning

- Scan HTTP
- Decrypt & Scan HTTPS
- Detect zero-day threats with Sandstorm
- Scan FTP

Advanced

User Applications

Intrusion Prevention

LAN TO WAN

Traffic Shaping Policy

User's policy applied

Web Policy

Default Workplace Policy

Apply Web Category based Traffic Shaping Policy

Application Control

Block very high risk [Risk Level 5] apps

Apply Application-based Traffic Shaping Policy

Synchronized Security

Minimum Source HB Permitted:

- GREEN
- YELLOW
- No Restriction
- Block clients with no heartbeat

Minimum Destination HB Permitted:

- GREEN
- YELLOW
- No Restriction
- Block request to destination with no heartbeat

NAT & Routing

Rewrite source address [Masquerading]

Use Gateway Specific Default NAT Policy

Use Outbound Address

MASQ

MASQ [Interface Default IP]

Primary Gateway

WAN Link Load Balance

Backup Gateway

None

DSCP Marking

Select DSCP Marking



Sophos Sandstorm Sandboxing

Protection contre les menaces Zero Day et les menaces avancées



Deep Memory Analysis

01010000101001010011
10011010010000001010
01010010010010010100

Initial & Post Execution Memory Inspection & Analysis

Frequent & Aggressive Run-Time Analysis

Deep Behavioural Analysis



Sandbox Evasion Techniques, API & File System Behavior

Intercept X Exploit Detection & CryptoGuard

Deep Network Analysis



Full port and protocol analysis

IPS detections

Deep Learning Analysis



Analysis of all dropped executables

Continuously adaptive learning model

Sophos Sandstorm



Intrusion Prevention System (IPS)

L'équivalent réseaux de la détection des Exploits



Comment cela fonctionne-t-il ?

- Inspecte le trafic réseaux à la recherche d'exploits
- Détecte les exploits sur les systèmes d'exploitation, les piles réseaux, les serveurs, les systèmes Endpoints, les navigateurs, les applications, etc

Pourquoi Sophos ?

- NSSLabs: Top 3 pour l'Efficacité sécurité et la Performance
- Granularité des catégories pour optimiser la performance et la protection

SOPHOS
XG Firewall

MONITOR & ANALYZE
Control center
Current activities
Reports
Diagnostics

PROTECT
Firewall
Intrusion prevention
Web
Applications
Wireless
Email
Web server
Advanced threat
Central Synchronization

CONFIGURE
VPN
Network
Routing
Authentication
System services

SYSTEM
Profiles

Intrusion prevention

DoS attacks | **IPS policies** | Custom IPS signatures

Category: browser | Severity: | Platform: | Target: | Individual signature

SID	Category	Severity	Platform
2200304	Server-Webapp	2 - Major	Windows
9000495	Os-Windows	4 - Minor	Windows
9000496	Os-Windows	1 - Critical	Windows
1000070	Policy-Other	4 - Minor	

List of matching signatures [1 - 50 of 11206]

Action: Drop packet

Advanced Threat Protection (ATP)

Bloque la communication avec les pirates et l'exfiltration de données



- Web and Email Protection
- Sandboxing
- Intrusion Prevention System
- Advanced Threat Protection
- Application Control
- Synchronized Security

The screenshot shows the Sophos XG Firewall Control Center interface. The left sidebar contains navigation menus for 'MONITOR & ANALYZE', 'PROTECT', 'CONFIGURE', and 'SYSTEM'. The main dashboard area is titled 'Control center' and includes several widgets: 'System' (Performance, Services, Interfaces, VPN), 'Traffic insight' (Web activity, Cloud applications, Allowed app categories, Allowed web categories), 'User & device insights' (Security Heartbeat, Synchronized Application Control, Sandstorm, ATP, UTQ), 'Active firewall rules', 'Reports', and 'Messages'. A callout box highlights the ATP widget, which shows '2 Sources blocked'.



Contrôle des Applications

Visibilité complète sur la totalité du trafic applicatif



SOPHOS XG Firewall

Control center
XG230 [SFOS 17.5.0 Beta-2] C240773Y2QQXTCA

MONITOR & ANALYZE

- Control center
- Current activities
- Reports
- Diagnostics

PROTECT

- Firewall
- Intrusion prevention
- Web
- Applications
- Wireless
- Email
- Web server
- Advanced threat
- Central Synchronization

CONFIGURE

- VPN
- Network
- Routing
- Authentication
- System services

SYSTEM

- Profiles
- Hosts and services

System

Performance: 0/0 RED
Services: 3/3 Wireless APs
Interfaces: 0 Connected remote users
VPN: 5 Live users

CPU: 55% Memory: 39%
Bandwidth: 57KB/s Sessions: 34

High availability: Not configured
Managed by Sophos Central
Running for 24 day(s), 5 hour(s), 16 minute(s)

Traffic insight

Web activity: 349 max | 161 avg
Hits every 5 minutes

Cloud applications: 16 Apps, 555 MB In, 56 MB Out

Allowed app categories: Infrastructure (1,585.36M), Streaming Media (1,082.71M), File Transfer (400.92M), Unknown (280.02M), General Business (219.59M)

Network attacks: server-webapp (56)

Allowed web categories: Information Tec... (6.08K), None (1.9K), Personal Networ... (997), Web E-Mail (779), Video hosting (600)

Blocked app categories: General Internet (710), Software Update (195), File Transfer (2)

User & device insights

Security Heartbeat®: 1 At risk, 1 Missing, 0 Warnings, 2 Connected

Synchronized Application Control™: 4 New, 218 Categorized, 302 Total

Sandstorm: 0 Malicious, 0 Clean, 0 Total

ATP: 1 Sources blocked, UTQ: 2 Acc. for 80% of risk

Active firewall rules

Business: 2, User: 6, Network: 5, Total: 13

Unused: 2, Disabled: 1, Changed: 0, New: 0

Reports

- 9 Risky apps seen (Yesterday)
- 204 Objectionable websites seen (Yesterday)
- 2005 MB Used by top 10 web users (Yesterday)
- 112 Intrusion attacks (Yesterday)

Messages

- Alert: Managing firewall from Sophos Central (2w ago)
- Warning: HTTPS, SSH-based management is allowed from the... (9:46)

Synchronized Application Control™

4
New

218
Categorized

302
Total

DES CENTAINES

D'APPS NON VISIBLES AUPARAVANT

INCLUANT DES APPLICATIONS

MALVEILLANTES

PRÉSENTES

SUR VOTRE RÉSEAU

Sécurité Synchronisée

Automatisation de la corrélation et de la remédiation



1

Détection

Intercept X détecte l'exécution d'Emotet

2

Communication Endpoint-Firewall

Intercept X informe immédiatement XG Firewall du système sur lequel il a détecté Emotet

3

Isolement du poste infecté

XG Firewall isole automatiquement les systèmes infectés par Emotet.

- Isolement du monde extérieur
- Isolement des autres Endpoint



Security Heartbeat™



5

Accès restauré automatiquement

XG Firewall restaure automatiquement l'accès réseaux. L'investigation guidée fournit une analyse détaillée de toute les séquences de la chaîne d'attaque.

4

Nettoyage

Intercept X nettoie automatiquement l'infection. Une fois Emotet éradiqué, Intercept X partage cette information d'état avec XG Firewall

Démocratiser l'EDR avec l'IA

Endpoint Detection & Response + Deep Learning

Détecter et éradiquer les menaces latentes



Expertise augmentée par l'IA

Visibilité

Compréhension, priorités et actions à mener

Explorer

Identifier, enquêter et rechercher

Données

Corrélées, contextualisées et organisées



- **Expertise d'identification et de gestion des priorités**

Bloquer les menaces avant qu'elles ne frappent

- **Expertise d'analyse**

Comprendre et circonscrire le risque

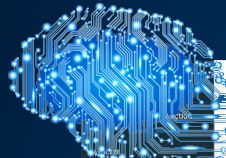
- **Réponse guidée aux incidents**

Activation des réponses sur un simple clic

Expertise cybersécurité augmentée par l'IA

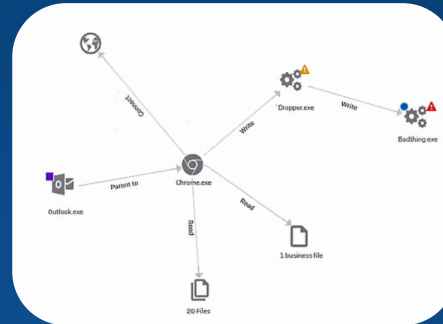
EDR: contribution du Deep Learning

Une journée dans la vie d'un analyste EDR



Date detected	Event name	Category	Threat score	Endpoints affected	Executed	Latest threat intelligence report
July 31, 2018 09:01 AM	Dropper.exe	PUJA	31	12	Yes	View
July 29, 2018 12:04 PM	Quiver.exe	Milware	25	3	No	View
July 26, 2018 10:57 AM	DancingCat.exe	PUJA	23	23	No	View
July 04, 2018 08:07 AM	Twitterbot.exe	PUJA	22	48	No	View
July 03, 2018 5:37 PM	Adware\WSPOR.exe	PUJA	18	54	No	View
June 28, 2018 2:19 PM	Patched Generic.B33	Milware	17	11	Yes	View
June 19, 2018 3:12 PM	Filewordthawaterig1	Milware	17	2	No	View

Identifier les "événements" suspects à examiner, tels que Dropper.exe



Examiner la chaîne d'attaque ayant mené à l'identification de Dropper.exe

Endpoint Protection - Threat Search Results

Search for Dropper.exe running... [complete]
Searched by SHAD56: 2f294da6f02a026a8b232c959e9d3131261c1a7d57a70439202080824
Found on 4 devices

Name	Company	Admin isolated	First run	Last status	Path	Actions
Dropper.exe	ESHAHMA	No	Apr 10 2018 3:56AM	Apr 10 2018 4:03 AM File modified	c:\program files\path name	Actions
virusbyteshack.exe	AJAXNETPC	Yes	Apr 10 2018 3:56AM	Apr 10 2018 4:03 AM File modified	c:\program files\second path name	Actions
virusbyteshack.exe	CANONICUP	No		Apr 10 2018 4:03 AM File modified	c:\program files\third path name	Actions
virusbyteshack.exe				Apr 10 2018 4:03 AM File modified	c:\program files\fourth path name	Actions
virusbyteshack.exe				Apr 10 2018 4:03 AM File modified	c:\program files\path name which is long and ends in the same way	Actions

Trouver tous les endroits où Dropper.exe est présent

Process details: dropper.exe

Process ID: 8888

Process path: c:\program files\path name

Process ID: 8888

Process path: c:\program files\path name

Process ID: 8888

Process path: c:\program files\path name

Obtenir une analyse détaillée des SophosLabs

Process details: dropper.exe

Code analysis: 100% analyzed

Code analysis: 100% analyzed

Code analysis: 100% analyzed

Analyser le code pour déterminer si le fichier est malveillant

Create forensic snapshot

Cleaned	Path	Actions
No	c:\program files\path name	Actions Clean and block Generate threat case Request threat intelligence report
No	c:\program files\path name	Actions

Remédier à la menace: bloquer, nettoyer et prévenir

Démocratiser l'EDR avec le Deep learning

Investigation guidée et analyse détaillée grâce au Deep Learning



SOPHOS CENTRAL Admin

Endpoint Protection

Endpoint Protection - Mal/ML-PE

Overview / Endpoint Protection Dashboard / Threat Cases / Mal/ML-PE

Marcus Jones - ABC Corp - Primay Admin

WMorrisPC 11.222.33.45

Outlook.exe

Badthing.exe

Detected Apr 12 2017 5:46AM

Blocked and cleaned Apr 12 2017 5:46AM

Summary

Malware detected: Mal/ML-PE at C:\program files\WMorris\badthing.exe

On: WMorrisPC that belongs to William Morris

Condition: RAN CLEANED BUSINESS FILES INVOLVED

1 1 1

Detection summary: The root cause tried to access a URL known to be associated with malware

Suggested next steps

- Set status and priority for the case
- Investigate 1 process we've marked with an "uncertain" reputation. See graph below for details
- Isolate the computer while you investigate.
- Scan the computer

DETAILS

Analyze Activity record

Showing Processes (4) Files (21) Network connections (1) Registry keys (0)

Click here for IX only version

Dropper.exe

Write

Badthing.exe

SOPHOSLABS Threat Intelligence

Request latest intelligence

No current intelligence on this file.

Note: Requesting the latest intelligence will cause your files to be sent to Sophos for additional analysis. Learn More

Path: c:\windows\syswow64\netsh.exe

Name: netsh.exe

Command line: netsh.exe advfirewall firewall delete rule name="Remote Assistance (50383)"

Process ID: 252

Process executed by: NT AUTHORITY\SYSTEM

Process details: fakedrop-cli.exe

Process details Report summary Machine learning analysis File properties File breakdown

SOPHOSLABS Threat Intelligence

Current report created: Oct 4, 2018 3:43 PM

Attributes: 84% Suspicious

Analyzed over 29 million known good and over 15 million known bad items

Attribute	Seen in:	Known bad files	Known good files
Imports -> Enumerates local disk drives		50.6k	118.7k
Imports -> [] The program may be hiding some of its i...		554.2k	916.1k
Imports -> [] The program may be hiding some of its i...		665.9k	1.2M
Findcrypt -> "Uses constants related to CRC32"		82.1k	187.6k
Imports -> [] The program may be hiding some of its i...		161.2k	307.9k

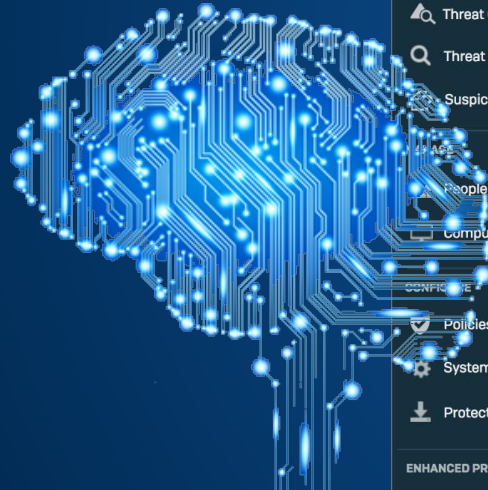
Code Similarity: 76% Suspicious

Analyzed over 30 million known good and over 29 million known bad items

File	Similarity
n/a	53%
runeplus.exe	47%
timeclick console.exe	47%
No file name	44%
s-000000737868.exe	41%
pyportify-copyall.exe	41%
ps4-exploit-host.exe	41%

Démocratiser l'EDR avec le Deep learning

Détection et organisation des priorités grâce au Deep Learning



SOPHOS CENTRAL Admin

Endpoint Protection

ANALYZE

- Dashboard
- Logs & Reports

DETECTION AND REMEDIATION

- Threat Cases
- Threat Searches
- Suspicious Events **BETA**

CONFIGURE

- Policies
- System Settings
- Protect Devices

ENHANCED PROTECTION

- Explore Products

Dashboard

Overview / Endpoint Protection Dashboard

Marcus Jones (ABC Corp - Primay Admin)

Most Recent Threat Cases

See all cases

CREATED ON	PRIORITY	TYPE	NAME	CONDITION	USER	DEVICE
Apr 18, 2016 12.23PM	High	Malware detected	Mal/ML-PE	Blocked and cleaned	William Morris	WMorrisPC
Apr 17, 2016 12.23PM	Medium	Exploit	Exploit Lockdown	Cleaned up	Brian Jones	BrianJComp
Apr 16, 2016 12.23PM	Low	Malicious traffic	Tro/PDFJs-AIA	Blocked	Brian Jones	BrianLaptop
Apr 15, 2016 12.23PM	High	Ransomware	Exploit Cryptoguard	Running	Eryn Havers	ErynMac
Apr 14, 2016 12.23PM	High	PUA	Troj/Loic-A	Clean up needed	Gina Baker	Gina Comp

Top Suspicious Events **BETA**

See all events

NAME	DETECTED ON	THREAT SCORE	ENDPOINTS AFFECTED
Dropper.exe	July 31, 2018 09:01 AM	31	12
Quiver.exe	July 29, 2018 12:04 PM	25	3
DancingCats.exe	July 20, 2018 10:57 AM	23	23
Tweetbot.exe	July 04, 2018 09:07 AM	22	46
Adware.WPSOffice	July 03, 2018 5:37 PM	19	54
Packed.Generic.533	June 28, 2018 2:19 PM	17	11

Threat Search

Search for potential threats on your network

Enter one or more SHA 256 file hashes or file names,

Searches on hashes or file names will return portable executable files with uncertain reputation.

Un seul agent ... pour une protection complète

Agent Endpoint unique = Protections classiques + Next-Gen



Technologies classiques

Technologies Next-Gen



Prévenir

Corréler les indicateurs de menaces pour bloquer les menaces web, les applications illégitimes, les URLs dangereuses et les codes malicieux avant exécution.



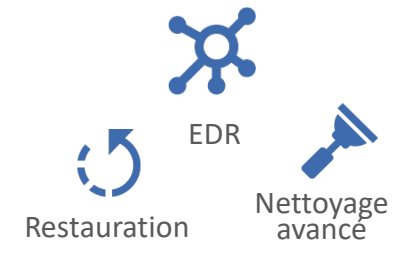
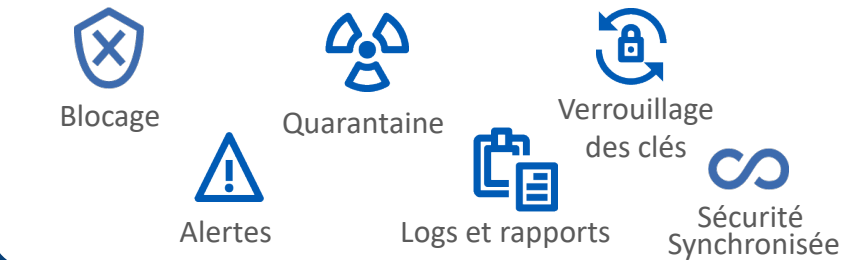
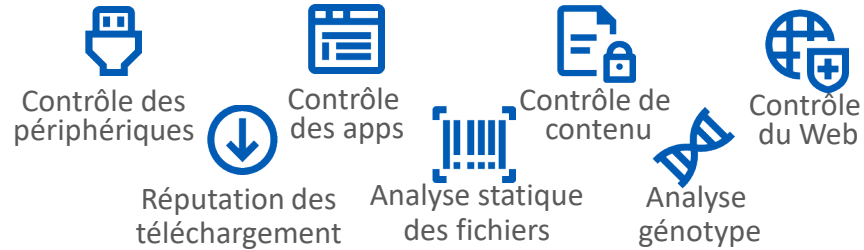
Détecter

Analyser le comportement à l'exécution des codes et du trafic réseau, vous alertant en cas de menaces cachées.



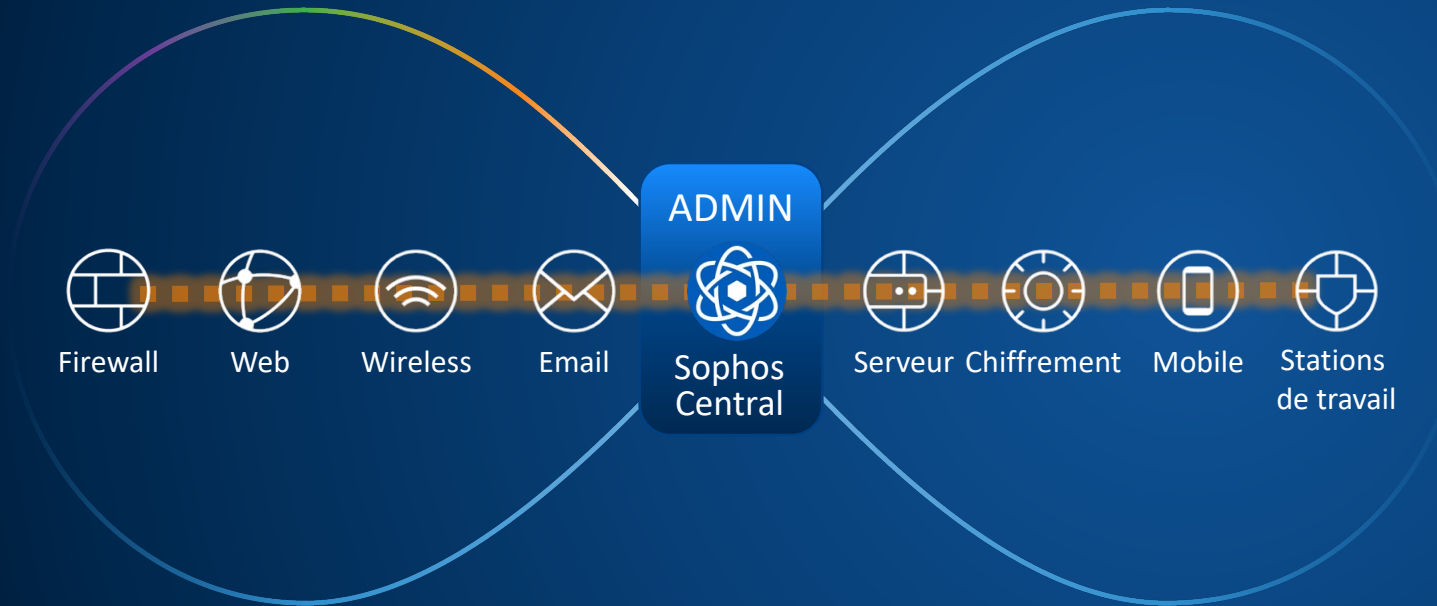
Répondre

Supprime les malwares, isoler les systèmes compromis, rechercher les menaces latentes, remédier et prévenir les attaques



Un seul agent ... synchronisé

Sécurité synchronisée avec l'ensemble de l'infrastructure



SOPHOS

Cybersecurity made simple.