ARTIFICIAL INTELLIGENCE

Is this how to prepare for an agentic AI driven future?

Mar 6, 2026

Agentic AI is quickly becoming pervasive, but it needs guardrails.
Image: Getty Images/iStockphoto

David Haber
VP AI Security, Check Point Software Technologies

is article is part of:

- **Agentic AI marks a real shift in how work gets done inside an enterprise.**
- **It's not just a technology evolution, it’s a governance and security problem that enterprises need to address head-on.**
- **Organizations that succeed in the agentic AI era will earn autonomy through visibility, clear policy boundaries and the ability to audit and override decisions when necessary.**

Agentic AI marks a real shift in how work gets done inside an enterprise. We’re moving beyond systems that assist humans to systems that are trusted to reason, decide and act on their own. That change is already underway and it’s happening inside core business workflows - not in labs or pilot programmes.

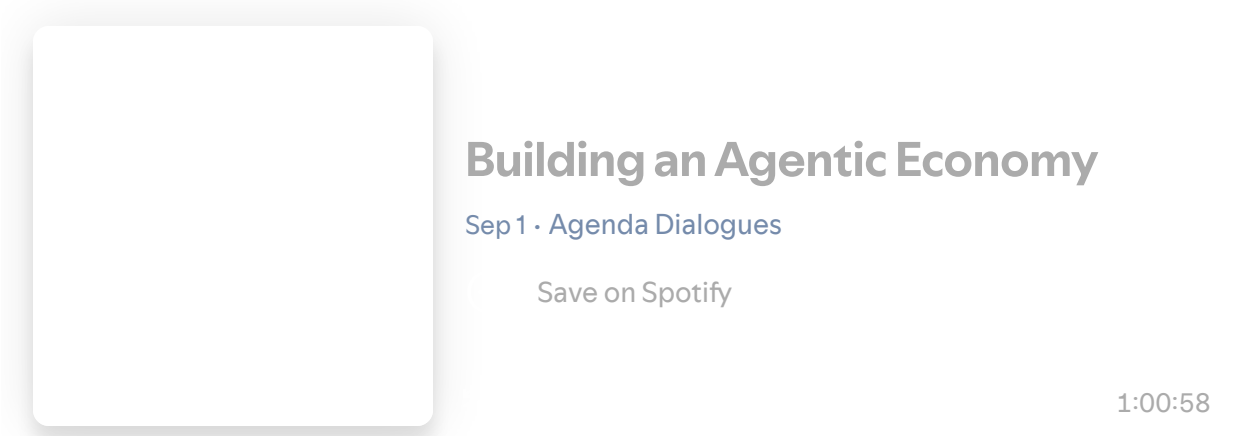
Let me be clear about why this matters. When AI systems are given autonomy, they become operational actors with authority. They initiate actions, interact with tools and APIs and influence outcomes in real time. At that point, many of the assumptions organizations rely on - about control, oversight and accountability - no longer hold. This isn’t just a technology evolution. It’s a governance and security problem that enterprises need to address head-on.

How can we move from alert fatigue to active defence?

Cybersecurity will also harness and deploy agentic AI in more demanding ways, including in the security operations centre. Security operations are under relentless pressure, with analysts facing a dizzying volume of alerts, false positives and incident response demands. The scale and velocity of threats have now nearly outpaced human capacity, leading to burnout, attrition and difficult trade-offs

Agentic AI promises to be the critical force multiplier to help solve this challenge. In this context, agents function as intelligent assistants that automate the monitoring, triage and management of security events. They classify alerts, enrich events with contextual data, correlate signals across disparate systems and escalate only what truly requires human judgment. Some are already being trained to dynamically adjust security and access policies as business contexts evolve, continuously monitoring for compliance, flagging anomalies in real time and taking limited corrective action autonomously.

Embracing agentic AI should further shift cybersecurity from reactive to proactive, helping to identify and prevent threats before they can damage organizations. Instead of merely alerting to suspicious activity, AI-driven security becomes an active defence system, capable of operating at machine speed without sacrificing precision or visibility. Mean time to detect and respond drops dramatically, blind spots shrink and human analysts regain the cognitive space to focus on higher-order strategy and complex investigations.



Why is agentic AI a tool not a takeover?

agents do exceptionally well is handle the repetitive, high-volume tasks that drain human attention: alert classification, log analysis, routine investigations and baseline threat correlation. They work continuously, without fatigue, across systems and silos that can be difficult for humans to monitor simultaneously.

Because agentic AI can rapidly process massive datasets and detect subtle patterns, it can surface threats that might otherwise be missed or discovered too late. Early deployments are already demonstrating tighter security postures, greater operational resilience and a significant reduction in bottlenecks that slow incident response. Agentic AI allows organizations to scale security outcomes without scaling headcount at the same rate.

How can we deploy and scale agentic AI responsibly?

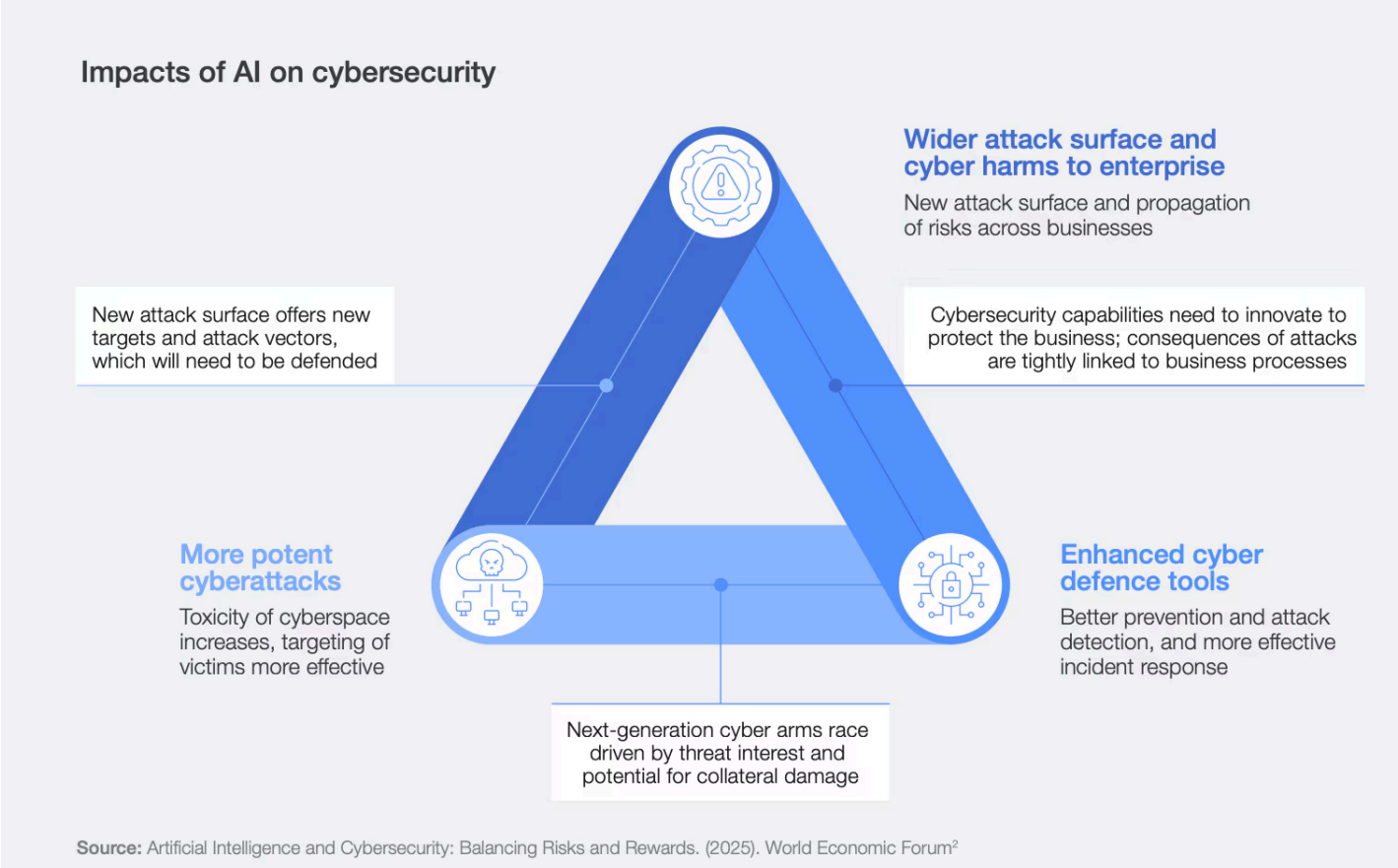
As AI agents are deployed and scaled within organizations, new governance gaps will inevitably emerge that will limit operational authority. Who validates an agent's actions? Who audits its decision logic? How do organizations intervene when an agent's intent diverges from the desired outcome or when optimization goals conflict with ethical or regulatory constraints?

Autonomous efficiency without accountability quickly becomes unmanaged risk. An agent that can change access policies, isolate systems or initiate remediation actions must be governed as rigorously – if not more so – than any privileged human user. Without strong guardrails, observability and auditability, organizations risk trading human error for machine-driven systemic failure.

As Agentic AI is adopted and scaled at a faster pace, enterprises will need formal AI governance councils that bring together security, risk, legal and business leadership. Those bodies will define where autonomy is permitted, under what conditions and through which escalation paths. Policy guardrails must be explicit, enforceable and

improvement.

This concern is not theoretical. The World Economic Forum's *Global Cybersecurity Outlook 2026* finds that accelerating AI adoption is expanding the cyber attack surface, while organizations struggle to align governance, skills and security controls with the speed of deployment. As AI systems and agents proliferate across enterprise workflows, the absence of governance may prove more dangerous than the absence of automation.



Impacts of AI on cybersecurity

Success in the agentic era hinges on visibility. Enterprises must be able to observe what their AI agents are doing, why they are doing it and what impact their actions have across the environment. This means security platforms must evolve to provide

operate within clearly defined boundaries aligned to organizational risk tolerance.

When agents act, humans must be able to understand, audit and override those actions when necessary. After all, visibility and control go hand in hand.

How to upskill for an AI Age: Workera CEO

Jan 30 · Meet The Leader

Save on Spotify

36:19

Autonomous adversaries versus autonomous defenders

The security challenge ahead is straightforward. Attackers are already using AI to automate reconnaissance, adapt techniques and operate at machine speed. Defending against that with human-driven processes alone is no longer sufficient. Enterprises are entering an environment where autonomy exists on both sides. The outcome depends on how well that autonomy is governed.

Agentic AI is not inherently risky. Unconstrained autonomy is. Organizations that succeed in the agentic era will be the ones that earn autonomy through visibility, clear policy boundaries and the ability to audit and override decisions when necessary. Security in this model isn't about reacting faster - it's about ensuring that autonomous systems act with intent. Intelligence without governance doesn't scale.

does.

- **How agentic, physical and sovereign AI are rewriting the rules of enterprise innovation**

Discover

How the Forum helps leaders make sense of AI and collaborate on responsible innovation

Show more

Don't miss any update on this topic

Create a free account and access your personalized content collection with our latest publications and analyses.

Sign up for free

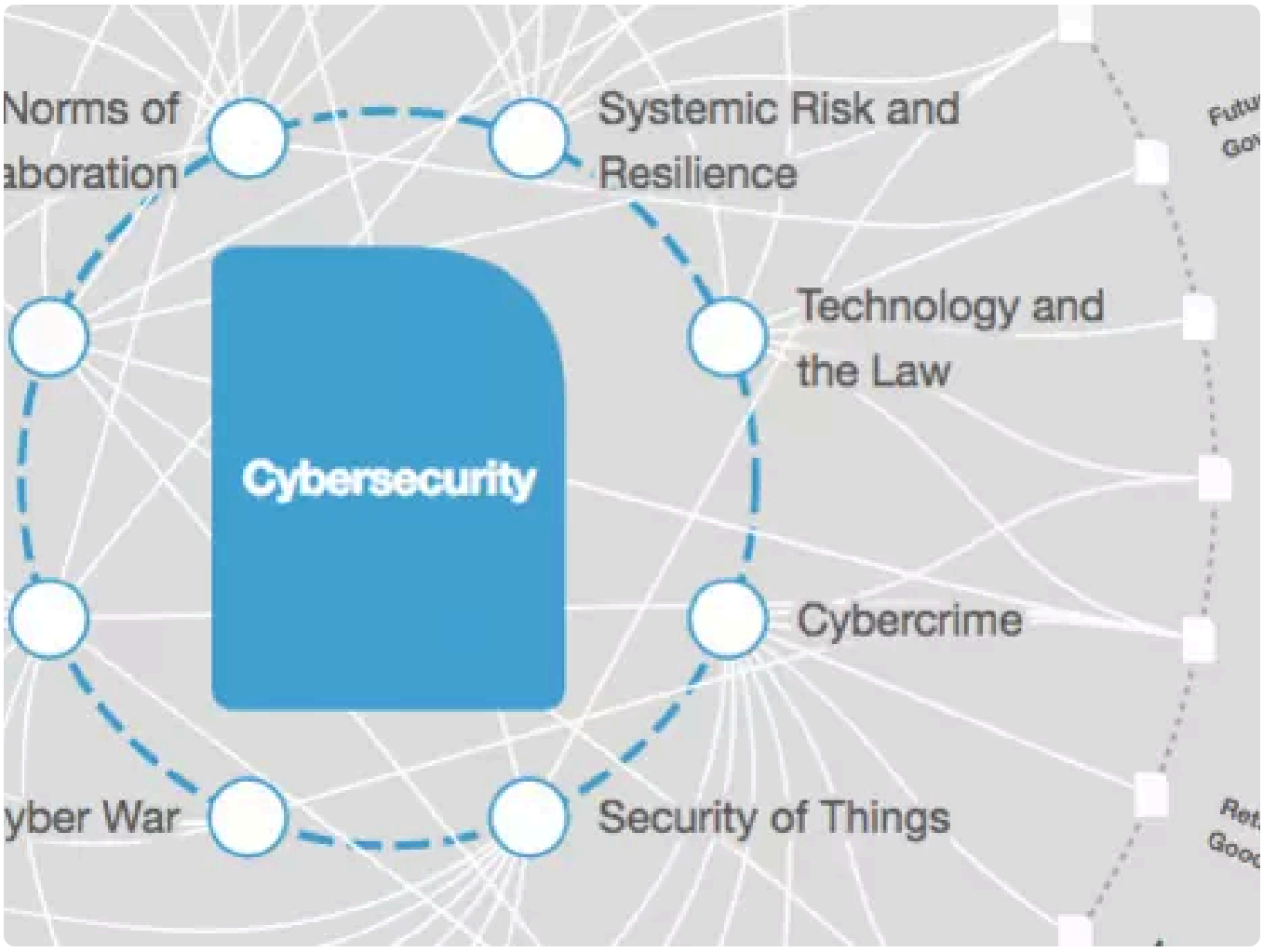
Stay up to date:

Cybersecurity

Follow +

Related topics:

Share:



THE BIG PICTURE

Explore and monitor how **Cybersecurity** is affecting economies, industries and global issues

Forum Stories newsletter

Bringing you weekly curated insights and analysis on the global issues that matter.

Subscribe today

More on **Artificial Intelligence**

SEE ALL

How AI could help fight financial crime by reinventing integrity

Jovanovic

11, 2026

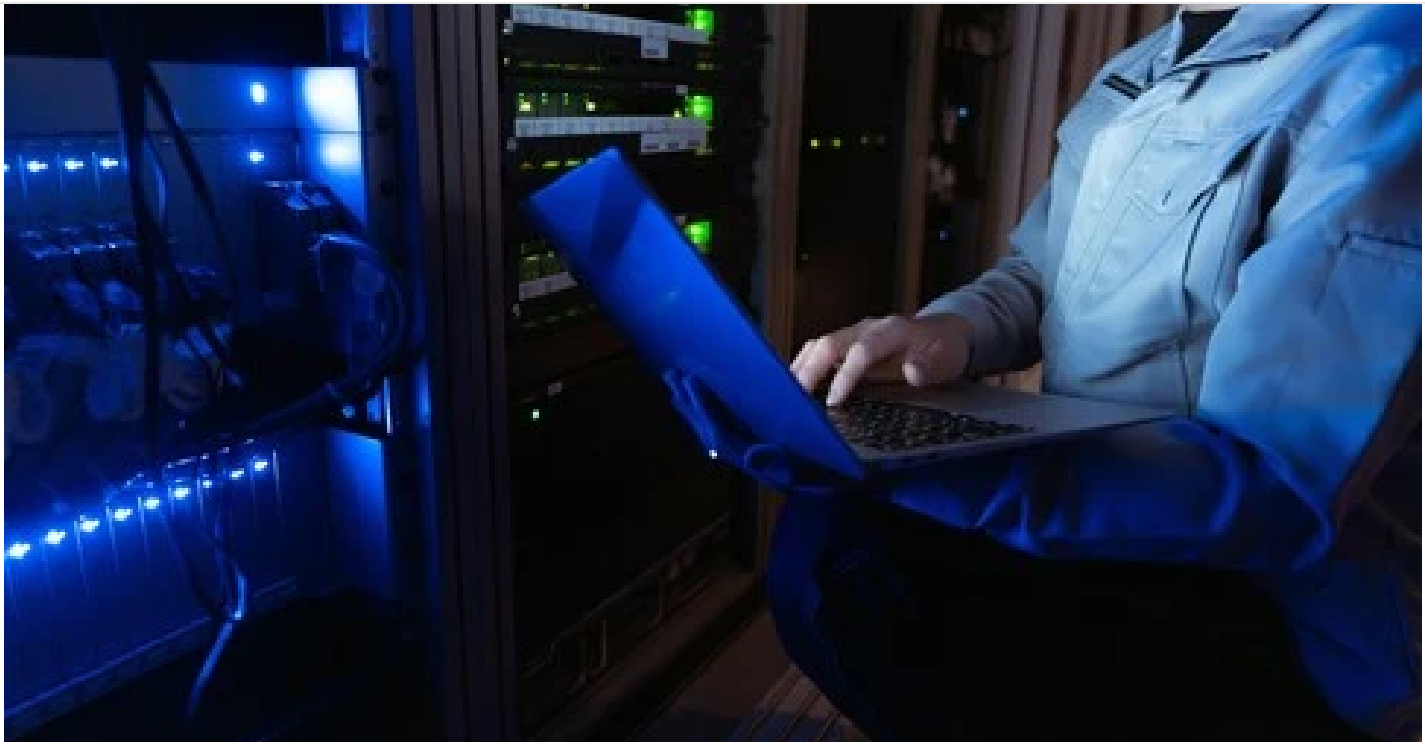
AI can unlock cancer's complexities — if we build the data infrastructure first

Alicia Zhou

March 5, 2026

n AI, children risk learning to be human from a machine

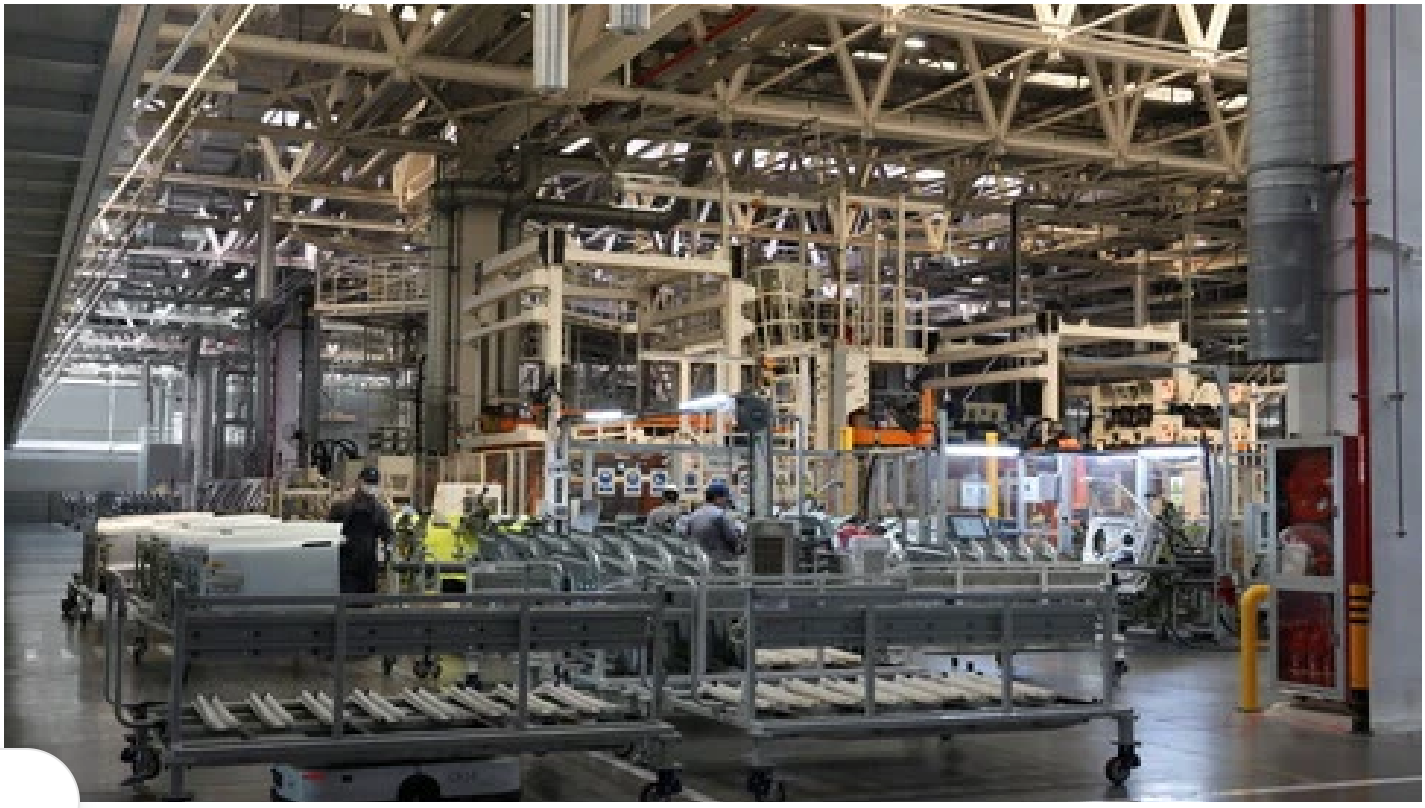
Grindal



AI is supercharging a global cyber fraud crisis. It could also solve it

Jeremy Jurgens

February 27, 2026



The AI-driven workforce is here. How should your industry transform itself?

How edge AI can unlock productivity for India’s MSMEs

Tejpreet S Chopra and Ayushi Sarna

February 27, 2026

About us

Who we are

Our strategy

How we work

Our leadership and governance

Our Impact

More from the Forum

Features