

Enterprise Management Associates (EMA)

Research Calendar

Information Security, Risk and Compliance Management

Information Security, Risk and Compliance Management

Governing the Agentic Enterprise: Identity, Guardrails, and Oversight for Autonomous AI Agents

Autonomous AI agents are moving from pilot projects to production workflows, each one acting with its own credentials, permissions, and decision-making authority. Unlike traditional software, an agent can chain tasks, invoke tools, and make judgment calls without a human in the loop for every action—turning a single compromised or misconfigured agent into a fast-moving insider threat. EMA will survey security and identity leaders to understand how organizations are discovering the agents already running in their environment, what governance and guardrail models are emerging (approval workflows, scoped permissions, and kill switches), and where responsibility sits between security, IT, and the business units deploying the agents.

Non-Human Identity at Scale: Securing Machine, Service Account, and Agentic Credentials

API keys, service accounts, workload identities, and autonomous agent credentials have quietly become the largest identity population in the enterprise—and the least governed. Traditional identity and access management (IAM) and privileged access management (PAM) tooling was built around human logins and struggles with the scale of NHIs, short lifecycles, and lack of a person to call when something looks wrong. This research examines how security and platform teams are discovering, classifying, and rotating machine credentials; where secrets sprawl is worst; and how organizations are deciding which NHIs need PAM-grade controls versus lighter-weight management.

AI Security Posture Management: Discovering and Governing Shadow AI Across the Enterprise

Employees are pasting sensitive data into unsanctioned AI tools, developers are wiring undocumented AI APIs into production applications, and business units are adopting AI copilots faster than security can review them. AI security posture management has emerged as the category meant to bring this sprawl under control—discovering AI usage across SaaS, code, and infrastructure, and assessing the risk it introduces. This research measures how much shadow AI usage organizations believe they have versus what they find when they look, and what a workable AI governance program looks like in practice.

Information Security, Risk and Compliance Management

The Autonomous SOC: Workforce Disruption, Human-in-the-Loop, and the Future of the Security Analyst

AI-powered security operations promise to close the analyst gap by triaging alerts, correlating telemetry, and even proposing (or taking) response actions at machine speed. But the shift raises hard questions for SOC leaders: which tasks are safe to fully automate, where must a human stay in the loop, and how does an organization reskill a Tier 1 analyst workforce whose job is being absorbed by AI? This research will survey SOC leaders on what they've automated, what broke when they did, and how they are restructuring roles and training as AI takes on a larger share of detection and response.

Securing the AI Development Lifecycle: Defending Against Prompt Injection, Model Manipulation, and Data Poisoning

Building AI into a product introduces an entirely new attack surface: prompts that manipulate model behavior, training data that can be poisoned, and models that can be coerced into leaking data or taking unintended actions. Traditional AppSec tooling was not built to test for these failure modes. This research examines how AppSec and AI/ML teams are collaborating (or failing to) to secure the AI development lifecycle, what tools and red-teaming practices are emerging, and how mature organizations' defenses are against these threats today.

Deepfakes and Synthetic Identity: Can Verification and Awareness Training Keep Pace with GenAI-Enabled Fraud?

Voice clones and video deepfakes have moved from novelty to a mainstream fraud vector, used to impersonate executives on video calls, bypass call-center identity checks, and manufacture synthetic identities that pass traditional verification. This research picks up where EMA's 2026 deepfake study left off, focused specifically on whether verification technology and employee training are keeping pace, or whether the arms race already favors the attacker.

Information Security, Risk and Compliance Management

Post-Quantum Migration in Motion: Crypto-Agility and the Countdown to Harvest-Now-Decrypt-Later Risk

For three years, EMA's quantum research asked whether organizations understood the threat. In 2027, the more useful question is whether they are moving. NIST's post-quantum standards are finalized, federal migration deadlines are in motion, and threat actors are already harvesting encrypted data today to decrypt once quantum computing matures. This research shifts focus from awareness to execution: what crypto-agility looks like in practice, where migrations are stalling, and what organizations need from vendors to make the transition tractable.

Continuous Threat Exposure Management: Moving Beyond Point-in-Time Vulnerability Scanning

Periodic vulnerability scans and annual penetration tests can't keep pace with environments that change hourly and attackers who move within minutes of a breach. Continuous threat exposure management reframes exposure as an ongoing program, discovering assets, validating which exposures are exploitable, and prioritizing remediation by real-world attack path rather than raw CVSS score. This research will measure how far organizations have moved from point-in-time scanning toward a continuous, validated exposure program, and examine what's blocking the rest.

Regulatory Whiplash: Navigating Global Compliance Volatility and Rising Executive Liability

The regulatory landscape security and compliance leaders navigate is moving rapidly and unpredictably. AI-specific regulation, evolving breach notification rules, and geopolitically driven data sovereignty requirements are all shifting simultaneously. At the same time, executives and boards face rising personal liability for compliance failures. This research will examine how organizations are building compliance programs resilient to regulatory volatility rather than reactive to the latest rule change, and how liability concerns are reshaping the relationship between security, legal, and the C-suite.

Securing the AI-Written Supply Chain: SBOMs, Code Provenance, and Trust in the Age of AI-Generated Code

AI coding assistants have accelerated software delivery, but a meaningful share of AI-generated code can reuse open-source snippets, sometimes with hallucinated or non-existent dependencies that attackers have begun registering and weaponizing. This research will examine how organizations are extending software supply chain security—software bill of materials (SBOM), dependency scanning, and code provenance—to account for AI-assisted development, and whether existing tooling and policy are keeping pace with how code gets written today.

Information Security, Risk and Compliance Management

The Browser as the New Endpoint: Enterprise Browser Security for a SaaS-First Workforce

For a SaaS-first, AI-augmented workforce, the browser is now the primary place where sensitive data is viewed, AI tools are accessed, and credentials are entered; yet it remains one of the least governed layers of the enterprise stack. Enterprise browser security and browser-based data loss prevention have emerged as a distinct market responding to this gap. This research will measure how organizations are thinking about the browser as a security control point, what's driving (or blocking) adoption, and how it complements or replaces existing endpoint and cloud access security broker (CASB) investments.

Cyber Resilience 2027: Business Continuity, Third-Party Risk, and the AI-Accelerated Incident Timeline

EMA's 2026 research established the shift from prevention-only security to a resilience posture that assumes breach. This follow-on study will test how that shift is holding up against a genuinely faster attacker: AI-accelerated attacks that move from initial access to lateral movement in under an hour. It will examine whether incident response plans, business continuity playbooks, and third-party risk programs have been re-timed to match, or whether resilience planning is still built around a response window that no longer exists.

Information Security, Risk and Compliance Management

Chris brings over 25 years of experience in IT leadership, cloud security, and regulatory compliance to EMA. He began his technical career as a systems administrator at a credit reporting company, later building its network operations, information security, and compliance practices. Prior to EMA, Chris served as CIO of a financial services company, guiding it through a NIST 800-53 evaluation to achieve Authority to Operate. He's a five-time Microsoft MVP for virtualization and cloud/data center management, and co-chairs the Cloud Security Alliance's zero trust working group.



Chris Steffen
VP of Research

Certifications
CISSP, CISA, CCZT

Sponsorship Opportunities

Engage with EMA Beyond the Research Report

In conjunction with the 2027 Research Calendar, EMA offers a range of sponsorship opportunities that connect you with enterprise IT decision-makers, elevate your brand, and generate qualified leads. These opportunities align with EMA's broader suite of services, give you more ways to engage with the market, and maximize your investment.

How the 2027 Research Calendar Connects to EMA's Services

The 2027 Research Calendar provides multiple ways to engage, and each opportunity can be tailored to your specific goals.

 Research Get the data and analysis you need to understand markets, buyers, and emerging technologies.	 Sponsor a report, provide input for research, and request custom data.
 Analyst Engagement Tap into EMA's analyst expertise through briefings, advisory support, subscription access, and speaking opportunities.	 Bring EMA analysts into product strategy, market discussions, events, and executive conversations.
 Content & Thought Leadership Showcase your expertise with case studies, white papers, eBooks, and infographics, developed with EMA's research and analyst insight.	 Turn research and analyst insight into credible content that supports education and thought leadership.
 Media & Demand Generation Reach and engage your target audience with webinars, podcasts, blogs, and videos that put your message in front of key decision-makers.	 Extend your message through analyst-led media and content designed to engage enterprise IT audiences.
 Market & Vendor Visibility Build credibility and stand out by participating in EMA™ PRISM, Radar, and Top 3 reports.	 Build visibility and credibility through EMA's market evaluation and vendor recognition programs.
 Subscriptions & Bundles Maximize your investment with flexible subscription options and bundles that combine multiple services for greater reach and value.	 Combine research, analyst access, content, and other services into an ongoing engagement.



About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading IT analyst research firm that specializes in going “beyond the surface” to provide deep insight across the full spectrum of IT management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help its clients achieve their goals. Learn more about EMA research, analysis, and consulting services at www.enterprisemanagement.com. You can also follow EMA on [X](#) or [LinkedIn](#).

This report, in whole or in part, may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice. Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. “EMA” and “Enterprise Management Associates” are trademarks of Enterprise Management Associates, Inc. in the United States and other countries.

©2026 Enterprise Management Associates, Inc. All Rights Reserved. EMA™, ENTERPRISE MANAGEMENT ASSOCIATES®, and the mobius symbol are registered trademarks or common law trademarks of Enterprise Management Associates, Inc.