SECURITY AT GARTNER SYMPOSIUM 2026

WHAT YOUR TEAM SHOULD TAKE BACK

From the ON2IT team in Barcelona, with commentary by **Tim Timmermans, CISO Nederland**

Your team is probably debriefing on Barcelona this week. ON2IT was there too, and we went back through the security track so your debrief can be shorter. Below: six things Gartner put on the screen, what we think they mean, and what to do on Monday morning. Figures are as Gartner presented them in the sessions.

01 PATCH SPEED IS NOW A VANITY METRIC

Frontier AI models speed up vulnerability discovery and lower the bar for attackers. Legacy systems cannot keep up with the update rate, and a raw CVSS score ignores business context. Gartner's board question shifts from "how fast do we patch?" to "how long are we willing to stay exposed to a known vulnerability?"

MONDAY

Pick your five most critical systems and set an exposure-based SLA for each: the maximum time a known, exploitable flaw may stay reachable.

OUR VIEW

A flaw you cannot patch today can still be made unreachable. Exposure is a design choice, not only a patch schedule.

02 FIND YOUR AI AGENTS BEFORE YOU GOVERN THEM

In a Gartner survey of 251 executives (July 2026), 74% already run endpoint productivity agents in production and 28% run AI browsers. The most frequent errors: agents without authentication, and agents with far more permissions than the task needs. Multi-agent setups quietly break segregation of duties: two agents together can reach what no single employee may.

MONDAY

List your agents, their owners, use cases and permissions. Within 90 days: an agent security policy and access model. Within 12 months: adversarial testing, least privilege and intent drift detection.

OUR VIEW

This is Zero Trust for agents: one unique identity per agent, least agency, nothing trusted by default. Humans and agents share the same problem: agency.

03 SHADOW AI IS A PEOPLE PROBLEM FIRST

The human is still the main attack vector, and AI makes phishing, deepfakes and help desk fraud cheaper. Gartner: 57% of employees use personal GenAI accounts for work, 33% admit putting sensitive work information into public or unapproved tools, and 36% use unapproved GenAI apps on work devices. Blocking everything drives AI underground. Gartner's target sits between restrictive and permissive: visibility, then coaching in the moment.

> **MONDAY**
>
> Find out which AI tools are actually in use, sanctioned or not, before you write the policy.

04 AI IN THE SOC: AUGMENT, DON'T REPLACE

Gartner's 2026 Cybersecurity Technology Adoption Roadmap (142 security leaders) shows AI for security at risk of getting stuck in pilot: unpredictable cost, scarce talent, vendor supply chain risk. It pays off in alert enrichment, false-positive classification, vulnerability prioritization and third-party risk input. Gartner's advice: mandate human-in-the-loop oversight, reinvest the time saved in skills, and protect the skills you cannot afford to lose, such as threat modeling and checking the AI's own false positives.

> **MONDAY**
>
> Audit low-value pilots. Define your security technology strategy around one primary objective: reduced exposure, faster incident response or lowest total cost.

05 CONSOLIDATION CUTS BOTH WAYS

Platforms suit mature domains, but over-consolidation creates a single point of failure. Gartner advises scoring vendors with its Vendor Trust Index before you consolidate. The continuity session was blunter: extreme disruption happens when several assumptions fail at once (cloud, supplier, geopolitics). Winning means running your minimum viable organization, and recovering identity first. On sovereignty: a fully sovereign stack is not a realistic goal today. Reduce and spread your "sovereign technical debt" in three-year sprints.

> **MONDAY**
>
> Map your single points of failure, including your vendors' vendors. Rehearse recovery as part of normal operations, not once a year.

06 QUANTUM AND REGULATION RUN ON A CLOCK

Half of organizations have not started postquantum work, while attackers harvest encrypted data today to decrypt later. On AI regulation, the EU AI Act moved: high-risk rules now apply from December 2027, the remaining rules from August 2028. Worldwide, more than 1,800 AI laws, regulations and guidelines are on the books. Gartner: "The goal is no longer regulatory compliance. It's regulatory resilience."

> **MONDAY**
>
> Start a cryptographic inventory and an inventory of where AI makes decisions in your processes. Both are the first step of every roadmap Gartner showed.

WHAT GARTNER DID NOT SAY

A week of slides on AI governance, and not one said: don't paste your password into the AI browser. Frameworks are the floor plan. Habits are the house. Three we run on ourselves:

01
Nobody types credentials into an AI browser or assistant.

02
No agent runs on a borrowed or service account. Every agent gets its own identity.

03
No assistant gets delete or send rights it does not need for its one job.

"BAD GOVERNANCE IS A TAX ON AI. GOOD GOVERNANCE IS A VALUE ACCELERATOR."

Gartner, Practical AI Governance session

TALK TO THE AUTHOR

TWENTY MINUTES WITH TIM TIMMERMANS

Would you like a conversation with the expert who wrote this report? We will set up twenty minutes with Tim Timmermans, our CISO. No slides, no product pitch.

Tim Timmermans, CISO Nederland, ON2IT

on2it.net/contact

BOOK THE CONVERSATION →

Sources: Gartner IT Symposium/Xpo 2026, Barcelona, sessions: Top Trends in Cybersecurity for 2026 (Akif Khan); Gartner's 2026 Cybersecurity Technology Adoption Roadmap for CIOs (Leigh McMullen, Christine Lee); The CIO 2027 Cybersecurity Radar (Leigh McMullen); AI Agents: Cybersecurity Strategies for Enterprise Protection (Dionisio Zumerle); Practical AI Governance (Nader Henein); European CIOs Sovereign Strategy Playbook (Nader Henein); Business Continuity Planning for Extreme Disruptions (Charlie Winckless). Statistics as presented by Gartner, not independently verified. Selection, interpretation and "Our view" are ON2IT's own and not endorsed by Gartner.