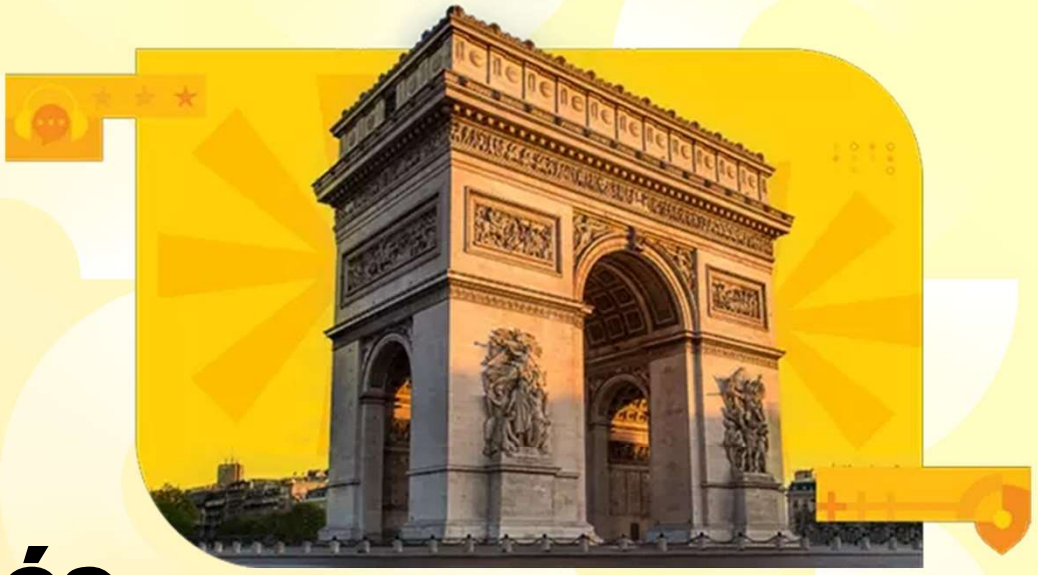
ManageEngine

ITCON

FRANCE 2026



UEM / EDR convergés

Quand opérations IT et cybersécurité ne font plus qu'un

ManageEngine

UNE QUESTION POUR COMMENCER

Dans votre organisation, combien de temps avant de corriger une faille cyber ?

ManageEngine

LE RANÇONGICIEL

Ryuk chiffre tout le système d'information.

L'IMPACT

Blocs à l'arrêt. Urgences redirigées.

LA QUESTION

Quand l'attaque a-t-elle commencé ?

15 FÉVRIER 2021

04h30

Hôpital Nord-Ouest de Villefranche-sur-Saône

800 lits · 3 sites · près de Lyon · en pleine vague COVID

ManageEngine

REMONTONS LE FIL

CVE-2019-19781 « Shitrix »

Faille critique Citrix NetScaler · CVSS 9.8

17 DÉC 2019
Faille publiée. Pas de. correctif

8 JAN 2020
Exploitation active.

10 JAN 2020
Scan mondial. 25 000 cibles.

19 JAN 2020
Correctif définitif.

— MARS 2020
Toujours vulnérable.

15 FÉV 2021
Ryuk. Chiffrement.

11 jours d'exploitation sans correctif

1 an avant que la faille ne soit corrigée

ManageEngine

CE N'EST PAS UN CAS ISOLÉ

Même faille. Même période. Plusieurs victimes françaises.

Bretagne Télécom

via CVE-2019-19781

Lab. Expanscience

via CVE-2019-19781

Scutum

via CVE-2019-19781

Dassault Falcon Jet

Ragnar Locker

À L'ÉCHELLE NATIONALE

30+

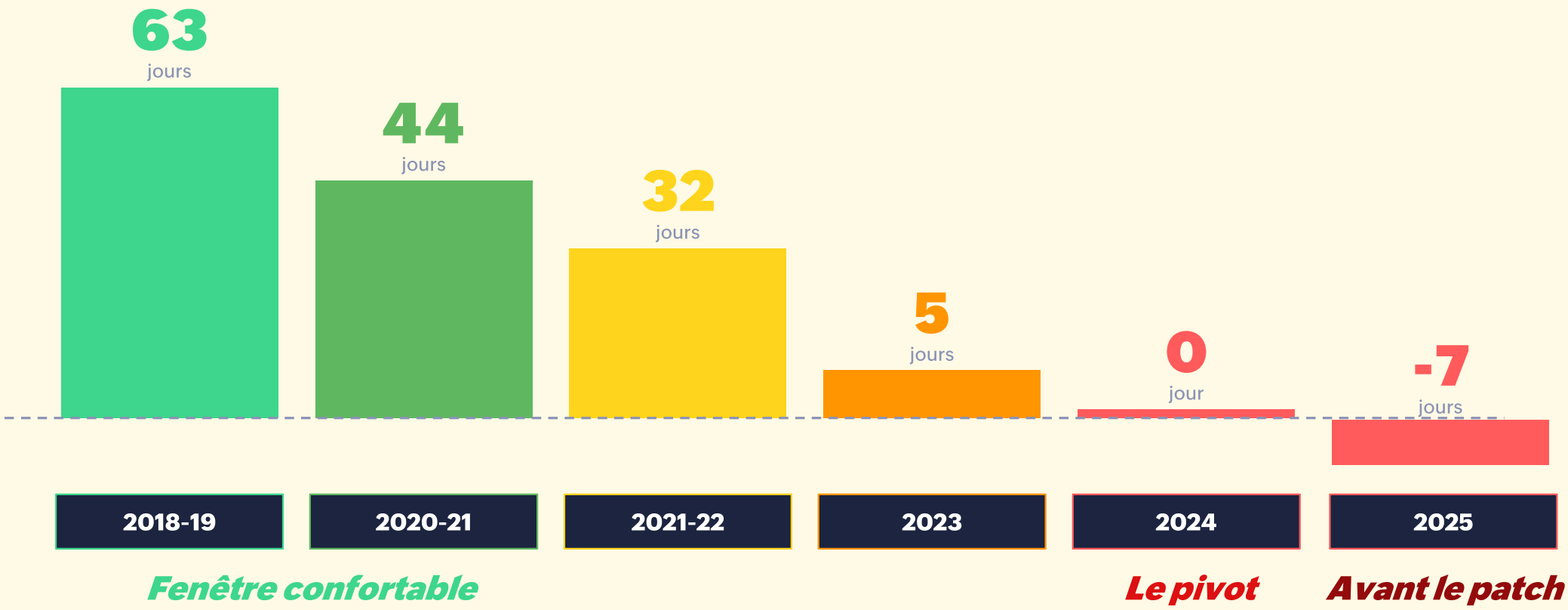
hôpitaux français victimes de cyberattaques majeures entre 2022 et 2023.

Source : ANSSI

ManageEngine

LE CHIFFRE QUI CHANGE TOUT

Le temps médian avant exploitation d'une vulnérabilité



Sources : Mandiant Time-to-Exploit Trends 2021-2022 · M-Trends 2024 · M-Trends 2026

ManageEngine

POURQUOI CETTE INVERSION

Trois facteurs aggravants

01

L'IA accélère les exploits

- Avis → code en heures
- Automatisation offensive

02

Les pipelines de divulgation fuitent

- Fuites en amont
- Exploit avant le patch

03

Le cybercrime s'industrialise

- Initial Access Brokers
- Hand-off : 22 secondes

ManageEngine

ET CE N'EST QUE LA MOITIÉ DU PROBLÈME

L'attaquant n'utilise même plus de malware...

82%

des détections en 2025 étaient sans malware.

CONCRÈTEMENT

29 min	Temps moyen de propagation (accès initial → mvt latéral)
27 sec	La propagation la plus rapide observée
+89%	D'attaques pilotées par IA en un an
14 j	Temps moyen avant détection

Source : CrowdStrike Global Threat Report 2026

ManageEngine

LE PIÈGE DES DÉFENSEURS

Double contrainte

01 · Patcher reste obligatoire

Le standard se durcit :

- CISA durcit ses délais de patching (US).
- NIS2 : visibilité endpoint, incident sous 24 h.
- DORA, ISO 27001 : auditabilité des correctifs.

02 · Patcher ne suffit plus

L'attaquant agit avant et autrement :

- Exploitation avant publication du correctif.
- 82 % sans malware : l'antivirus est aveugle.
- 14 jours en moyenne avant détection.

Patcher vite et détecter ce qui passe : deux métiers, un seul combat.

ManageEngine

L'ORGANISATION CRAQUE OÙ ELLE EST DIVISÉE

Deux équipes. Deux consoles. Une seule attaque.

CÔTÉ IT

« Quel est mon inventaire exact ? »

- Combien de postes affectés ? Sur quels OS ?
- Lesquels sont en télétravail / offline ?
- Quand pousser le correctif ?
- Aurai-je un rapport pour l'audit ?

CÔTÉ CYBER

« Est-ce qu'il est déjà entré ? »

- Quels postes ont un comportement anormal ?
- Depuis combien de temps ?
- Quelle est la timeline de l'attaque ?
- Comment isoler sans tout paralyser ?

Vendredi 18h. Une CVE critique vient d'être publiée. Qui agit ? Avec quel inventaire ? À quelle vitesse ? Et qui détecte si l'attaquant est déjà entré ?

ManageEngine

CE QUE LES ANALYSTES DOCUMENTENT

Le mouvement est déjà en marche.

+ de 50%

des organisations adopteront la gestion autonome des endpoints (AEM) d'ici 2029 - contre près de 0 % en 2024.

AEM (Autonomous Endpoint Management) : l'évolution de l'UEM, enrichie d'IA, d'automatisation et de conformité continue.

La transition d'endpoint management la plus rapide de la décennie.

Source : Gartner, Innovation Insight / Market Guide for Endpoint Management Tools - Cipolla & Wilson, 15 janvier 2025.

ManageEngine

CE QUE ÇA RAPPORTE

Le coût mesuré de la convergence

ÉCONOMIE PAR BRÈCHE

-1,9 M€

pour les organisations qui déploient massivement IA et automatisation.

3,62 M€ vs 5,52 M€ sinon.

CYCLE DE VIE D'UNE BRÈCHE

-80 jours

entre l'intrusion et la complète remédiation.

Coût moyen mondial : 4,44 M€ en 2025 (–9 %).

Source : IBM Cost of a Data Breach Report 2025 (montants convertis en euros à titre indicatif).

ManageEngine

LA COUCHE RÉGLEMENTAIRE

La conformité n'est plus optionnelle

FOCUS **NIS2**

Quatre exigences directement adressées par un UEM unifié

01

Inventaire à jour

Chaque endpoint actif connu.

02

Gestion des vulnérabilités

Patching documenté et continu.

03

Notification 24/72 h / 1 mois

Détecter et documenter en réel.

04

Auditabilité

Journaux et preuves opposables.

Et aussi :

DORA

Résilience opérations financières

ISO 27001

Management de la sécurité

ReCyF (ANSSI, 2026)

Référentiel français NIS2

ManageEngine

LA RÉPONSE

Un agent.
Une console.
Une équipe étendue.

Visibilité unifiée

IT et SOC voient la même chose au même instant.

Remédiation continue

Patch + config + détection dans un flux unique.

Réduction du TCO

Moins d'agents, de licences, de formation.

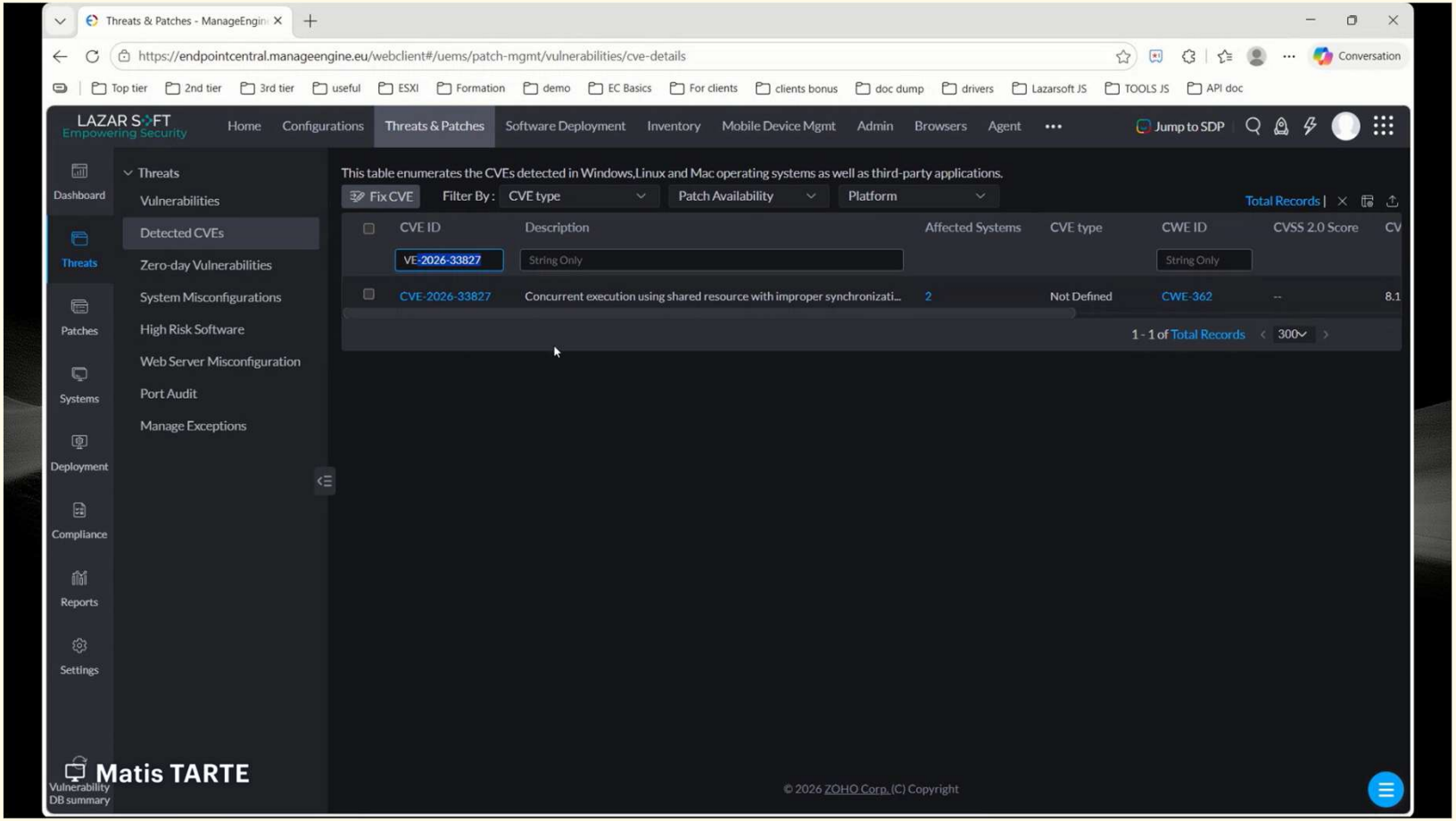
Réponse accélérée

Du signal à l'action, sans passage de relais.

ManageEngine

CAS D'USAGE · 1

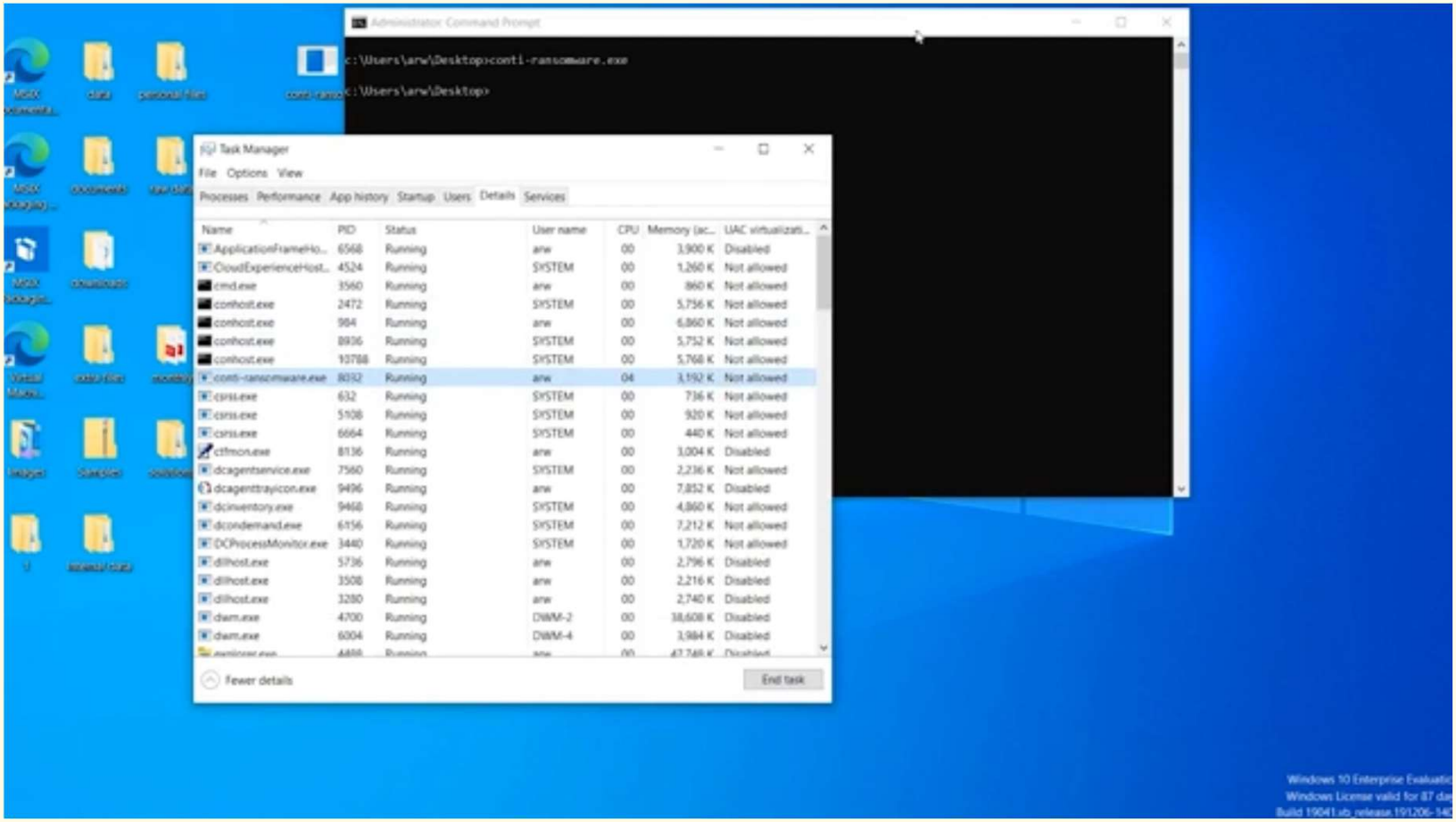
Vendredi 18h. Une nouvelle CVE critique.



ManageEngine

CAS D'USAGE · 2

Et si l'attaquant passait quand même ?



ManageEngine

CE QUI CHANGE CONCRÈTEMENT

Quatre indicateurs qui bougent immédiatement

TIME-TO-PATCH

Heures

vs jours / semaines

RÉPONSE INCIDENT

Minutes

vs heures / jours

TCO ENDPOINT

-30 %

moins d'agents, de consoles

CONFORMITÉ

Continue

vs ponctuelle / par audit

ManageEngine

La sécurité n'est plus un coût additionnel à l'IT...

c'est une capacité native de la plateforme qui gère vos endpoints.

ManageEngine

Merci

Matis TARTE
#RocketExpert
UEM / SIEM

Jérôme PEQUIN
#RocketExpert
FSO / UEM

REX CLIENT

GRAND LARGE YACHTING

Patching, MDM, prise en main, déploiements : comment Grand Large Yachting tient la barre de ses 1000 endpoints en multi-site.

Thomas BOUCHARD

Chef de Projet SI

ManageEngine

REX CLIENT

ORCHESTRA©
CHAQUE JOUR, GRANDIR EST UNE FÊTE

385 magasins, 1 incident, 1 console : comment l'outil de gestion unifiée des terminaux a joué un rôle essentiel dans la gestion d'une crise IT.

Jean-Philippe Forestier
Architecte IT