



Der Wettlauf mit den Maschinen: Cyberabwehr im KI-Zeitalter

Olivier Schraner, Chief Security Advisor, Microsoft Corporation

Vulnerability Management Update

7 days

Mean time between first exploitation of a CVE and the availability of a patch

51 %

Increase in the number of CVEs published between 1st half of 2026 over 2025

90 %

Estimated level of campaign work delegated to AI by threat actors

The Emperor's New Clothes, Cyber Edition

1 trillion

Ballpark figure of how much lines of code are in use out there globally

3 %

Very rough average of the number of incremental vulnerabilities found in well-honed code using AI

99 %

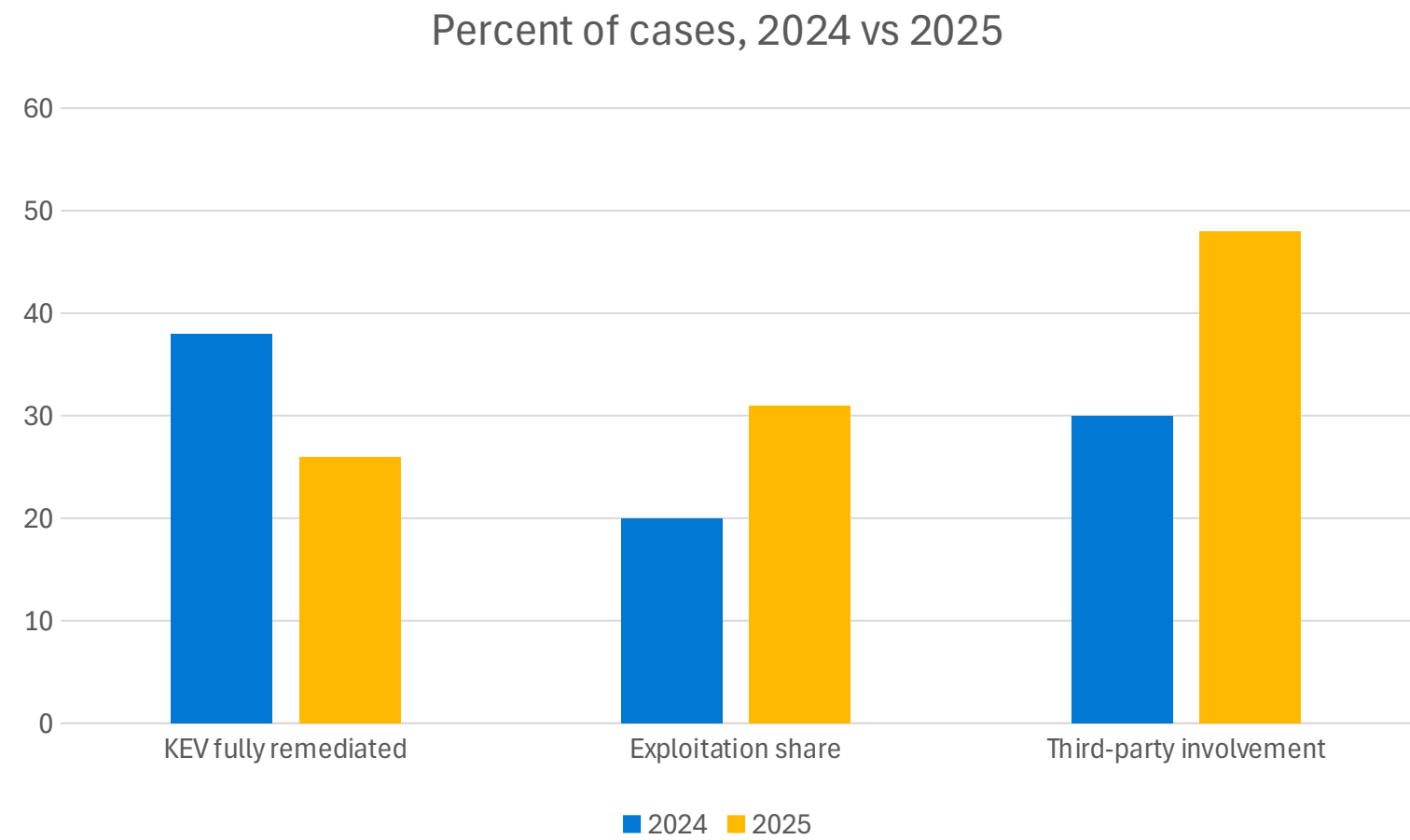
Approximation of how much AI reduced the human effort to find, prove – and exploit – vulnerabilities

That said...

The Top Three Attack Vectors in 2026, so far:

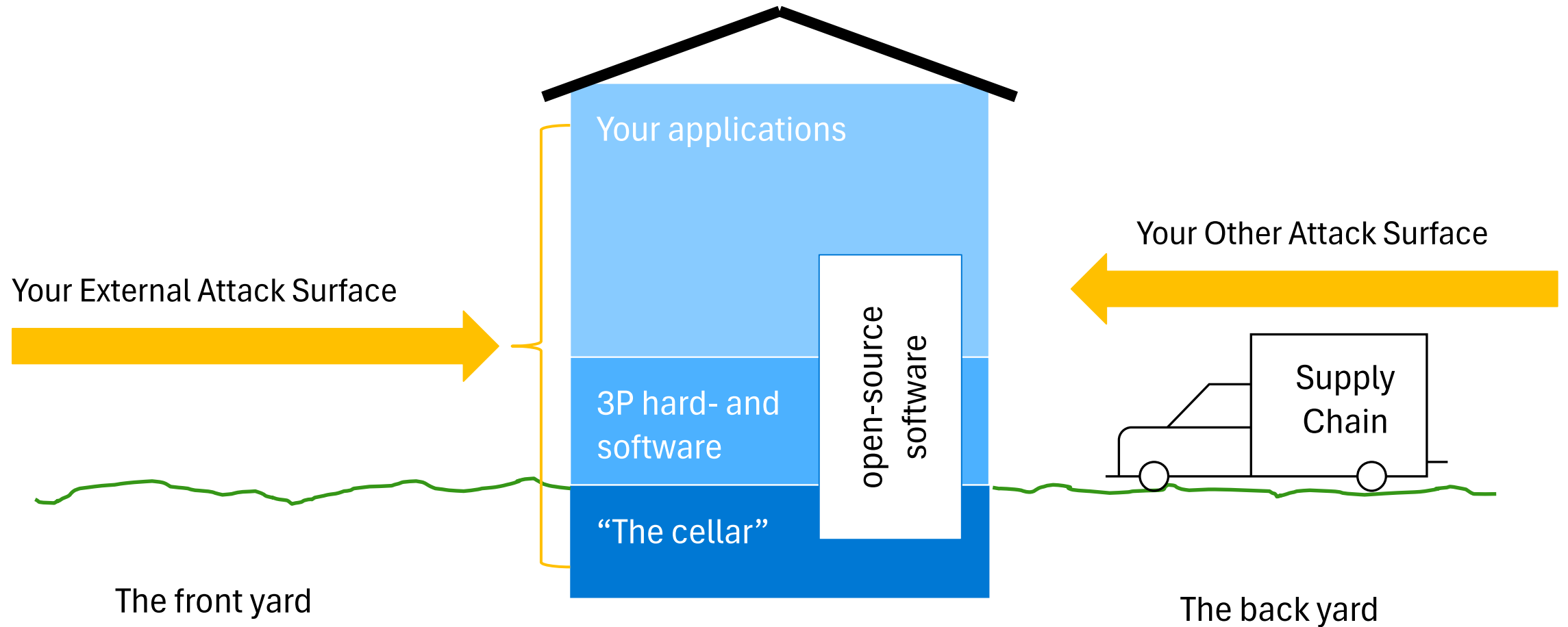
1. Exploitation of Internet-facing vulnerabilities
2. Identity and credential compromise
3. Third-party and supply chain compromise

Remediation is slowing while exploitation accelerates



Median time to fully remediate a critical vulnerability also rose, from 32 days to 43 days.

Your Code Is Now Also The Attack Surface



Structural Asymmetry (Or Why Life Isn't Fair)

Defender (that's you):

- Must play by the rules
- Needs to be right all the time
- Lives in an organization's reality
- Has limited access to frontier AI capabilities subject to approvals and budget
- Must be vigilant 7x24
- Foots the bill for all defensive measures
- Sees only their own tenant

Threat Actor (the bad guy):

- Has only one rule – must turn a profit
- Needs to be right just once (weakest link)
- Shapes reality to fit the opportunity
- Does his own inferencing for the ungated cyber model just downloaded from xyz
- Waits for Christmas dinner
- Springs for just the cost of the attack
- Sees and can compare across tenants

The list goes on... but you get the point.

The Need for Speed – And Accuracy

1

We need to be faster – and not just at patching.

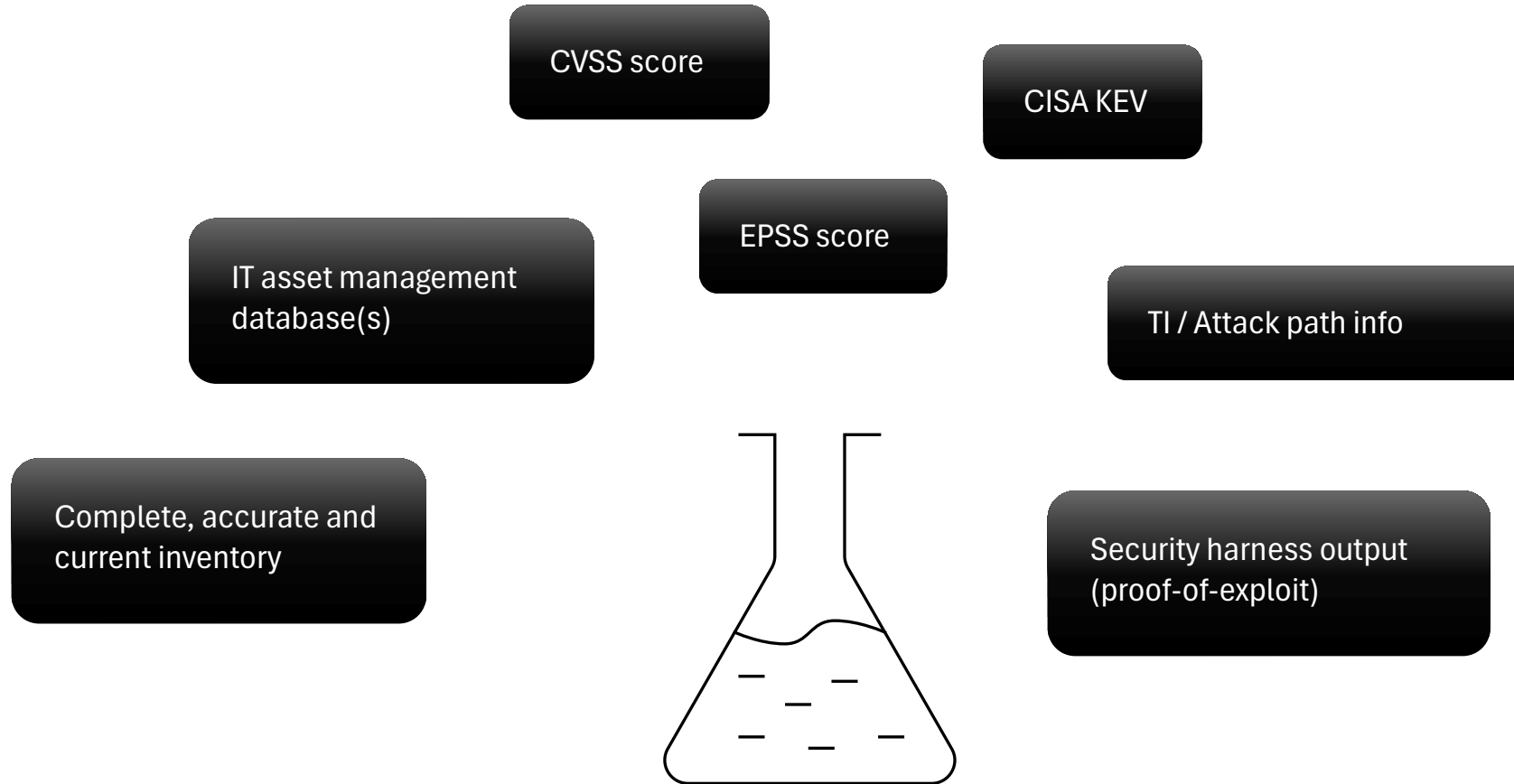
2

We need to prioritize based on real risk to our own estate.

3

#1 and #2 need better data and new governance models.

Patch smarter, not harder!



Your priority = KEV (certainty) + EPSS (likelihood) + proof-of-exploit (for you) + asset value

Go together if you want to go far

Implementing operational resilience practices will allow you to be fast and resilient at the same time.

Infrastructure, Security and
Policy as code

Allows policy and corresponding configuration treated and managed like code

Immutable Infrastructure

Eliminates certain attack vectors and traditional patching, makes going evergreen safer

Continuous Delivery

Removes manual activities, surfaces uncontrolled dependencies and surfaces breaking changes quicker

Blue/Green &
Canary Deployment

Improves agility in release management

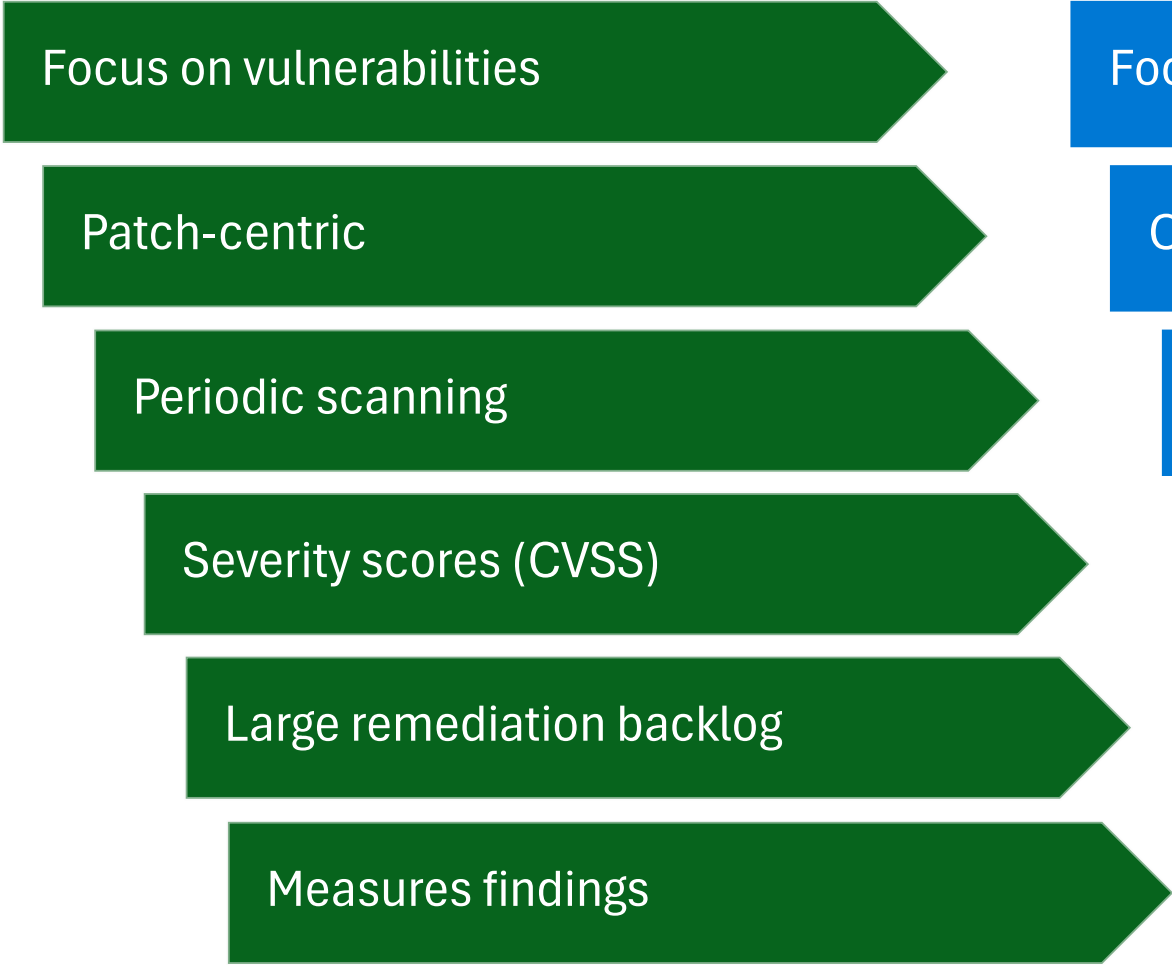
Chaos Engineering

Constantly tests and improves the resilience of both infrastructure and applications

Continuous Threat and Exposure Management (CTEM)

5 Phases: Scoping – Discovery – Prioritization – Validation – Mobilization

Traditional vulnerability/patch management



CTEM



Thank you