

EMA 2024 Planner

for Research and Services



Enterprise Management Associates (EMA) is not a typical analyst firm. Since 1996, we've specialized in delivering deep insights across business verticals and technology innovations. We differ from other firms by providing personalized research and analysis that focuses on the issues that are important to your organization. Our analysts furnish detailed information on market and technology trends, competitive landscapes, and product analysis that deliver actionable data.

The primary focus of every team member is meeting the needs of our clients. With EMA, you interact directly with an analyst, not a nameless assistant, who is a noted expert in his or her field of study. On average, EMA analysts have more than 20 years of industry experience at all levels: from engineers and developers to middle managers and decision-makers to technology and business-line executives. We're passionate about what's going on in all aspects of the technology space and how those trends are impacting your business.

We also have a wide array of offerings to meet the needs of every facet of your business, from marketing and sales to corporate leadership and strategic vision. We back these offerings with our world-class research capabilities, and those capabilities continue to evolve and improve as markets and technologies change.

The EMA 2024 Planner for Research and Services includes information on EMA's conference presence throughout the upcoming year, coverage information, subscription and service offerings, and research plans. If you have any questions, please don't hesitate to reach out. We'd love to hear from you!

The EMA Team



Table of Contents

1	2024 Planned Conference Attendance
2	Coverage Areas
6	Subscription Offerings
8	Other EMA Offerings
14	Upcoming Research
35	EMA Analysts

2024 Planned Conference Attendance

EMA attends multiple events every year, either in a speaking capacity or in covering the event. Here are some of the events that EMA analysts will attend in 2024:



If you'd like an EMA analyst to participate in your marketing efforts for a conference, please let us know. If you would like to arrange an in-person briefing with an analyst while at the event, please [contact us](#) for more information.

A solid orange horizontal bar is located in the top left corner of the page.

Coverage Areas

Application Management

Application Management – includes the entire lifecycle of application operations, architecture, testing, and upgrades.

Included coverages

- » Application dependencies
 - » DevOps
 - » Proactive monitoring
 - » Application performance and analytics
 - » End-user experience
-

Business Intelligence

Business Intelligence – the combination of analytics, infrastructure, visualization, and data mining to enable organizations to make data-driven decisions.

Included coverages

- » Business outcomes
 - » Predictive analytics
 - » Self-service
 - » Data mining
 - » Reporting and visualization
-

Digital Service Execution: IT Service, Experience, and Operations Management

Digital Service Execution: IT Service, Experience, and Operations Management – takes a service-centric, cross-functional approach to delivering and managing IT excellence. The practice area encompasses ITSM, ESM, AIOps, DevOps, ITAM, SRE, and advances that promote an evolving ServiceOps reality.

Included coverages

- » Business operations
- » IoT/OT
- » Organizational/cultural considerations
- » Customer service excellence
- » ITAM
- » Site reliability engineering
- » DevOps
- » ITOM/AIOps
- » Digital experience management
- » ITSM/ESM
- » Digital transformation initiatives
- » Managing innovation

Information Security, Risk, and Compliance Management

Information Security, Risk, and Compliance Management – The process by which organizations predict and manage risk by adhering to boundaries set by a business. The practice area encompasses most of the areas and concepts in information security, risk mitigation, and technology regulatory compliance.

Included coverages

- » AI security
- » Application security
- » Advanced breach detection
- » Advanced threat analytics and anomaly detection
- » Advanced testing attack simulation
- » Antivirus
- » Bot detection and protection
- » Cloud application security management
- » Cloud access security broker
- » Cloud security
- » Cryptography and key management
- » Container security
- » Data leak prevention and data classification
- » Deception technology
- » Digital threat intelligence management
- » Distributed denial of service protection
- » Electronic governance risk and compliance
- » Endpoint protection
- » Hardware security modules
- » Intrusion detection/prevention
- » IoT security
- » Information rights management
- » Mainframe security
- » Managed security service provider
- » Mobile security tools
- » Network admission control
- » Network APT detection/analysis
- » Next-generation endpoint security
- » Next-generation firewall/unified threat management
- » Patch management
- » Runtime application security protection
- » Remote access
- » Risk management
- » Secure email gateways and services
- » Security incident and event management and log management
- » Security operations automation and orchestration
- » Security policy orchestration and automation
- » Shared responsibility model
- » SSL appliances
- » Threat intelligence service feeds
- » Third-party risk management
- » Anti-phishing
- » Unified threat management
- » Vulnerability management
- » Web application firewall
- » Workload microsegmentation
- » Web security gateway
- » Zero trust

Endpoint and Identity Management – Incorporates the processes necessary to ensure IT systems are operational and enable secure access to enterprise digital resources to ensure end-user productivity. The practice encompasses solutions for managing endpoint devices and support for the breadth of identity and access management practices.

Included coverages

- » Browser isolation
- » Client lifecycle management
- » Consumer identity and access management
- » Desktop virtualization
- » Digital employee experience management
- » Digital workspaces
- » Identity and access management
- » Identity governance
- » Mobile device management
- » Privileged access management
- » Unified endpoint management

Intelligent Automation

Intelligent Automation – A holistic solution for digital transformation. The practice area encompasses workload automation, robotic process automation, and blockchain-based and AI-driven automation. It examines the management of process orchestration and workflows.

Included coverages

- » AI-driven automation
- » Blockchain-based automation
- » Process orchestration
- » Robotic process automation (RPA)
- » Workflow automation
- » Workload automation (WLA)

Intelligent Hybrid Multi-Cloud

Intelligent Hybrid Multi-Cloud – An intelligent hybrid multi-cloud forms when services from private cloud, public cloud, and edge combine into the foundation for the policy-driven deployment and management of cloud-native applications, data sources, and machine learning models. The practice encompasses observability, GitOps, MLOps, DevOps, and serverless functions.

Included coverages

- » AutoML
- » Cloud-native application stacks
- » Continuous compliance
- » Infrastructure as code and GitOps
- » Intelligent edge
- » Machine learning platforms
- » Observability for DevOps and MLOps
- » Operationalizing machine learning and AI
- » Self-driving hybrid multi-cloud
- » Serverless functions
- » Site reliability engineering

Network Infrastructure and Operations

Network Infrastructure and Operations – The process by which organizations design, build, and manage networks. The practice area encompasses data centers, the cloud, local-area networks, and wide-area networks. It examines the management of network capacity, performance, and security.

Included coverages

- » Application delivery controllers/load balancers
- » Cloud networking
- » Data center networking
- » DDI management
- » Enterprise switching and routing
- » Internet of Things
- » Network automation
- » Network change and configuration management
- » Network fault and availability management
- » Network packet brokers
- » Network packet capture
- » Network performance management
- » Network security
- » Network as a service
- » Secure access service edge
- » Software-defined WAN and hybrid WAN
- » Wi-Fi infrastructure and management
- » Work-from-anywhere networking

Subscription Offerings

EMA Subscription Offerings

Enterprise Management Associates (EMA) offers a variety of research subscription packages to meet the needs of vendors large and small. With an EMA subscription, you get dedicated analyst time, in-depth market insights, and help aligning your sales motion with market trends. EMA subscriptions can assist your company in the development cycle – from early **launch**

to the next stage of **growth**, all the way to **success** in the marketplace and **sustained** presence as a leader in industry verticals. By choosing your base level of subscription and then selecting a consulting focus, marketing focus, or research focus, you'll have many EMA offerings to guide your company's strategy.

1 Choose Your Base Subscription

Launch (\$1,000)	Growth (\$6,500)	Success (\$18,000)	Sustain (\$21,000)
Includes: • 2 hours of advisory time	Includes: • 2 hours of advisory time • 1 impact brief or vendor to watch writeup	Includes: • 4 hours of advisory time • 1 seat for research access • 1 blog or 3 social micro-assets • 1 impact brief or vendor to watch writeup • 1 speaking engagement (T&E not included)	Includes: • 4 hours of advisory time • 1 seat for research access • 1 blog or 3 social micro-assets • 1 lead gen research sponsorship

2 Choose Your Add-On

Consulting Focus \$7,500	• Additional 3 Hours of Advisory • 1 Seat Research Access	• Additional 3 Hours of Advisory • 1 Seat Research Access	• Additional 3 Hours of Advisory • 1 Seat Research Access	• Additional 3 Hours of Advisory • 1 Seat Research Access
Marketing Focus \$8,500	• Blog Post or 3 Social Micro-Assets • 1 Seat Research Access	• Blog Post or 3 Social Micro-Assets • 1 Seat Research Access	• Blog Post or 3 Social Micro-Assets • 1 Seat Research Access	• Blog Post or 3 Social Micro-Assets • 1 Seat Research Access
Research Sponsorship \$8,500	• 1 Research Report Basic Sponsorship	• 1 Research Report Basic Sponsorship	• 1 Research Report Basic Sponsorship	• Speaking Engagement (T&E Not Included) • Blog Post or 3 Social Micro Assets

At any time, you can add additional research access seats for \$5,500 each.

Contact an EMA business development manager at +1.303.543.9500 or ema-sales@enterprisemanagement.com to get started today!

Other EMA Offerings

EMA Analyst Speakers


Add the Credibility of a Third-Party Expert to Your Next Sales Meeting, Customer Event, or Conference

What better way is there to gain market validation, showcase thought leadership, and provide valuable education to customers and employees than by having a trusted expert deliver research-based insights tied to your messaging?

Since 1996, leading industry analyst firm Enterprise Management Associates (EMA) has been the tried and trusted source for analyst research for enterprise to SMBs. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions.

Whether the audience includes prospects, customers, or your own internal staff, including an EMA analyst in your event adds credibility and importance – to both the message and the event. EMA analysts routinely speak on webinars, podcasts, and conferences around the world to provide industry leadership, technical expertise, and a unique, hands-on perspective.

EMA also develops and delivers custom training programs on topics, such as selling in a converging market or IT and data management market trends for vendor clients with diverse needs, budgets, and timeframes.



Stand out in a crowded market by having a trusted EMA analyst speak at your next event, including:

Industry events – Conference presentations, either virtual or in person, to support vendor messaging and positioning

Executive/leadership team meetings – Provide insights on IT and data management research, topics, and trends to help you shape your product roadmap

Sales kickoff meeting and/or other internal meetings – For endorsement and authority for your product launch

Podcasts – Join EMA's industry experts as a speaker on an EMA-established podcast series or have an EMA analyst as a guest on a podcast of your choosing

Videos – Make your videos more compelling when you work with an EMA analyst for social media, internal use, or marketing assets to lend additional validation of your brand

Webinars – EMA-hosted (optionally with lead guarantees) or vendor-hosted on a topic of your choice (or related to EMA research)

Using our proven research methodologies and hands-on industry experience, EMA analysts can work collaboratively with your team to make your in-person or digital engagements more effective and relevant.


Contact an EMA business development manager at +1.303.543.9500 or ema-sales@enterprisemanagement.com to get started today!

EMA Consulting Services

Use EMA's Expertise and Insights to Navigate Evolving Technology Landscapes

IT teams are tasked with improving service quality, controlling costs, and aligning IT with business outcomes during a time of rapid change and skyrocketing complexity. IT cannot simply work harder – IT must work smarter.

EMA analysts can help you understand how to streamline processes within your roadmap, detect potential points of improvement within your platform, and strengthen your product to become a recognized must-have in business.



Work with an EMA analyst as partner and advisor who will provide recommendations to help your organization achieve its objectives in any or all of the following areas:

Market sizing and opportunity analysis – Understand how to identify potential customers and solidify your marketing and sales messaging to bring them home

Channel strategy development – Once you've finished your market sizing, it's time to choose the right marketing channels to reach your target audience

Competitive analysis and comparisons – EMA regularly conducts industry-specific vendor comparisons to evaluate cost-efficiency and product strength among top players in each technology space

Product roadmap development and go-to-market planning – To discern the best way to drive demand for your product supported with data from existing roadmaps

Using our proven research methodologies and hands-on industry experience, EMA analysts can work collaboratively with your team to make your IT initiatives more effective.

Contact an EMA business development manager at +1.303.543.9500 or ema-sales@enterprisemanagement.com to get started today!

EMA Custom Research and Market Coverage

Utilize EMA Research and Insights to Strengthen Your Roadmap and Validate Your Message

Enterprise Management Associates (EMA) regularly conducts primary research to gain in-depth insight into key business and data management technologies and trends. EMA studies use online surveys, focal interviews, and real-world case studies to help organizations gain competitive advantage with market insight, market awareness, and leads.

When you work with an EMA analyst on a custom research project, you can influence the questions asked

within each research focus. Such a hands-on approach is unique in the marketplace and reinforces the collaboration between EMA analysts and vendors that benefit most from the resulting data. This ensures that the research outcomes are directly relevant to your organization's needs and challenges.

All EMA research is posted in the EMA Research Library on the website and promoted via a monthly newsletter, social media promotions, and more.



Industry research is finalized and presented in one of the following formats to our end-user audience:

Radar reports – A broad vendor evaluation within a specific technology category to help businesses quickly and efficiently determine a shortlist of vendors to fill their product needs

Vendor-focused research reports – In-depth reports to share critical market data, including market growth, purchasing drivers, and feature priorities

End-user-focused research reports – To highlight key findings and best practice advice

Impact briefs – EMA's take on the implications and ramifications of industry events like mergers, major product releases, etc.

Vendor to Watch briefs – One-page analysis of companies that provide unique customer value by solving problems that were previously unaddressed within a market space

Using our proven research methodologies and hands-on industry experience, EMA analysts work collaboratively with your team to differentiate your solutions to every size of organization and increase your competitive value in a complicated and crowded market.

Contact an EMA business development manager at +1.303.543.9500 or ema-sales@enterprisemanagement.com to get started today!

EMA ROI Services

Build a Strong Business Case for Your Platform

Business leaders must be able to clearly communicate how investments will help them improve service levels, increase productivity, cut costs, and deliver measurable value to the enterprise. ROI services will act as a standard for shaping your marketing strategies.

By tracking marketing success, business leaders are empowered to use data-driven decision-making for their budgets, forecasting, and omnichannel strategies. ROI sets the stage for competitor analysis and the inclusion, when needed, of new technologies.



Let the data speak for itself with EMA ROI services, including:

Case studies – Either single or multi-customer in-depth studies to evaluate platforms, competitors, end-users of your product, or events

ROI calculator – Demonstrate the value of organizations looking to invest your solution with a proven ROI tool from a trusted third-party analyst

Sales training – Use EMA experience to preemptively boost your technical and non-technical sales messaging

Using our proven research methodologies and hands-on industry experience, EMA analysts can create ROI services that will effectively communicate the business case for your platform.


Contact an EMA business development manager at +1.303.543.9500 or ema-sales@enterprisemanagement.com to get started today!

EMA Collateral Offerings

Accelerate Your Customer Engagement by Leveraging EMA's Expertise

Whether your goal is to educate the marketplace or your in-house sales team, EMA analysts can craft custom sales and marketing tools to help you be more competitive. While the market is crowded with contractors willing to write about vendor solutions, EMA backs our conclusions with independent research, user interviews, and verification.

A key reason IT professionals trust EMA is because our analysts merge real-world technical expertise with knowledge of emerging technologies, trends, and industry developments to craft relevant and compelling research studies, analyses, and accompanying reports.



Use EMA's third-party, expert opinion to add credibility to your sales and marketing messages, including:

eBooks – Deliver valuable data and insights in an easy-to-read format. Perfect for audiences that want to obtain data without wading through an overabundance of explanatory text

Guest blogging – EMA regularly contributes to vendor blogs as a way to offer credibility to platform updates, business events, or product launches

Infographics – Quick but effective designs to attract wider audiences as you deliver your brand

White papers – Time-proven papers to go more in-depth on research without overwhelming readers

Using our proven research methodologies and hands-on industry experience, EMA analysts can work collaboratively with your team to generate collateral that will elevate your platform.

Contact an EMA business development manager at +1.303.543.9500 or ema-sales@enterprisemanagement.com to get started today!

Upcoming Research

Digital Service Execution

The state of ServiceOps 2024: automation and AI-powered IT service and operations

This third annual research tracks the evolving practical considerations, enabling 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 is gathering momentum. 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 slashes wasted time on both sides. EMA anticipates more structure and formalization as the practice gains organizational recognition and will explore the progression in order to offer practical guidance to IT practitioners and vendors alike.

Modern ITSM – a work in progress

IT service management (ITSM) 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.

On the road to predictive and proactive AIOps

AIOps has the power to transform IT service quality, performance, and cost. However, it stands on the shoulders of foundational capabilities, such as discovery and dependency mapping and organizational adaptations to leverage cross-functional processes, workflows, and collaboration, as well as automation to instantiate insight into action. This research will examine the fabric of AIOps success in real-world applications. Special attention will be paid to technologies, practices, and organizational changes that make the difference between moderate improvements and sea-change impact.

Optimizing IT service for business performance – the next frontier

The need to view IT in its business context is critical, but it's not simple. New technologies and capabilities challenge traditional answers to even basic questions, like “What is an asset?” The answers increasingly include new entries, such as generative AI, edge devices, industrial IoT, operational technology (OT), and technologies in the clouds and across the globe. IT is challenged to run in a way that optimizes performance from both a business service and a financial standpoint. This research probes the state of IT business service management as it is implemented today, including the innovations in technology, processes, and functional organizations needed to align the interests and actions of IT and the business it serves.

Information Security, Risk, and Compliance Management

Information Security and Compliance FutureTrends 2024: How Regulation, Sophisticated Attacks and Artificial Intelligence Will Shape Security Spending in 2024

For 26 years, technology vendors and enterprise leaders have relied on Enterprise Management Associates (EMA) to provide authoritative insights into markets across verticals and industries, providing the most comprehensive picture of the technology landscape to better serve their customers.

This year, EMA will undertake a FutureTrends report in the Information Security and Compliance spaces, concentrating on those areas of greatest interest to vendors and customers alike:

- Regulatory changes have made security leadership more critical than ever, finally earning a legitimate seat at the executive table, instead of a subordinate “manager of tech nerds” position.
- Hacker and nation-states have increased the tempo of cyber-attacks, from multi-national corporations (like MGM Resorts) to the smallest of health care and financial services firms (such as 23andMe) to near constant attacks on government resources. The attacks have become costly and potentially even deadly, as customers scramble to partner with vendors offering solutions and protection.
- All of these attacks shadow the possible impacts that artificial intelligence will have on the security space: how customers implement and secure their AI infrastructure to how they can possibly defend against automated and intelligent attacks on their organizations.

EMA’s Information Security and Compliance FutureTrends 2024 research will provide sponsors with data and analysis in the following key areas:

- AI Security
- API Security/App Security
- Data Security/DSPM
- Endpoint/Email Security
- Identity
- Network Security
- Regulatory Compliance
- SIEM/Observability
- XDR (including an authoritative definition)
- Zero Trust

Information Security, Risk, and Compliance Management

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 API, as well as the expectations that organizations have of their solution providers to secure and manage their API infrastructure.

Security Operations and Technology Megatrends: Driving Better Security Outcomes

After several years on hiatus, Enterprise Management Associates is revisiting a Security Management Megatrends study as the definitive benchmark for tracking the evolution of enterprise security management tools, issues, and practices. This ongoing research will survey security management teams on emerging tool requirements, organizational strategies, and operational challenges. EMA's Megatrends research also examines the impact of critical technology trends on security managers. EMA is collaborating with research sponsors to determine the trends to focus on in 2022-2023. Security Megatrends topic considerations include managed services adoption, security considerations and views on public and hybrid cloud adoption, the expansion of security automation, the security team impacts from NetOps and DevOps, the perceived levels of need for convergence of network operations and security operations, and more.

Data Security: The Critical Path to an Organization's Security Strategy

Does your security team know where your sensitive data resides, who has access to it, and the best way to protect it?

Without the right tools and resources, you may struggle to mitigate threats or address new compliance mandates, while strategic technology initiatives – such as moving data to the cloud – can fall flat. Data security is a primary consideration when migrating data to the cloud, but understanding the data estate is critical for compliance with regulatory privacy concerns. Data security is the center of an enterprise's security plan. There are many considerations for an enterprise that aims to move critical workloads and data stores to the cloud. In addition, GDPR and CCPA regulators are starting to issue violations. As the various courts issue verdicts, the scope of how data privacy is regulated and the impacts that will have on organizations big and small will add complexity to a crowded regulatory framework. Organizations are turning to security vendors to understand these regulations and gain control of their data estates using tools and services from the security ecosystem. In this research project, Enterprise Management Associates will survey IT and business leaders across all verticals to discover the attitudes and perspectives business leaders and technical decision-makers have toward data security and the needs those organizations have when dealing with their data estates.

Information Security, Risk, and Compliance Management

The Transformation From Cybersecurity Management to Risk Management

Under various names, such as information assurance and information security, what we know today as “cybersecurity” has been around for nearly 50 years, constantly evolving to address new vulnerabilities and threats. The methods, tools, and procedures for security management vary greatly between different organizations – sometimes, there is significant variance in the organizations themselves. Risk management has matured its processes and requirements to produce high-quality decision-making information. Ironically, security and risk management are often separate, non-integrated processes. The result is a diminished risk assessment and a security practice that often does not receive necessary visibility. Security teams must be able to communicate how proposed business tools and processes will negatively affect the business risk profile and attack surface. Security teams must also be able to communicate how tools they use and want to purchase will positively affect the same.

The Rise of Zero Trust Security: Is Zero Trust the Future of Enterprise Security?

Zero trust is on the radar of every executive in every business vertical. Even non-technical executives have heard of zero trust and are asking hard questions of their technology leadership. Many solution providers have embraced the “hype cycle” and market their solutions as the “best thing since sliced bread” regarding zero trust, including some companies that believe purchasing their solution will make an organization “zero trust certified,” whatever that means. As organizations evaluate how to implement and approach zero trust, they are turning to industry leaders to provide the necessary guidance to start them on their zero trust journey. Plenty of security vendors claim to have a zero trust solution, but how does that fit into the zero trust ecosystem and how does it work for the customer? In this research project, Enterprise Management Associates will survey IT and business leaders across all verticals to discover the attitudes and perspectives business leaders and technical decision-makers have toward zero trust security and the requirements those organizations have when implementing a zero trust project.

DevSecOps and Securing Today’s Enterprise

As organizations attempt to “shift left” and incorporate security controls into development, delivery, and operations, how successful are these efforts and what are the challenges being encountered? Open source software provides a low-cost means of implementing, or developing, software. With many commercial solutions incorporating open source code, is it truly possible for an organization to avoid it and the security vulnerabilities that come with it? How can open source libraries be incorporated into commercial products securely, without running the risk of vulnerabilities (such as recent Log4j)? Is commercial software more secure or still susceptible (as was recently seen with SolarWinds)? Do the long-term maintenance and support costs of open source security software compare with closed source? How are closed-source and open source software developers affected by President Biden’s executive order targeting software supply chain attacks? This research looks at the true cost and return on investment of implementing DevSecOps and examines the security issues that are potentially addressed (or introduced) by usage of open and closed-source software libraries.

Information Security, Risk, and Compliance Management

50+ Years of Email: Why is Email Security Still Failing?

Since 1971, email has increasingly become part of daily life for most businesses across the globe. Great improvements have been seen across the IT industry in securing email to protect confidentiality and verifiability of this critical business communication tool, but some estimates are that billions of malicious emails are sent each day, including phishing, imposter scams, advance fee fraud, and other malicious links and attachments. Organizations have invested heavily into keeping malicious email out and allowing legitimate emails through. Yet, the billions of malicious emails sent each day are proof that email is still a profitable channel for bad actors. At the same time, email is one of the most common accidental data breach methods, with misdirected or unencrypted emails containing personally identifiable information (PII) a serious security risk to organizations. How are organizations addressing this serious security concern without impeding productivity? This research will examine today's email security methods and tools and evaluate where the industry is struggling and where they are succeeding.

Viruses, Trojans, and Worms, Oh My! Fighting the Wicked Witch in the Land of Malware

In the early days of computing malware wasn't very common, and antivirus companies could provide excellent coverage as new variants were discovered. Unfortunately, malware has increased at an exponential rate, with over 450,000 new samples processed each day by antivirus vendors. Antivirus vendors struggle to keep up, not only with signatures for new variants, but also development of heuristic detections. Many vendors have attempted to augment or even replace antivirus software with more advanced detection and prevention techniques, such as intrusion detection software and sandboxing. How is today's malware impacting organizations? What role do potentially unwanted programs, such as spyware, play in today's antivirus arms race? This research will explore the depths of the malware problem, how organizations are combatting it, and where these efforts are succeeding or failing.

Investing in Your Most Valuable Asset – Cybersecurity Workforce Development

Beyond keeping the enterprise safe, organizations must constantly work to improve and educate their existing security workforce to keep up with changes in technology. How are these workforce development activities occurring, and are employers seeing a return on investment? What role do security certifications play in hiring and employee retention? Do workforce development programs improve employee retention? What about organizations that require employees to get training outside of the workplace, on their own time? What are the benefits seen through certifications? Are organizations more secure? Is there a sub-focus on security awareness training? This research will examine organizations' investments in strengthening their cybersecurity workforce and observed return on this investment.

Information Security, Risk, and Compliance Management

The Shared Responsibility Model: Tools, Practices, and Partners to Close the Largest Cloud Security Gap

Cloud providers and other SaaS models have subscribed to the shared responsibility model: a practice in which the service provider is responsible for some aspects of securing an environment, leaving other aspects to the customer. Despite years of practice and millions of dollars spent on information campaigns, the largest failures in cloud computing are nearly always related to failures of the customer to understand and adhere to the tenants of the shared responsibility model. Organizations can engage with their security vendor/partners to close the gaps in their cloud infrastructure while better understanding their information security responsibilities.

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.

Best Practices to Address Data Privacy Regulations: Partners, Processes, and Practices

Data privacy regulations are becoming more relevant to every size of business. GDPR and CCPA regulators are starting to issue violations, and as they issue verdicts, the scope of how data privacy is regulated and the impacts that it will have on organizations big and small will add complexity to a crowded regulatory framework. Organizations are turning to security vendors to understand these regulations and gain control of their data estates using tools and services from the security ecosystem. Data privacy tools and services are continuing to gain momentum as vendors ramp up to address the growing market – but like all compliance regulations, there is no one-size-fits-all approach. Vendors are looking to understand the critical needs of all organizations, from the smallest privately-owned business to the largest enterprises. Organizations have dollars that they want and need to spend to address data privacy controls and services. Vendors that develop a message that appeals to the broader market and addresses those critical needs will be well positioned to take advantage of this continually growing trend. In this research project, Enterprise Management Associates will survey IT and business leaders across all verticals to discover the attitudes and perspectives business leaders and technical decision-makers have toward data privacy regulations, as well as the needs those organizations have when dealing with their data estates.

Information Security, Risk, and Compliance Management

Security Compliance Frameworks – Are They Enough?

PCI, DISA STIG, FISMA, NIST, and CIS all provide compliance frameworks to secure enterprises. Is security compliance enough, or should organizations strive for more? The 2013 Target data breach occurred only a few weeks after Target was certified as PCI compliant. How do we find an appropriate balance between risk and cost? Do compliance frameworks need further evolution, or should organizations use them as a starting point to develop their own security baselines? This research will explore current security compliance frameworks/baselines and identify whether they are enough to secure organizations, or if additional steps need to be taken to be truly secure.

Are Today's Security Decision-Makers Buying the Tool or the End-User Support?

As the cybersecurity industry continues to struggle with a workforce shortage with almost 3 million unfilled cybersecurity positions in 2022, organizations are often turning to software and services to augment the gap. Are decision-makers purchasing tools based on functionality or are they purchasing based on end-user support and the ability of that support to augment inexperienced cybersecurity professionals? How much does upfront tool cost actually influence purchases? How much does ongoing support of service-level agreements and cost influence? This research will examine the tough questions and challenges industry decision-makers face and what ultimately results in a decision-maker's agreement to sign on the dotted line.

Guardians of the Digital Realm – Advancing Cybersecurity Workforce Development

The federal government invested in nine different cybersecurity workforce development R&D programs in FY2022 across multiple agencies, including DoD, DHS, NIST, NIH, and the NSA. Is the federal government leading the way in what should be across-the-board industry standards for workforce development and training? Beyond keeping the enterprise safe and secure, organizations must constantly work to improve and educate their existing security workforce to keep up with changes in technology. What are the current trends in cybersecurity workforce development demand and offerings? What are users and organizations looking for when it comes to cybersecurity workforce development? This research, which performs in-depth analysis of open data sources, will explore the availability and demand of cybersecurity workforce certification and training, including practitioners, developers, and even leadership and executives. It will help vendors better understand the current gaps in the workforce development market and buyers' needs.

Patch This! Vulnerabilities, Breaches, and Exploits Trends

The number of new vulnerabilities in the NIST National Vulnerability Database grows significantly every year, with an overwhelming 25,082 vulnerabilities published in 2022. What was once as simple as subscribing to vendor notification lists and routinely checking for new updates has now become a massively complex vulnerability management challenge, with many vulnerabilities now published as zero-days without any known patch. How can organizations possibly keep up with existing vulnerabilities while also mitigating zero-day threats? This research, which performs in-depth analysis of open data sources, will explore the current trends in attacks against organizations. It will help vendors better understand the current gaps in the vulnerability management and incident response market and buyers' needs.

Information Security, Risk, and Compliance Management

The Rise of Managed Service Providers – Lending Out the Keys to the Kingdom

With the ever-increasing challenges of cybersecurity, combined with the ongoing cybersecurity workforce shortage, small and medium businesses struggle to find adequate staffing to meet their cybersecurity needs. As a result, many organizations are turning to managed service providers or managed security service providers. What roles and duties are organizations looking to truly have filled? How safe do organizations feel about outsourcing their IT departments and essentially handing over the “keys to the kingdom” to a company that does not have an onsite presence within their company? This research, which will be user survey-driven supplemented with analysis of open data sources, will explore the current trends in managed service providers and managed security service providers. It will help vendors better understand the current gaps in the MSP/MSSP markets.

EMA Radar for Network Visibility Architecture

 *Joint project with Network Infrastructure and Operations*

This research will assess the capabilities of the leading vendors for network visibility solutions. These vendors offer hardware and software for extracting packets and metadata from production networks and delivering them to the network analytics solutions that IT operations and security groups use.

This report is intended to help IT organizations better understand the network visibility 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 networks.

Reshaping Tech Landscapes – AI's Megatrends in Cybersecurity and Beyond

In the rapidly evolving landscape of technology, the convergence of cybersecurity, networks, business automation, and artificial intelligence (AI) has given rise to transformative megatrends that are reshaping industries, economies, and societies. This comprehensive report delves into the key trends and their implications within these domains, offering insights for businesses, policymakers, and technology enthusiasts alike. This report will provide actionable recommendations for organizations to navigate this landscape effectively, emphasizing the importance of investing in AI literacy, talent acquisition, and ethical frameworks, while giving vendors critical insight into which AI technologies organizations want integrated with their products and services.

Beyond SIEM and Visibility – How Organizations are Moving Toward Security Observability

In recent years, the field of cybersecurity underwent a profound transformation with the emergence of security observability as a compelling alternative to traditional security information and event management (SIEM) systems and visibility approaches. This research report delves into the growing trend of organizations across various industries gravitating toward security observability to enhance their threat detection, incident response, and overall cybersecurity posture. By analyzing decision-maker surveys and publicly available data, this study uncovers the reasons behind this shift, the key differentiators that make security observability attractive, and the challenges and considerations associated with its adoption.

Information Security, Risk, and Compliance Management

Cybersecurity Maturity Model Certification (CMMC): Why This Latest Certification Matters to Your Organization (Even if You Think it Doesn't)

The Cybersecurity Maturity Model Certification (CMMC) is a framework designed to enhance the cybersecurity posture of organizations participating in government contracts. Its primary aim is to safeguard sensitive information, control and secure access, and mitigate supply chain cyber threats. CMMC builds upon existing frameworks, like NIST SP 800-171, but adds a tiered approach with five certification levels, each with specific security requirements. If you are an organization that does business with another organization that does business with the government in any way, it is likely that these requirements will apply to you to some degree. While your organization may not have a direct contract with the government, because of the width and breath of government contractors, it is likely that you are doing business with a contractor or subcontractor that is.

However, CMMC is not without its controversy. CMMC version 1.0 created such difficulties with its requirements for third-party assessments that the DoD suspended the pilot program in 2021 in order to revise the framework. Now, CMMC 2.0 has been released and is taking effect, requiring comprehensive, but slightly less burdensome, assessments of DoD contractors and subcontractors. Faced with these new compliance requirements, defense contractors must navigate these challenging assessment procedures from logistical and cost perspectives. CMMC requirements will apply to all defense contractors, from contractors building warships and airplanes to contractors providing lawncare and food services.

EMA Radar for Extended Detection and Response (XDR)

Over the past few years, there were tons of new players in the XDR market – and every single one (at least among the ones that are actually viable solutions) added or contributed something to the overall conversation as to what the “X” in XDR really means. Despite the plethora of available tools, security incidents continue to increase, and high-profile attacks have enterprise leaders asking how they can prevent their companies from appearing on the 9:00 o'clock news.

This research will assess the capabilities of the leading vendors in the extended detection and response (XDR) space. These vendors offer detection and response solutions but provide differentiation beyond those basic capabilities. This report is intended to help IT organizations better understand the XDR market and create shortlists of vendors when seeking a detection and response 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 networks.

Information Security, Risk, and Compliance Management

Unified Identity Management: The Convergence of Enterprise Requirements and Practices Across Identity, Governance, and Privileged Access Management

Traditionally, enterprise management processes and solutions supporting identity and access management (IAM), identity governance and administration (IGA), and privileged access management were adopted and implemented as independent solutions. However, recent market trends indicate businesses are now more apt to adopt solutions from a single vendor to reduce costs, improve interoperability, and simplify vendor relationships. In many cases, organizations are seeking an integrated and modular approach to implement specific functionality across the three disciplines, but without having to adopt full product sets for each. To help provide guidance on the types of converged identity solutions businesses should adopt, EMA is embarking on a detailed investigation of the current market. For this research, EMA will survey a wide range of business horizontals and verticals to identify the level of interest in adopting converged solutions, determine the specific features that are most valued, and quantify the benefits of adopting a converged identity platform.

2024 EMA Radar for Digital Employee Experience Management

All modern businesses are dependent on digital technologies to drive workforce productivity to achieve company performance and financial success. Digital experience management (DEX) solutions are designed to directly gauge and respond to user experience issues. Related solutions collect comprehensive contextual information on user interactions with digital technologies, analyze the data to quantify user experiences, and provide support for remediating any deficiencies. In this EMA Radar Report, leading DEX solutions are empirically compared side by side across five key metrics—architecture and integration, deployment and administration, functionality, cost advantage, and vendor strength—to provide purchase guidance for organizations seeking to balance a product's strength against its total cost of ownership. This updated report edition will include the most current product updates to be reflected in detailed vendor profiles that provide full transparency on the scores that they receive. Additionally, the report will recognize innovation leaders in specific DEX disciplines.

Unmasking Identity Threats: The Rise of Identity Threat Detection and Response (ITDR)

Security threat vectors evolved in recent years to include a wider range of attacks with greater degrees of complexity. In particular, attacks targeting user identities—such as phishing and vishing, man-in-the-middle, credential stuffing, password spraying, and pass-the-hash attacks—continue to accelerate and more frequently breach traditional identity security protections. To better combat these rapidly evolving threats, leading identity management solution providers have introduced new feature sets specifically designed to monitor and intelligently analyze user activities, flag any malicious access event, and provide immediate and appropriate threat mediation. To help bring clarity to the types of ITDR solutions organizations should adopt, EMA will conduct primary research that will reveal the most significant identity threats and the ITDR functionality that most effectively prevents them. Additionally, the research report will clearly make the case as to why ITDR should now be considered an essential component of any identity security strategy.

Information Security, Risk, and Compliance Management

2024 EMA Radar for Privileged Access Management and Protection

In the rapidly evolving landscape of cybersecurity, businesses have long relied on privileged access management (PAM) as a fundamental component of their defense strategies. Recognizing the critical role of controlling and monitoring access to sensitive systems and data, organizations have implemented robust PAM solutions to safeguard against unauthorized access and potential security breaches. However, as cyber threats continue to advance in sophistication, a paradigm shift is underway within the industry, marking a transition from mere management to a more proactive approach—privileged access protection. This radar report will delve into this transformative trend, exploring how solution providers are redirecting their focus towards not only managing privileged access but also enhancing protective measures to preemptively thwart potential security risks. The report aims to shed light on the innovative technologies and methodologies shaping this shift, providing invaluable insights for organizations navigating the evolving landscape of cybersecurity.

2024 EMA Radar for Endpoint Management and Protection

As the dynamics of the modern workplace continue to evolve, the landscape of endpoint management is undergoing a profound transformation. The advent of remote work and bring-your-own-device (BYOD) policies, as well as the widespread integration of mobile devices into corporate networks have fueled a paradigm shift in the industry. In response to this evolution, this radar report will closely examine the trend of incorporating endpoint protection seamlessly within management platforms. This report aims to provide a comprehensive overview of the solutions and vendors at the forefront of this integration, offering insights into how organizations can effectively navigate the complexities of securing diverse endpoints. With a focus on the intersection of endpoint management and protection, the report promises to be an indispensable resource for businesses seeking to fortify their cybersecurity posture in the face of the ever-expanding threat landscape.

2024 Identity and Endpoint Trends Year-In-Review

This report will delve into the nuanced interconnections among Unified Identity Management, Identity Protection, and Endpoint Management and Protection. It aims to provide a thorough examination of prevailing industry trends that have influenced the cybersecurity landscape throughout the year. The emphasis lies in dissecting how businesses strategically align their efforts to ensure comprehensive protection for users, identities, and devices. Through an insightful exploration of the intricate relationships among these essential components, the report seeks to illuminate the progress made and challenges encountered in fortifying defenses against dynamic cybersecurity threats. Positioned as a valuable resource, this Year-In-Review report offers a retrospective analysis and forward-thinking strategies for businesses navigating the intricacies of cybersecurity in the approaching year.

Information Security, Risk, and Compliance Management

2024 Software Security Trends Year-In-Review

This report will rigorously examine the industry landscape, with a particular focus on exploits, vulnerabilities, and the broader attack surface. Seeking to provide insightful observations on the present state of software security, the report aims to unravel the intricate web of challenges and advancements that have characterized the field throughout the year. Positioned as a reflective resource, it is expected to offer professionals and organizations a discerning understanding of the evolving threat landscape and valuable insights for enhancing their software security measures.

Intelligent Automation

2024 Radar Report for Managed File Transfer

The inaugural EMA Radar Report on Managed File Transfer (MFT) marks a significant milestone in the assessment of leading vendors and solutions within this critical domain of data management and integration. With a focus on providing comprehensive insights into the evolving MFT market landscape, this report offers an in-depth analysis of vendor positions, product capabilities, and strategic alignments. Through intuitive market maps, Radar Charts, and meticulous evaluation criteria, the report enables organizations to navigate the complexities of the MFT market and make informed decisions when selecting solutions tailored to their business needs.

Designed to highlight functionality breadth, cost-effectiveness, architecture, integration capabilities, deployment options, administration features, and vendor reliability, the inaugural EMA Radar Report identifies industry value leaders and innovators in the realm of Managed File Transfer. By offering a detailed methodology overview and high-level market segment analysis, the report serves as a foundational resource for strategic planning and technology investment in the realm of data management and integration. As organizations embark on their MFT journey, the EMA Radar Report sets the benchmark for excellence and innovation in this critical aspect of modern enterprise operations.

Data in Motion: Managed File Transfer's Crucial Role in Modern Data Pipelines

In the era of data-driven decision-making, efficient and secure data transfer between systems and applications is crucial. Managed file transfer (MFT) has become a pivotal component in ensuring seamless data flow within contemporary data pipelines. While MFT tools securely move the data, workload automation and orchestration (WLA) tools provide the framework and capabilities needed to manage and optimize the execution of data pipeline tasks. Traditionally, WLA tools integrated MFT tools to affect the transfer of data. In recent years, WLA tools increasingly included native MFT capabilities. This comprehensive study will examine the current state of MFT solutions, their role within data pipelines, and their relationship with workload automation.

This research will survey a diverse group of IT professionals, including data engineers, system administrators, and IT managers, to gain insights into their adoption of MFT technologies and their integration within data pipelines. We will also investigate the ways in which workload automation tools are leveraged alongside, or in place of, MFT solutions to optimize data workflows. Key findings of this study will include the challenges organizations face in managing data transfers, encompassing security concerns and scalability issues, and best practices for integrating MFT within modern data pipelines. Additionally, we will analyze the extent to which workload automation tools are employed to orchestrate and streamline data transfer processes.

Intelligent Automation

Workload Automation and Orchestration in 2024: Empowering the Modern Digital Enterprise

Enterprises are working hard to leverage digital technologies to enhance business processes, improve customer experiences, and drive operational efficiency. Workload automation and orchestration, with support for DevOps practices, create a powerful synergy that accelerates digital transformation by automating processes, improving collaboration, increasing efficiency, and enhancing the overall agility of an organization. In 2023, EMA research identified a significant correlation between enterprises that have achieved maturity in digital transformation and enterprises in which workload automation and orchestration are valued and leveraged by architects, developers, and business executives in addition to IT operations. Workload automation and orchestration serves as a foundational element of digital transformation by providing the means to digitize, optimize, and automate processes and workflows. It allows organizations to adapt to the digital age, capitalize on data-driven opportunities, and enhance their overall agility and competitiveness in a rapidly evolving business landscape.

This research will explore the continued progress of digital transformation efforts and the important role of workload automation and orchestration. The research will also update many of the key metrics EMA has been tracking since 2013 to add current data to the trends being tracked.

Intelligent Hybrid Multi-Cloud

EMA Top 3 Series of Reports on Observability

The EMA Top 3 Product Guides for Observability are individual components of a larger market research initiative. These guides are intentionally divided into separate publications to cater to different audiences within the IT, development, and data science ecosystems. Each report will deliver actionable insights tailored to the unique challenges and priorities of each relevant user persona.

Observability Platforms: EMA Top 3 Product Guide

Observability remains a crucial pain point for platform engineers, site reliability engineers, security roles, and application developers. This is reflected in an expected market growth for 2023 of over 50%. This EMA Top 3 Product Guide for Observability Platforms will provide an overview of critical requirements for modern observability platforms based on real-life enterprise pain points and priorities. The report will crown the top three products that best help customers address these challenges.

AI-Powered Observability: EMA Top 3 Product Guide

The integration of AI into observability platforms is revolutionizing the way organizations monitor, manage, and continuously optimize their infrastructure and application stacks. This EMA Top 3 Product Guide will identify three platforms that seamlessly incorporate AI to provide actionable and proactive insights, root cause analyses, recommendations, and automation capabilities that are continuously aligned with an organization's specific business priorities.

Data Observability – EMA Top 3

Data is the lifeblood of modern organizations, but ensuring its quality, availability, and security is a growing challenge. This EMA Top 3 Product Guide will identify platforms that make data observability processes more intelligent, efficient, and proactive while keeping an eye on data privacy and ethical considerations. These platforms offer robust features for automated insights, anomaly detection, dynamic dashboards, predictive analysis, data quality, troubleshooting, and compliance monitoring, enabling businesses to gain a 360-degree view of their data landscape across various storage solutions and cloud environments.

Code-Level Observability – EMA Top 3

Understanding the behavior of code in production is critical for optimizing performance and debugging issues. This EMA Top 3 Product Guide will focus on identifying platforms that provide granular and intelligent insights into code execution, dependencies, and bottlenecks. These platforms are essential tools for developers and SREs who need to understand how code changes impact system performance and user experience in real time.

Intelligent Hybrid Multi-Cloud

Observability for AI and Machine Learning – EMA Top 3

As AI and ML models become integral to business operations, the need for specialized observability solutions is evident. This EMA Top 3 Product Guide will identify platforms that offer specialized observability features for monitoring the performance, fairness, and data drift of AI/ML models. These platforms are crucial for data scientists and ML engineers who need to ensure that their models are performing as expected in live environments.

Platform Engineering: The Backbone of Modern Software

Platform engineering has emerged as the cornerstone of modern software development, driving rapid innovation, scalability, and operational efficiency. The adoption of microservices architecture, cloud native technologies, and DevSecOps practices amplified this pivotal role. However, the field is not without its challenges. The complexity of managing distributed systems, a growing skill gap, and the need to balance cutting-edge technology with cost-efficiency are pressing issues – yet these challenges also present opportunities. Advanced observability tools, infrastructure as code (IaC), and open source collaboration are just a few avenues that offer promising solutions.

This study will aim to serve as a comprehensive guide for platform engineers, DevOps teams, and technology leaders. It will delve into the current trends shaping the field from AI-driven automation to agile methodologies and GitOps. The report will also address the challenges and skill gaps that professionals face, offering insights into best practices and emerging solutions. The goal is to provide a comprehensive view of the tools, methodologies, and practices that are setting the standard in platform engineering today.

Platform engineering is more than just a technical discipline; it's the engine that powers modern software development. By understanding its current landscape, challenges, and opportunities, stakeholders can better navigate this rapidly evolving field. This study will aim to equip its readers with the knowledge and insights needed to excel in this dynamic environment, making it an invaluable resource for anyone committed to advancing in the realm of platform engineering.

Intelligent Hybrid Multi-Cloud

Generative AI and DevOps: Real-World Insights

Generative AI is revolutionizing the DevOps landscape, automating intricate tasks, and offering intelligent insights that were previously unattainable. From auto-generating code to streamlining testing and deployment processes, the technology is reshaping how DevOps teams operate. However, the integration of AI into DevOps is not without its challenges, such as ethical considerations around automated decision-making and the need for specialized skills to manage AI-driven systems. Despite these hurdles, the opportunities for efficiency and innovation are compelling, making it crucial for organizations to understand both the benefits and potential pitfalls.

This report will aim to provide a comprehensive analysis of generative AI's impact on DevOps practices. It will delve into real-world applications, examining how AI-driven automation can accelerate development cycles, improve code quality, and enhance system reliability. At the same time, the study will address the challenges that come with AI adoption, such as data privacy concerns and the complexities of implementing AI algorithms within existing DevOps pipelines. The objective is to offer a balanced perspective that serves as a roadmap for organizations contemplating the integration of AI into their DevOps strategies.

Generative AI is poised to be a game-changer in the DevOps arena, offering a new level of automation and intelligence that can significantly impact business outcomes. By dissecting its real-world applications, benefits, and challenges, this report aims to equip organizations with the insights needed to make informed decisions about adopting AI-driven DevOps solutions. It serves as an invaluable guide for technology leaders, DevOps professionals, and organizations looking to navigate the complexities of this emerging field.

Network Infrastructure and Operations

Network Management Megatrends 2024

The ultimate benchmarking study of enterprise network operations strategies. Since 2008, EMA's biennial Network Management Megatrends research has examined the tools and processes that IT organizations use to manage, monitor, and troubleshoot their networks. This report explores everything from network tool sprawl to NetOps MTTR objectives.

In 2024, the Megatrends research will examine how industry trends, including network engineering talent shortages, sustainability initiatives, enterprise AI initiatives, hybrid and multi-cloud architecture, and edge computing and cloud edge, impact NetOps strategies.

Networking for Kubernetes: How Network Infrastructure and Operations Teams Support Cloud Native Application Platforms

According to EMA research, cloud native application platforms like Kubernetes are driving 52% of enterprise network infrastructure and operations strategies. As Kubernetes proliferates in the cloud and the data center, traditional network teams are struggling to provide connectivity, maintain visibility, and enforce security. Some may elect to abdicate responsibility to platform teams and DevOps teams. Others will fight to remain relevant and stay in control.

This multi-sponsor research will survey enterprise networking pros about how they respond to cloud native platform adoption. EMA will identify the politics and the technology involved. The research will explore the connectivity solutions, security controls, and observability tools that network teams will adopt as they fight for relevancy in a future dominated by microservices, API gateways, and eBPF.

EMA Radar for Network Operations Observability

This report is an update and evolution of the 2021 "EMA Radar for Network Performance Management." 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 Radar 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 report 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

Generative AI and IT Operations

The emergence of ChatGPT, a large language model with a generative AI front-end, sparked massive interest in AI in 2023 with millions of people using it for day-to-day tasks. In IT operations, generative AI can enable chatbots that are knowledgeable about infrastructure and services. It can also find hidden insights in data and generate configs, scripts, and other content that admins can use to automate IT management.


EMA will examine how IT organizations are engaging with generative AI today. We will evaluate how organizations prepare their data for this technology, manage security and privacy, and enable their people to leverage generative AI. We will identify the use cases organizations want to tackle with generative AI and how vendors can help them achieve success.

Converging Operational Technology on IT Networks

Converging operational technology (OT) like manufacturing systems, medical equipment, and water treatment systems onto IT networks offers plenty of benefits, like operational efficiency, automation, and improved customer service – but this presents risks and challenges that network teams must address.

This research will explore how key industries are addressing connectivity and security requirements as OT infrastructure converges onto enterprises networks. It will also identify how organizations are evolving their network operations tools and processes to address these converged environments.

EMA Radar for Network Visibility Architecture

 *Joint project with Information Security, Risk, and Compliance Management*

This research will assess the capabilities of the leading vendors for network visibility solutions. These vendors offer hardware and software for extracting packets and metadata from production networks and delivering them to the network analytics solutions that IT operations and security groups use.

This report is intended to help IT organizations better understand the network visibility 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 networks.

Network Operations Observability: Modernizing the NetOps Toolset

In 2022, EMA found that 90% of network managers believe “network observability” is a useful term for describing the tools they use to monitor and manage their networks. Network managers also told EMA they expect a network observability solution to provide more actionable insights than their legacy network monitoring and network performance management tools.

This new market research will take a deep dive into the kinds of actionable insights network managers need from their vendors and how they expect to get those insights. It will explore what makes a network observability solution effective and valuable, and it will establish an innovation roadmap for network management tool vendors.

Network Infrastructure and Operations

Network as a Service: What is it? Why Do you Need it?

Network as a service (NaaS) offerings based on network access technology, such as switching, Wi-Fi, and network security, have become mainstream in recent years. However, the industry has never agreed on a precise definition of NaaS given that the vendors in multiple adjacent markets have co-opted the term. Everyone does agree that NaaS brings a cloud consumption model to networks, and that message is resonating with many customers.

This research will explore what NaaS means to IT decision-makers, particularly in the context of network access technology. EMA will identify the requirements organizations have of such solutions, how vendors can ensure a successful integration of NaaS services into an IT organization, and what roadblocks vendors might encounter as they develop and sell their NaaS offerings.

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 it, especially around 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. It will also explore how they collaborate with security groups to achieve a successful zero trust implementation

The background features a series of overlapping, semi-transparent geometric shapes. A dark maroon horizontal bar is at the top left. A large, light green triangle points from the top right towards the center. A darker maroon shape is at the bottom, and a lighter green shape is in the middle, creating a layered effect.

EMA Analysts



Chris

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.

B.A., Political Science (Summa Cum Laude), Metropolitan State College of Denver

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

Coverage Definition:

Security, risk, and compliance management is the process by which organizations predict and manage risk by adhering to boundaries set by a business. The practice area encompasses most of the areas and concepts in information security, risk mitigation, and technology regulatory compliance.

Primary Coverage: Security, Risk, and Compliance Management

Secondary Coverage:

- Application security
- Advanced threat analytics and anomaly detection
- Advanced testing attack simulation
- Bot detection and protection
- Cloud application security management
- Cloud access security broker
- Cryptography and key management
- Container security
- Data leak prevention and data classification
- Electronic governance risk and compliance
- Endpoint protection
- Hardware security modules
- IoT security
- Information rights management
- Managed security service provider
- Patch management
- Runtime application security protection
- Remote access
- Risk management
- Security incident and event management and log management
- Security policy orchestration and automation
- SSL appliances
- Threat intelligence service feeds
- Third-party risk management
- Anti-phishing
- Unified threat management
- Vulnerability management
- Web application firewall
- Workload microsegmentation
- Web security gateway
- Zero trust

Tertiary Coverage:

- Advanced breach detection
- Antivirus
- Distributed denial of service protection
- Deception technology
- Digital threat intelligence management
- Intrusion detection/prevention
- Mobile security tools
- Network admission control
- Network APT detection/analysis
- Next-generation endpoint security
- Next-generation firewall/unified threat management
- Secure email gateways and services
- Security operations automation and orchestration
- Consumer Identity and Access Management
- Digital Workspaces
- Identity and Access Management
- Privileged Access Management
- Unified Endpoint Management



Dan

As President and COO of Enterprise Management Associates, 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 & 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*.

In his spare time, Dan enjoys playing pool and working on furniture restoration.

M.B.A., Marketing, University of North Texas

Certified Management Accountant

B.S., Finance and Economics, Saint Cloud State University

Coverage Definition:

Intelligent automation is a holistic solution for digital transformation. The practice area encompasses workload automation, robotic process automation, and blockchain-based and AI-driven automation. It examines the management of process orchestration and workflows.

Primary Coverage: Intelligent Automation

Secondary Coverage:

- Workload automation (WLA)
- Robotic process automation (RPA)
- Process orchestration
- Workflow automation
- AI-driven automation
- Blockchain-based automation



Ken

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).

Ken loves history and the outdoors, and spends his spare time metal detecting and magnet fishing in Western Maryland, working to find lost pieces of history for future generations to enjoy.

B.S., Computer Science, Mount Saint Mary's University

CompTIA Advanced Security Practitioner (CASP)

CompTIA Security+

Coverage Definition:

Security, risk, and compliance management is the process by which organizations predict and manage risk by adhering to boundaries set by a business. The practice area encompasses most of the areas and concepts in information security, risk mitigation, and technology regulatory compliance.

Primary Coverage: Security, Risk, and Compliance Management

Secondary Coverage:

- Application security
- Advanced threat analytics and anomaly detection
- Advanced testing attack simulation
- Bot detection and protection
- Cloud application security management
- Cloud access security broker
- Cryptography and key management
- Container security
- Data leak prevention and data classification
- Electronic governance risk and compliance
- Endpoint protection
- Hardware security modules
- IoT security
- Information rights management
- Managed security service provider
- Patch management
- Runtime application security protection
- Remote access
- Risk management
- Security incident and event management and log management
- Security policy orchestration and automation
- SSL appliances
- Threat intelligence service feeds
- Third-party risk management
- Anti-phishing
- Unified threat management
- Vulnerability management
- Web application firewall
- Workload microsegmentation
- Web security gateway
- Zero trust

Tertiary Coverage:

- Advanced breach detection
- Antivirus
- Distributed denial of service protection
- Deception technology
- Digital threat intelligence management
- Intrusion detection/prevention
- Mobile security tools
- Network admission control
- Network APT detection/analysis
- Next-generation endpoint security
- Next-generation firewall/unified threat management
- Secure email gateways and services
- Security operations automation and orchestration
- Consumer Identity and Access Management
- Digital Workspaces
- Identity and Access Management
- Privileged Access Management
- Unified Endpoint Management



Shamus

Shamus McGillicuddy leads the network management practice at Enterprise Management Associates (EMA). His practice focuses on all aspects of managing enterprise networks, including network automation, AIOps-driven network operations, 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.

In his spare time, Shamus enjoys reading, fiction writing, playing guitar, and cooking.

M.S., Journalism, Boston University

B.A., English and Urban Studies,
Vassar College

Coverage Definition:

Network infrastructure and operations is the process by which organizations design, build, and manage networks. The practice area encompasses data centers, the cloud, local-area networks, and wide-area networks. It examines the management of network capacity, performance, and security.

Primary Coverage: Network Infrastructure and Operations

Secondary Coverage:

- Application delivery controllers/ load balancers
- Cloud networking
- Data center networking
- DDI management
- Enterprise switching and routing
- Internet of Things
- Network automation
- Network change and configuration management
- Network fault and availability management
- Network packet brokers
- Network packet capture
- Network performance management
- Network security
- Network as a service
- Secure access service edge
- Software-defined WAN and hybrid WAN
- Wi-Fi infrastructure and management
- Work-from-anywhere networking



Torsten

With over 15 years of enterprise IT experience, Torsten helps end users and vendors leverage the opportunities presented by today's hybrid cloud and software-defined infrastructure environments in combination with advanced machine learning. He specializes in topics that lead the way from hybrid cloud and the software-defined data center (SDDC) toward a business-defined concept of enterprise IT.

Torsten served as Vice President of Product Management and Marketing for cloud and end-user computing at ASG Technologies. While in this role, Torsten re-focused ASG's cloud strategy toward delivering individualized end-user experiences specific to job role and industry, disrupting the traditional device-centric management concept.

In 2005, Torsten joined MadWolf Technologies and received numerous research grants aimed to advance business through the use of leading edge and sometimes experimental technologies. A decade before the availability of machine learning services by Amazon, Google, Microsoft, and IBM, and with the financial support of the Rockefeller Foundation, Torsten's team created a self-learning SaaS solution to automatically classify vast bodies of online content and deliver end-user specific news streams based on this content.

In his free time, Torsten goes nuts with his race FPV quadcopters, replicates a little bit of the Amazon in his planted aquariums, and lets his kids beat him in soccer.

BSc., Business Economics, University of Konstanz, Germany

M.B.A., Strategy, University of Konstanz, Germany

Coverage Definition:

An intelligent hybrid multi-cloud forms when services from private cloud, public cloud, and edge combine into the foundation for the policy-driven deployment and management of cloud-native applications, data sources, and machine learning models. The practice encompasses observability, GitOps, MLOps, DevOps, and serverless functions.

Primary Coverage: Intelligent Hybrid Multi-Cloud

Secondary Coverage:

- Self-driving hybrid multi-cloud
- Site reliability engineering
- Infrastructure as code and GitOps
- Cloud-native application stacks
- Operationalizing machine learning and AI
- Machine learning platforms
- AutoML
- Intelligent edge
- Observability for DevOps and MLOps
- Continuous compliance
- Serverless functions



Valerie

Valerie O'Connell leads the Digital Service Execution practice at Enterprise Management Associates (EMA). Her practice encompasses intersections and innovations across AIOps, asset management, end-user experience, ITSM/ESM, 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.

In her spare time, Valerie mentors teens who are too ready for trouble and enjoys lazy afternoons filled with laughter, friends, food, and good dogs.

M.A. Boston College

B.A. University of Massachusetts

Coverage Definition:

Digital service execution takes a service-centric, cross-functional approach to delivering and managing IT excellence. The practice area encompasses ITSM, ESM, AIOps, DevOps, ITAM, SRE, and advances that promote an evolving ServiceOps reality.

Primary Coverage:

Digital Service Execution: IT Service, Experience, and Operations Management

Secondary Coverage:

- Business operations
- Customer service excellence
- DevOps
- Digital experience management
- Digital transformation initiatives
- IoT/OT
- ITAM
- ITOM/AIOps
- ITSM/ESM
- Managing innovation
- Organizational/cultural considerations
- Site reliability engineering

About Enterprise Management Associates, Inc.

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

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

©2024 Enterprise Management Associates, Inc. All Rights Reserved. EMA™, ENTERPRISE MANAGEMENT ASSOCIATES®, and the mobius symbol are registered trademarks or common law trademarks of Enterprise Management Associates, Inc.

