EMA™ IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

2026
Enterprise Management Associates (EMA) Research Calendar

Introducing the EMA 2026 Research Calendar

Enterprise Management Associates (EMA) is pleased to present our 2026 Research Calendar, highlighting the flagship studies, PRISM and Radar reports, and emerging coverage areas that will define our research agenda in the coming year.

The 2026 calendar reflects EMA's continued commitment to delivering independent, actionable insights across the evolving technology landscape. These research initiatives provide IT leaders and solution providers with independent insights and analysis that inform decisions, shape strategies, and drive success.

Research Highlights for 2026

Our research this year covers both enduring priorities and newly emerging frontiers:

Data and Analytics: AI/ML integration in analytics, the urgency of real-time streaming, and the evolution of semantic interoperability frameworks such as the Open Semantic Interchange initiative.

Cybersecurity: AI-driven WAAP and API protection, quantum readiness, deepfake-enabled threats, and a broad suite of PRISM reports spanning cloud-native security, IAM, DLP, SOAR, SASE, DSPM, and SIEM.

Intelligent Automation: The impact of GenAI on observability, the evolution of workload orchestration, the transformation of the DevOps toolchain into an AI-first stack, and the flagship Radar report on workload automation.

Service and Operations: Modern IT asset management (ITAM), IT financial and technology business management (ITFM/TBM), and the evolving role of IT service management (ITSM) in hybrid and AI-enabled environments with Radar and PRISM reports providing insight into capabilities and adoption strategies.

Network Infrastructure and Operations: NetOps megatrends, collaboration between NetSecOps, adoption of open networking, zero trust networking architectures, and Radar research on network operations observability.

These studies deliver strategic guidance to support technology adoption, influence product direction, and clarify the operational implications of market shifts.

The Value of Research

EMA's research is informed by a strong understanding of how IT and cybersecurity decision-makers consume information. In a recent EMA survey, 94% of IT decision-makers rated industry analyst insights as "extremely" or "very important" in their product evaluation process.

Key findings highlight that decision-makers value:

- Detailed solution information (57%) and ranked comparative reports (47%) for evaluating vendor capabilities.
- Chart-based reports (42%) and third-party analysis (46%) as trusted, efficient tools for distilling complex technical details.
- Analysts' credibility, context, and foresight are critical advantages over vendor-provided content.

The research also underscores broader industry trends: a "buyer beware" mentality driving demand for independent validation, a rising reliance on data-driven decision making, and the need to understand interoperability and consolidation across IT ecosystems.

These findings validate EMA's mission: to deliver research that is detailed, comparative, unbiased, and strategic.

Looking Ahead

The 2026 Research Calendar reflects EMA's perspective on the year's most important technology and market developments. We also recognize that new priorities emerge quickly, and we welcome input on additional research topics of interest.

For more information or to schedule a **briefing** with EMA analysts, please visit our **website**.

When looking for comparative information about solution capabilities, what is your preferred method of receiving that information?

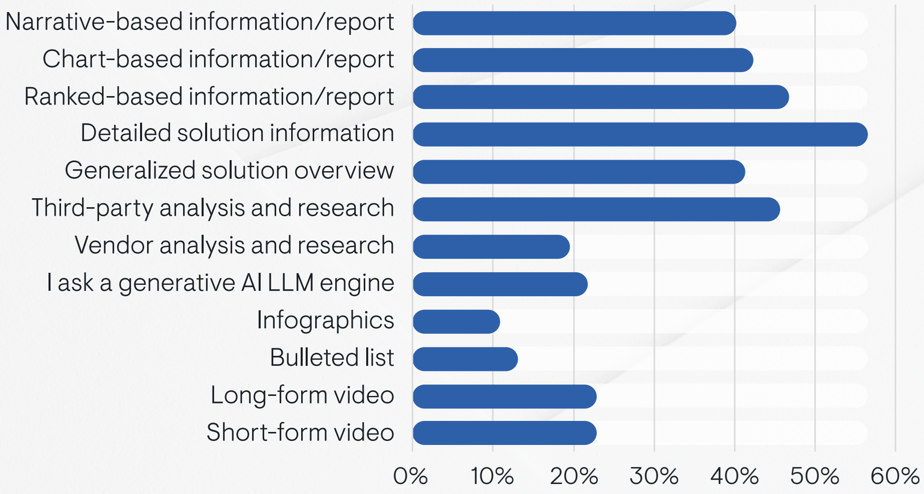

Table of Contents

Table of Contents

Data and Analytics

The Synergistic Integration of AI and Machine Learning in Data and Analytics

As organizations grapple with an unprecedented volume, velocity, and variety of data, traditional analytical methods are proving insufficient for extracting deep, actionable insights. This study posits that the synergy between AI's cognitive capabilities and ML's predictive power is not merely an evolutionary step but a revolutionary one, enabling a new era of data-driven decision-making. The study will explore how AI and ML models automate critical stages of the analytics lifecycle, such as data cleaning and pattern recognition, reducing manual effort and accelerating the path to insight. It will also highlight their impact on predictive and prescriptive analytics, enabling businesses to forecast trends with greater accuracy and optimize strategies proactively. Together, these findings offer a comprehensive roadmap for organizations aiming to harness AI and ML to gain a lasting competitive edge.

The Urgency of Now: Understanding Real-Time and Streaming Analytics

As data from sources like IoT devices, financial markets, and social media platforms grows exponentially, traditional batch processing methods are becoming obsolete. This study argues that the ability to process and analyze data the moment it is generated is no longer a luxury but a critical necessity for maintaining a competitive edge. The research will investigate the technological frameworks and methodologies that enable real-time analytics, including stream processing engines, in-memory databases, and event-driven architectures. It will also examine the practical applications across various sectors, such as fraud detection in banking and predictive maintenance in manufacturing. The findings will provide a strategic guide for organizations aiming to implement real-time analytics to make more informed decisions and drive business value.

A New Paradigm for Data: The Intersection of Data Democratization and Data Mesh

This research investigates the convergence of data democratization and the data mesh architectural paradigm as a strategic approach to overcome the limitations of centralized data management. As organizations aim to empower all employees with timely, accessible data for decision-making, traditional monolithic data warehouses and lakes often create bottlenecks and silos. This study posits that the data mesh, with its decentralized, domain-oriented structure, is the key enabler for true data democratization. The research will analyze how data mesh principles—such as treating data as a product, domain-oriented ownership, and federated computational governance—facilitate a culture of self-service analytics and widespread data literacy. A mixed-methods approach will be used to evaluate both the benefits, such as enhanced business agility and faster time-to-insight, and the challenges, including organizational change management and technical complexity. The findings will provide a practical framework for organizations seeking to implement a decentralized data strategy to unlock the full value of their data assets.

Information Security, Risk and Compliance Management

Beyond the Firewall: Securing the Modern Web with AI-Driven WAAP and API Protection

Traditional web application firewalls (WAFs) are a foundational security layer, but their static, rule-based approach is increasingly inadequate against modern threats. This research explores the evolution from WAF to web application and API protection (WAAP), a next-generation security paradigm that is more adaptive and proactive. Key trends driving this shift include the widespread adoption of cloud native applications, the proliferation of APIs as a primary attack vector, and the rise of machine learning-driven attacks. This project will investigate how modern WAAP solutions leverage AI and machine learning to provide real-time, behavioral-based threat detection and analyze their critical role in securing APIs, which traditional WAFs were not built to protect. The findings will assess the efficacy of these new technologies in mitigating zero-day vulnerabilities, sophisticated botnets, and API-specific exploits, ultimately providing a framework for organizations to evaluate and adopt advanced application security solutions.

Beyond Prevention: Architecting a Resilient Cybersecurity Framework for the Modern Enterprise

This research investigates the evolving landscape of cyber resilience, a critical shift from prevention-focused security to a proactive model that assumes a breach. The study addresses key trends, including the widespread adoption of a zero trust architecture, which mandates continuous verification and microsegmentation to contain threats and prevent lateral movement. We will also explore the increasing integration of artificial intelligence and machine learning to power predictive threat intelligence and automate incident response, enabling organizations to anticipate and react to attacks with unprecedented speed. The abstract highlights the trend of integrating business continuity and risk quantification into cybersecurity strategy, aligning resilience efforts with core business objectives and financial impact. Finally, the research will analyze how enterprises are strengthening their defense by managing and monitoring third-party and supply chain risk. The findings will provide a comprehensive framework for organizations to build a robust, business-driven, and truly resilient cybersecurity posture.

Information Security, Risk and Compliance Management

The Mainframe in 2026: An Era of AI, Hybrid Cloud, and Business Resilience

Four years after our initial research, the conversation around the mainframe evolved from a simple "mainframe or cloud" debate to a nuanced discussion of coexistence. This research revisits the topic, analyzing the mainframe's position within a mature hybrid cloud and multi-cloud landscape. It will investigate the transformative role of generative AI in modernizing operations and its potential to unlock new value from mainframe data. We will explore how automation and AI are addressing the longstanding talent and administrative challenges and whether they can finally close the perceived gap in business agility and innovation. The study will also quantify the often-overlooked costs of migration, including hidden cyber resilience and operational risks, to provide a true total cost of ownership (TCO) comparison. By surveying IT and business leaders, this research will offer a definitive look at the mainframe's role in the future of enterprise computing and whether it can serve as a secure, efficient, and intelligent foundation for a data-driven world.

Supply Chain Security: Enterprise Strategies for Mitigating Cybersecurity Risk

The interconnected nature of modern business has made the supply chain a primary target for cyber attackers, necessitating a fundamental shift in cybersecurity strategy. This research will analyze how enterprises are addressing supply chain security beyond traditional perimeter defense. It will investigate the efficacy of emerging technologies, such as AI-driven continuous monitoring and extended detection and response in providing real-time risk visibility across a complex web of third-party vendors. The study will also examine frameworks for securing the software development lifecycle, including the use of Software Bill of Materials (SBOMs) and code integrity validation to mitigate software supply chain attacks. By exploring how organizations integrate these tools to create a holistic security posture, this research will provide a best practice model for building a resilient supply chain and mitigating the cascading risk that compromised business partners pose.

Data Security and Privacy at the Endpoint in a Distributed World

The distributed nature of modern business rendered traditional perimeter security obsolete, elevating the need for a data-centric approach to cybersecurity. This research investigates the emerging field of data security posture management (DSPM) as a core component of enterprise security. It will examine the key capabilities of DSPM solutions, including continuous data discovery and classification, real-time risk assessment, and automated remediation across cloud and hybrid environments. The study will analyze how these capabilities address critical vulnerabilities, such as misconfigurations, over-permissioning, and data sprawl, which are common in a decentralized world. By exploring the role of DSPM in providing holistic data visibility and enforcing least privilege access, this research aims to provide a definitive framework for organizations seeking to proactively manage their data security posture and ensure compliance with modern privacy regulations.

Information Security, Risk and Compliance Management

Digital Attacks, Physical Impact: Trends and Solutions for Attacks Against IoT and OT Systems

The growing convergence of information technology (IT) and operational technology (OT) created a new era of cyber threats with tangible, physical consequences. This project investigates the key trends in attacks against IoT and OT systems, moving beyond traditional data theft to focus on real-world disruption. The research will analyze the shift in attacker motivations from financial gain to operational sabotage, as evidenced by ransomware campaigns designed to halt critical infrastructure. It will also explore the expanding attack surface that the proliferation of unmanaged IoT devices presents, as well as the commoditization of hacking tools that lower the barrier to entry for adversaries. By examining the increasing convergence of IT and OT attack vectors, this study aims to provide a comprehensive framework for understanding and mitigating the physical impacts of digital threats, informing a proactive approach to securing the cyber-physical world.

Are Security Best Practices Enough to be Quantum-Ready?

The security space is abuzz with news about quantum computing, and it is not a matter of if it is coming, but when. The US government is already evaluating quantum encryption standards and selected four candidates for review. Apart from world governments and bleeding-edge adopters, is quantum computing really something enterprise leadership needs to be concerned about? Does adherence to security best practices provide security that is “good enough” for most organizations? Are there strategies and tools that enterprises should adopt to be quantum-ready? Since many workloads and data stores migrated (or are being migrated) to the cloud, is this a problem for the cloud service providers to deal with?

Identity Attacks in Cyber: Are Current Defenses Keeping Up?

Identity-based attacks increasingly plague the cybersecurity landscape, with adversaries exploiting stolen credentials, phishing schemes, and weak authentication mechanisms to breach organizations. As remote work and digital transformation accelerate, identity has become the new perimeter for security. Are existing identity and access management (IAM) solutions robust enough to counter sophisticated attacks, like deepfake-enabled social engineering or credential stuffing? Can organizations rely on multi-factor authentication (MFA) and zero trust models to mitigate risks, or are new approaches needed? With the rise of AI-driven attack tools, how are threat actors evolving their tactics to target identities?

Information Security, Risk and Compliance Management

Deepfakes and the New Dawn of Social Engineering

The rapid advancement of deepfake technology ushered in a new era of social engineering, in which hyper-realistic audio and video forgeries are being weaponized to manipulate individuals and organizations. From impersonating executives to bypassing biometric authentication, deepfakes pose unprecedented challenges to trust and security. Are current detection tools and employee training programs sufficient to counter these sophisticated threats? How are organizations preparing for the psychological and operational impacts of deepfake-driven scams? As AI continues to democratize access to deepfake creation, what proactive measures can enterprises adopt to stay ahead?

The Human Impact of Cyber Attacks: Identity Theft, Disrupted Critical Services, and Beyond

Cyber attacks are no longer just a technical concern. Their ripple effects profoundly impact individuals, disrupting lives through identity theft, financial loss, and interruptions to critical services, like health care and emergency response. As cybercriminals increasingly target personal data and essential systems, the human toll – emotional, financial, and societal – continues to grow. Are organizations adequately addressing the human consequences of these breaches? Can existing cybersecurity frameworks mitigate the cascading effects on individuals and communities? How are victims supported in the aftermath of attacks targeting medical services or personal identities?

Behavioral Analytics and AI for Proactive Threat Hunting Across Diverse Endpoints

In an era of expanding attack surfaces, behavioral analytics powered by AI are transforming proactive threat hunting from reactive forensics to predictive defense across diverse endpoints, like IoT devices, mobile platforms, and hybrid cloud environments. As threat actors leverage polymorphic malware and insider threats, traditional signature-based detection falls short – can AI-driven anomaly detection and user behavior profiling identify subtle indicators of compromise before they escalate? Are organizations equipped to integrate these technologies across fragmented endpoint ecosystems without overwhelming their security operations centers? With the proliferation of edge computing, how can enterprises scale behavioral analytics to maintain visibility and response agility?

Security First App Design: Building Trust Through User-Centric Security

As mobile apps become integral to daily life, designing applications with security as a foundational principle is critical to protecting user data and maintaining trust. With rising threats like data breaches, insecure APIs, and phishing via apps, can developers embed robust security without compromising usability or performance? Are organizations prioritizing security-first principles in app design to address vulnerabilities early in the development lifecycle? How can user-centric design balance intuitive interfaces with advanced security features, like secure authentication or encrypted data storage? As privacy regulations tighten, what strategies ensure apps remain compliant and resilient?

Information Security, Risk and Compliance Management

Securing Edge Computing: Balancing Performance and Protection in Distributed Systems

Edge computing is transforming how data is processed by bringing computation closer to the source, but its distributed nature introduces new security challenges, from unprotected IoT devices to unsecured data pipelines. As organizations deploy edge solutions to enhance speed and efficiency, are they adequately addressing risks like data interception, device tampering, or lateral attacks across edge nodes? Can existing security frameworks scale to protect dynamic, low-latency environments without sacrificing performance? With edge adoption accelerating in industries like health care and manufacturing, what measures ensure resilience against evolving threats?

Cyber Threat Intelligence and Proactive Defense

Cyber threat intelligence (CTI) is pivotal in transforming raw data into actionable insights to anticipate and counter sophisticated cyber threats. As attackers leverage advanced tactics like zero-day exploits and nation state campaigns, can organizations harness CTI to stay ahead of adversaries? Are current CTI tools and processes effective in integrating real-time data from diverse sources, such as dark web monitoring or open source intelligence, to enable proactive defense? With the growing complexity of hybrid IT environments, how can enterprises operationalize CTI without overwhelming security teams?

EMA™ PRISM Reports

The EMA™ PRISM report, an acronym for PRoduct and Functionality, Integrations and Operability, and Strength and Maturity, provides a structured approach for evaluating security vendors and their solutions. Each offering is assessed against these criteria to measure its ability to deliver value across both on-premises and cloud environments. The report equips organizations with actionable insights to make informed IT and security investment decisions, helping them identify the best solutions to safeguard critical assets and reduce risk.

EMA™ PRISM Report for Cloud Native Security & Container Security

This EMA PRISM Report will assess the capabilities of leading vendors for cloud native security and container security solutions. The widespread adoption of microservices, serverless computing, and containers created new security challenges, including fragmented visibility, a highly dynamic attack surface, and the risk of misconfigurations in multi-cloud environments. This report will evaluate how vendors are addressing these complexities by offering solutions that integrate security into the CI/CD pipeline, provide runtime protection for ephemeral workloads, and manage risk across diverse cloud platforms.

Information Security, Risk and Compliance Management

EMA™ PRISM Report for Identity and Access Management (IAM)

This EMA PRISM Report will assess the capabilities of leading vendors for identity and access management (IAM) solutions. The rise of remote work, third-party access, and non-human identities made IAM a primary security perimeter. This report will evaluate vendor approaches to key challenges, such as managing privileged access, enforcing a zero trust architecture, securing a distributed workforce, and using AI to detect identity-based threats, like deepfakes and account takeovers. The study will also explore how modern IAM solutions are addressing the complexities of managing identities across hybrid and multi-cloud environments.

EMA™ PRISM Report for Data Loss Prevention (DLP)

This EMA PRISM Report will assess the capabilities of leading vendors for data loss prevention (DLP) solutions. As sensitive data is created, stored, and shared across a wide range of platforms – from cloud applications to employee endpoints – traditional perimeter-based DLP is no longer sufficient. This report will evaluate how vendors are tackling challenges like securing data in motion and at rest, protecting against insider threats in a hybrid work environment, and automating data classification to ensure compliance with a growing number of privacy regulations. The study will also examine the evolution of DLP into a data-centric security model.

EMA™ PRISM Report for Security Orchestration, Automation, and Response (SOAR)

This EMA PRISM Report will assess the capabilities of leading vendors for security orchestration, automation, and response (SOAR) solutions. The overwhelming volume of security alerts and the shortage of skilled analysts have created a significant burden for security operations centers. This report will evaluate how SOAR platforms are helping organizations overcome these challenges by automating repetitive tasks, orchestrating complex workflows across disparate security tools, and accelerating incident response. The study will also look at how vendors are integrating AI and machine learning to provide more intelligent, adaptive playbooks and reduce analyst fatigue.

EMA™ PRISM Report for AppSec & DevSecOps – Actionable Vulnerability Insights

This EMA PRISM Report will assess the capabilities of leading vendors for application security (AppSec) and DevSecOps solutions. The demand for rapid software delivery often comes at the expense of security, leaving organizations vulnerable to attacks against their applications. This report will evaluate how vendors are helping to address these issues by integrating security into the entire software development lifecycle (SDLC) through actionable vulnerability insights. The study will focus on how solutions are providing developers with the tools and context needed to "shift left" and fix vulnerabilities before they reach production, reducing risk and accelerating the remediation process.

Information Security, Risk and Compliance Management

EMA™ PRISM Report for SASE

This EMA PRISM Report will assess the capabilities of leading vendors for secure access service edge (SASE) solutions. The shift to a decentralized workforce and the adoption of multi-cloud architectures have made the traditional network perimeter obsolete. SASE seeks to address this by converging network and security functions into a single cloud-delivered service. This report will evaluate vendor offerings and their ability to tackle challenges, like inconsistent network performance, lack of visibility into SaaS applications, and the complexity of managing a fragmented security stack across a distributed enterprise.

EMA™ PRISM Report for Next-Generation Antivirus (NGAV)

This EMA PRISM Report will assess the capabilities of leading vendors for next-generation antivirus (NGAV) solutions. Traditional signature-based antivirus is no longer effective against sophisticated, file-less, and polymorphic malware. This report will evaluate how vendors are tackling advanced threats by leveraging machine learning, behavioral analytics, and threat intelligence to prevent, detect, and respond to threats in real time. The study will also examine how NGAV is evolving to integrate with endpoint detection and response (EDR) to provide a more comprehensive endpoint security solution.

EMA™ PRISM Report for Data Security Posture Management (DSPM)

This EMA PRISM Report will assess the capabilities of the leading vendors for data security posture management (DSPM) solutions. The proliferation of data across multi-cloud environments, SaaS applications, and unmanaged endpoints created a significant challenge for security teams, with "shadow data" and misconfigurations leading to widespread data exposure. This report will evaluate how vendors are helping to solve these problems by providing continuous discovery, classification, and risk assessment of all sensitive data. The study will also examine how DSPM solutions automate policy enforcement and streamline compliance to protect against data breaches.

EMA™ PRISM Report for Email Security

This EMA PRISM Report will assess the capabilities of leading vendors for email security solutions. As phishing, business email compromise (BEC), and ransomware continue to evolve with the use of AI and deepfake technology, email remains the number one attack vector. This report will evaluate how vendors are addressing these advanced threats by moving beyond simple signature-based filtering to leverage machine learning, behavioral analytics, and impersonation defense. The study will also examine the growing importance of securing collaboration platforms that are now closely integrated with email workflows.

Information Security, Risk and Compliance Management

EMA™ PRISM Report for Attack Surface Management (ASM)

This EMA PRISM Report will assess the capabilities of leading vendors for attack surface management (ASM) solutions. The proliferation of assets across cloud environments, third-party partners, and a distributed workforce made it nearly impossible for organizations to maintain a complete and accurate inventory of all their internet-facing assets. This report will evaluate how vendors are helping to solve these problems by providing continuous discovery, asset classification, and automated vulnerability prioritization. The study will also examine how ASM solutions help to identify and mitigate misconfigurations and other exposures that adversaries could exploit.

EMA™ PRISM Report for SIEM

This EMA PRISM Report will assess the capabilities of leading vendors for security information and event management (SIEM) solutions. As data from disparate sources continues to grow at an unprecedented rate, SOCs are overwhelmed with a high volume of uncontextualized alerts, leading to missed threats and analyst burnout. This report will evaluate how vendors are addressing these challenges by leveraging AI and machine learning to provide intelligent correlation, behavioral analytics, and automated threat prioritization. The study will also examine the integration of SIEM with other security tools to streamline investigation and response.

EMA™ PRISM Report for Deception Technology

This EMA PRISM Report will assess the capabilities of leading vendors for deception technology solutions. As cybercriminals become more adept at bypassing traditional defenses and moving laterally within networks, organizations need a proactive way to detect their presence. Deception technology addresses this by planting decoys, traps, and lures that mimic legitimate assets, baiting attackers into revealing themselves. This report will evaluate how vendors are helping organizations to overcome the challenges of deploying and managing these decoys while also providing early and high-fidelity alerts to internal security teams.

EMA™ PRISM Report for Threat Hunting

This EMA PRISM Report will assess the capabilities of leading vendors for threat hunting solutions. The average time to detect a breach remains unacceptably high, since sophisticated attackers are often able to bypass automated defenses and remain undetected for months. This report will evaluate how vendors are helping organizations overcome this challenge by providing the tools and analytics needed for proactive threat hunting. The study will examine how solutions provide enriched telemetry, behavioral analytics, and query languages that empower security analysts to search for and neutralize hidden threats before a major incident occurs.

Information Security, Risk and Compliance Management

EMA™ Radar Report for Privileged Access Management (PAM)

The EMA Radar for PAM identifies leading solution providers and empirically compares and grades their offered solutions against a broad range of measurements to determine overall product strengths and cost-efficiencies.

This EMA Radar report is designed to assist organizations in identifying privileged access management solutions that will most effectively meet their requirements for improving security postures while minimizing management efforts and related costs.

Information Security, Risk and Compliance Management

Chris Steffen

VP of Research

Certifications

Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), Certificate of Competency in Zero Trust (CCZT)

Chris brings over 25 years of industry experience to Enterprise Management Associates, focusing on IT management/leadership, cloud security, and regulatory compliance. Chris has had a variety of roles as a professional, from Camping Director for the Boy Scouts to Press Secretary for the Colorado Speaker of the House. His technical career started in financial services as the systems administrator for a credit reporting company. As the company continued to grow, Chris built the network operations, information security, and technical compliance practices before leaving as the Principal Technical Architect. He was the Director of IT for a manufacturing company and the Chief Evangelist for several technical companies, focusing on cloud security.

Prior to joining EMA, Chris served as the CIO of a financial services company and supervised their technology-related functions, including the development and implementation of the company's technical vision and management of the technical staff. He also guided the company through a NIST 800-53 evaluation and successfully obtained an authority to operate (ATO). Chris was also awarded the Microsoft Most Valuable Professional Award five times for virtualization and cloud and data center management (CDM). He is currently the co-chair of the zero trust working group for the Cloud Security Alliance.

Ken Buckler

Research Director

Certifications

CompTIA Advanced Security Practitioner (CASP), CompTIA Security+, Proofpoint Certified AI/ML Specialist, Proofpoint Certified Security Awareness Specialist, Lakera 101 AI Security, CodeFresh GitOps Fundamentals, ASSA ABLOY Certificates for Electronic Security and Electronic Access Control Systems

Ken has over 15 years of industry experience as a noted information and cybersecurity practitioner, software developer, author, and presenter, focusing on endpoint security and Federal Information Security Management Act (FISMA) and NIST 800-53 compliance. Focusing on strict federal security standards, Ken has consulted with numerous federal organizations, including Defense Information Systems Agency (DISA), Department of Veterans Affairs, and the Census Bureau.

He was previously board chair of The Mars Generation's Student Space Ambassador Leadership Program, an advisory board made up of students and professional mentors focused on STEAM learning and advocacy. His technical career started in the defense sector as a quality assurance and information assurance engineer contracted with the DISA Defense Message System (DMS), eventually designing the top-level architecture of the host-based security system (HBSS) integration for the DMS global messaging backbone. Ken has presented at industry conferences with his research on early warning of cyber-attacks based on open source intelligence (OSINT).

Intelligent Automation

Tuning the Signal: Rethinking Observability and Application Performance in the GenAI Era

As observability and application performance monitoring (APM) begin to converge, this research explores how enterprises are recalibrating their monitoring strategies to focus on business outcomes, user experience, and incident resolution. With generative AI enabling deeper correlations and narrative storytelling from telemetry data, the boundaries between APM, infrastructure monitoring, and full-stack observability are shifting. This study examines how organizations are adapting platform selection, team responsibilities, and performance KPIs in response to AI and the rising complexity of distributed systems.

Orchestrating the Digital Core: Workload Automation Strategies for a Federated, AI-Driven Enterprise

This major research initiative revisits the strategic role of workload automation (WLA) as it evolves from centralized job scheduling to orchestrated, intelligent execution across hybrid IT, business operations, and AI-driven processes. The study will track WLA maturity metrics dating back to 2013 while exploring how generative AI is influencing automation logic, exception handling, and decision support. It will also analyze how observability and integration requirements are reshaping the definition of orchestration platforms and their role in digital transformation.

The OpenTelemetry Imperative: Standardizing Signals in a Fragmented Observability World

OpenTelemetry (OTel) has become the de facto standard for instrumenting modern cloud native systems, but adoption remains uneven and misunderstood. This research will evaluate how enterprises are deploying OTel across traces, metrics, logs, events, and profiles – and where toolchain gaps and vendor limitations persist. It will explore deployment models, real-world signal coverage, and how OTel is enabling or disrupting broader observability strategies. The study will help buyers navigate standardization decisions while giving vendors data on what's working and what's lagging.

Navigating the Observability Maze: A PRISM View into Platform Differentiation and Market Traction

With observability platforms increasingly claiming end-to-end visibility, GenAI copilots, and service intelligence, this PRISM Report will map the true shape of the market. It will categorize vendors based on architecture, telemetry integration, workflow coverage, and AI sophistication while clarifying which platforms offer differentiation and which blur into sameness. The report will help IT decision-makers cut through inflated claims and understand where real product innovation, convergence, or specialization is occurring across the observability landscape.

Intelligent Automation

The AI-First DevOps Stack: Building Secure, Productive, and Auditable Toolchains

As AI becomes embedded throughout the DevOps lifecycle, this research will assess how teams are rethinking productivity, code security, compliance, and tooling alignment. The study will explore the adoption of AI-powered code generation, agentic test automation, automated AppSec enforcement, and CI/CD orchestration, along with challenges around auditing and governing AI-generated assets. It will highlight how internal developer platforms and toolchain convergence are changing the nature of software delivery in high-AI organizations.

Architects of Autonomy: How Intelligent Orchestration is Rewiring the Enterprise Nervous System

Orchestration has moved beyond IT job management and is emerging as a unifying layer for coordinating services, agents, and business processes across the digital enterprise. This research explores how intelligent orchestration – powered by AI, event-driven triggers, and agent-based logic – is enabling enterprises to build self-healing, adaptive systems. It will analyze platform adoption, decision logic complexity, observability integration, and use cases spanning IT, ops, and line-of-business automation.

EMA™ Radar for Workload Automation and Orchestration: Evaluating the Engines of Enterprise Execution

This flagship Radar will assess the leading platforms powering enterprise workload automation and orchestration. Vendors will be scored across five key dimensions, with expanded 2026 criteria for agentic orchestration, observability transparency, GitOps readiness, SaaS platform maturity, and orchestration intelligence. The Radar will include structured surveys, customer reference interviews, and KPI-aligned scoring to guide enterprise buyers and highlight innovation across this evolving segment of the automation landscape.

Seeing with New Eyes: How GenAI is Reshaping Observability, Insight, and Action

This study examines the transformative impact of GenAI on observability platforms, from simplifying telemetry interpretation to enabling story-based diagnostics and guided remediation. It will assess how observability teams are incorporating LLM-based insights into workflows, dashboards, and team collaboration. The research will explore how GenAI is improving time to insight, reducing operator fatigue, and enhancing platform usability for both expert SREs and non-technical stakeholders.

Intelligent Automation

Dan Twing

President and COO

As President and COO of EMA, Dan develops and executes strategic market research, delivers value to IT organizations through consulting engagements, and directs product developments and marketing efforts. Dan has over 30 years of experience in information systems, software development, and technology outsourcing.

Prior to joining EMA, Dan was the President and CEO of NETdelivery. Dan led the company through changing strategic direction, identifying and penetrating new markets, and realigning corporate assets to support a new strategy. He also led the product development, engineering, quality assurance, program management, professional services, and customer support functions.

As VP of Financial Products for the Electronic Commerce division of EDS, a leading global information technology services company, Dan spearheaded product strategy, system development, operations, and customer support functions. During his 14 years with EDS, Dan also held product management and systems engineering positions, managing and operating a variety of banking systems, payment systems, and other electronic commerce services.

Dan's experience managing multi-site and multi-cultural service operations gives him a unique, hands-on perspective into outsourcing and managed service providers. He is a coauthor of *CMDB Systems: Making Change Work in the Age of Cloud and Agile*.

IT Service/Operations (ServiceOps)

Redefining Modern Service Management: ServiceOps, ESM, and the Rise of AI-Powered Services

This multi-sponsor research is EMA's latest annual exploration into the evolving state of service delivery across the modern enterprise. As organizations seek to modernize and unify the way services are defined, delivered, and optimized, two dominant strategies emerged: service operations (ServiceOps) and enterprise service management (ESM).

This survey explores the convergence of ServiceOps and ESM strategies, assessing how AI-enabled workflows, cross-domain automation, and integrated platforms are transforming efficiency, responsiveness, and user experience. The research identifies the strategies, adoption patterns, and operational outcomes that are shaping the next generation of service management.

EMA™ PRISM Report for IT Asset Management (ITAM)

The EMA PRISM Report provides a comprehensive overview of the ITAM market, focusing on solutions that combine asset lifecycle automation, compliance, and governance across hybrid environments. It analyzes how leading platforms deliver visibility, optimize costs, and mitigate risk through integration with broader ServiceOps and ESM strategies. The study offers an accessible market map for understanding the capabilities and differentiators that define modern ITAM.

Breaking Boundaries: The Convergence of ITOM and Service Management

This research investigates the expansion of service management platforms into IT operations domains, incorporating capabilities such as discovery, event correlation, and automation triggers. It examines how convergence impacts architecture, tool strategy, and operational outcomes, as well as where specialized ITOM and observability tools remain critical. The analysis maps integration patterns, value drivers, and adoption trends that define this evolving platform footprint.

The New Metrics for ServiceOps

This focused study explores the shift from traditional service-level agreements to experience-driven and outcome-based metrics in ServiceOps environments. It examines how organizations balance SLAs and XLAs, link service performance to business value, and use AI-driven analytics to deliver real-time insights. The research highlights measurement strategies that elevate IT's role in improving customer and employee experience while aligning with strategic objectives.

IT Service/Operations (ServiceOps)

EMA™ Radar Report for AIOps – Intelligent Service and Operations

Building on EMA's established Radar research from 2020 and 2024, this research evaluates how platforms advance intelligent operations for both ServiceOps and ITOM use cases. It benchmarks vendor capabilities in incident analysis, automation, and real-time insight delivery, distinguishing between aspirational claims and proven outcomes. The report offers an evidence-based guide to solutions that improve agility, service quality, and operational resilience.

EMA™ PRISM Report for IT Financial Management/ Technology Business Management (ITFM/ TBM)

Financial transparency is now a critical dimension of IT service delivery. As CIOs are pressed to link cost, value, and business outcomes, ITFM and TBM solutions are gaining momentum within the ServiceOps and ESM ecosystem. The PRISM Report evaluates how financial management capabilities integrate with service and operations platforms to support budgeting, chargeback/showback, and cost optimization. The analysis offers a clear market view of solutions that bring financial transparency and business alignment into the ServiceOps ecosystem.

IT Service/Operations (ServiceOps)

Parker leads the IT service operations (ServiceOps) practice at EMA, focusing on the convergence of IT service management (ITSM), IT operations management (ITOM), enterprise service management (ESM), business service management (BSM), and AIOps in ways that help enterprises align business objectives with technology strategies.

With over a decade of senior-level experience in product marketing, competitive research, and analyst engagement, Parker led teams in enterprise information management, process automation, discovery, observability, and digital accessibility at top companies, including Dynatrace, Redwood Software, and others. Parker brings a unique client-side perspective to EMA research, having worked extensively with EMA and other analyst firms in his communications and product marketing roles at enterprise technology vendors. The experience provides him with deep insights into how organizations engage with analyst research and implement complex technology solutions.

Parker Hathcock

Research Director

Network Infrastructure and Operations

Network Management Megatrends 2026

The ultimate benchmarking study of enterprise network operations returns! EMA's biennial "Network Management Megatrends" research explores the effectiveness of today's NetOps teams and their tools with statistics on alert noise, reactive troubleshooting, and tool strategy.

In 2026, the megatrends research will examine how industry trends – including enterprise AI initiatives, hybrid and multi-cloud architecture, network engineering skills gaps, and automated Day 2 operations – are impacting network operations strategy.

Networks as Code: Aligning NetOps with DevOps Through Network Automation

EMA research increasingly finds that network engineering teams are adopting DevOps principles to improve their approach to network automation and to align network services with DevOps and cloud groups. As NetDevOps takes hold in enterprises, these teams are developing and buying tools that align with infrastructure as code and CI/CD principles.

This research will explore the state of NetOps and DevOps alignment and how it impacts network automation strategy.

Striving for a Single Pane of Glass: Exploring the Realities of IT Observability Tool Consolidation

Tool sprawl is a fact of life for large IT organizations. Across networking, systems, storage, applications, cloud, and security groups, each has its preferred tools for monitoring and observability. This practice creates operational silos and a war-room mentality where mean time to innocence is an informal but essential metric.

With this new research, EMA will explore interest in consolidating and integrating tools across functional groups. It will identify the drivers and goals of these consolidation efforts, which tools fall within the scope of the project, and which are excluded. The report will also explore cultural and technical barriers to achieving a consolidated toolset. EMA will ask IT leaders to identify how they attack the problem of tool sprawl, including full-stack platform adoption, AI-driven tool rationalization, and multi-vendor integrations. Finally, this research will identify the benefits organizations experience with observability consolidation and the mistakes they made along the way.

Network Infrastructure and Operations

NetSecOps: Exploring Partnerships Between Cybersecurity and Network Engineering

EMA's biennial NetSecOps research explores the deepening partnerships between network infrastructure and operations teams and cybersecurity teams. Technical and cultural gaps traditionally undermined these partnerships. In EMA's 2024 NetSecOps report, 86% of IT professionals reported that these teams increased their level of collaboration., but nly 45% reported that these partnerships were completely successful.

This new research will explore drivers of NetSecOps collaboration, the key technical enablers of collaboration (including automation and observability), and the challenges that undermine convergence.

Open Networking: Exploring Enterprise Engagement with Disaggregated Solutions

Vertically integrated network hardware dominated the IT industry for decades, but open networking is gaining ground. Hyperscalers consistently champion open networking, but enterprises are starting to inch in that direction, partially thanks to a maturing vendor ecosystem for the open source network operating system, SONiC.

This new research will survey enterprise IT stakeholders about their disposition toward open networking platforms. It will reveal their interest in adopting open solutions for data centers, campus networks (switching and Wi-Fi), and beyond. EMA will also explore drivers and barriers of adoption, as well as best practices for implementing and operating networks based on open platforms.

Zero Trust Networking: Modernizing Network Segmentation and Secure Remote Access

Network infrastructure and operations teams rarely lead a zero trust security initiative, but they are almost always drafted into implementing and managing core components of zero trust – especially secure remote access and network segmentation.

This research will explore the role that network teams play in enabling zero trust. It will reveal their technology strategies for zero trust network access (ZTNA) and microsegmentation. The report will also explore how to leverage the power of network teams' automation and observability solutions to collaborate with security groups and achieve a successful zero trust implementation.

EMA™ Radar for Network Operations Observability

This report updates the "2024 EMA Radar for Network Operations Observability" report. With this primary research, EMA will assess the leading vendors that offer solutions for network fault and performance monitoring, troubleshooting, assurance, and capacity planning.

This report will assess NetOps tool vendors by overall solution impact, vendor strength, and cost of ownership. By exploring the experiences that customers have when they evaluate, procure, implement, and use these products, this Radar will serve as a guide for IT organizations that are creating vendor shortlists for a new investment in network operations observability solutions.

Network Infrastructure and Operations

Network Compliance: Strategies for Improving Resilience and Eliminating Risk

Compliance is an essential function of network engineering. In EMA's experience, network teams vary wildly in their ability to fulfill this mission. Network compliance requires the establishment, enforcement, and auditing of network design and configuration standards. These efforts ensure infrastructure resiliency, reduce security risk, and prove compliance with regulatory standards.

Unfortunately, many network engineers tell us they cannot establish a standard to serve as the basis of compliance due to legacy infrastructure, complexity, and a lack of documentation and tools. This research will explore the state of network compliance and identify key benchmarks for establishing a successful compliance strategy.

Connectivity for Critical Infrastructure: Strategies for Infrastructure and Operations

Many enterprises and government entities have critical infrastructure that enable operations, including factory automation, oil and gas production, utility networks, and logistics and warehouse systems. These systems often have more stringent requirements for network connectivity than traditional IT infrastructure, but the operational technology (OT) teams that own them lack networking expertise.

In this research, EMA will explore how network infrastructure and operations teams collaborate with and support OT teams as they build and operate resilient networks for critical infrastructure. It will identify the infrastructure and security solutions, management tools, and expertise that network teams bring to the table to ensure OT excellence.

Network Observability for Unmanaged Networks

Network teams have tools that excel at monitoring and operating their managed networks, such as data centers, campuses, and branches. However, today's enterprises typically have a mix of managed and unmanaged networks across their digital infrastructure. This includes public cloud environments, the internet, SaaS applications, remote worker connectivity, and partner and customer networks. NetOps teams lack administrative access to these networks, which limits their ability to collect telemetry from them.

This report will survey IT stakeholders about how to gain visibility into these unmanaged networks. It will explore shifts in strategy around data, tooling, and operations. Many network teams simply add a new tool to their existing toolset, which fragmentation and sprawl already undermine. EMA will identify how enterprises can adopt a more integrated strategy to ensure effective operations in today's complex network environments.

Network Infrastructure and Operations

Shamus leads the network infrastructure and operations practice at Enterprise Management Associates (EMA). His practice focuses on all aspects of managing enterprise networks, including network automation, AI-driven network management, network observability, multi-cloud networking, and WAN transformation.

Prior to joining EMA, Shamus worked as a technology journalist for nearly a decade. He served as the news director for TechTarget's networking publications. He led the news team's coverage of all networking topics and published hundreds of articles. Shamus was previously a daily newspaper journalist who covered crime, education, government, and politics.

Shamus McGillicuddy

VP of Research

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**.

2770 Arapahoe Road, Ste 132 - 544, Lafayette, CO 80026 +1 303.543.9500 **www.enterprisemanagement.com**

4592.100325