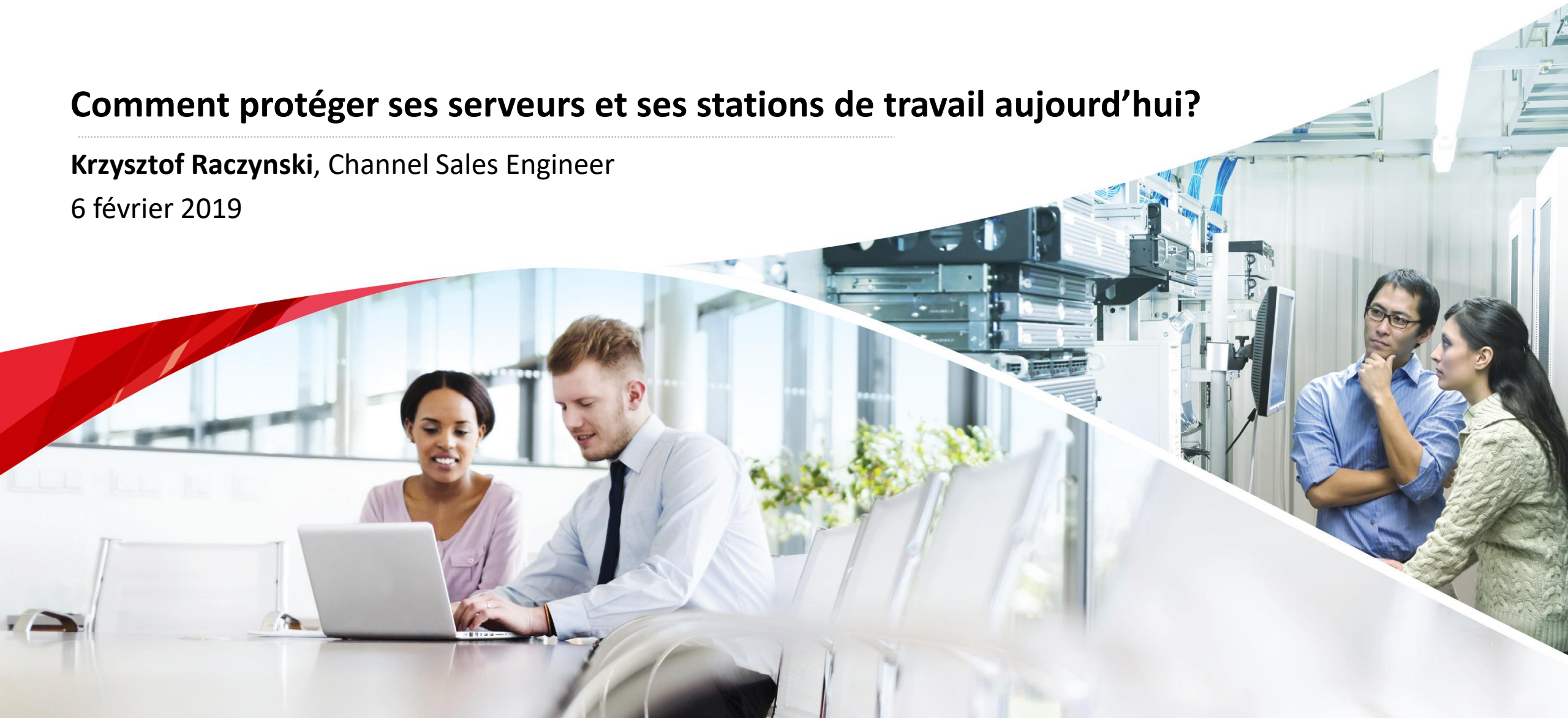
Comment protéger ses serveurs et ses stations de travail aujourd'hui?

Krzysztof Raczynski, Channel Sales Engineer

6 février 2019



Société Trend Micro

Leader de solutions globales de sécurité

- + de 30 ans d'activité dans la sécurité informatique
- Siège social à Tokyo au Japon
- Cotation au Nikkei
- Chiffre d'affaires 2017: 1,5 Mrd $
- + de 6000 employés, présents dans 50 pays dans le monde
- Protège 45 du top 50 des société mondiales

Grandes Entreprises

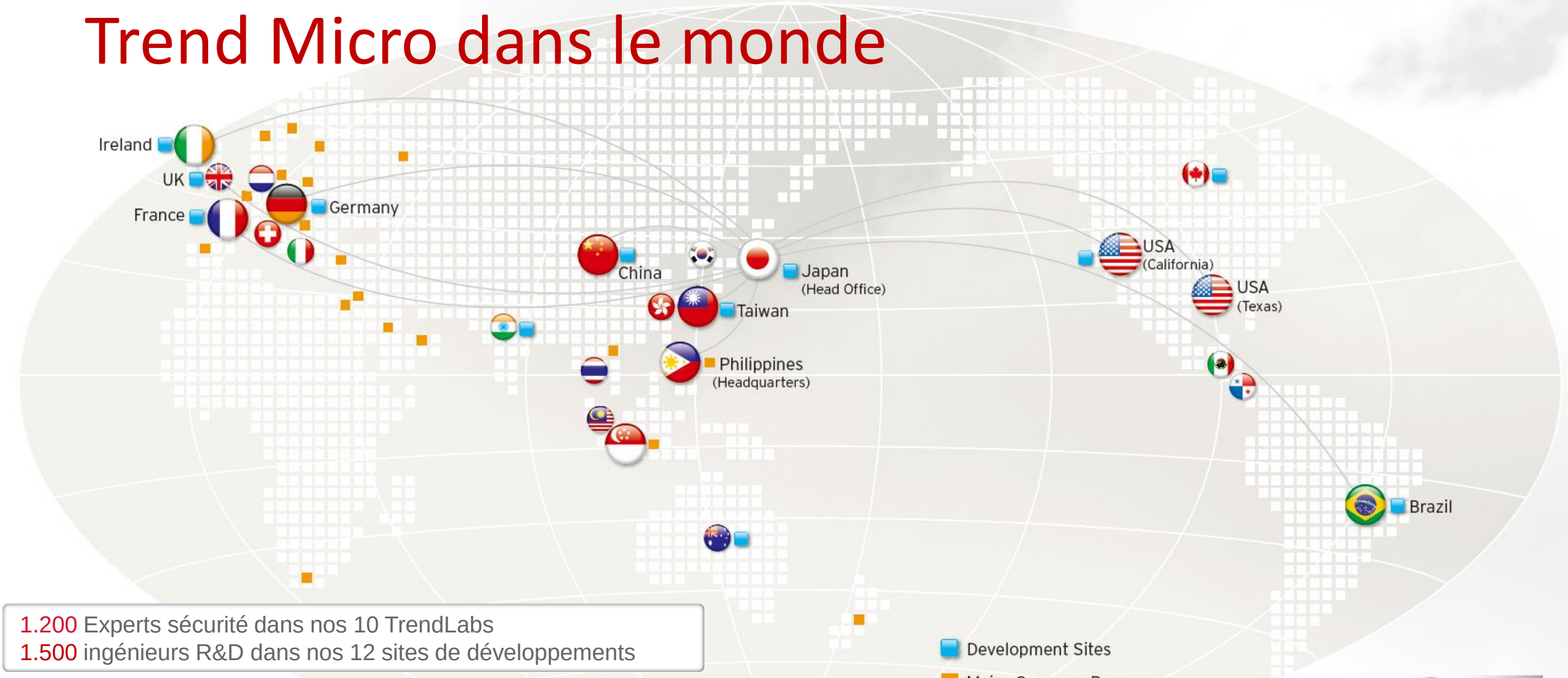
Moyennes Entreprises

TPE et PME

Particuliers

+ 500k clients &
+ 250M postes protégés

Trend Micro dans le monde



1.200 Experts sécurité dans nos 10 TrendLabs
1.500 ingénieurs R&D dans nos 12 sites de développements

Head Office	Japan											
TrendLabs Regional Trend Labs	Philippines (Headquarters)	USA	Japan	Taiwan	Germany	Ireland	China	France	Brazil	Singapore		
Development Sites	Japan	USA	Canada	Germany	UK	Taiwan	China	India	Australia	Ireland	France	Brazil

TrendLabs Philippines received ISO 20000-12005 certification for adhering to IT service excellence in compiling malicious software information, detection and cleanup procedures, and technical services.

Notre histoire
30 ans d'innovation

1995:
Sécurité des serveurs LAN

1996:
Sécurité des passerelles

2008:
Réputation

2010:
Intégration de la virtualisation

2012:
Défense personnalisée (Sandboxing)

2015:
Défense interconnectée

2016:
XGen™

PORTFOLIO TREND MICRO

PROTECTION DES SERVEURS

Deep Security

ServerProtect For Storage

PROTECTION DES RESEAUX INDUSTRIELS

Safe Lock

Portable Security

PROTECTION COLLABORATIF

PortalProtect for Ms SharePoint

IM Security for Skype/Lync

PRODUITS SAAS

IWSaaS

HES

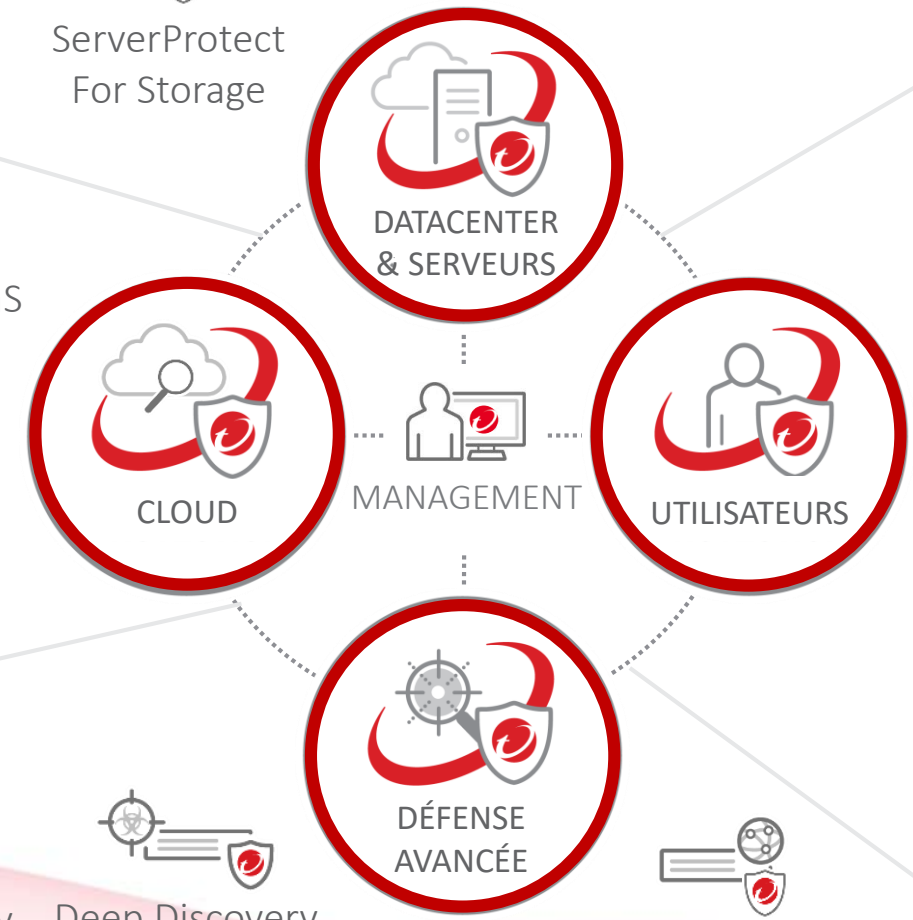
Apex One SaaS

DDAN SaaS

PROTECTION DES RESSOURCES CLOUD

Deep Security as a Service

Cloud App Security



PROTECTION WEB

IWSVA

PROTECTION MAIL

IMSVA

ScanMail Exch. / Lotus

PROTECTION DES ENDPOINTS

Mobile Security

Apex One

EPP				EDR
Files Reputation	Web	Virtual Patching	Sandbox	Investigation
Machine Learning	BM	App Control	DLP & Device Control	Isolation / Quarantine

Deep Discovery Analyzer

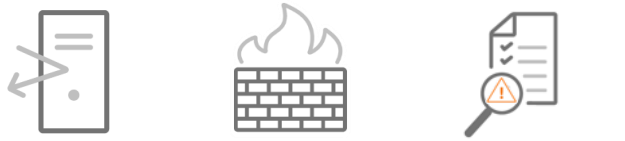
Deep Discovery Email Inspector

Deep Discovery Inspector

TippingPoint IPS

DeepSecurity – Protection modulaire

Network Security



Intrusion Prevention | Firewall | Vulnerability Scanning

Arrêter les attaques/propagations réseaux, protéger les applications & serveurs vulnérables

System Security

Application Control | Integrity Monitoring | Log Inspection

Verrouillage des systèmes & détection des activités suspects

Malware Prevention

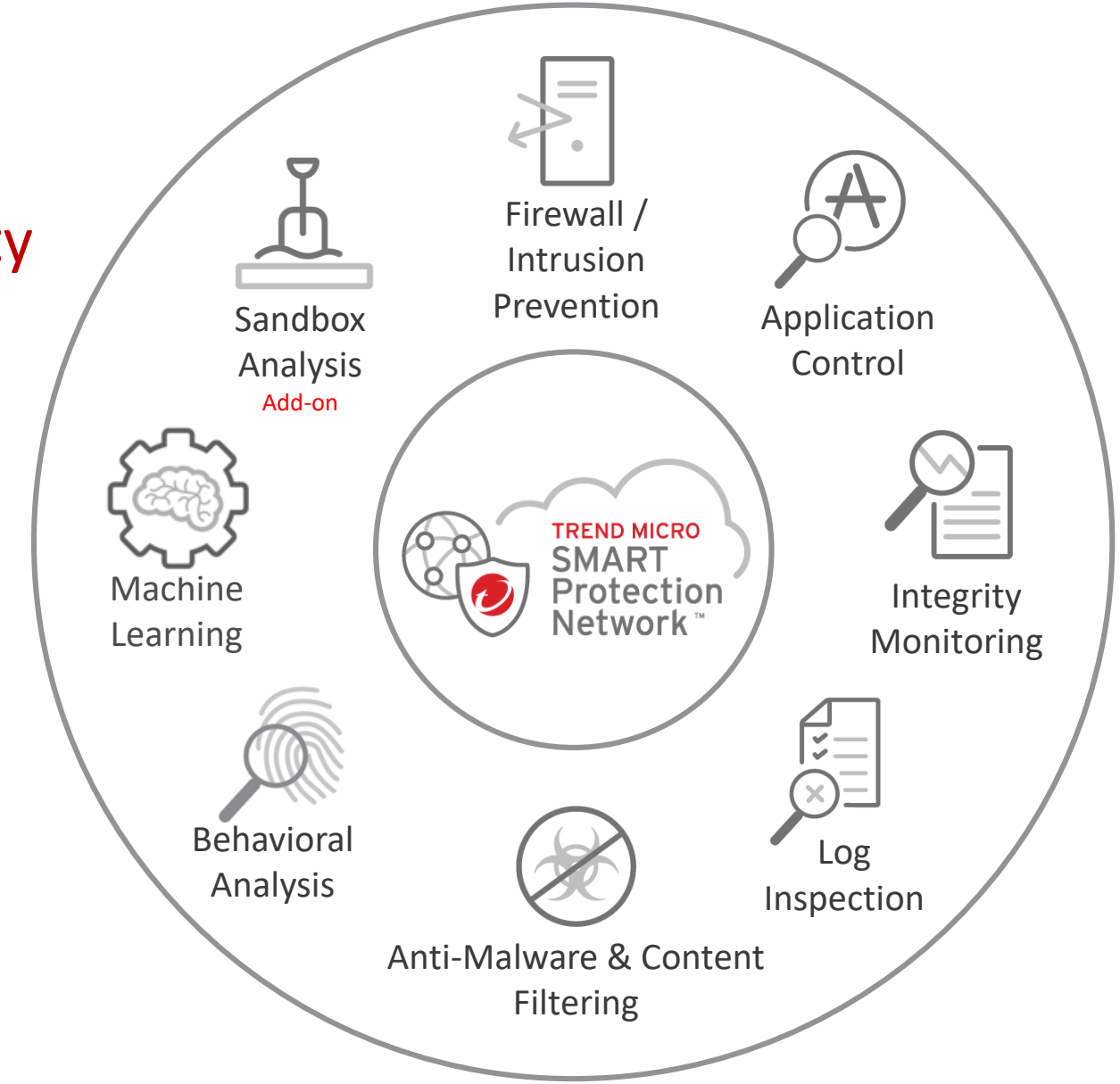
Anti-Malware | Behavioral Analysis & Machine Learning | Sandbox Analysis

Stop les malwares & attaques ciblées

vmware | Microsoft Hyper-V | openstack CLOUD SOFTWARE | amazon web services | Google Cloud Platform | docker | NUTANIX | VCE | SAP | Microsoft Azure | IBM | TREND MICRO

Network Security

Protection système et réseau complète grâce à une approche modulaire



Network Security

Intrusion Prevention

Protection contre les menaces réseau et applicative

Firewall

Stop les mouvements latéraux et réduit la surface d'attaque des serveurs

Vulnerability Scanning

Scan automatique des vulnérabilités & application des politiques

Protection des vulnérabilités OS & applications
(ex: Struts 2, Shellshock, Heartbleed, Ethernalblue …)

Détecte & stoppe les ransomwares (ex: WCRY)

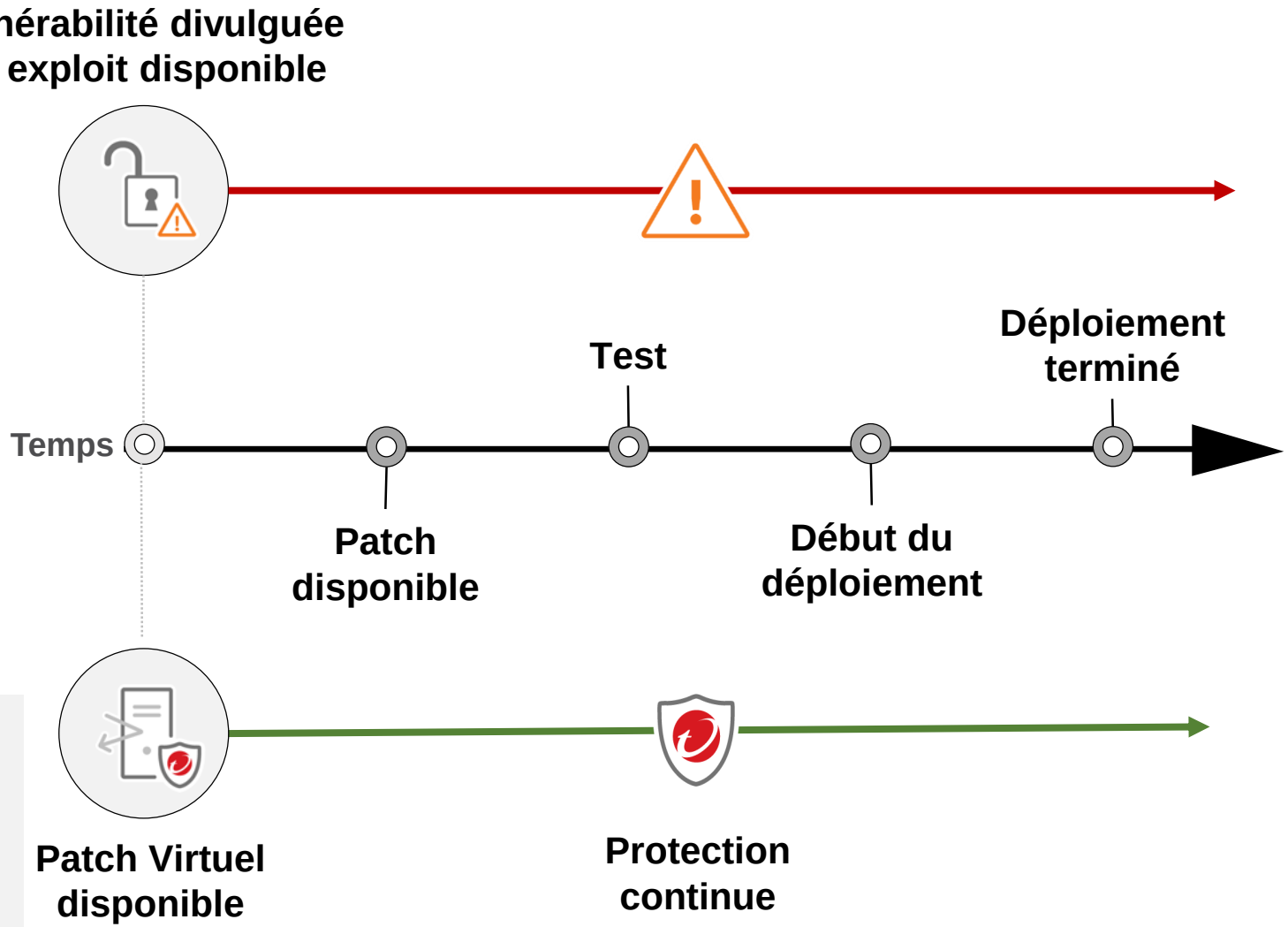
Réduction des campagnes de patch en urgence

Couverture des systèmes & applications en fin de vie

Réduction des impacts opérationnels

ZERO DAY INITIATIVE

- Réduire les coûts opérationnels dans l'urgence & correctifs en cours
- Protéger les systèmes où aucun correctif n’est fourni
- Sécurise les OS et applications vulnérables

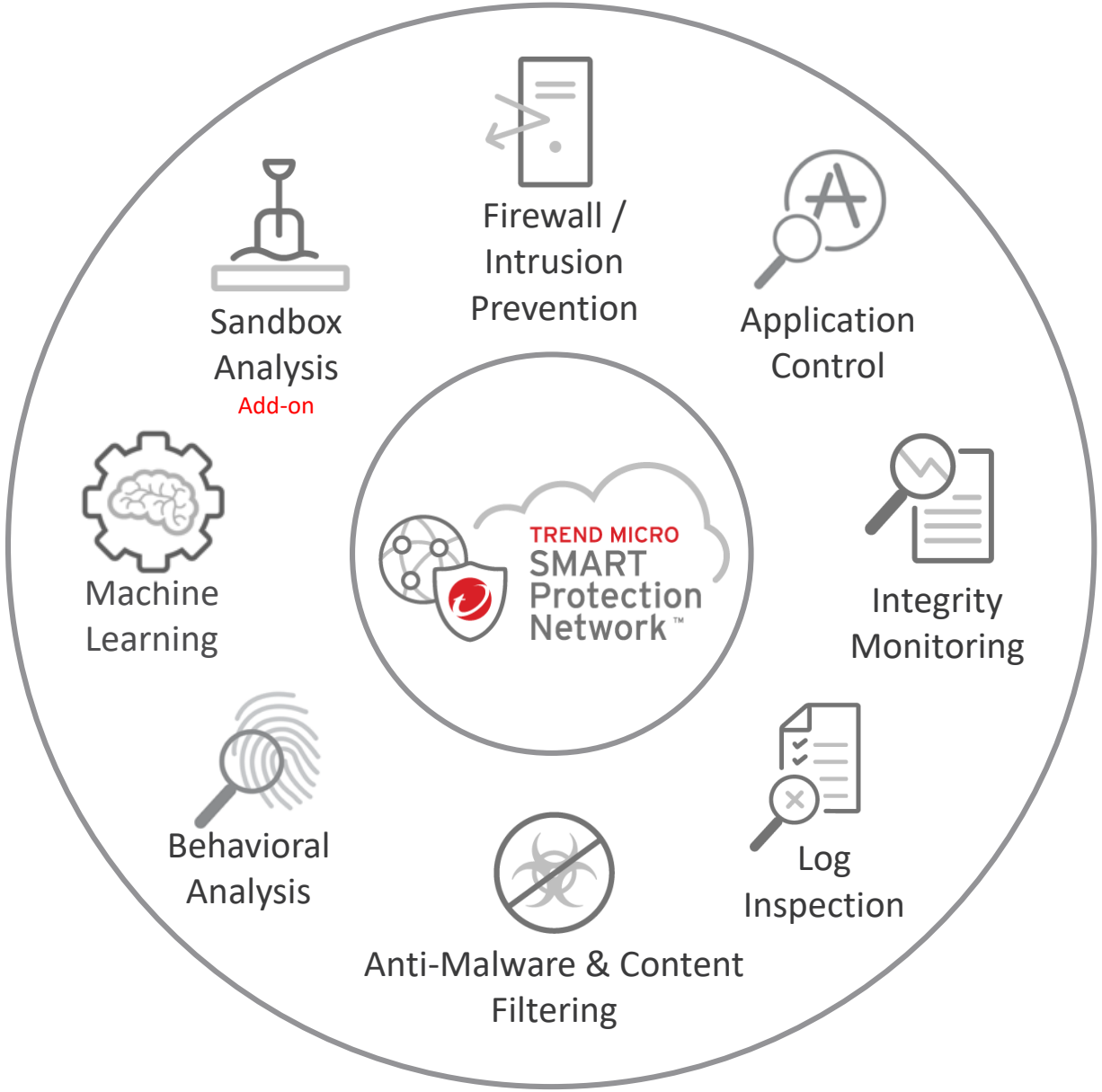


La protection du ransomware WannaCry a été disponible dès mars 2017, avec des améliorations lors de la divulgation publique (mai 2017)

TREND MICRO

System Security

Protection système et réseau complète grâce à une approche modulaire



System Security

Application Control

Verrouillage des serveurs et prévention des changements (whitelisting)

Integrity Monitoring

Détection des changement suspects ou non-autorisés sur les fichiers, ports, clés de registre …

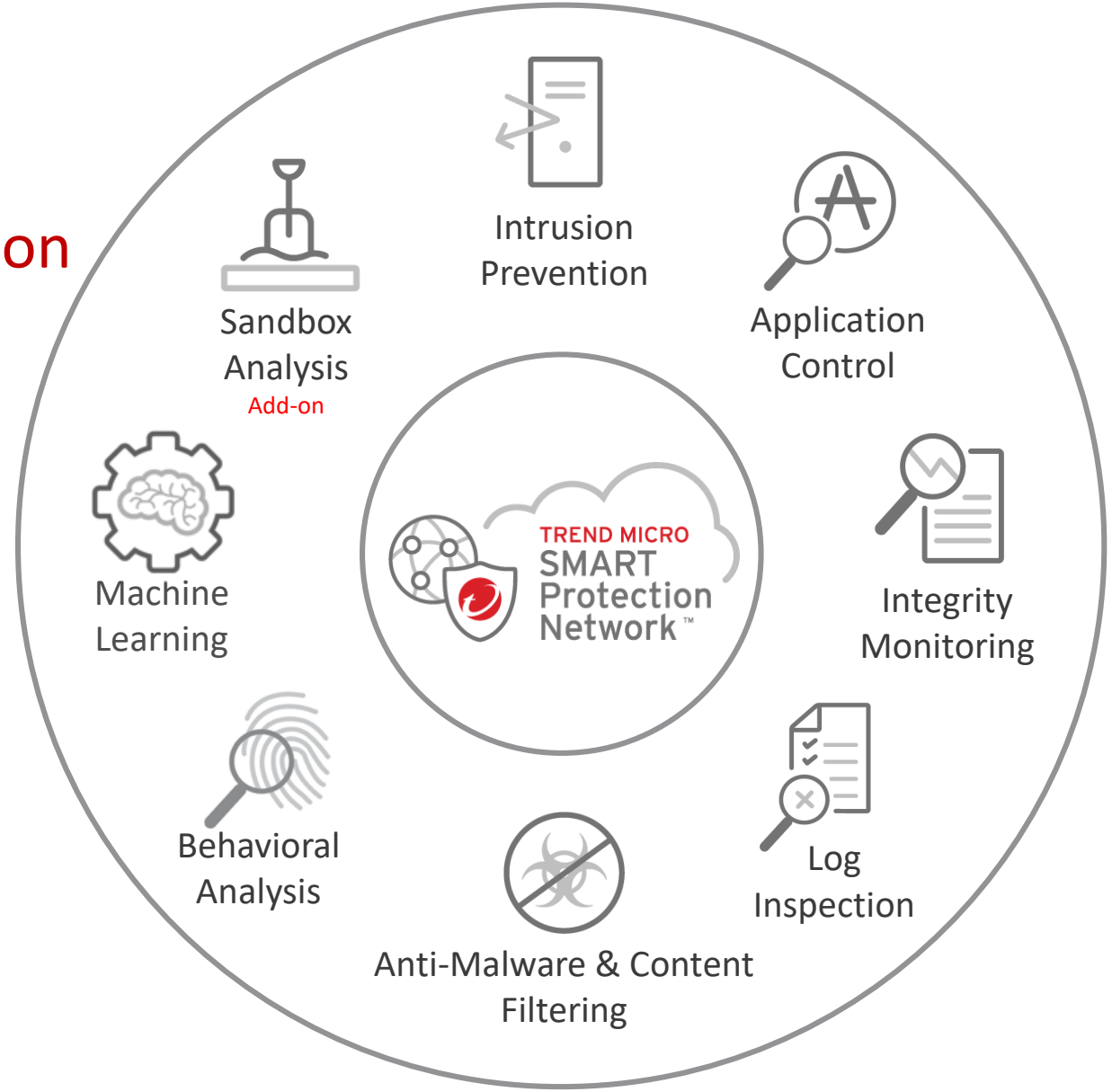
Log Inspection

Consolidation / alertes basées sur les logs systèmes et applicatifs

- Protection automatique contre les comportements malicieux type ransomware
- Intègre la sécurité au process DevOps et CI/CD
- Réduire la surface d'attaque et permet de satisfaire la mise en conformité
- Détection des indicateurs de compromission (IOC)

Malware Prevention

Protection système et réseau complète grâce à une approche modulaire



Malware Prevention

Anti-Malware & Content Filtering

Détection / blocage des malware connus

Arrête les malwares et les attaques avancées

Behavioral Analysis

Machine Learning

Détection des fichiers et comportements suspects, stoppe les changements malicieux

Détecte & arrête les ransomwares (ex: WannaCry)

Stopper les attaques zero-day

Sandbox Analysis

Envoi les objets suspects aux sandbox personnalisées

Analyse les menaces inconnues & partage au travers des solutions de sécurité


Trend Micro **Apex One™**

Redéfinition de la sécurité des Endpoints

Automatique

Détection & Réponses efficace

Technologie moderne pour bloquer les dernières menaces (incl. sans fichier)

Fonction de Virtual Patching reconnue par le secteur

Clairvoyance

Visibilité & contrôle centralisés de toutes les fonctions

Option d'investigation EDR pour rechercher les causes et chasser les menaces

Option de service SDR* pour renforcer les équipes sécurité (SOC)

Tout-en-un

Sécurité des Endpoint & EDR ensemble dans un seul agent

Pas besoin de plusieurs fournisseurs (agents) sur le même Endpoint

Versions On-premise et SaaS identique (SaaS en 1er)

* H1 2019

Points d'entrée

Site Malicieux

Réputation Web
Blocage des connexions au niveau noyau (et pas seulement au niveau du navigateur)

Exploit de vulnérabilité de l'OS

Patching Virtuel
Bloque les nouveaux exploits avec le #1 de recherche des vulnérabilités

Exploit des navigateurs

Protection du navigateur
Détecte les exploits basés sur l'inspection des script & le comportement des sites

Clef USB malicieuse

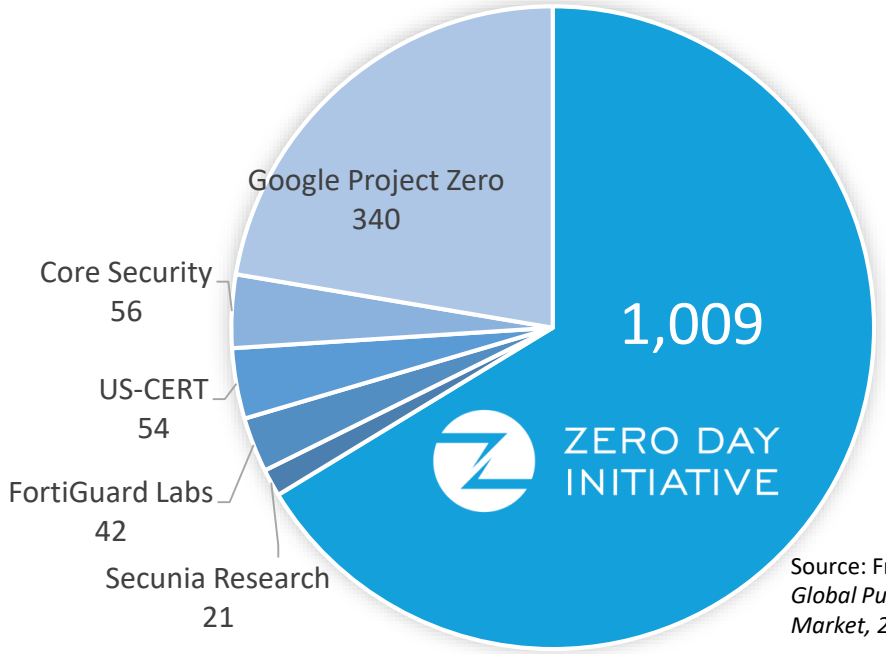
Contrôle des périphériques
Bloque les périphériques de support amovibles inconnus

ZERO DAY INITIATIVE

En 2017, Trend Micro ZDI a détecté 66% de toutes les vulnérabilités. Cela nous permet le meilleur Patching virtuel.

66.3% de vulnérabilités découvertes en 2017

LEADER dans la découverte de vulnérabilités depuis 2017



Source: Frost & Sullivan. *Analysis of the Global Public Vulnerability Research Market, 2017.* February 2018.

ZERO DAY INITIATIVE

R&D Trend Micro

- Menaces
- Vulnerabilités & Exploits
- Attaques ciblées
- AI & Machine Learning
- IoT
- OT / IIoT
- Réseaux Cybercriminels
- Future Threat Landscape

TELUS Security Labs (maintenant gérés Par Trend Micro)

TREND MICRO

Pré-exécution

Menaces basée sur les fichiers
ex. EXE, DLL, Document Office avec macros

Détection des Packers
Identifie les logiciels malveillants empaquetés en mémoire lors de leur décompression, avant leur exécution

Machine Learning à la pré-exécution NOUVEAU sur Mac
Evalue les fichiers par rapport à un modèle basé dans le cloud ou local / hors ligne pour détecter les menaces inconnues NOUVEAU

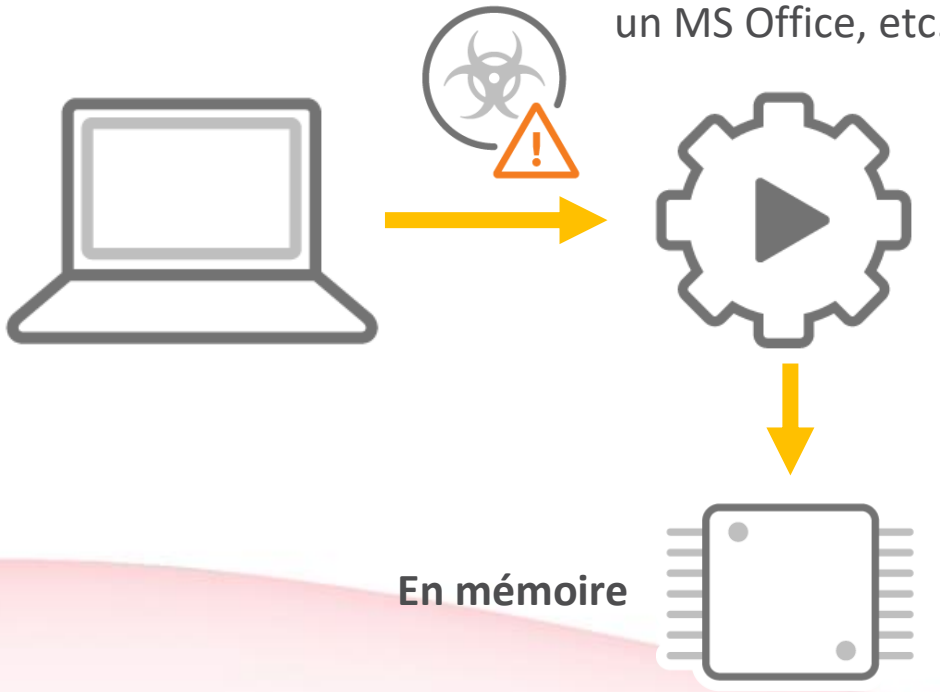
Contrôle des Applications
Bloque l'exécution de tout ce qui ne figure pas sur la liste blanche (simple à utiliser)

Protection contre les Variantes
Détecte les mutations des codes malveillants en reconnaissant des fragments connus de ceux-ci

Signatures basé sur les fichiers
Détecte les fichiers malveillants connus
(+ de 3 milliards de détections H1/2018)

Exécution

Tout ce qui s'exécute
EXE, DLL, PowerShell, Comportement des documents dans un MS Office, etc.



Machine Learning à l'exécution
Analyse le comportement en temps réel par rapport à un modèle basé dans le cloud pour détecter des menaces auparavant inconnues

Analyse comportementale des IOA AMELIORATION
Détecte les comportements correspondant aux indicateurs d'attaque connus (IOA), y compris le chiffrement des ransomwares et le lancement de scripts

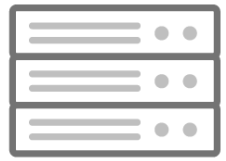
Analyse d'exécution en mémoire AMELIORATION
Détection de scripts malveillants, d'injection de codes malveillants, détection de décompression à l'exécution

Point de sortie

Réputation Web
Blocage des connections au niveau noyau (et pas seulement au niveau du navigateur)

Serveur de commande et contrôle

Prévention d'intrusion sur l'hôte
Détecte et bloque le comportement des mouvements latéraux

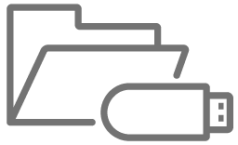


Mouvements latéraux

Détection de l'exfiltration des données
Le module DLP détecte et bloque les données sensibles sortant de l'ordinateur.

NOUVEAU sur Mac

Contrôle des périphériques
Bloque les périphériques de support amovibles inconnus



Exfiltration des données

Réponse Automatique

Isolation
Mise en quarantaine
Mettre fin au processus suspect
Bloquer l'exécution
Retour en arrière (nettoyage)
Interactions via API **Etendues**
Mises à jour rapides de la protection de la réponse sur d'autres terminaux / produits* **Etendues**

*manuelle

Capacités d'investigations puissantes (EDR)

Investigation:

Recherche d'IOC **NOUVEAU sur Mac**

(Recherche des métadonnées côté serveur) **NOUVEAU**

Identification du patient Zéro /

Analyse de la ''Root Cause''

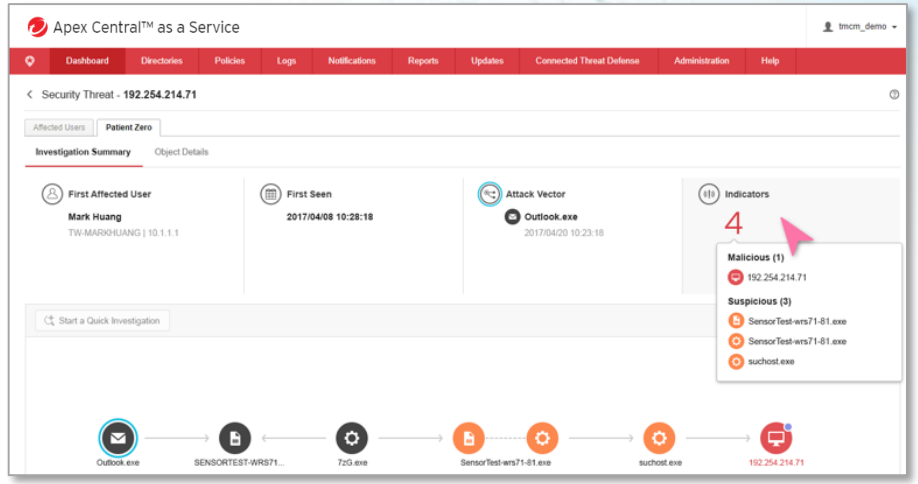
Détection et recherche des IOA

Automatisation via requête API **ETENDU**

Service Support SDR(Win/Mac)

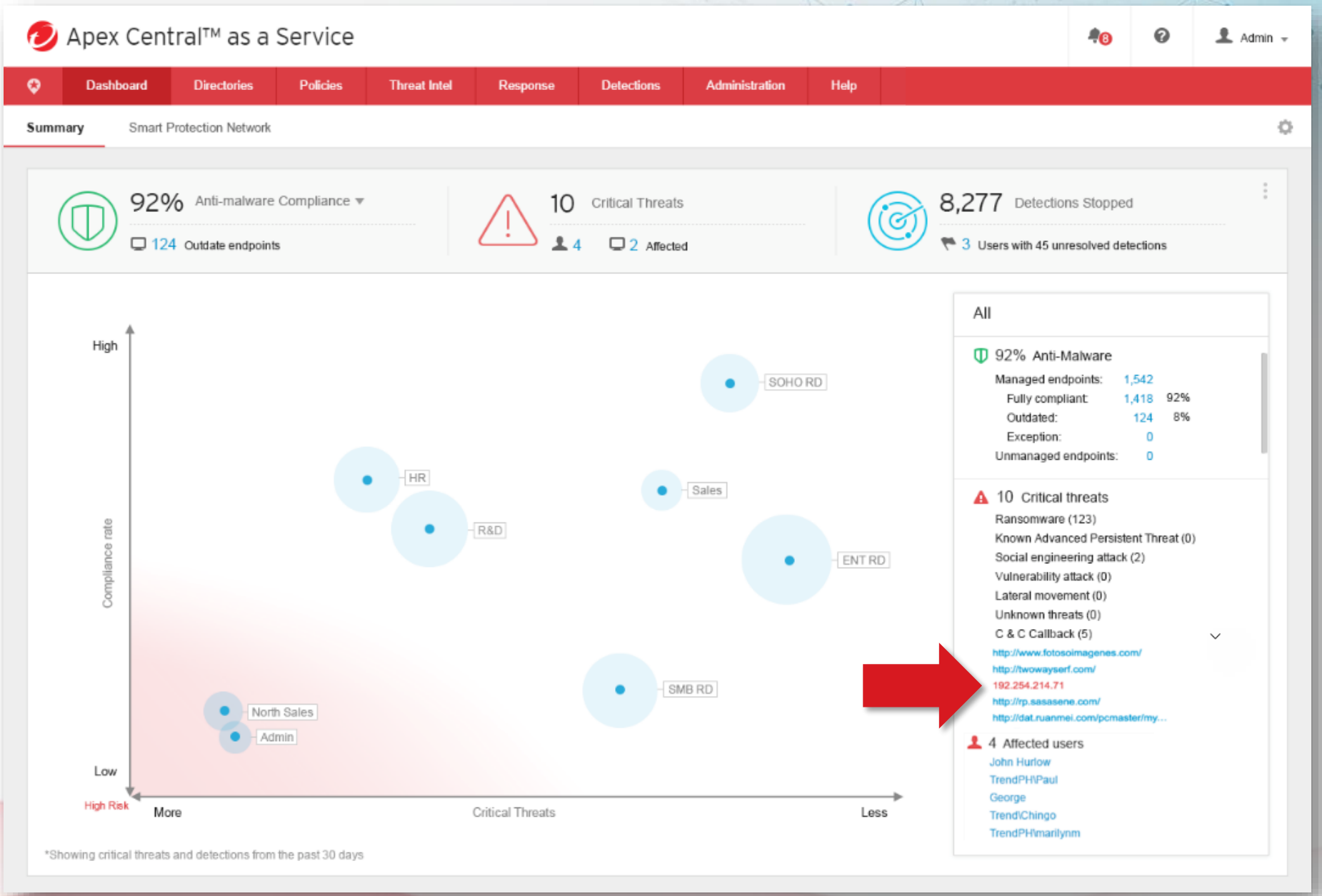
UX moderne avec guidage hiérarchisé

Guide de fichier inconnu **NOUVEAU**



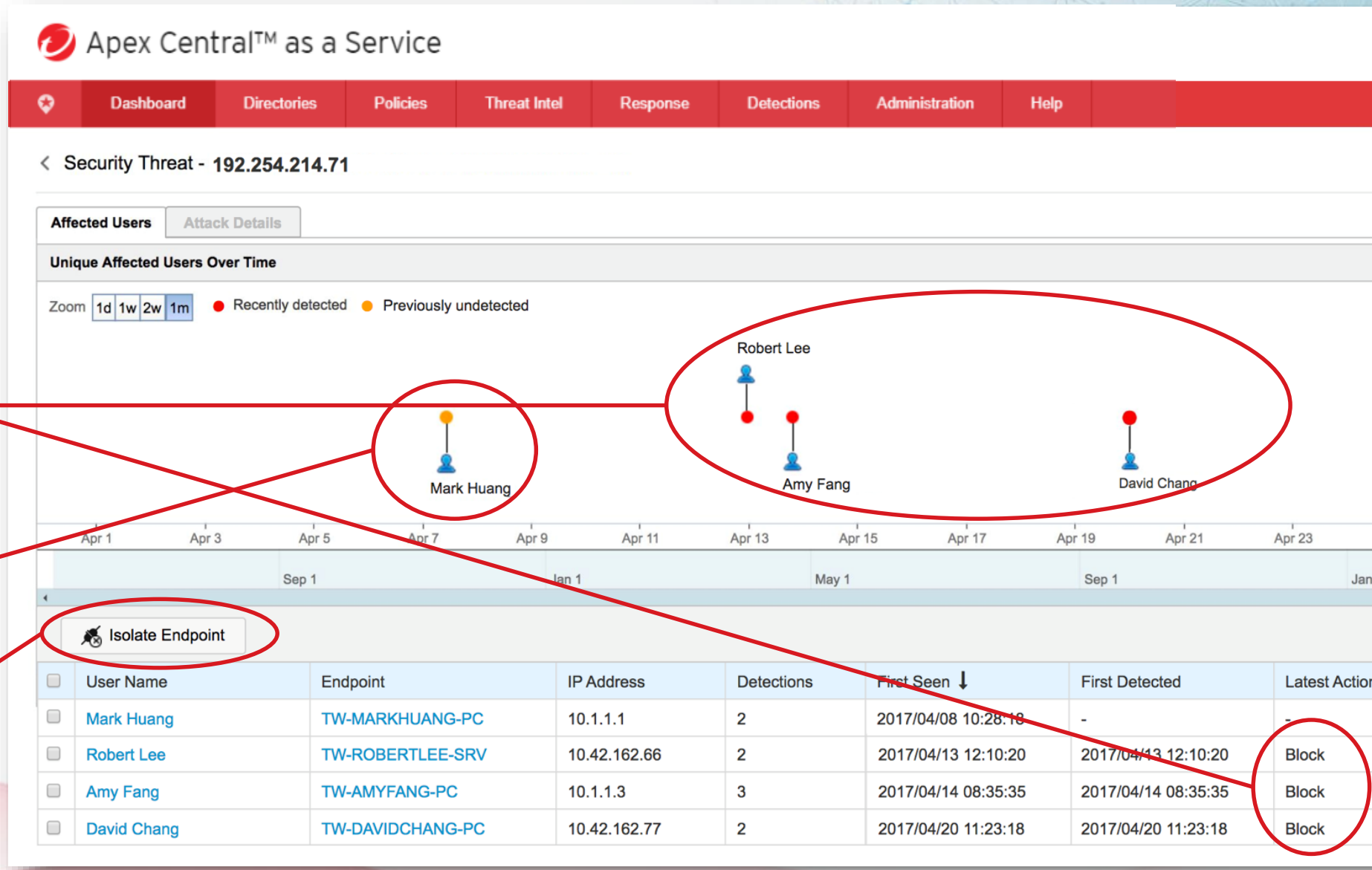
Détection et réponse totalement intégrées

- Pas d'aller/retour entre les produits ou consoles
- Intégration transparente des investigations EDR et automatisations des détections / réponses
- Sélectionnez n'importe quelle détection pour investiguer



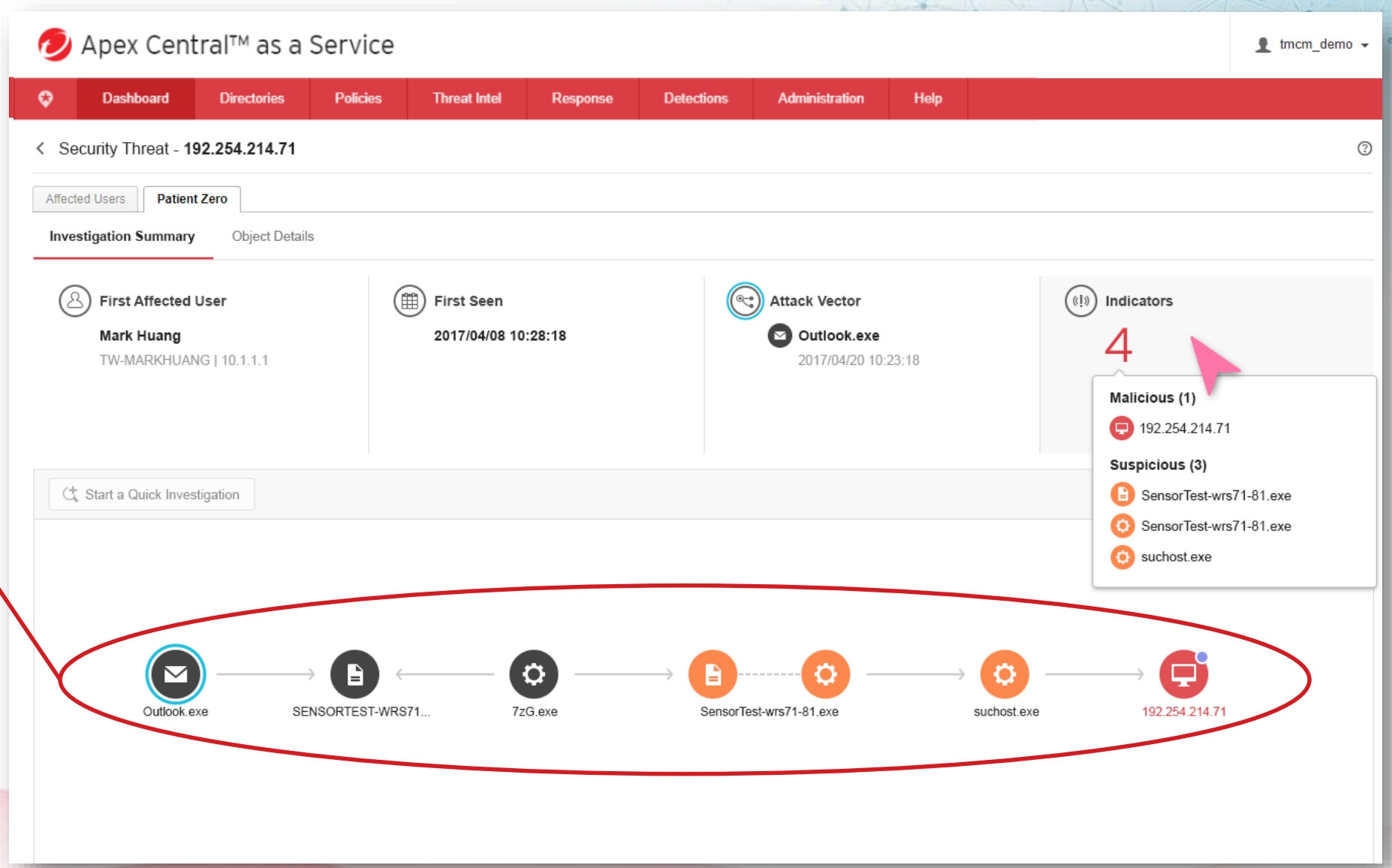
“Qui d'autre a été touché ?”

- Recherche immédiate du côté serveur : analyse d’impact
- Bloqué car l’@IP était connue comme dangereuse (rouge)
- **“Patient zéro” inconnu** (orange) non bloqué
- **Isolation** du patient zéro et lancement de l'analyse de la ‘Root Cause’’



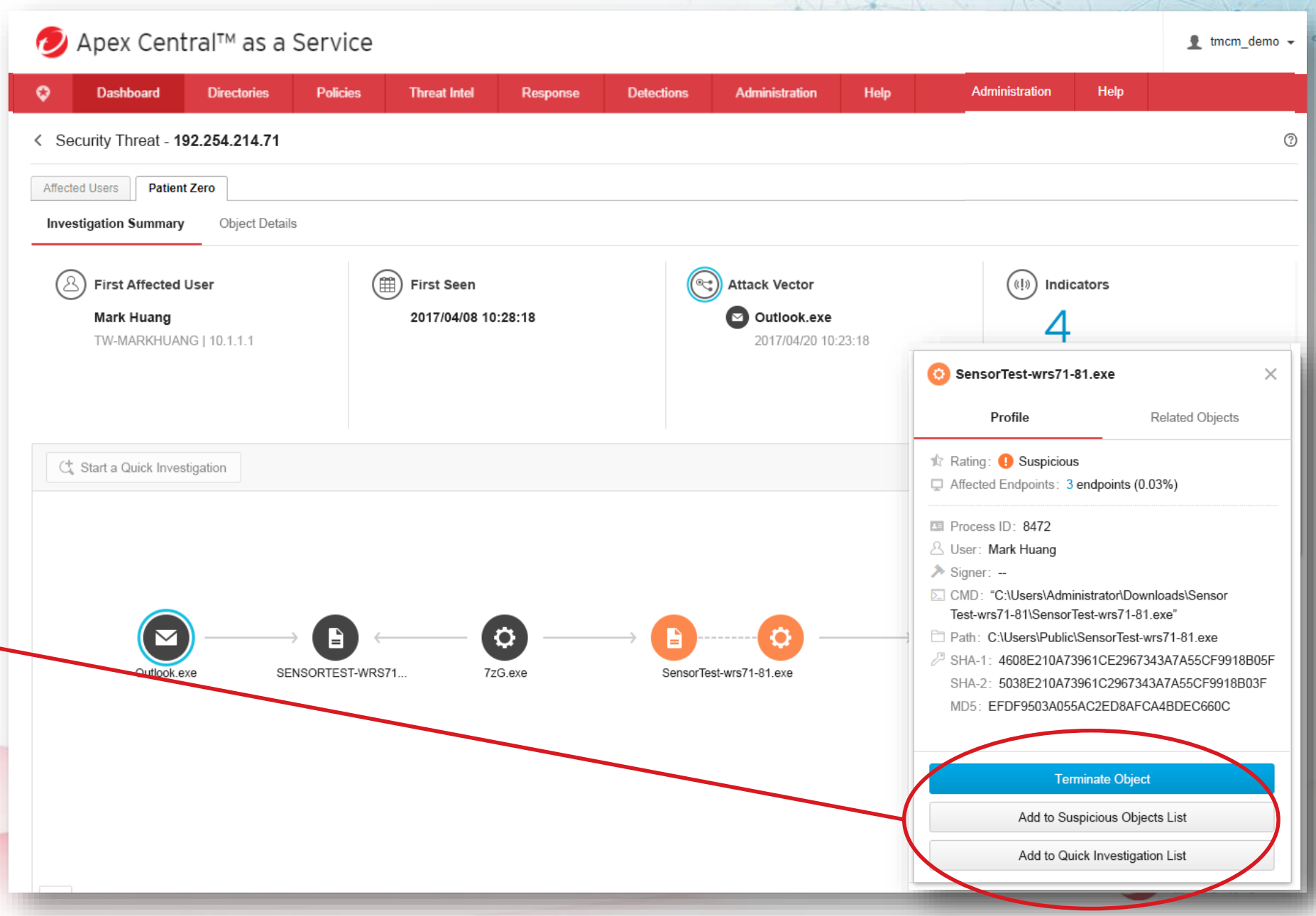
“Comment est-ce arrivé?”

- **Analyse “Root Cause”** pour une “kill chain” simple ou complète
- Amélioré par Trend Micro Threat Intelligence
  - Rouge (élément malveillant)
  - Orange (élément suspect)
  - Noir (élément sain)



“Comment dois-je répondre ?”

- **Analyse “Root Cause”** pour une “kill chain” simple ou complète
- Amélioré par Trend Micro Threat Intelligence
  - Rouge (élément malveillant)
  - Orange (élément suspect)
  - Noir (élément sain)
- Options de réponses
  - Terminer l'objet
  - Ajouter une nouvelle détection automatisées à tous les Endpoints
  - Rechercher cet objet



Merci !!