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

2025
Enterprise Management Associates (EMA) Research Calendar

Table of Contents

Table of Contents

Information Security, Risk, and Compliance Management

2025 IT Market Report

This comprehensive market report provides a detailed analysis of key trends and emerging technologies in the IT security landscape. By providing in-depth analysis and vendor overviews, this report aims to assist organizations in making informed decisions about their IT security strategies and staying ahead of emerging threats. The report focuses on the following areas:

- Microsegmentation: Explore the latest advancements in microsegmentation technologies and their impact on network security.
- Data security: Analyze emerging threats and best practices for protecting sensitive data.
- API security: Discuss the challenges and solutions for securing APIs in modern applications.
- Observability: Examine the role of observability in improving IT operations and incident response.
- Application development security: Explore best practices for building secure applications from the start.
- Threat hunting and XDR: Discuss the latest trends in threat hunting.

Revisiting API Security: Integral Integrations and Cautious Connections

Organizations of every size will invest in application security tools, and tools that address every market of every size will have a decisive advantage to exploit this emerging trend. As application security teams and development organizations pivot to address these new risks, solutions and security tool providers need a better understanding of how organizations will prioritize API management and security as part of their overall strategic vision. Technology is the primary method of connection organizations use to communicate and interact. In 2023, EMA looked at the role of the API: how it was being used, who was responsible for maintaining the various connections, and how those connections were secured. EMA will revisit the role of the API and concentrate on the tooling necessary to create, administer, and secure those APIs, as well as the expectations that organizations have of their solution providers to secure and manage their API infrastructure. Key research directions include:

- What is the primary method your organization currently uses to identify an attack on your APIs?
- What do you perceive to be a good solution to protect APIs?
- Is security integrated within the delivery process of the API-based web and mobile applications?
- How has artificial intelligence changed the way your organization looks at and leverages APIs?

Information Security, Risk, and Compliance Management

AI-Driven Threat Hunting and Detection

The increasing complexity of cyber threats necessitates advanced techniques for threat hunting and detection. This research aims to explore the application of AI and machine learning algorithms to automate and enhance threat hunting processes. By leveraging techniques such as anomaly detection, natural language processing, and deep learning, it is possible to identify and respond to emerging threats more efficiently. Key research directions include:

- Will quantum computing really impact your organization?
- Does your organization's leadership understand the potential threat from quantum computing?
- What are the immediate needs for your organization regarding data security?
- What is an organization looking for from vendors to address quantum and data security concerns?

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? Key research directions include:

- Will quantum computing really impact your organization?
- Does your organization's leadership understand the potential threat from quantum computing?
- What are the immediate needs for your organization regarding data security?
- What is an organization looking for from vendors to address quantum and data security concerns?

Information Security, Risk, and Compliance Management

No Longer a Networking Science Project: The Maturing Microsegmentation Market

Microsegmentation, once considered a complex and niche security solution, is rapidly maturing into a mainstream enterprise defense strategy. The escalating sophistication of cyber threats and the increasing recognition of the benefits it offers in terms of reduced attack surface, enhanced breach containment, and improved overall security posture drove this evolution. However, the path to widespread adoption is not without its challenges. Complex IT environments, skill shortages, and the need for significant upfront investments hinder the rapid uptake of microsegmentation. Additionally, vendors face hurdles in educating the market about the technology's value proposition and differentiating their offerings in a crowded marketplace. To effectively navigate this evolving landscape, microsegmentation vendors must focus on understanding the unique challenges and requirements of their target market. By asking insightful questions about organizational structure, IT environments, security priorities, and technology adoption, vendors can tailor their solutions to resonate with potential customers. Key research directions include:

- What are the key components in a microsegmentation solution?
- How important is it that a microsegmentation solution supports both physical and virtual environments?
- How important is it that a microsegmentation solution handles dynamic workloads, such as containers and microservices?
- What is your approach to microsegmentation policy creation and management? Is it automated or manual?

Information Security, Risk, and Compliance Management

Using the Latest Technical Innovations to Solve Data Security and Privacy Challenges

Securing and protecting data is at the center of the modern enterprise security plan. There are many considerations for any enterprise aiming to move critical workloads and data stores to the cloud, and understanding how companies will access and store business-critical data is a paramount concern. In addition, GDPR and CRPA regulators are starting to issue violations, and as the various courts issue verdicts, the scope of how data privacy is regulated and the impacts that scope will have on organizations big and small will add complexity to a crowded regulatory framework. Organizations are turning to trusted security vendors to understand these regulations and gain control of their data estates using the latest technical innovations, from artificial intelligence to data security posture management (DSPM). Key research directions include:

- What are the immediate needs for your organization regarding data security?
- What is an organization looking for from vendors to address data security concerns?
- What use cases is your organization looking for AI to solve in regard to data security/privacy?
- Are data security/data privacy competitive differentiators for your organization?

Have Advances in Security Rendered Security Orchestration, Automation, and Response Tools Irrelevant?

Organizations must do more with less. With the current positive economy and increasing budget trends, more tools are an option, but only the largest budgets are getting people. Without human capital, most tools and processes won't run effectively. To keep forward progress, automated incident and alert processing and response are becoming greater necessities. However, to fully utilize these tools, organizations must have some foundational work in place. Automation and orchestration can significantly increase an organization's ability to achieve outcomes. Whether automation and orchestration accelerate positive business and operational outcomes or accelerate failure depends greatly on how the organization prepares. This research asks IT security professionals how they are using orchestration and automation to achieve success and what they would have done to improve the outcomes on the first try to help companies avoid the same problems. Key research directions include:

- Have XDR and next-gen SIEM solutions replaced SOAR solutions?
- Are SOAR solutions considered a critical piece of security architecture?
- What capabilities are customers looking for in SOAR solutions?
- Does SOAR complement SIEM, or is SOAR now a SIEM feature?

Information Security, Risk, and Compliance Management

Zero Trust Architecture for IoT and Edge Devices

The proliferation of IoT devices and edge computing introduces new security challenges. This research aims to develop effective zero trust architectures for securing IoT and edge environments. Key research directions include:

- Designing and implementing microsegmentation techniques to isolate IoT devices and limit lateral movement of threats.
- Developing lightweight authentication and authorization mechanisms suitable for resource-constrained IoT devices.
- Investigating the use of blockchain technology to secure IoT data and ensure its integrity.

Blockchain Technology: A Comprehensive Exploration

Blockchain technology emerged as a transformative force with the potential to revolutionize various industries. This research aims to provide a comprehensive exploration of blockchain, encompassing its underlying principles, practical applications, and security considerations. Key research directions include:

- Analyzing the decentralized nature, consensus mechanisms, and cryptographic underpinnings of blockchain.
- Investigating the potential applications of blockchain in sectors such as finance, supply chain management, health care, and voting systems.
- Addressing the security challenges and vulnerabilities associated with blockchain technology.
- Developing strategies to mitigate risks and ensure the resilience of blockchain-based systems.

Enhancing Microservices Security: A Comprehensive Approach

The increasing adoption of microservices architecture introduced new security challenges due to its distributed and modular nature. This research aims to explore effective strategies for enhancing microservices security. Key research directions include:

- Understanding the fundamental principles of microservices architecture, including service discovery, load balancing, and API gateways.
- Identifying the specific security risks associated with microservices, such as API vulnerabilities, data breaches, and denial-of-service attacks.
- Developing and evaluating security best practices for microservices, including authentication, authorization, encryption, and secure communication protocols.
- Investigating the impact of emerging technologies, such as zero trust architecture and cloud native security on microservices security.

Information Security, Risk, and Compliance Management

Security-First Application Design: A Comprehensive Approach

The increasing complexity of modern applications necessitates a proactive approach to security. This research aims to explore the principles and practices of security-first application design, emphasizing the importance of integrating security considerations throughout the development lifecycle. Key research directions include:

- Understanding the concept of "security-first" design and its benefits in mitigating security risks.
- Investigating key security practices, such as secrets management, infrastructure as code (IaC), and shifting left security implementation.
- Analyzing the impact of security-first design on application development efficiency and time-to-market.
- Exploring emerging trends and best practices in security-first application design, such as zero trust architecture and DevSecOps

Low-Friction Identity Solutions: Reducing Frustration While Improving Security

The increasing demand for convenient and secure authentication methods led to the development of low-friction identity solutions. This research aims to explore the various technologies and approaches that enable seamless and secure authentication while minimizing user friction. Key research directions include:

- Examining biometric solutions, such as facial recognition, fingerprint recognition, and iris recognition.
- Investigating behavioral biometrics, like keystroke dynamics and gait analysis.
- Exploring non-biometric methods, including mobile device authentication, wearable devices, and self-sovereign identity (SSI).
- Evaluating the advantages and limitations of each approach by considering factors like accuracy, user experience, and security implications.

Information Security, Risk, and Compliance Management

Software Vulnerability Detection and Mitigation

The increasing complexity of software applications necessitates robust security measures to protect against vulnerabilities. This research aims to explore effective strategies for detecting and mitigating software vulnerabilities. Key research directions include:

- Examining traditional testing methods, such as penetration testing and vulnerability scanning.
- Investigating static and dynamic analysis tools for automated vulnerability detection.
- Exploring emerging techniques, like fuzzing and symbolic execution, for more comprehensive testing.
- Analyzing the role of bug bounty programs in crowdsourced vulnerability discovery.
- Addressing the importance of supply chain security in mitigating risks associated with third-party components.

AI-Driven Observability

The increasing complexity of modern systems created a demand for more intelligent and effective monitoring solutions. This research aims to explore the potential of AI-driven observability to enhance traditional monitoring practices. Key research directions include:

- Investigating the benefits of AI-powered observability, such as improved anomaly detection, predictive analytics, and automated root cause analysis.
- Addressing the challenges and limitations associated with AI-driven approaches, including data quality, model interpretability, and potential biases.
- Exploring the integration of AI-driven observability with existing monitoring tools and frameworks.
- Evaluating the impact of AI-driven observability on operational efficiency and decision-making.

Information Security, Risk, and Compliance Management

Identity Governance: A Comprehensive Exploration

The increasing complexity of modern organizations necessitates robust identity governance strategies to ensure the security and compliance of their systems and data. This research aims to explore the key principles, challenges, and best practices of identity governance. Key research directions include:

- Understanding the fundamental principles of identity governance, including role-based access control (RBAC), least privilege, and segregation of duties.
- Identifying the challenges and risks associated with identity management, such as unauthorized access, data breaches, and compliance violations.
- Examining various identity governance frameworks and standards, such as ISO 27001 and NIST 800-53.
- Developing strategies for effective implementation of identity governance practices.

EMA Radar™ for Threat Hunting

This Radar Report will assess the capabilities of leading vendors for threat hunting solutions. These vendors offer a solution that provides methods of searching for and identifying potential threats within an organization's network, even before they have triggered any alarms or alerts.

This report is intended to help IT organizations better understand threat hunting solutions and create shortlists of vendors when seeking a new solution. Vendors will be evaluated for their overall solution impact, cost of ownership, and corporate strength. EMA will especially look at the abilities of vendors to deliver value across both on-premises and cloud-based environments.

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

This Radar Report will assess the capabilities of leading vendors for security orchestration, automation, and response (SOAR) solutions. These vendors offer a solution typically designed to improve the efficiency and effectiveness of security operations.

This report is intended to help IT organizations better understand SOAR solutions and create shortlists of vendors when seeking a new solution. Vendors will be evaluated for their overall solution impact, cost of ownership, and corporate strength. EMA will especially look at the abilities of vendors to deliver value across both on-premises and cloud-based environments.

Information Security, Risk, and Compliance Management

EMA Radar™ for Microsegmentation

This Radar Report will assess the capabilities of leading vendors for microsegmentation solutions. These vendors offer a solution designed to divide a network into smaller, isolated segments to restrict lateral movement of threats within an organization, going beyond traditional perimeter-based security by creating micro-perimeters within the network.

This report is intended to help IT organizations better understand the microsegmentation solution market and create shortlists of vendors when seeking a new solution. Vendors will be evaluated for their overall solution impact, cost of ownership, and corporate strength. EMA will especially look at the abilities of vendors to deliver value across both on-premises and cloud-based environments.

EMA Radar™ for Data Security

This Radar Report will assess the capabilities of leading vendors for data security solutions. These vendors offer a solution to address data security challenges in any environment, including (but not limited to) data privacy, data compliance, data custodianship, data policy, and data security management.

This report is intended to help IT organizations better understand the data security solutions market and create shortlists of vendors when seeking a new solution. Vendors will be evaluated for their overall solution impact, cost of ownership, and corporate strength. EMA will especially look at the abilities of vendors to deliver value across both on-premises and cloud-based environments.

EMA Radar™ for Endpoint Management and Security

This Radar Report will provide a comprehensive analysis of the endpoint management and security market, evaluating leading vendors in the space. These vendors offer solutions to address a wide range of endpoint security challenges, including endpoint protection, patch management, and mobile device management (MDM).

This report is intended to help IT organizations better understand the endpoint management and security market and create shortlists of vendors when seeking a new solution. The report will assess vendors based on their overall solution impact, cost of ownership, and corporate strength.

Information Security, Risk, and Compliance Management

EMA Radar™ for Identity Threat Detection and Response

This Radar Report will provide a comprehensive analysis of the identity threat detection and response market, evaluating leading vendors in the space. These vendors offer solutions to address a wide range of identity security challenges, including user behavior analytics, identity and access management (IAM) integration, and threat intelligence.

This report is intended to help IT organizations better understand the identity threat detection and response market and create shortlists of vendors when seeking a new solution. The report will assess vendors based on their overall solution impact, cost of ownership, and corporate strength. Additionally, we will evaluate their ability to deliver value across both on-premises and cloud-based environments.

EMA Radar™ for Runtime Application Security

This Radar report will provide a comprehensive analysis of the runtime application security market, evaluating leading vendors in the space. These vendors offer solutions to address a wide range of runtime application security challenges, including runtime application self-protection (RASP), behavior analysis, and integration with development workflows.

This report is intended to help IT organizations better understand the runtime application security market and create shortlists of vendors when seeking a new solution. The report will assess vendors based on their overall solution impact, cost of ownership, and corporate strength. Additionally, we will evaluate their ability to deliver value across both on-premises and cloud-based environments.

EMA Radar™ for Bug Bounty and Vulnerability Disclosure

This Radar Report will provide a comprehensive analysis of the bug bounty and vulnerability disclosure market, evaluating leading vendors in the space. These vendors offer solutions to address a wide range of bug bounty and vulnerability disclosure challenges, including program management, vulnerability triage, and reward structures.

This Radar is intended to help IT organizations better understand the bug bounty and vulnerability disclosure market and create shortlists of vendors when seeking a new solution. The report will assess vendors based on their overall solution impact, cost of ownership, and corporate strength.

EMA Radar™ for Digital Asset Protection with Blockchain

This Radar Report will provide a comprehensive analysis of the digital asset protection market with a specific focus on blockchain technologies. These vendors offer solutions to address a wide range of digital asset protection challenges, including smart contracts, decentralized identity management, and blockchain-based data privacy solutions.

Information Security, Risk, and Compliance Management

Chris Steffen

VP of Research

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.

Certifications

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

Ken Buckler

Research Director

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).

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

Intelligent Automation

From Rules to Reasoning: Transforming Process Automation with Agentic AI

This research will examine how agentic AI is transforming traditional rules-based automation into intelligent, adaptive systems. It will explore how AI-driven automation is being integrated into low-code/no-code platforms to enable citizen developers to build complex workflows that can make autonomous decisions, improving operational efficiency and scalability.

EMA Radar™ for Workload Automation and Orchestration

The EMA Radar Report will provide a comprehensive evaluation of leading vendors in the workload automation and workflow orchestration space. As organizations shift toward multi-cloud and hybrid IT environments, orchestration becomes a critical capability. This report will focus on how vendors are enabling orchestration for dynamic workloads and application workflows with enhanced agility, scalability, and operational resilience.

The report will evaluate vendors on their orchestration capabilities, hybrid IT integration, and AI-assisted orchestration logic while highlighting how low-code/no-code tools are empowering organizations to streamline automation workflows.

The Rise of Intelligent Orchestration: Coordinating Workloads and Service Automation Across the Digital Enterprise

This research will explore how intelligent orchestration is transforming workload automation, with orchestration playing a central role in managing both IT workloads and application workflows. As organizations adopt hybrid IT and multi-cloud environments, orchestration is key to improving agility, scalability, and operational efficiency. AI advancements, such as machine learning and predictive analytics, are enabling smarter orchestration logic, and this study will measure those advancements.

Observability in the Age of AI: Enhancing IT Monitoring and Performance with Intelligent Automation

In the digital age, where user experience is a top priority, the need for robust observability tools has become mission-critical. With the increasing complexity of IT environments, observability alone is not enough – AI and machine learning are becoming essential tools for enhancing insights and automation across monitoring and incident response.

This comprehensive study will survey IT leaders from enterprises with 500+ employees to provide insights into how organizations are maturing their observability practices and integrating AI/ML to improve operational efficiency, reduce MTTR, and streamline incident resolution. The data will be instrumental for observability vendors in refining their product roadmaps and for IT decision-makers making informed choices about AI-driven observability tools.

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*.

Intelligent Hybrid Multi-Cloud

Unlocking the Future of Observability: OpenTelemetry's Role in IT Performance and Innovation

OpenTelemetry is one of the most popular cloud native, open source projects globally. Representing a shift from proprietary instrumentation to a standards-based approach for generating and ingesting telemetry data, OpenTelemetry helps organizations ensure IT performance.

This comprehensive study surveys IT leaders and practitioners from enterprises with 500+ employees to provide key insights into the perception, adoption, and use of OpenTelemetry. It examines the challenges organizations face, the technical benefits and ROI of OpenTelemetry, and its role in the future of observability. The data will be critical for observability vendors to refine their product roadmaps and for IT decision-makers to make informed choices about adopting OpenTelemetry.

The Future of Platform Engineering: AI-Enhanced Automation for Scalable Infrastructure

This research will explore how AI-driven automation is reshaping platform engineering, enabling organizations to build scalable internal developer platforms (IDPs). It will delve into how AI is used for self-service automation, scalable infrastructure management, and enhancing developer productivity. Real-world use cases will show the transformative impact of AI on DevOps practices and business agility.

Intelligent Observability: Enabling Adaptive Systems for Improved Outcomes

This research will explore how AI/ML and AIOps are enhancing IT monitoring, incident detection, and response times. It will examine how AI-driven observability enables adaptive systems that autonomously adjust to changes in infrastructure, improve operational efficiency, and reduce mean time to resolution (MTTR). The study will focus on real-world case studies and future trends in observability as organizations adopt Kubernetes and multi-cloud architectures.

Mainframe Modernization 2025: Who's Achieving Better Outcomes, Cloud Migrators or On-Mainframe Innovators?

This research will assess the outcomes of two main approaches to mainframe modernization: cloud migration and on-mainframe reengineering. The study will provide a detailed comparison of ROI, operational efficiencies, and long-term scalability for organizations that have chosen either path. Real-world case studies will highlight the key challenges and successes of each strategy, helping organizations decide which modernization approach aligns with their business goals.

Intelligent Hybrid Multi-Cloud

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)

ServiceOps 2025: Automation and AI-Powered IT Service and Operations

This fourth annual research tracks the evolving practical considerations, technologies, challenges, and outcomes of ServiceOps as practiced today and as planned for the near future. With 78% of last year's research panel reporting either an active ServiceOps movement underway or a formal program in place, this technology-enabled approach to unifying IT service and IT operations management continues to gather momentum and positive impact. Running on automation and AI/ML technology tracks already laid down in cross-functional workflows, ServiceOps makes sense to the people doing and funding the work because it is practical and delivers results across the enterprise. EMA will also explore the role of GenAI today and as planned in the near term to delineate reasonable hope and practical help.

Modern IT Service Management (ITSM) – A Work in Progress

IT service management is not grabbing many headlines today, but maybe it should. ITSM is a mature market that finds itself in uncharted waters of AI, automation, and cross-functional collaboration. The very definition of "service" has swung from problem and request response to delivering business value and enterprise service management (ESM) functionality. This research will examine the changes, challenges, and opportunities for ITSM in the high-velocity interaction of cloud, innovation, technologies, security demands, governance, and business imperatives. Special attention will focus on the role of GenAI in shaping the next generation of IT service management.

IT Service/Operations (ServiceOps)

Valerie O'Connell

Research Director

Valerie's practice encompasses intersections and innovations across ITSM/ESM, ITOM, AIOps, asset management, end-user experience, and business context as they interact to deliver excellence in digital service. Valerie works with her clients to drive business. She excels at making the value proposition of complex products clear in crowded markets and at equipping sales forces to strike with precision.

Valerie came to EMA with decades of senior-level experience in the effective marketing of technology. Her experience ranges from VP of product marketing at what was then CA to a successful run as an independent practitioner, serving industry giants such as Microsoft and EMC, as well as cutting-edge startups.

Network Infrastructure and Operations

Hybrid and Multi-Cloud Networking Strategies

Hybrid cloud and multi-cloud architectures are driving network complexity, and this complexity threatens cloud application performance and security. In 2023, only 35% of IT organizations believed they were fully successful with their multi-cloud networking strategies.[1] This new multi-sponsor research will explore how network engineering and operations teams are working to reduce complexity, streamline operations, and build networking and security guardrails for cloud teams to ensure that hybrid, multi-cloud architectures support digital enterprises. It will explore engagement with network observability and automation tools and cloud networking solutions and services.

Building Networks for Enterprise AI

Artificial intelligence (AI) requires a new approach to networking. As enterprises invest in AI to develop new products and services and to transform business operations, they will need to adopt new data center networking technologies, new cloud networking solutions, and new wide-area network (WAN) services. Furthermore, AI will require deep network observability. This research will explore the investments that network teams are making to support AI and the challenges they encounter along the way.

EMA Radar™ for DDI (DNS, DHCP, and IP Address Management)

This EMA Radar Report will assess leading providers of DDI solutions based on a direct evaluation of products and interviews with reference customers. It will serve as a buyer's guide for IT organizations. For this primary research, EMA will evaluate each DDI vendor based on solution impact, cost of ownership, and vendor strength. In addition to traditional DDI requirements, EMA will evaluate vendors based on their ability to support emerging DDI security use cases and multi-cloud networking requirements.

WAN Transformation: Optimizing the Transition from SD-WAN to SASE

EMA's biennial WAN transformation research has been tracking the evolution of enterprise wide-area networks (WANs) since 2016, exploring the adoption of hybrid WAN connectivity and software-defined WAN (SD-WAN) in depth. Recent research revealed that many enterprises are struggling with the transition from SD-WAN to secure access service edge (SASE). This new edition of the report will explore the SD-WAN-to-SASE transition in depth, offering insights into how enterprises can successfully execute this next stage of WAN transformation.

[1] EMA, "Multi-Cloud Networking: Connecting and Security the Future," January 2023.

Network Infrastructure and Operations

Wi-Fi in the Hybrid Work Era

IT organizations have discovered that pre-pandemic Wi-Fi networks are failing to meet new requirements. People work differently today than they did five years ago. Use of real-time video and meeting applications has spiked, putting increased demands on wireless connectivity. Also, workers are no longer tethered to desks. IT organizations must implement new wireless networks that offer more bandwidth, broader coverage, high-density connectivity, and more. This research will examine how enterprises are navigating the evolving wireless landscape, gearing up for the widespread adoption of Wi-Fi 7.

DDI (DNS, DHCP, and IP Address Management) Directions 2025

In 2023, EMA conducted the most comprehensive market research study of enterprise DNS, DHCP, and IP address management (DDI) strategies in decades. That study found that only 40% of enterprises are completely successful with DDI technology, due in part to cloud complexity, security risks, cultural issues, and data quality problems.[2] EMA will refresh this landmark study in 2025, surveying network and cloud engineering teams about how DDI solutions can best address their requirements for cloud networking, network automation, cybersecurity, and more.

NetDevOps: How Network Operations Teams are Aligning with DevOps

According to EMA's 2024 research, DevOps and CI/CD pipelines are a top driver of enterprise network operations strategies.[3] Network management tools and processes must evolve to support the alignment of NetOps and DevOps groups as enterprises embrace hybrid multi-cloud architecture and cloud native application transformation. This multi-sponsor research will survey IT organizations about how network automation and observability tools can enable NetDevOps convergence. It will also explore the technical and cultural challenges that emerge when the network infrastructure team tries to partner with DevOps.

Converging Operational Technology (OT) on IT Networks

Converging operational technology (OT) – such as manufacturing systems, medical equipment, and water treatment systems – onto IT networks offers plenty of benefits, including operational efficiency, automation, and improved customer service. However, this convergence also introduces new risks and challenges that network teams must address. This research will explore how industries are addressing connectivity, security, and observability requirements as OT infrastructure converges onto enterprise networks.

[2] EMA, "DDI Directions: DNS, DHCP, and IP Address Management Strategies for the Multi-Cloud Era," September 2023.
[3] EMA, "Network Management Megatrends 2024," April 2024.

Network Infrastructure and Operations

AI-Driven Network Operations: Exploring Engagement with AIOps and Generative AI

EMA's ongoing research consistently finds that network operations teams turn to network infrastructure vendors and tool vendors for AI-driven network management solutions. Network engineers are generally skeptical of AI hype, but they admit to EMA anecdotally that they see the potential for AI to streamline operations, reduce human error, and advance network automation. Networking vendors can truly differentiate themselves with strategic investments in AI. This research will help vendors identify the best way forward.

Network Infrastructure and Operations

Shamus McGillicuddy

VP of Research

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.

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**

4454.092624