

Gartner Insights

Emerging Tech: Research Roundup for Security, 2026

Elizabeth Kim, Apeksha Kaushik, Luis Castillo,
Jorge Lopez, Alfredo Ramirez IV, Mark Wah



Emerging Tech: Research Roundup for Security, 2026

2 April 2026 - ID G00846774 - 13 min read

By: Elizabeth Kim, Apeksha Kaushik, Luis Castillo, Jorge Lopez, Alfredo Ramirez IV, Mark Wah

Initiatives: Technologies and Markets; Develop a Scalable, Secure AI Tech Stack; Delivery of Functional Responsibilities

Every security product leader must consider the disruptive forces in 2026 to align with the future direction of security — global attack surface grid, digital trust and authenticity platforms, preemptive exposure management, AI security and securing the industrialization of AI.

Analysis

The top security disruptors that are central to the 2026 emerging security technology and trends research agenda include (see Figure 1):

1. Global attack surface grid (see Emerging Tech: AI Vendor Race: Invest in Cyberkinetic Security to Defend Against Threats in the Growing Global Attack Surface Grid)
2. Digital trust and authenticity platforms (see Emerging Tech: AI Vendor Race: Eroding Digital Trust Threatens the Global Economy, Forcing Adoption of Digital Trust and Authenticity Platforms)
3. Preemptive exposure management (see Emerging Tech: The Future of Exposure Management Will Be Preemptive — Driven by Autonomous Interdiction)
4. AI cybersecurity ecosystem (see Emerging Tech: The Future of AI Security Is in Securing Agent Actions, Not Prompts)
5. Securing the industrialization of AI (see Emerging Tech: The Industrialization of AI Will Break Every Business Model We Know in Cybersecurity)

Figure 1: Emerging Technologies and Trends Research — Security



Additionally, the emerging security technology and trends research agenda is part of the broader Emerging Technologies and Trends Impact on Product and Services key initiative. The top disruptors in security will be addressed with specific content structure that will help C-level executives and product leaders answer the following questions:

- **Discovery and tracking:**
 - What are the emerging trends and technologies we need to watch?
 - Why are these emerging technologies important to the future state of our product roadmap?
 - When do we need to act on these emerging technologies?

- **Market dynamics:**
 - Who are the key players in the market?
 - How are buyers adopting technology today, and what are the future opportunities?
 - How are tech vendors pursuing the market, and what are the best opportunities?
 - Are there specific services needed to compete?
 - Are there specific capabilities to gain from partners?
- **Competitive opportunities:**
 - How do we find and pursue competitive opportunities with emerging technologies?
 - How do we deliver a differentiated value proposition for competitive success?
 - What use cases will best communicate the value of an emerging tech?
- **Monetization:**
 - What monetizable value and revenue opportunity does the emerging technology add to the current market?
 - What are the business and pricing model alternatives?
 - What are the underlying economics that determine when and how to invest in an emerging technology?
 - Which business models or practices should be pursued?
 - Which sales, pricing and marketing strategies should be pursued or avoided?

Research Highlights

Some recommended content may not be available as part of your current Gartner subscription. Additionally, the upcoming research is subject to change based on research priorities. It is only intended to provide an example of some of the topics that Gartner will focus on throughout 2026.

Global Attack Surface Grid — Cyberkinetic Security

By 2030, at least 50% of new security investments for autonomous systems, including robotics, vehicles, and industrial automation, will prioritize cyberkinetic security measures over traditional information confidentiality controls.

The integration of digital and physical systems has transformed the global attack surface grid, making cyberkinetic threats a rapidly evolving danger to critical assets and human safety. AI-driven robotics and autonomous systems are no longer isolated, but are now connected to broader digital networks and increasingly integrated into the global attack surface grid. The interconnectedness of assets means that an attack vector in one segment of the grid can have cascading effects throughout an organization. Defending high-risk cyber-physical systems, such as autonomous vehicles and surgical robotics requires cyberkinetic security, which protects physical assets, mechanical systems, and human safety from digital attacks by prioritizing the safety and reliable operation of physical systems above information confidentiality. It includes approaches of embedding “inside-out” autonomous defenses in endpoints and tightly integrating security with safety engineering.

Cyberkinetic security demand will be driven by nation-state kinetic cyber incidents, a surge in valuations for companies specializing in industrial automation and robotics security, and high-profile initiatives such as Tesla’s pending deployment of Optimus robots and Amazon’s rapid expansion of robotics in its logistics operations.

Research in 2026 will center around emerging technologies required to successfully protect the global attack surface grid such as autonomous cyber defense systems, cyberkinetic security, cyber electronic defense and Earth intelligence.

Research Highlights in 2025

- Quick Answer: What Is the Global Attack Surface Grid?
- Emerging Tech Impact Radar: Global Attack Surface Grid
- Emerging Tech: The Global Attack Surface Grid Demands Unified Exposure Management

Research Highlights in 2026

- Emerging Tech: AI Vendor Race: Invest in Cyberkinetic Security to Defend Against Threats in the Growing Global Attack Surface Grid

- Tech FutureSight: Protect the Global Attack Surface With an Autonomous Cyber Defense System

What Lies Ahead for 2026?

- Emerging Tech: Startups to Watch for Cyber Electronic Defense
- Emerging Tech: Top Security Concerns for Cyber Electronic Defense
- Emerging Tech: Failure to Secure Autonomous Drones Will Create Massive Global Risk
- Today's Cybersecurity Is Not Enough for Tomorrow's Autonomous Systems
- Emerging Tech: Win the Physical AI Race Without Injuries By Securing 8 Critical Layers
- Emerging Tech: Use Earth Intelligence to Improve Attack Surface Management

Disinformation Security — Digital Trust and Authenticity Platforms

Trust in digital content is so important that, in 2030, enterprises will spend more than \$25 billion authenticating it.

Disinformation has evolved into a global, industrialized threat, amplified by generative AI that enables large-scale, low-cost influence operations and impersonation attacks. Media platforms lack incentives and capability to regulate synthetic content, while policy and enforcement for digital authenticity remain underdeveloped worldwide. As a result, organizations must independently safeguard their operations.

It is currently cheaper and easier for bad actors to create and deploy deepfakes and disinformation campaigns than it is for the average person to access reliable digital trust and authenticity tools. "AI-as-a-service" kits sold in dark web marketplaces provide tools to clone voices, impersonate executives, and bypass biometric verification. Threat actors can easily generate a convincing AI generated voice or video to deceive even trained employees, in order to successfully carry out social engineering attacks and financial fraud.

Digital trust and authenticity platforms (DTAPs) offer a technological solution to counter the industrialized disinformation supply chain by combining the primary features of disinformation security, which include content authenticity, impersonation prevention, and narrative intelligence, for the dual purposes of alerting on what is fake and authenticating what is real.

Research in 2026 will explore the convergence of fragmented disinformation security capabilities such as content authenticity, narrative intelligence and deepfake detection toward DTAPs that will be effective in combating the ever-evolving disinformation attacks.

Research Highlights in 2025

- Tech FutureSight: Without Narrative Intelligence, AI Disinformation Attacks Will Win
- Emerging Tech Impact Radar: Disinformation Security
- Emerging Tech: Top-Funded Startups in Disinformation Security
- Emerging Tech: Top Funded Startups for Deepfake Detection
- Critical Insights: Impact of U.S. Federal Policy Changes on Disinformation Security
- Emerging Tech: The 3 Pillars of Disinformation Security Solutions
 - Emerging Tech: Leverage Disinformation Security to Neutralize Influence Operations
 - Emerging Tech: Counter Weaponized Trust With the 6Ws of Disinformation Security
 - Emerging Tech: AI Vendor Race: Defend the Digital Attack Surface With Disinformation Security
 - Emerging Tech: AI Vendor Race: The Impact of AI and Deepfakes on Identity Verification
 - Emerging Tech: AI Vendor Race: Disinformation Security Products Must Be Part of Cybersecurity
- Emerging Tech: Disinformation Security Techniques Must Be Used as Part of ITDR

Research Highlights in 2026

- Emerging Tech: AI Vendor Race: Eroding Digital Trust Threatens the Global Economy Forcing Adoption of Digital Trust and Authenticity Platforms

- Emerging Tech: Digital Trust and Authenticity Are the Keys to Preemptive Cyber Resilience for Autonomous Systems
- Emerging Tech: Startups to Watch in Disinformation Security
- AI Vendor Race: Reality Defender Is the Company to Beat in Deepfake Detection
- AI Vendor Race: Blackbird.AI Is the Company to Beat for Disinformation Narrative Intelligence

What Lies Ahead for 2026?

- Emerging Tech: AI Vendor Race — Digital Trust and Authenticity Platforms Are Essential to Defend Against Disinformation Campaigns
- Executive Briefing on Emerging Technology: Digital Trust and Authenticity
- Startups to Watch in Deepfake Detection
- Emerging Tech: Emergence Cycle/Innovation Spectrum for Digital Trust and Authenticity Platforms (DTAPs)

Preemptive Exposure Management

By 2029, 60% of unified exposure management solutions will incorporate domain-specialized automated mitigation, remediation and threat containment capabilities to interdict threats before they can manifest.

Preemptive exposure management (PEM) is transforming cybersecurity by aiming for a state where threats are neutralized before they can manifest. To achieve this state, PEM demands progressive techniques to accelerate tasks from continuous discovery of attack surfaces and exposures to validating exposures with high accuracy by leveraging intelligent simulations combined with predictive threat intelligence, AI and analytics to accelerate mitigation actions and interdict attacks before they begin. Central to PEM is “autonomous interdiction,” which is the autonomy to plan and execute necessary countermeasures, including containment, mitigation and resolution, to operate at machine speed and scale, outpacing attackers and neutralizing threats instead of relying solely on human-led remediation and mitigation.

Adopting PEM requires a cultural shift within security teams, moving from hands-on intervention to oversight and governance, fostering trust in autonomous systems. The evolution toward fully autonomous exposure management will progress in phases, from workflow automation to the eventual development of cyber immune systems. PEM aims to outpace attackers, minimize manual intervention, and establish a new standard for adaptive resilient cybersecurity.

Research in 2026 will center around how to accelerate the shift toward unified exposure management architecture that will serve as a foundation to drive more end-to-end automation of exposure assessment, validation and remediation of exposure, leveraging emerging technologies such as intelligent simulation and agentic AI.

Research Highlights in 2025

- Tech FutureSight: Preemptive Cybersecurity Is the Only Way to Secure Emerging AI Attack Surfaces
- Emerging Tech Impact Radar: Preemptive Cybersecurity
- Critical Insights: Impact of U.S. Federal Policy Changes on Preemptive Cybersecurity
- Emerging Tech: The Future of Exposure Management is Preemptive
- Emerging Tech: AI Vendor Race: Intelligent Simulation Accelerates Proactive Exposure Management
- Emerging Tech: AI Vendor Race: Pivot to Preemptive Exposure Management Services to Grow Revenue
- Emerging Tech: AI Vendor Race: Future-Proof MDR With Automated Exposure Management and Zero Trust
- Emerging Tech: Prioritize Security Risks Smarter With Predictive Threat Intelligence
- Emerging Tech: AI Vendor Race: Unified Exposure Management Will Drive Displacement of Fragmented Point Solutions

Research Highlights in 2026

- Emerging Tech: The Future of Exposure Management Will Be Preemptive — Driven by Autonomous Interdiction
- Emerging Tech: Simulation Twins Will Separate the Competition in Exposure Management Services

What Lies Ahead for 2026?

- Reasoning Models for Preemptive Cybersecurity
- Emerging Tech: Top Funded Startups for Preemptive Exposure Management
- Emerging Tech: Startups to Watch in Preemptive Exposure Management
- Emerging Tech: Successfully Executing Unified Exposure Management
- Agentic AI Will Unlock Unified Exposure Management's Promise
- Emerging Tech: AI Vendor Race — Agentic AI in Adversarial Exposure Validation (Autonomous Adversarial Emulation)
- Autonomous Remediation is the Next Exposure Management Opportunity
- Emerging Tech: Future of Preemptive Cyber Resilience
- Emerging Tech: Security — Deception as a Service for Preemptive Cyber Defense
- Emerging Tech: Top Funded Startups in Advanced Cyber Deception

AI Security

By 2029, more than 25% of organizations that deployed AI agents at scale will leverage guardian agent capabilities deployed as independent and deterministic supervisory entities, up from less than 2% in 2026.

The landscape of AI TRiSM is moving in lockstep, as AI technologies expand their scope from text-based models to complex multimodal systems, AI agents and AI browsers. This expansion has exposed significant security, trust and risk gaps that established approaches are ill-equipped to address. The market is racing to develop innovative solutions to secure these advanced AI implementations.

AI security encompasses a wide range of capabilities from securing the AI engineering pipeline through integrating AI supply chain security, AI code security, information governance and AI security testing, to securing AI in runtime.

Recent emphasis is on securing AI agents, as the transition to autonomous multiagent systems introduces new risks, such as behavioral drift and destructive actions. The urgency to govern autonomous actions and implement AI agent security life cycle management, continuously validating agent integrity from initial deployment to safe retirement, will mean that a significant market opportunity exists to differentiate through securing the agentic ecosystem.

Central to 2026 research will be topics addressing comprehensive measures in AI security platforms, agentic AI security, information governance, AI governance and AI security testing. However, there will be more focus on securing AI agents and their ecosystems to mitigate the risk of rogue agent actions.

Research Highlights in 2025

- Emerging Tech Impact Radar: AI Cybersecurity Ecosystem
- Emerging Tech: Top-Funded Startups in AI TRiSM: Agentic AI and Beyond
- Emerging Tech: AI Vendor Race — Address Top Constraints to Sustain AI Security Market Growth

Research Highlights in 2026

- Emerging Tech: The Future of AI Security Is in Securing Agent Actions, Not Prompts
- Emerging Tech: AI Agent Management Platforms Are Required for Agentic Cybersecurity Success
- AI Vendor Race: Palo Alto Networks Is the Company to Beat in AI Security Platforms
- Emerging Tech: AI Context Layer Wins the New AI Security Race

What Lies Ahead for 2026?

- Emerging Tech Impact Radar: AI Cybersecurity Ecosystem, 2026
- Emerging Tech: Top-Funded Startups in Sovereign AI
- Emerging Tech: Startups to Watch in Sovereign AI
- Emerging Tech: AI Vendor Race — Startups to Watch in AI TRiSM, Agentic AI and Beyond

- Navigating the Cognitive Frontier — AI Ethics, Privacy, and Security for Product Leader
- Emerging Tech: Top Security Concerns of GenAI
- AI Security Platform's Role in Securing Emerging GenAI Technologies
- Emerging Tech: Assuring Confidentiality Across Multiple Untrusted AI Models
- Emerging Tech: AI Vendor Race — Unsecured Simulation Data Will Derail Your AI Strategy
- Emerging Tech: Security Best Practices for Intelligent Simulation Deployment
- Small Language Models Solve Sovereign Cyber Data Privacy
- Emerging Tech: Preparing for the Future of AI Security Threats

Securing the Industrialization of AI

By 2030, the cybersecurity market will undergo a major consolidation. Driven by AI, over half of today's independent cybersecurity companies will cease to exist, either through acquisition or by leaving the business entirely. A few will emerge as large, independent players.

The industrialization of AI represents a structural pivot where intelligence moves from a "human-crafted" experimental tool to a secured, mass-produced utility, effectively collapsing traditional cybersecurity business models. This shift will not only break the reliance on human-intensive managed services by replacing human efforts with autonomous agents that operate at machine speed but also drive the formation of integrated suites of cybersecurity tools that deliver high value at lower costs. The industrialization of AI will force security service providers to transform their current business model, which is built on headcount toward autonomous security models that are able to operate at near-zero marginal costs.

At the same time, as agents gain "agency," they effectively become nonhuman identities (NHIs) with high-level system access. Adoption of autonomous security platforms will depend on their ability to deliver rigorous governance that enforces proper authorization and access rights to agent identities and provides audit trails for every autonomous decision.

Research in 2026 will track the development of AI SOC agents that will drive toward more autonomous SOC and its impact on service providers. Additionally, topics exploring the industrialization of AI include agentic identity management, AI-optimized infrastructure, AI marketplaces and adaptive dynamic resilience.

Research Highlights in 2026

- Emerging Tech: The Industrialization of AI Will Break Every Business Model We Know in Cybersecurity
- Emerging Tech: AI Agent Management Platforms Are Required for Agentic Cybersecurity Success
- AI Vendor Race: Conifers Is the Company to Beat in AI SOC Agents for Threat Investigation

What Lies Ahead for 2026?

- Securing the Industrialization of AI — The CIO Perspective
- Emerging Tech: AI Vendor Race — Critical Insights on AI Optimized Infrastructure
- Emerging Tech: AI Vendor Race — Critical Insights on AI Marketplaces
- Emerging Tech: Agentic Identity and Access Management Is Unavoidable for AI Success
- Emerging Tech: Top-Funded Startups in Machine/AI Agent Identity
- Startups to Watch AI Agent Identity/Machine Identity

Document Revision History

Emerging Tech: Research Roundup for Security, 2025 - 10 February 2025

2023 Research Roundup for Emerging Tech and Trends — Security - 14 March 2024

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

[Emerging Tech Impact Radar: Preemptive Cybersecurity](#)

[Emerging Tech Impact Radar: Digital Identity and Edge Security](#)

[Emerging Tech Disruptors: Top 5 Early Disruptive Trends in Cybersecurity for 2025](#)

[Emerging Technologies and Trends Impact on Products and Services Primer for 2025](#)

[Emerging Tech: Top-Funded Startups in Security Software](#)

© 2026 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. It consists of the opinions of Gartner's Business and Technology Insights Organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner insights may address legal and financial issues, Gartner does not provide legal or investment advice and its insights should not be construed or used as such. Your access and use of this publication are governed by [Gartner's Usage Policy](#). Gartner prides itself on its reputation for independence and objectivity. Its insights is produced independently by its Business and Technology Insights Organization without input or influence from any third party. For further information, see "[Guiding Principles on Independence and Objectivity](#)." Gartner insights may not be used as input into or for the training or development of generative artificial intelligence, machine learning, algorithms, software, or related technologies.

Actionable, objective insights

Position your organization for success. Explore these additional complimentary resources and tools for CIOs:

Webinar



Outlook for Cybersecurity Threat Landscape: Prioritizing Threats With Gartner's ThreatScape

Learn how to make smarter cybersecurity decisions amid uncertainty.

[Watch Now](#)

Hub Page



Gartner AI Hub

Discover practical AI insights for confident decision making.

[Learn More](#)

Virtual Briefing



IT 2030: Empowerment or Chaos? CIO's Role in AI-Powered Democratization

Learn how CIOs can enable AI innovation while managing risk.

[Watch Now](#)

Tool



Gartner AI Maturity Assessment

Assess your AI maturity and build a roadmap to scale impact.

[Explore Tool](#)

Already a client? Get access to even more resources in your client portal.
[Log In ↗](#)

Connect with us

Get actionable, objective business and technology insights that drive smarter decisions and stronger performance on your mission-critical priorities. Contact us to become a client:

U.S.: 1 855 322 5484

International: +44 (0) 3300 296 946

[Become a Client](#)

Learn more about Gartner for CIOs
gartner.com/chief-information-officer

Stay connected to the latest insights



Attend a Gartner conference
[View Conference](#)